interface

設定するインターフェイスを選択し、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** コマンドを使用します。

interface *type number*

構文の説明

type	設定するインターフェイスのタイプです。有効値については、表 2-6 を参照してください。
number	モジュールおよびポート番号です。

デフォルト

インターフェイス タイプは設定されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(25)EW	10 ギガビット イーサネット インターフェイスを含めるように拡張されました。

使用上のガイドライン

表 2-6 に、*type* の有効値を示します。

表 2-6　type の有効値

キーワード	定義
ethernet	イーサネット IEEE 802.3 インターフェイスです。
fastethernet	100 Mbps イーサネット インターフェイスです。
gigabitethernet	ギガビット イーサネット IEEE 802.3z インターフェイスです。
tengigabitethernet	10 ギガビット イーサネット IEEE 802.3ae インターフェイスです。
ge-wan	ギガビット イーサネット WAN IEEE 802.3z インターフェイスです。Supervisor Engine 2 のみが設定された Catalyst 4500 シリーズ スイッチでサポートされています。
pos	Packet over SONET インターフェイス プロセッサ上のパケット OC-3 インターフェイスです。Supervisor Engine 2 のみが設定された Catalyst 4500 シリーズ スイッチでサポートされています。
atm	ATM インターフェイスです。Supervisor Engine 2 のみが設定された Catalyst 4500 シリーズ スイッチでサポートされています。
vlan	VLAN インターフェイスです。**interface vlan** コマンドを参照してください。
port-channel	ポート チャネル インターフェイスです。**interface port-channel** コマンドを参照してください。
null	ヌル インターフェイスです。有効値は **0** です。

例

次の例では、ファスト イーサネット インターフェイス 2/4 でインターフェイス コンフィギュレーション モードを開始する方法を示します。

```
Switch(config)# interface fastethernet2/4
Switch(config-if)#
```

関連コマンド

コマンド	説明
show interfaces	インターフェイス情報を表示します。

interface port-channel

ポート チャネル インターフェイスにアクセスしたり、このインターフェイスを作成したりするには、**interface port-channel** コマンドを使用します。

interface port-channel *channel-group*

構文の説明

channel-group	ポート チャネル グループ番号です。有効値の範囲は 1 ～ 64 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

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

物理インターフェイスをチャネル 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。ポート チャネル インターフェイスは、チャネル グループがその最初の物理インターフェイスに到達したときに自動的に作成されます（まだ作成されていない場合）。

また、**interface port-channel** コマンドを入力して、ポート チャネルを作成することもできます。この場合には、レイヤ 3 ポート チャネルが作成されます。レイヤ 3 ポート チャネルをレイヤ 2 ポート チャネルに変更するには、物理インターフェイスをチャネル グループに割り当てる前に、**switchport** コマンドを使用します。ポート チャネルにメンバ ポートがある場合は、ポート チャネルをレイヤ 3 からレイヤ 2 に、またはレイヤ 2 からレイヤ 3 に変更できません。

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　レイヤ 3 ポート チャネル インターフェイスはルーテッド インターフェイスです。物理ファスト イーサネット インターフェイスではレイヤ 3 アドレスをイネーブルにしないでください。

CDP を使用する場合は、物理ファスト イーサネット インターフェイスのみで設定し、ポート チャネル インターフェイスでは設定しないでください。

例

次の例では、チャネル グループ番号が 64 のポート 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 64
Switch(config)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel グループに EtherChannel インターフェイスを割り当てて設定します。
show etherchannel	チャネルの EtherChannel 情報を表示します。

interface range

複数のポートで同時にコマンドを実行するには、**interface range** コマンドを使用します。

interface range {**vlan** *vlan_id* - *vlan_id*} {*port-range* | **macro** *name*}

構文の説明

vlan *vlan_id* - *vlan_id*	VLAN 範囲を指定します。有効値の範囲は 1 ～ 4094 です。
port-range	ポート範囲です。*port-range* の有効値のリストについては、「使用上のガイドライン」を参照してください。
macro *name*	マクロ名を指定します。

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 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	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張 VLAN アドレスのサポートが追加されました。

使用上のガイドライン

interface range コマンドは、既存の VLAN SVI でのみ使用できます。VLAN SVI を表示するには、**show running config** コマンドを入力します。表示されない VLAN は、**interface range** コマンドで使用できません。

interface range コマンドで入力した値は、既存のすべての VLAN SVI に適用されます。

マクロを使用するには、事前に **define interface-range** コマンドで範囲を定義しておく必要があります。

ポート範囲のコンフィギュレーションの変更はすべて NVRAM に保存されますが、**interface range** コマンドで作成したポート範囲については NVRAM に保存されません。

ポート範囲は次の 2 つの方法で入力できます。

- 最大 5 つまでのポート範囲を指定します。
- 定義済みのマクロを指定します。

ポートを指定するか、またはポート範囲マクロの名前を指定できます。ポート範囲は同一のポート タイプで構成されている必要があり、1 つの範囲内のポートが複数のモジュールをまたがることはできません。

1 回のコマンドで定義できるポート範囲は最大で 5 つです。各範囲をカンマで区切って指定します。

範囲を定義するときは、最初のポートとハイフン（-）の間にスペースを入力する必要があります。

```
interface range gigabitethernet 5/1 -20, gigabitethernet4/5 -20.
```

port-range を入力するときは、次の形式を使用します。

- *interface-type* {*mod*}/{*first-port*} - {*last-port*}
- *interface-type* {*mod*}/{*first-port*} - {*last-port*}

interface-type の有効値は次のとおりです。

- **FastEthernet**
- **GigabitEthernet**
- **Vlan** *vlan_id*

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。マクロの作成後、追加の範囲を入力できます。インターフェイス範囲をすでに入力している場合は、CLI でマクロを入力できません。

port-range 値では単一インターフェイスを指定できます。この点で、このコマンドは **interface** *interface-number* コマンドと類似しています。

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 FE 5/18 ～ 20 を指定する方法を示します。

```
Switch(config)# interface range fastethernet 5/18 - 20
Switch(config-if)#
```

次の例では、ポート範囲マクロを実行する方法を示します。

```
Switch(config)# interface range macro macro1
Switch(config-if)#
```

関連コマンド

コマンド	説明
define interface-range	インターフェイスのマクロを作成します。
show running config（Cisco IOS のマニュアルを参照）	スイッチの実行コンフィギュレーションを表示します。

interface vlan

レイヤ 3 の Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）を作成したり、このインターフェイスにアクセスしたりするには、**interface vlan** 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 の番号です。有効値の範囲は 1 ～ 4094 です。

デフォルト

Fast EtherChannel 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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張アドレッシングのサポートが追加されました。

使用上のガイドライン

SVI は、特定の VLAN について **interface vlan** *vlan_id* コマンドを最初に入力したときに作成されます。*vlan_id* 値は、ISL または 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。VLAN インターフェイスが新たに作成されると常にメッセージが表示されるため、正しい VLAN 番号を入力したことを確認できます。

no interface vlan *vlan_id* コマンドを入力して SVI を削除すると、関連付けられているインターフェイスは強制的に管理ダウン状態になり、削除済みとマークされます。削除したインターフェイスは、それ以降 **show interface** コマンドで表示されなくなります。

削除した SVI は、削除したインターフェイスに対して **interface vlan** *vlan_id* コマンドを入力することで、元に戻すことができます。インターフェイスは元に戻りますが、以前のコンフィギュレーションの大部分が失われます。

例

次の例では、新しい VLAN 番号に対して **interface vlan** *vlan_id* コマンドを入力した場合の出力を示します。

```
Switch(config)# interface vlan 23
% Creating new VLAN interface.
Switch(config)#
```

ip arp inspection filter vlan

DAI がイネーブルの場合にスタティック IP 用に設定されたホストからの ARP を許可したり、ARP アクセス リストを定義して VLAN に適用したりするには、**ip arp inspection filter vlan** コマンドを使用します。この適用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 *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	アクセス コントロール リスト名です。
vlan-range	VLAN 番号または範囲です。有効値の範囲は 1 ～ 4094 です。
static	（任意）アクセス コントロール リストをスタティックに適用するように指定します。

デフォルト

VLAN に適用される ARP ACL が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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ダイナミック ARP インスペクションを実行するために ARP アクセス コントロール リストを VLAN に適用すると、IP-to-Ethernet MAC 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。それ以外のタイプのパケットはすべて検証なしで着信 VLAN でブリッジングされます。

このコマンドでは、着信 ARP パケットが ARP アクセス コントロール リストと比較されるようにし、アクセス コントロール リストで許可されている場合にのみそれらのパケットが許可されるように指定します。

アクセス コントロール リストで明示的な拒否によってパケットが拒否された場合、それらのパケットはドロップされます。暗黙的な拒否によってパケットが拒否された場合、ACL がスタティックに適用されていなければ、それらのパケットは DHCP バインディングのリストと照合されます。

例

次の例では、DAI を実行するために ARP ACL スタティック ホストを VLAN 1 に適用する方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection filter static-hosts vlan 1
Switch(config)# end
Switch#
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
```

```
 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active      static-hosts      No

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Acl-Match        Deny
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip arp inspection limit（インターフェイス）

インターフェイスの着信 ARP 要求および応答のレートを制限し、DoS 攻撃の場合にシステムのすべてのリソースを DAI が消費してしまわないようにするには、**ip arp inspection limit** コマンドを使用します。制限を解除するには、このコマンドの **no** 形式を使用します。

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

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。レートの範囲は 1 ～ 10000 です。
none	処理できる着信 ARP パケットのレートの上限を設定しないように指定します。
burst interval *seconds*	（任意）高レートの ARP パケットについてインターフェイスをモニタする間隔（秒）を指定します。設定可能な間隔は 1 ～ 15 秒です。

デフォルト

このレートは、信頼できないインターフェイス上で 15 pps（パケット / 秒）に設定されています。ただし、1 台のホストが 1 秒間に 15 台の新規ホストに接続できるスイッチド ネットワークであると仮定しています。

このレートは、信頼できるすべてのインターフェイス上で無制限になっています。

デフォルトでは、バースト間隔は 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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(20)EW	インターフェイス モニタリングのサポートが追加されました。

使用上のガイドライン

トランク ポートにはより高いレートを設定して、集約が反映されるようにする必要があります。着信パケットのレートがユーザ設定のレートを超えると、インターフェイスは errdisable ステートになります。errdisable タイムアウト機能を使用して、ポートを errdisable ステートから解除できます。このレートは、信頼できるインターフェイスと信頼できないインターフェイスのいずれにも適用されます。DAI に対応した複数の VLAN 間のパケットを処理できるようにトランク上で適切なレートを設定するか、または **none** キーワードを使用してレートを無制限にします。

チャネル ポート上の着信 ARP パケットのレートは、すべてのチャネル メンバーからのパケットの着信レートの合計と等しくなります。チャネル ポートのレート制限を設定するのは、チャネル メンバー上の着信 ARP パケットのレートを調べたあとだけです。

バースト期間にわたって設定された 1 秒間のレートを超えるパケットをスイッチが連続して受信すると、インターフェイスが errdisable ステートになります。

例

次の例では、着信 ARP 要求のレートを 25 pps（パケット / 秒）に制限する方法を示します。

```
Switch# config terminal
Switch(config)# interface fa6/3
Switch(config-if)# ip arp inspection limit rate 25
Switch(config-if)# end
Switch# show ip arp inspection interfaces fastEthernet 6/3
Interface        Trust State     Rate (pps)
 ---------------  -----------     ----------
 Fa6/3            Trusted                25
Switch#
```

次の例では、着信 ARP 要求のレートを 20 pps（パケット / 秒）に制限する方法とインターフェイス モニタリング間隔を 5 秒に設定する方法を示します。

```
Switch# config terminal
Switch(config)# interface fa6/1
Switch(config-if)# ip arp inspection limit rate 20 burst interval 5
Switch(config-if)# end
```

関連コマンド

コマンド	説明
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip arp inspection log-buffer

ログ バッファに関連付けられているパラメータを設定するには、**ip arp inspection log-buffer** コマンドを使用します。パラメータ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 log-buffer {**entries** *number* | **logs** *number* **interval** *seconds*}

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

構文の説明

entries *number*	ログ バッファのエントリの数です。範囲は 0 ～ 1024 です。
logs *number*	一定間隔内にロギングされるエントリの数です。範囲は 0 ～ 1024 です。値 0 は、エントリがこのバッファ外でロギングされないことを示します。
interval *seconds*	ロギング レートです。範囲は 0 ～ 86400（1 日）です。値 0 は、即座にロギングされることを示します。

デフォルト

ダイナミック ARP インスペクションをイネーブルにした場合は、拒否またはドロップされた ARP パケットがロギングされます。

エントリの数は 32 に設定されています。

ロギングされるエントリの数は 1 秒あたり 5 つに制限されています。

間隔は 1 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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

特定のフローで最初にドロップされたパケットは即座にロギングされます。同じフローの後続のパケットは登録されますが、即座にはロギングされません。これらのパケットの登録は、すべての VLAN で共有されているログ バッファで行われます。このバッファのエントリは、レート制御に基づいてロギングされます。

例

次の例では、エントリを 45 個まで保持できるようにログ バッファを設定する方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection log-buffer entries 45
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 5 entries per 1 seconds.
No entries in log buffer.
Switch#
```

次の例では、ロギング レートを 3 秒あたり 10 ログに設定する方法を示します。

```
Switch(config)# ip arp inspection log-buffer logs 10 interval 3
Switch(config)# end
Switch# show ip arp inspection log
Total Log Buffer Size : 45
Syslog rate : 10 entries per 3 seconds.
No entries in log buffer.
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip arp inspection trust

着信 ARP パケットを検査する一連のインターフェイスを判別する、ポート単位で設定可能な信頼状態を設定するには、**ip arp inspection trust** コマンドを使用します。インターフェイスを信頼できない状態にするには、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

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	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、信頼できるインターフェイスを設定する方法を示します。

```
Switch# config terminal
Switch(config)# interface fastEthernet 6/3
Switch(config-if)# ip arp inspection trust
Switch(config-if)# end
```

コンフィギュレーションを確認するには、このコマンドの show 形式を使用します。

```
Switch# show ip arp inspection interfaces fastEthernet 6/3

 Interface        Trust State     Rate (pps)     Burst Interval
 ---------------  -----------     ----------     --------------
 Fa6/3            Trusted              None                  1
Switch#
```

関連コマンド

コマンド	説明
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip arp inspection validate

ARP インスペクションの特定のチェックを実行するには、**ip arp inspection validate** コマンドを使用します。チェック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 validate [**src-mac**] [**dst-mac**] [**ip**]

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

構文の説明

src-mac	（任意）イーサネット ヘッダーの送信元 MAC アドレスを ARP 本文の送信元 MAC アドレスと照合します。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。 **（注）** **src-mac** をイネーブルにした場合、異なる MAC アドレスが割り当てられたパケットは無効と見なされてドロップされます。
dst-mac	（任意）イーサネット ヘッダーの宛先 MAC アドレスを ARP 本文の宛先 MAC アドレスと照合します。このチェックは、ARP 応答に対して行われます。 **（注）** **dst-mac** をイネーブルにした場合、異なる MAC アドレスが割り当てられたパケットは無効と見なされてドロップされます。
ip	（任意）ARP 本文をチェックして、無効な IP アドレスや予期しない IP アドレスがないかを確認します。0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスがこれに該当します。 送信元 IP アドレスはすべての ARP 要求および応答内でチェックされ、宛先 IP アドレスは ARP 応答内でのみチェックされます。

デフォルト

チェック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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

チェックをイネーブルにする場合は、コマンドラインにキーワード（**src-mac**、**dst-mac**、および **ip**）の少なくとも 1 つを指定します。コマンドを実行するごとに、その前のコマンドのコンフィギュレーションは上書きされます。**src** および **dst mac** の検証をイネーブルにするコマンドのあとに、IP 検証のみをイネーブルにするコマンドを実行すると、2 番目のコマンドによって **src** および **dst mac** の検証がディセーブルになります。

このコマンドの **no** 形式を使用すると、指定したチェックだけがディセーブルになります。これらのチェック オプションがいずれもイネーブルになっていない場合は、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 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
Switch(config)# end
Switch# show ip arp inspection vlan 1
Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip arp inspection vlan

VLAN 単位で Dynamic ARP Inspection（DAI; ダイナミック ARP インスペクション）をイネーブルにするには、**ip arp inspection vlan** コマンドを使用します。DAI 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*

no ip arp inspection vlan *vlan-range*

構文の説明

vlan-range	VLAN 番号または範囲です。有効値の範囲は 1 ～ 4094 です。

デフォルト

すべての VLAN 上で ARP インスペクションが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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

DAI をイネーブルにする VLAN を指定する必要があります。設定済みの VLAN が作成されていない場合、または設定済みの VLAN がプライベートの場合、DAI は機能しないことがあります。

例

次の例では、VLAN 1 で DAI をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# ip arp inspection vlan 1
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : Disabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled
Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active
Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Deny             Deny
Switch#
```

次の例では、VLAN 1 で DAI をディセーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# no ip arp inspection vlan 1
Switch(config)#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip arp inspection vlan logging

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** 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** {**permit** | **all** | **none**}}

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

構文の説明

vlan-range	指定したインスタンスにマッピングされる VLAN の番号です。この番号には、1 つの値または範囲を入力します。有効値の範囲は 1 ～ 4094 です。
acl-match	ACL の一致条件に基づいてドロップまたは許可されるパケットのロギング基準を指定します。
matchlog	ACL と一致したパケットのロギングを、ACL の許可および拒否アクセス コントロール エントリ内の **matchlog** キーワードで制御するように指定します。 **（注）** デフォルトでは、ACE の **matchlog** キーワードは使用できません。このキーワードを使用した場合、拒否されたパケットはロギングされません。パケットがロギングされるのは、**matchlog** キーワードを含む ACE とパケットが一致した場合のみです。
none	ACL と一致したパケットをロギングしないように指定します。
dhcp-bindings	DHCP バインディングの一致条件に基づいてドロップまたは許可されるパケットのロギング基準を指定します。
permit	DHCP バインディングによって許可された場合にロギングを行うように指定します。
all	DHCP バインディングによって許可または拒否された場合にロギングを行うように指定します。
none	DHCP バインディングによって許可または拒否されたパケットのロギングをすべて禁止します。

デフォルト

拒否またはドロップされたパケットがすべてロギングされます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

acl-match および **dhcp-bindings** キーワードは連携しています。ACL 照合コンフィギュレーションを設定すると、DHCP バインディング コンフィギュレーションはイネーブルになります。このコマンドの **no** 形式を使用すると、ロギング基準の一部がデフォルトにリセットされます。いずれのオプションも指定しない場合は、すべてのロギング タイプがリセットされ、ARP パケットが拒否されたときにロギングされるようになります。使用可能なオプションは次の 2 つです。

- **acl-match**：ACL の一致条件に基づくロギングがリセットされ、拒否に基づくロギングが実行されます。
- **dhcp-bindings**：DHCP バインディングの一致条件に基づくロギングがリセットされ、拒否に基づくロギングが実行されます。

例

次の例では、**logging** キーワードを含む ACL と一致した場合にパケットを追加するように、VLAN 1 の ARP インスペクションを設定する方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip arp inspection vlan 1 logging acl-match matchlog
Switch(config)# end
Switch# show ip arp inspection vlan 1

Source Mac Validation      : Enabled
Destination Mac Validation : Disabled
IP Address Validation      : Disabled

 Vlan     Configuration    Operation   ACL Match          Static ACL
 ----     -------------    ---------   ---------          ----------
    1     Enabled          Active

 Vlan     ACL Logging      DHCP Logging
 ----     -----------      ------------
    1     Acl-Match        Deny
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
show ip arp inspection	特定の範囲の VLAN に対するダイナミック ARP インスペクションのステータスを表示します。

ip cef load-sharing algorithm

送信元および宛先 IP アドレスに加えて送信元 TCP/UDP ポート、宛先 TCP/UDP ポート、またはその両方のポートをハッシュに含めることができるよう負荷分散ハッシュ機能を設定するには、**ip cef load-sharing algorithm** コマンドを使用します。ポートを含まない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。

ip cef load-sharing algorithm {**include-ports** {**source** *source* | **destination** *dest*} | **original** | **tunnel** | **universal**}

no ip cef load-sharing algorithm {**include-ports** {**source** *source* | **destination** *dest*} | **original** | **tunnel** | **universal**}

構文の説明

include-ports	レイヤ 4 ポートを含むアルゴリズムを指定します。
source *source*	負荷分散ハッシュ機能での送信元ポートを指定します。
destination *dest*	負荷分散ハッシュでの宛先ポートを指定します。ハッシュ機能での送信元および宛先を使用します。
original	オリジナル アルゴリズムを指定します。これは推奨されません。
tunnel	トンネルだけの環境で使用されるアルゴリズムを指定します。
universal	デフォルトの Cisco IOS 負荷分散アルゴリズムを指定します。

デフォルト

デフォルトの負荷分散アルゴリズムはディセーブルです。

（注）　このオプションには、負荷分散ハッシュの送信元または宛先ポートは含まれません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

original アルゴリズム、tunnel アルゴリズム、および universal アルゴリズムは、ハードウェアを通してルーティングされます。ソフトウェアによってルーティングされるパケットの場合、アルゴリズムはソフトウェアで処理されます。**include-ports** オプションは、ソフトウェアによってスイッチングされたトラフィックには適用されません。

例

次の例では、レイヤ 4 ポートを含む IP CEF 負荷分散アルゴリズムを設定する方法を示します。

```
Switch(config)# ip cef load-sharing algorithm include-ports
Switch(config)#
```

次の例では、レイヤ 4 トンネリング ポートを含む IP CEF 負荷分散アルゴリズムを設定する方法を示します。

```
Switch(config)# ip cef load-sharing algorithm include-ports tunnel
Switch(config)#
```

関連コマンド

コマンド	説明
show ip cef vlan	IP CEF VLAN インターフェイスのステータスおよびコンフィギュレーション情報を表示します。

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** コマンドを使用します。DHCP スヌーピ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 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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

VLAN で DHCP スヌーピングを使用するには、事前に DHCP スヌーピングをグローバルにイネーブルにしておく必要があります。

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
Switch(config)#
```

次の例では、DHCP スヌーピングをディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping
Switch(config)#
```

関連コマンド

コマンド	説明
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 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します。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

ip dhcp snooping binding

再起動時にバインディングを復元するように、DHCP バインディング コンフィギュレーションを設定および生成するには、**ip dhcp snooping binding** コマンドを使用します。バインディング コンフィギュレーション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 binding *mac-address* **vlan** *vlan-#* *ip-address* **interface** *interface* **expiry** *seconds*

no ip dhcp snooping binding *mac-address* **vlan** *vlan-#* *ip-address* **interface** *interface*

構文の説明

mac-address	MAC アドレスを指定します。
vlan *vlan-#*	有効な VLAN 番号を指定します。
ip-address	IP アドレスを指定します。
interface *interface*	インターフェイスのタイプおよび番号を指定します。
expiry *seconds*	バインディングが無効となるまでの間隔（秒）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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)EW	10 ギガビット イーサネット インターフェイスのサポートが、Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドを使用してバインディングを追加または削除すると、常にバインディング データベースが変更済みとマークされ、書き込みが開始されます。

例

次の例では、VLAN 1 のインターフェイス gigabitethernet1/1 に、有効期限が 1000 秒の DHCP バインディング コンフィギュレーションを生成する方法を示します。

```
Switch# ip dhcp snooping binding 0001.1234.1234 vlan 1 172.20.50.5 interface gi1/1 expiry 1000
Switch#
```

関連コマンド

コマンド	説明
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 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 上で DHCP スヌーピングをイネーブルにします。

コマンド	説明
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

ip dhcp snooping database

DHCP スヌーピングによって生成されたバインディングを保存するには、**ip dhcp snooping database** コマンドを使用します。タイムアウトのリセット、書き込み遅延のリセット、または URL によって指定されたエージェントの削除を行うには、このコマンドの **no** 形式を使用します。

ip dhcp snooping database {*url* | **timeout** *seconds* | **write-delay** *seconds*}

no ip dhcp snooping database {**timeout** | **write-delay**}

構文の説明

url	URL を次のいずれかの形式で指定します。 • tftp://<host>/<filename> • ftp://<user>:<password>@<host>/<filename> • rcp://<user>@<host>/<filename> • nvram:/<filename> • bootflash:/<filename>
timeout *seconds*	バインディング データベースが変更されてからデータベース転送プロセスを中止するまでの期間を指定します。 遅延の最小値は 15 秒です。0 は、無限の期間として定義されます。
write-delay *seconds*	バインディング データベースが変更されたあとに、転送を遅らせる期間を指定します。

デフォルト

timeout 値は 300 秒（5 分）に設定されています。

write-delay 値は 300 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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ネットワークベースの URL（TFTP や FTP など）上の設定済み URL に事前に空のファイルを作成し、スイッチがこの URL で一連のバインディングの初回書き込みを行えるようにする必要があります。

（注） NVRAM とブートフラッシュはいずれも記憶容量がかぎられているため、TFTP またはネットワークベースのファイルを使用することを推奨します。データベース ファイルの保存にフラッシュを使用する場合は、（エージェントによる）新規更新によって新しいファイルが作成されます（フラッシュはすぐに満杯になります）。また、フラッシュで使用されるファイル システムの性質上、大量のファイルを保存すると、アクセスが極端に低速化します。ファイルを TFTP によってアクセス可能なリモートの位置に保存しておくと、スイッチオーバーが発生した場合に、RPR/SSO スタンバイ スーパーバイザ エンジンがバインディング リストを引き継ぐことができます。

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データベース 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 terminal
Switch(config)# ip dhcp snooping database tftp://10.1.1.1/directory/file
Switch(config)# end
Switch# show ip dhcp snooping database
Agent URL : tftp://10.1.1.1/directory/file
Write delay Timer : 300 seconds
Abort Timer : 300 seconds

Agent Running : Yes
Delay Timer Expiry : Not Running
Abort Timer Expiry : Not Running

Last Succeded Time : None
Last Failed Time : None
Last Failed Reason : No failure recorded.

Total Attempts       :        1   Startup Failures :        0
Successful Transfers :        0   Failed Transfers :        0
Successful Reads     :        0   Failed Reads     :        0
Successful Writes    :        0   Failed Writes    :        0
Media Failures       :        0

Switch#
```

関連コマンド

コマンド	説明
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 binding	DHCP バインディング コンフィギュレーションを設定および生成し、再起動後もバインディングを復元します。
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 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

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** 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 format remote-id {**hostname** | **string** {*word*}}

no ip dhcp snooping information option format remote-id {**hostname** | **string** {*word*}}

構文の説明

format	オプション 82 情報の形式を指定します。
remote-id	オプション 82 のリモート ID を指定します。
hostname	リモート ID にユーザ設定のホスト名を指定します。
string *word*	リモート ID にユーザ定義の文字列を指定します。word は、スペースを含まない 1 ～ 63 文字の文字列です。

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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	オプション 82 の強化をサポートする **remote-id** キーワードが追加されました。

使用上のガイドライン

63 文字を超えるホスト名を使用すると、リモート ID では 63 文字に切り捨てられます。

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
Switch(config)#
```

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

```
Switch(config)# no ip dhcp snooping information option
Switch(config)#
```

次の例では、ホスト名をリモート ID として設定する方法を示します。

```
Switch(config)# ip dhcp snooping information option format remote-id hostname
Switch(config)#
```

次の例では、VLAN 500 ～ 555 で DHCP スヌーピングをイネーブルにし、オプション 82 リモート ID を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
```

```
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
```

関連コマンド

コマンド	説明
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 binding	DHCP バインディング コンフィギュレーションを設定および生成し、再起動後もバインディングを復元します。
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 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します。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan information option format-type	VLAN で回線 ID（DHCP スヌーピング オプション 82 のサブオプション）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 エントリを表示します。

ip dhcp snooping information option allow-untrusted

オプション 82 データが挿入された DHCP パケットを、信頼できないスヌーピング ポートから受信できるようにするには、**ip dhcp snooping information option allow-untrusted** コマンドを使用します。このような DHCP パケットの受信を禁止するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping information option allow-untrusted

no ip dhcp snooping information option allow-untrusted

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

オプション 82 を含む DHCP パケットは、信頼できないスヌーピング ポートでは許可されません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(25)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、オプション 82 データが挿入された DHCP パケットを、信頼できないスヌーピング ポートから受信できるよう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 information option allow-untrusted
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
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 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 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します。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

ip dhcp snooping limit rate

インターフェイスで 1 秒あたりに受信できる DHCP メッセージの数を設定するには、**ip dhcp snooping limit rate** コマンドを使用します。DHCP スヌーピング レート制限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 limit rate *rate*

no ip dhcp snooping limit rate

構文の説明

rate	スイッチで 1 秒あたりに受信できる DHCP メッセージの数です。

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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

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のすべての DHCP トラフィックを集約するので、インターフェイスのレート制限を大きい値に調整する必要があります。

例

次の例では、DHCP メッセージ レート制限をイネーブルにする方法を示します。

```
Switch(config-if)# ip dhcp snooping limit rate 150
Switch(config)#
```

次の例では、DHCP メッセージ レート制限をディセーブルにする方法を示します。

```
Switch(config-if)# no ip dhcp snooping limit rate
Switch(config)#
```

関連コマンド

コマンド	説明
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 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 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

ip dhcp snooping trust

DHCP スヌーピング用にインターフェイスを信頼できるインターフェイスとして設定するには、**ip dhcp snooping trust** コマンドを使用します。インターフェイスを信頼できないインターフェイスとして設定するには、このコマンドの **no** 形式を使用します。

ip dhcp snooping 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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、インターフェイスで 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
Switch(config)#
```

次の例では、インターフェイスで DHCP スヌーピング信頼をディセーブルにする方法を示します。

```
Switch(config-if)# no ip dhcp snooping trust
Switch(config)#
```

関連コマンド

コマンド	説明
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 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 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します。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

ip dhcp snooping vlan

VLAN で DHCP スヌーピングをイネーブルにするには、**ip dhcp snooping vlan** コマンドを使用します。VLAN で DHCP スヌーピ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 dhcp snooping [**vlan** *number*]

no ip dhcp snooping [**vlan** *number*]

構文の説明

vlan *number*	（任意）単一の VLAN 番号または VLAN の範囲です。有効値の範囲は 1 ～ 4094 です。

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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

DHCP スヌーピングが VLAN でイネーブルになるのは、グローバル スヌーピングと VLAN スヌーピングが両方ともイネーブルの場合のみです。

例

次の例では、DHCP スヌーピングを VLAN でイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10
Switch(config)#
```

次の例では、DHCP 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 ip dhcp snooping vlan 10
Switch(config)#
```

次の例では、DHCP スヌーピングを VLAN のグループでイネーブルにする方法を示します。

```
Switch(config)# ip dhcp snooping vlan 10 55
Switch(config)#
```

次の例では、DHCP スヌーピングを VLAN のグループでディセーブルにする方法を示します。

```
Switch(config)# no ip dhcp snooping vlan 10 55
Switch(config)#
```

関連コマンド

コマンド	説明
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 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 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します。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan information option format-type	VLAN で回線 ID（DHCP スヌーピング オプション 82 のサブオプション）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 エントリを表示します。

ip dhcp snooping vlan information option format-type

VLAN で回線 ID（DHCP スヌーピング オプション 82 のサブオプション）をイネーブルにするには、**ip dhcp snooping vlan information option format-type** コマンドを使用します。VLAN で回線 ID 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 vlan *number* **information option format-type circuit-id string** *string*

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

構文の説明

number	単一の VLAN 番号または VLAN の範囲です。有効値の範囲は 1 ～ 4094 です。
circuit-id	文字列を回線 ID として使用するように指定します。
string *string*	回線 ID にユーザ定義の文字列を指定します。

デフォルト

VLAN-mod-port です（DHCP スヌーピング オプション 82 がディセーブルになっている場合）。

コマンド 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	変更内容
12.2(40)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

DHCP オプション 82 の回線 ID サブオプションがサポートされるのは、DHCP オプション 82 を使用して VLAN で DHCP スヌーピングをグローバルにイネーブルにした場合のみです。

例

次の例では、VLAN 500 ～ 555 で DHCP スヌーピングをイネーブルにし、オプション 82 回線 ID を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 500 555
Switch(config)# ip dhcp snooping information option format remote-id string switch123
Switch(config)# interface GigabitEthernet 5/1
Switch(config-if)# ip dhcp snooping trust
Switch(config-if)# ip dhcp snooping limit rate 100
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-555
Switch(config-if)# interface FastEthernet 2/1
Switch(config-if)# ip dhcp snooping vlan 555 information option format-type circuit-id
string customer-500
Switch(config)# end
```

関連コマンド

コマンド	説明
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 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 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します。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

ip igmp filter

IGMP プロファイルをインターフェイスに適用することにより、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** コマンドを使用します。インターフェイスから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 プロファイル番号です。有効値の範囲は 1 ～ 429496795 です。

デフォルト

プロファイルは適用されません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(11b)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

IGMP フィルタはレイヤ 2 の物理インターフェイスだけに適用できます。ルーテッド ポート、Switch Virtual Interface（SVI）、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。

IGMP のプロファイルは 1 つまたは複数のポート インターフェイスに適用できますが、1 つのポートに対して 1 つのプロファイルのみ適用できます。

例

次の例では、IGMP プロファイル 22 をインターフェイスに適用する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp filter 22
Switch(config-if)#
```

関連コマンド

コマンド	説明
ip igmp profile	IGMP プロファイルを作成します。
show ip igmp profile	設定済みのすべての IGMP プロファイルまたは指定した IGMP プロファイルを表示します。

ip igmp max-groups

レイヤ 2 インターフェイスが加入できる IGMP グループの最大数を設定するには、**ip igmp max-groups** コマンドを使用します。最大数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。

ip igmp max-groups *number*

no ip igmp max-groups

構文の説明

number	インターフェイスが加入できる IGMP グループの最大数です。有効値の範囲は 0 ～ 4294967294 です。

デフォルト

最大数の制限はありません。

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	変更内容
12.1(11b)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ip igmp max-groups コマンドは、レイヤ 2 物理インターフェイス上でだけ使用できます。IGMP グループの最大数は、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は設定できません。

例

次の例では、インターフェイスが加入できる IGMP グループの数を 25 に制限する方法を示します。

```
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# ip igmp max-groups 25
Switch(config-if)
```

ip igmp profile

IGMP プロファイルを作成するには、**ip igmp profile** コマンドを使用します。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 プロファイル番号です。有効値の範囲は 1 ～ 4294967295 です。

デフォルト

プロファイルは作成されません。

コマンド モード

グローバル コンフィギュレーション モード

IGMP プロファイル コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(11b)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

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 つのみです。

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

関連コマンド

コマンド	説明
ip igmp filter	IGMP プロファイルをインターフェイスに適用することにより、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します。
show ip igmp profile	設定済みのすべての IGMP プロファイルまたは指定した IGMP プロファイルを表示します。

ip igmp query-interval

スイッチが IGMP ホスト クエリー メッセージを送信する頻度を設定するには、**ip igmp query-interval** コマンドを使用します。デフォルトの頻度に戻すには、このコマンドの **no** 形式を使用します。

ip igmp query-interval *seconds*

no ip igmp query-interval

構文の説明

seconds	IGMP ホスト クエリー メッセージを送信する頻度（秒）です。有効値は IGMP スヌーピング モードによって異なります。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

クエリー間隔は 60 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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

デフォルトの IGMP スヌーピング コンフィギュレーションを使用する場合、有効なクエリー間隔の値は 1 ～ 65535 秒です。デフォルト コンフィギュレーションを変更して、CGMP を IGMP スヌーピング学習方式としてサポートするようにしている場合、有効なクエリー間隔の値は 1 ～ 300 秒です。

LAN の指定スイッチだけが IGMP ホスト クエリー メッセージを送信します。IGMP バージョン 1 の場合、指定スイッチは、LAN 上で実行されるマルチキャスト ルーティング プロトコルに従って選択されます。IGMP バージョン 2 の場合、指定クエリアはサブネット上の IP アドレスが最下位のマルチキャスト スイッチです。

（**ip igmp query-timeout** コマンドによって制御する）タイムアウト期間の間にクエリーが送信されなかった場合、スイッチがクエリアとなります。

（注）　タイムアウト期間を変更すると、マルチキャスト転送に深刻な影響が生じる可能性があります。

例

次の例では、指定スイッチが IGMP ホスト クエリー メッセージを送信する頻度を変更する方法を示します。

```
Switch(config-if)# ip igmp query-interval 120
Switch(config-if)#
```

関連コマンド

コマンド	説明
ip igmp querier-timeout（Cisco IOS のマニュアルを参照）	前のクエリアがクエリーを停止してから、ルータがインターフェイスのクエリアを引き継ぐまでのタイムアウト期間を設定します。
ip pim query-interval（Cisco IOS のマニュアルを参照）	Protocol Independent Multicast（PIM）ルータ クエリー メッセージの頻度を設定します。
show ip igmp groups（Cisco IOS のマニュアルを参照）	ルータに直接接続されていて、Internet Group Management Protocol（IGMP; インターネット グループ管理プロトコル）経由で学習されたレシーバーを持つマルチキャスト グループを表示します。**show ip igmp groups** コマンドは EXEC モードで使用します。

ip igmp snooping

IGMP スヌーピングをイネーブルにするには、**ip igmp snooping** コマンドを使用します。IGMP スヌーピ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 query count** *count* | **query solicit**}]

no ip igmp snooping [**tcn** {**flood query count** *count* | **query solicit**}]

構文の説明

tcn	（任意）トポロジ変更コンフィギュレーションを指定します。
flood	（任意）トポロジ変更が発生した場合にスパニング ツリー テーブルをネットワークにフラッディングするように指定します。
query	（任意）TCN クエリー コンフィギュレーションを指定します。
count *count*	（任意）スパニング ツリー テーブルをフラッディングする頻度を指定します。有効値の範囲は 1 ～ 10 です。
solicit	（任意）IGMP 一般クエリーを指定します。

デフォルト

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 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	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(11)EW	スパニング ツリー テーブルのフラッディングのサポートが追加されました。

使用上のガイドライン

tcn flood オプションは、レイヤ 2 スイッチ ポートおよび EtherChannel にのみ適用されます。ルーテッド ポート、VLAN インターフェイス、またはレイヤ 3 チャネルには適用されません。

マルチキャスト ルータでは、**ip igmp snooping** コマンドはデフォルトでディセーブルです。

（注）　インターフェイス コンフィギュレーション モードで **tcn flood** オプションを使用できます。

例

次の例では、IGMP 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 igmp snooping
Switch(config)#
```

次の例では、IGMP スヌーピングをディセーブルにする方法を示します。

```
Switch(config)# no ip igmp snooping
Switch(config)#
```

次の例では、9 つのトポロジ変更が発生したあとでスパニング ツリー テーブルのネットワークへのフラッディングをイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping tcn flood query count 9
Switch(config)#
```

次の例では、スパニング ツリー テーブルのネットワークへの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)# no ip igmp snooping tcn flood
Switch(config)#
```

次の例では、IGMP 一般クエリーをイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping tcn query solicit
Switch(config)#
```

次の例では、IGMP 一般クエリーをディセーブルにする方法を示します。

```
Switch(config)# no ip igmp snooping tcn query solicit
Switch(config)#
```

関連コマンド

コマンド	説明
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 インターフェイスを VLAN のマルチキャスト ルータ インターフェイスとして設定します。
ip igmp snooping vlan static	レイヤ 2 インターフェイスをグループのメンバーとして設定します。

ip igmp snooping report-suppression

レポート抑制をイネーブルにするには、**ip igmp snooping report-suppression** コマンドを使用します。レポート抑制をディセーブルにして、レポートをマルチキャスト デバイスへ転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no 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 スヌーピング 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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ip igmp snooping report-suppression コマンドがディセーブルの場合、すべての IGMP レポートがマルチキャスト デバイスへ転送されます。

このコマンドがイネーブルの場合、レポート抑制は IGMP スヌーピングによって行われます。

例

次の例では、レポート抑制をイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping report-suppression
Switch(config)#
```

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
Switch(config)#
```

次の例では、レポート抑制のシステム ステータスを表示する方法を示します。

```
Switch# show ip igmp snoop
vlan 1
----------
 IGMP snooping is globally enabled
 IGMP snooping TCN solicit query is globally disabled
 IGMP snooping global TCN flood query count is 2
 IGMP snooping is enabled on this Vlan
 IGMP snooping immediate-leave is disabled on this Vlan
 IGMP snooping mrouter learn mode is pim-dvmrp on this Vlan
 IGMP snooping is running in IGMP_ONLY mode on this Vlan
 IGMP snooping report suppression is enabled on this Vlan
Switch#
```

関連コマンド

コマンド	説明
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 インターフェイスを VLAN のマルチキャスト ルータ インターフェイスとして設定します。
ip igmp snooping vlan static	レイヤ 2 インターフェイスをグループのメンバーとして設定します。

ip igmp snooping vlan

VLAN の IGMP スヌーピングをイネーブルにするには、**ip igmp snooping vlan** コマンドを使用します。IGMP スヌーピ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 vlan *vlan-id*

no ip igmp snooping vlan *vlan-id*

構文の説明

vlan-id	VLAN の番号です。有効値の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

IGMP スヌーピングは、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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張アドレッシングのサポートが追加されました。

使用上のガイドライン

このコマンドを入力できるのは、VLAN インターフェイス コンフィギュレーション モードにかぎります。

マルチキャスト ルータでは、**ip igmp snooping vlan** コマンドはデフォルトでディセーブルです。

例

次の例では、IGMP スヌーピングを VLAN でイネーブルにする方法を示します。

```
Switch(config)# ip igmp snooping vlan 200
Switch(config)#
```

次の例では、IGMP 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 ip igmp snooping vlan 200
Switch(config)#
```

関連コマンド

コマンド	説明
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 インターフェイスを VLAN のマルチキャスト ルータ インターフェイスとして設定します。
ip igmp snooping vlan static	レイヤ 2 インターフェイスをグループのメンバーとして設定します。

ip igmp snooping vlan explicit-tracking

VLAN 単位の明示的ホスト トラッキングをイネーブルにするには、**ip igmp snooping vlan explicit-tracking** コマンドを使用します。明示的ホスト トラッキ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 vlan *vlan-id* **explicit-tracking**

no ip igmp snooping vlan *vlan-id* **explicit-tracking**

構文の説明

vlan_id	（任意）VLAN を指定します。有効値の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

明示的ホスト トラッキ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 モード

コマンド履歴

リリース	変更内容
12.1(20)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、インターフェイス VLAN 200 で IGMP 明示的ホスト トラッキングをディセーブルにし、そのコンフィギュレーションを確認する方法を示します。

```
Switch(config)# no ip igmp snooping vlan 200 explicit-tracking
Switch(config)# end
Switch# show ip igmp snooping vlan 200 | include explicit tracking
Global IGMP Snooping configuration:
-----------------------------------
IGMP snooping             : Enabled
IGMPv3 snooping           : Enabled
Report suppression        : Enabled
TCN solicit query         : Disabled
TCN flood query count     : 2

Vlan 2:
--------
IGMP snooping                  : Enabled
IGMPv2 immediate leave         : Disabled
Explicit host tracking         : Disabled
Multicast router learning mode : pim-dvmrp
CGMP interoperability mode     : IGMP_ONLY
Explicit host tracking         : Disabled
Switch#
```

関連コマンド

コマンド	説明
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 インターフェイスを VLAN のマルチキャスト ルータ インターフェイスとして設定します。
ip igmp snooping vlan static	レイヤ 2 インターフェイスをグループのメンバーとして設定します。
show ip igmp snooping membership	ホスト メンバーシップ情報を表示します。

ip igmp snooping vlan immediate-leave

IGMP 即時脱退処理をイネーブルにするには、**ip igmp snooping vlan immediate-leave** コマンドを使用します。即時脱退処理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 vlan *vlan_num* **immediate-leave**

no ip igmp snooping vlan *vlan_num* **immediate-leave**

構文の説明

vlan_num	VLAN の番号です。有効値の範囲は 1 ～ 4094 です。
immediate-leave	即時脱退処理をイネーブルにします。

デフォルト

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張アドレッシングのサポートが追加されました。

使用上のガイドライン

このコマンドを入力できるのは、グローバル コンフィギュレーション モードにかぎります。

即時脱退機能は、特定の VLAN の MAC グループに対して単一のレシーバーが存在する場合にのみ使用してください。

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 4 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 4 immediate-leave
Switch(config)#
```

次の例では、VLAN 4 で IGMP 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 ip igmp snooping vlan 4 immediate-leave
Switch(config)#
```

関連コマンド

コマンド	説明
ip igmp snooping	IGMP スヌーピングをイネーブルにします。
ip igmp snooping vlan mrouter	レイヤ 2 インターフェイスを VLAN のマルチキャスト ルータ インターフェイスとして設定します。
ip igmp snooping vlan static	レイヤ 2 インターフェイスをグループのメンバーとして設定します。

コマンド	説明
show ip igmp interface	IGMP インターフェイスのステータス情報およびコンフィギュレーション情報を表示します。
show mac-address-table multicast	マルチキャスト MAC アドレス テーブル情報を表示します。

ip igmp snooping vlan mrouter

VLAN のマルチキャスト ルータ インターフェイスとしてレイヤ 2 インターフェイスをスタティックに設定するには、**ip igmp snooping vlan mrouter** 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。

ip igmp snooping vlan *vlan-id* **mrouter** {**interface** {{**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

no ip igmp snooping vlan *vlan-id* **mrouter** {**interface** {{**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}} | {**learn** {**cgmp** | **pim-dvmrp**}}

構文の説明

vlan *vlan-id*	コマンドで使用する VLAN ID 番号を指定します。有効値の範囲は 1 ～ 4094 です。
interface	マルチキャスト スイッチへのネクストホップ インターフェイスを指定します。
fastethernet *slot/port*	ファスト イーサネット インターフェイス、およびスロットとポートの番号を指定します。
gigabitethernet *slot/port*	ギガビット イーサネット インターフェイス、およびスロットとポートの番号を指定します。
tengigabitethernet *slot/port*	10 ギガビット イーサネット インターフェイス、およびスロットとポートの番号を指定します。
port-channel *number*	ポート チャネル番号です。有効値の範囲は 1 ～ 64 です。
learn	マルチキャスト スイッチの学習方式を指定します。
cgmp	マルチキャスト スイッチのスヌーピング CGMP パケットを指定します。
pim-dvmrp	マルチキャスト スイッチのスヌーピング PIM-DVMRP パケットを指定します。

デフォルト

マルチキャスト スイッチのスヌーピング PIM-DVMRP パケットが指定されます。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張アドレッシングのサポートが追加されました。
12.2(25)EW	10 ギガビット イーサネット インターフェイスのサポートが、Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドを入力できるのは、VLAN インターフェイス コンフィギュレーション モードにかぎります。

スイッチへのインターフェイスは、コマンドを入力する VLAN 内になければなりません。スイッチは管理上のアップ状態にあり、ライン プロトコルもアップになっている必要があります。

CGMP 学習方式により、制御トラフィックを減少させることができます。

設定する学習方式は NVRAM に保存されます。

マルチキャスト インターフェイスへのスタティック接続は、スイッチ インターフェイス上でだけサポートされます。

例

次の例では、マルチキャスト スイッチへのネクストホップ インターフェイスを指定する方法を示します。

```
Switch(config-if)# ip igmp snooping 400 mrouter interface fastethernet 5/6
Switch(config-if)#
```

次の例では、マルチキャスト スイッチの学習方式を指定する方法を示します。

```
Switch(config-if)# ip igmp snooping 400 mrouter learn cgmp
Switch(config-if)#
```

関連コマンド

コマンド	説明
ip igmp snooping	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 static	レイヤ 2 インターフェイスをグループのメンバーとして設定します。
show ip igmp snooping	ダイナミックに学習され、手動で設定された VLAN スイッチ インターフェイスに関する情報を表示します。
show ip igmp snooping mrouter	ダイナミックに学習され、手動で設定されたマルチキャスト スイッチ インターフェイスに関する情報を表示します。

ip igmp snooping vlan static

レイヤ 2 インターフェイスをグループのメンバーとして設定するには、**ip igmp snooping vlan static** 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。

ip igmp snooping vlan *vlan_num* **static** *mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *slot/port*} | {**port-channel** *number*}}

no ip igmp snooping vlan *vlan_num* **static** *mac-address* {**interface** {**fastethernet** *slot/port*} | {**gigabitethernet** *slot/port*} | {**tengigabitethernet** *mod/interface-number*} | {**port-channel** *number*}}

構文の説明

vlan_num	VLAN の番号です。
mac-address	グループ MAC アドレスです。
interface	マルチキャスト スイッチへのネクストホップ インターフェイスを指定します。
fastethernet *slot/port*	ファスト イーサネット インターフェイス、およびスロットとポートの番号を指定します。
gigabitethernet *slot/port*	ギガビット イーサネット インターフェイス、およびスロットとポートの番号を指定します。
tengigabitethernet *slot/port*	10 ギガビット イーサネット インターフェイス、およびスロットとポートの番号を指定します。
port-channel *number*	ポート チャネル番号です。有効値の範囲は 1 ～ 64 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

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)EW	10 ギガビット イーサネット インターフェイスのサポートが、Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、インターフェイスでホストをスタティックに設定する方法を示します。

```
Switch(config)# ip igmp snooping vlan 4 static 0100.5e02.0203 interface fastethernet 5/11
Configuring port FastEthernet5/11 on group 0100.5e02.0203 vlan 4
Switch(config)#
```

関連コマンド

コマンド	説明
ip igmp snooping	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。

コマンド	説明
ip igmp snooping vlan mrouter	レイヤ 2 インターフェイスを VLAN のマルチキャスト ルータ インターフェイスとして設定します。
show mac-address-table multicast	マルチキャスト MAC アドレス テーブル情報を表示します。

ip local-proxy-arp

ローカル プロキシ ARP 機能をイネーブルにするには、**ip local-proxy-arp** コマンドを使用します。ローカル プロキシ ARP 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。

ip local-proxy-arp

no ip local-proxy-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

ローカル プロキシ ARP 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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

この機能は、ホストが接続されているスイッチに直接通信することが意図的に禁止されているサブネット上でだけ使用してください。

ICMP リダイレクトは、ローカル プロキシ ARP 機能がイネーブルのインターフェイスではディセーブルになります。

例

次の例では、ローカル プロキシ ARP 機能をイネーブルにする方法を示します。

```
Switch(config-if)# ip local-proxy-arp
Switch(config-if)#
```

ip mfib fastdrop

MFIB 高速ドロップをイネーブルにするには、**ip mfib fastdrop** コマンドを使用します。MFIB 高速ドロップをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip mfib fastdrop

no ip mfib fastdrop

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

MFIB 高速ドロップはイネーブルです。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、MFIB 高速ドロップをイネーブルにする方法を示します。

```
Switch# ip mfib fastdrop
Switch#
```

関連コマンド

コマンド	説明
clear ip mfib fastdrop	MFIB 高速ドロップ エントリをすべてクリアします。
show ip mfib fastdrop	現在アクティブな高速ドロップ エントリをすべて表示し、高速ドロップがイネーブルであるかどうかも示します。

ip route-cache flow

IP ルーティングの NetFlow 統計情報をイネーブルにするには、**ip route-cache flow** コマンドを使用します。NetFlow 統計情報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 route-cache flow [**infer-fields**]

no ip route-cache flow [**infer-fields**]

構文の説明

infer-fields	（任意）ソフトウェアによって推測された場合に、入力 ID、出力 ID、ルーティング情報といった NetFlow フィールドを含めます。

デフォルト

NetFlow 統計情報はディセーブルです。

推測される情報は除外されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(19)EW	推測フィールドをサポートするようにコマンドが強化されました。

使用上のガイドライン

これらのコマンドを使用するには、Supervisor Engine IV および NetFlow Service Card を搭載する必要があります。

NetFlow 統計機能は、一連のトラフィック統計情報を取得します。これらのトラフィック統計情報には、送信元 IP アドレス、宛先 IP アドレス、レイヤ 4 ポート情報、プロトコル、入出力 ID など、ネットワークの分析、計画、アカウンティング、課金、および DoS 攻撃の識別に使用可能なルーティング情報が含まれます。

NetFlow スイッチングは、すべてのインターフェイス タイプの IP トラフィックおよび IP カプセル化トラフィックでサポートされます。

ip route-cache flow コマンドのあとに **ip route-cache flow infer-fields** コマンドを入力すると、既存のキャッシュが消去されます。この逆も同様です。これは、キャッシュ内に推測フィールドを持つフローと持たないフローが混在しないようにするためです。

NetFlow スイッチングの詳細については、『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

（注） NetFlow は他のスイッチング モデルよりも多くのメモリおよび CPU リソースを消費します。NetFlow をイネーブルにする前に、スイッチに必要なリソースを把握する必要があります。

例　次の例では、スイッチで NetFlow スイッチングをイネーブルにする方法を示します。

```
Switch# config terminal
Switch(config)# ip route-cache flow
Switch(config)# exit
Switch#
```

（注）　このコマンドは、インターフェイス単位では機能しません。

ip source binding

スタティック IP ソース バインディング エントリを追加または削除するには、**ip source binding** コマンドを使用します。対応する IP ソース バインディング 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 source binding *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-name*

no ip source binding *ip-address mac-address* **vlan** *vlan-id* **interface** *interface-name*

構文の説明

ip-address	バインディング対象 IP アドレスです。
mac-address	バインディング対象 MAC アドレスです。
vlan *vlan-id*	VLAN 番号
interface *interface-name*	バインディング対象インターフェイスです。

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

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ip source binding コマンドは、スタティック IP ソース バインディング エントリを追加するためにのみ使用します。

対応する IP ソース バインディング 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。削除を正常に行うには、すべての必須パラメータを一致させる必要があります。

各スタティック IP バインディング エントリは、MAC アドレスおよび VLAN 番号で指定します。CLI に既存の MAC および VLAN を含めると、既存のバインディング エントリが新しいパラメータで更新されます。別のバインディング エントリは作成されません。

例

次の例では、スタティック IP ソース バインディングを設定する方法を示します。

```
Switch# config terminal
Switch(config)# ip source binding 11.0.0.1 0000.000A.000B vlan 10 interface
fastethernet6/10
Switch(config)#
```

関連コマンド

コマンド	説明
show ip source binding	システムに設定されている IP ソース バインディングを表示します。

ip sticky-arp

スティッキ ARP をイネーブルにするには、**ip sticky-arp** コマンドを使用します。スティッキ 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

イネーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、PVLAN のみでサポートされています。

レイヤ 3 PVLAN インターフェイスで学習される ARP エントリは、スティッキ ARP エントリになります（PVLAN インターフェイスの ARP エントリを表示および確認するには、**show arp** コマンドを使用する必要があります）。

セキュリティ上の理由から、PVLAN インターフェイスのスティッキ ARP エントリは期限切れになりません。同一の IP アドレスを持つ新しい装置を接続すると、メッセージが生成され、その ARP エントリは作成されません。

PVLAN インターフェイスの ARP エントリは期限切れにならないため、MAC アドレスの変更が生じた場合は、PVLAN インターフェイスの ARP エントリを手動で削除する必要があります。

スティッキ ARP エントリはスタティック エントリとは異なり、**reboot** および **restart** コマンドを入力しても保存および復元されません。

例

次の例では、スティッキ ARP 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 sticky-arp
Switch(config)# end
Switch#
```

次の例では、スティッキ ARP をディセ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) no ip sticky-arp
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
arp（Cisco IOS のマニュアルを参照）	Switched Multimegabit Data Service（SMDS; スイッチド マルチメガビット データ サービス）ネットワーク経由のスタティック ルーティングの Address Resolution Protocol（ARP; アドレス解決プロトコル）エントリをイネーブルにします。
show arp（Cisco IOS のマニュアルを参照）	ARP 情報を表示します。

ip verify header vlan all

レイヤ 2 でスイッチングされた IPv4 パケットの IP ヘッダー検証をイネーブルにするには、**ip verify header vlan all** コマンドを使用します。IP ヘッダー検証をディセーブルにするには、このコマンドの **no** 形式を使用します。

ip verify header vlan all

no ip verify header vlan all

構文の説明

このコマンドには、デフォルト設定はありません。

デフォルト

ブリッジングおよびルーティングされた IPv4 パケットの IP ヘッダーが検証されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(20)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、レイヤ 3 でスイッチング（ルーティング）されたパケットには適用されません。

Catalyst 4500 シリーズ スイッチは、スイッチングされたすべての IPv4 パケットの IPv4 ヘッダーについて、次のフィールドの有効性を調べます。

- バージョンは 4 である必要があります。
- ヘッダー長は 20 バイト以上である必要があります。
- 全体長がヘッダー長の 4 倍以上であり、レイヤ 2 パケット サイズからレイヤ 2 カプセル化サイズを引いた値よりも大きくなければなりません。

IPv4 パケットが IP ヘッダー検証の基準を満たさない場合、パケットはドロップされます。ヘッダー検証をディセーブルにすると、IP ヘッダーが無効なパケットはブリッジングされますが、ルーティングが必要な場合であってもルーティングされません。また、IPv4 アクセス リストも IP ヘッダーに適用されません。

例

次の例では、レイヤ 2 でスイッチングされた IPv4 パケットの IP ヘッダー検証をディセーブルにする方法を示します。

```
Switch# config terminal
Switch(config)# no ip verify header vlan all
Switch(config)# end
Switch#
```

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するには、**ip verify source** 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 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**} [**port-security**]

no ip verify source {**vlan dhcp-snooping**} [**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。
port-security	（任意）ポート セキュリティ機能を使用して、送信元 IP アドレスと MAC アドレスの両方をフィルタリングします。

デフォルト

IP ソース ガードが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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(37)SG	IP ポート セキュリティおよびトラッキングのサポートが追加されました。

例

次の例では、VLAN 10 ～ 20 で IP ソース ガードをポート単位でイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface fastethernet6/1
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 f6/1
Interface  Filter-type  Filter-mode  IP-address       Mac-address        Vlan
---------  -----------  -----------  ---------------  -----------------  ----------
Fa6/1      ip-mac       active       10.0.0.1                            10
Fa6/1      ip-mac       active       deny-all                            11-20
Switch#
```

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 dhcp snooping	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 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 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 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します。
ip dhcp snooping trust	信頼できる VLAN 上で DHCP スヌーピングをイネーブルにします。
ip source binding	スタティック IP ソース バインディング エントリを追加または削除します。
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 source binding	システムに設定されている IP ソース バインディングを表示します。
show ip verify source	特定のインターフェイス上の IP ソース ガード コンフィギュレーションおよびフィルタを表示します。

ip verify unicast source reachable-via

Supervisor Engine 6-E および Catalyst 4900M シャーシ IPv4 インターフェイスでユニキャスト RPF チェックをイネーブルにして設定するには、**ip verify unicast source reachable-via** コマンドを使用します。ユニキャスト RPF 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 unicast source reachable-via rx allow-default

no ip verify unicast source reachable-via

構文の説明

rx	送信元アドレスがパケットを受信したインターフェイスで到達可能であることを確認します。
allow-default	デフォルト ルートが送信元アドレスと一致することを確認します。

デフォルト

ディセーブル

コマンド 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	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6-E および Catalyst 4900M シャーシを使用する Catalyst 4500 に追加されました。

使用上のガイドライン

基本 RX モードでは、ユニキャスト RPF により、着信インターフェイス側で送信元アドレスが到達可能になっていなければならないことが保証されます。たとえば、負荷分散なしで送信元が到達可能になっていなければいけません。

（注） ユニキャスト RPF は入力機能であり、接続のアップストリーム エンドにあるルータの入力インターフェイスにのみ適用されます。

ユニキャスト RPF を内部ネットワーク インターフェイスで使用しないでください。内部インターフェイスにはルーティングに非対称性が存在する可能性があります。つまり、パケットの送信元へのルートが複数存在します。固有または指定の対称性が存在するところにのみユニキャスト RPF を適用します。

例

次の例では、ユニキャスト RPF exist-only チェック モ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)# interface gigabitethernet1/1
Switch(config-if)# ip verify unicast source reachable-via rx allow-default
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
ip cef（Cisco IOS のマニュアルを参照）	スイッチで Cisco Express Forwarding（CEF; シスコ エクスプレス フォワーディング）をイネーブルにします。
show running-config	スイッチの現在の実行コンフィギュレーションを表示します。

ipv6 mld snooping

IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピングをグローバルにイネーブルにするか、または指定した VLAN でイネーブルにするには、キーワードを指定せずに **ipv6 mld snooping** コマンドを使用します。スイッチまたは VLAN で MLD スヌーピ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 mld snooping [**vlan** *vlan-id*]

no ipv6 mld snooping [**vlan** *vlan-id*]

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 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ようにするには、事前に MLD スヌーピングをグローバルにイネーブルにしておく必要があります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Catalyst 4500 に追加されました。

使用上のガイドライン

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 コンフィギュレーションは、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。

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no ipv6 mld snooping vlan 11
Switch(config)# end
Switch#
```

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
show ipv6 mld snooping	スイッチまたは VLAN の IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピング コンフィギュレーションを表示します。

ipv6 mld snooping last-listener-query-count

クライアントが期限切れになる前に送信される IP version 6（IPv6）マルチキャスト リスナー検出 Mulitcast Address Specific Query（MASQ）を設定するには、**ipv6 mld snooping last-listener-query-count** コマンドを使用します。クエリー カウントをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **last-listener-query-count**

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 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	指定できる範囲は整数の 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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Catalyst 4500 に追加されました。

使用上のガイドライン

MLD スヌーピングでは、IPv6 マルチキャスト スイッチはマルチキャスト 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される MASQ の数が決まります。

VLAN に last-listener クエリー カウントを設定した場合、グローバルに設定された値より優先されます。VLAN カウントを設定しない場合（デフォルトの 0 に設定される）、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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping last-listener-query-count 1
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 10 last-listener-query-count 3
Switch(config)# end
Switch#
```

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	スイッチまたは VLAN 上の IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピングの last-listener クエリー間隔を設定します。
show ipv6 mld snooping	スイッチまたは VLAN の IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピング コンフィギュレーションを表示します。
show ipv6 mld snooping querier	スイッチまたは VLAN で最後に受信した IP version 6（IPv6）MLD スヌーピング クエリア関連の情報を表示します。

ipv6 mld snooping last-listener-query-interval

スイッチまたは VLAN 上の IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）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** コマンドを使用します。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**

構文の説明

vlan *vlan-id*	（任意）指定の VLAN で last-listener クエリー間隔を設定します。指定できる VLAN ID 範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	MASQ を送信してからマルチキャスト グループからポートを削除するまでにマルチキャスト スイッチが待機する時間（1000 分の 1 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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Catalyst 4500 に追加されました。

使用上のガイドライン

last-listener-query-interval の時間は、Mulitcast Address Specific Query（MASQ）を送信してからマルチキャスト グループからポートを削除するまでにマルチキャスト スイッチが待機する最大時間です。

MLD スヌーピングでは、IPv6 マルチキャスト スイッチが 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、スイッチはマルチキャスト アドレスのメンバーシップ データベースからそのポートを削除します。last-listener クエリー間隔は、応答のないポートをマルチキャスト グループから削除するまでにスイッチ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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping last-listener-query-interval 2000
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 last-listener-query-interval 5500
Switch(config)# end
Switch#
```

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	クライアントを期限切れにする前に送信される IP version 6（IPv6）マルチキャスト リスナー検出 Mulitcast Address Specific Queries（MASQ）を設定します。
show ipv6 mld snooping querier	スイッチまたは VLAN で最後に受信した IP version 6（IPv6）MLD スヌーピング クエリア関連の情報を表示します。

ipv6 mld snooping listener-message-suppression

IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）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** 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

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Catalyst 4500 に追加されました。

使用上のガイドライン

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 スイッチに転送されます。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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping listener-message-suppression
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no ipv6 mld snooping listener-message-suppression
Switch(config)# end
Switch#
```

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	IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピングをグローバルに、または指定した VLAN でイネーブルにします。
show ipv6 mld snooping	スイッチまたは VLAN の IP version 6（IPv6）MLD スヌーピング コンフィギュレーションを表示します。

ipv6 mld snooping robustness-variable

応答のないリスナーを削除する前にスイッチが送信する IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）クエリーの数を設定するか、または VLAN ID を入力して VLAN 単位でクエリーの数を設定するには、**ipv6 mld snooping robustness-variable** コマンドを使用します。変数をデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable** *integer_value*

no ipv6 mld snooping [**vlan** *vlan-id*] **robustness-variable**

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 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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Catalyst 4500 に追加されました。

使用上のガイドライン

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、応答しないリスナーを削除するまでにスイッチが待機するクエリー数が決まります。この値は、VLAN 値が設定されていないすべての VLAN に適用されます。

VLAN に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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping robustness-variable 3
Switch(config)# end
Switch#
```

次の例では、VLAN 1 に対してロバストネス変数を設定する方法を示します。この値により、VLAN のグローバル コンフィギュレーションが無効化されます。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 robustness-variable 1
Switch(config)# end
Switch#
```

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	クライアントを期限切れにする前に送信される IP version 6（IPv6）マルチキャスト リスナー検出 Mulitcast Address Specific Queries（MASQ）を設定します。
show ipv6 mld snooping	スイッチまたは VLAN の IP version 6（IPv6）MLD スヌーピング コンフィギュレーションを表示します。

ipv6 mld snooping tcn

IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）Topology Change Notification（TCN; トポロジ変更通知）を設定するには、**ipv6 mld snooping tcn** コマンドを使用します。デフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

no ipv6 mld snooping tcn {**flood query count** *integer_value* | **query solicit**}

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、クエリーを要求したポートに対しマルチキャスト 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 モード

コマンド履歴

リリース	変更内容
12.2(25)SG	このコマンドが、Catalyst 4500 に追加されました。

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping tcn query solicit.
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping tcn flood query count 5.
Switch(config)# end
Switch#
```

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
show ipv6 mld snooping	スイッチまたは VLAN の IP version 6（IPv6）MLD スヌーピング コンフィギュレーションを表示します。

ipv6 mld snooping vlan

VLAN インターフェイスで IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピング パラメータを設定するには、**ipv6 mld snooping vlan** コマンドを使用します。パラメータをデフォルト設定にリセットするには、このコマンドの **no** 形式を使用します。

ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ipv6-multicast-address* **interface** *interface-id*]

no ipv6 mld snooping vlan *vlan-id* [**immediate-leave** | **mrouter interface** *interface-id* | **static** *ip-address* **interface** *interface-id*]

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 スイッチ 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 スイッチ 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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Catalyst 4500 に追加されました。

使用上のガイドライン

VLAN の各ポート上に 1 つのレシーバーだけが存在する場合、即時脱退処理の機能だけを設定してください。設定は、NVRAM に保存されます。

static キーワードは MLD メンバー ポートを静的に設定するために使用されます。

設定およびスタティック ポートとグループは、NVRAM に保存されます。

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 immediate-leave
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no ipv6 mld snooping vlan 1 immediate-leave
Switch(config)# end
Switch#
```

次の例では、ポートをマルチキャスト スイッチ ポートとして設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 1 mrouter interface gigabitethernet1/0/2
Switch(config)# end
Switch#
```

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# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ipv6 mld snooping vlan 2 static FF12::34 interface gigabitethernet1/0/2
Switch(config)# end
Switch#
```

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	IP version 6（IPv6）Multicast Listener Discovery（MLD; マルチキャスト リスナー検出）スヌーピングをグローバルに、または指定した VLAN でイネーブルにします。
show ipv6 mld snooping	スイッチまたは VLAN の IP version 6（IPv6）MLD スヌーピング コンフィギュレーションを表示します。

issu abortversion

実行中の ISSU アップグレードまたはダウングレード プロセスを中止し、Catalyst 4500 シリーズ スイッチをプロセス開始前の状態に戻すには、**issu abortversion** コマンドを使用します。

issu abortversion *active-slot* [*active-image-new*]

構文の説明

active-slot	現在のスタンバイ スーパーバイザ エンジンのスロット番号を指定します。
active-image-new	（任意）現在のスタンバイ スーパーバイザ エンジンに格納された新規イメージの名前です。

デフォルト

デフォルト値は設定されていません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ISSU プロセスは、**issu abortversion** コマンドを使用することでいつでも中止できます。プロセスを完了するには、**issu commitversion** コマンドを入力します。何らかのアクションが実行される前に、両方のスーパーバイザ エンジンが Run Version（RV; 実行バージョン）または Load Version（LV; ロードバージョン）ステートであることを検証するためのチェックが行われます。

issu runversion コマンドの前に **issu abortversion** コマンドを入力すると、スタンバイ スーパーバイザ エンジンはリセットされ、古いイメージがリロードされます。**issu runversion** コマンドのあとに **issu abortversion** コマンドを入力すると、変更が適用され、新しいスタンバイ スーパーバイザ エンジンがリセットされ、古いイメージがリロードされます。

例

次の例では、スタンバイ スーパーバイザ エンジンをリセットおよびリロードする方法を示します。

```
Switch# issu abortversion 2
Switch#
```

関連コマンド

コマンド	説明
issu acceptversion	ロールバック タイマーを停止し、ISSU プロセス中に新しい Cisco IOS ソフトウェア イメージが自動的に停止されないようにします。
issu commitversion	新しい Cisco IOS ソフトウェア イメージを新しいスタンバイ スーパーバイザ エンジンにロードします。
issu loadversion	ISSU プロセスを開始します。

コマンド	説明
issu runversion	アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替え、新たにアクティブとなったスーパーバイザ エンジンで、指定した新規イメージを実行します。
show issu state	ISSU プロセスの実行中に ISSU の状態、および現在起動されているイメージの名前を表示します。

issu acceptversion

ロールバック タイマーを停止し、ISSU プロセスの実行中に新規 Cisco IOS ソフトウェア イメージが自動的に中止されないようにするには、**issu acceptversion** コマンドを使用します。

issu acceptversion *active-slot* [*active-image-new*]

構文の説明

active-slot	現在のアクティブ スーパーバイザ エンジンのスロット番号を指定します。
active-image-new	（任意）現在のアクティブ スーパーバイザ エンジンに格納された新規イメージの名前です。

デフォルト

ロールバック タイマーは、**issu runversion** コマンドを入力してから 45 分後に自動的にリセットされます。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

新規イメージに問題がなく、新しいスーパーバイザ エンジンがコンソールからもネットワークからも到達可能であることを確認できたら、**issu acceptversion** コマンドを入力してロールバック タイマーを停止します。**issu runversion** コマンドの入力後 45 分以内に **issu acceptversion** コマンドを入力しないと、ISSU プロセス全体が前バージョンのソフトウェアに自動的にロールバックされます。ロールバック タイマーは、**issu runversion** コマンドの入力後ただちに開始されます。

スタンバイ スーパーバイザ エンジンがホット スタンバイ ステートに移行する前にロールバック タイマーが満了した場合、タイマーは自動的に最大 15 分延長されます。この延長時間中にスタンバイ ステートがホット スタンバイ ステートに移行した場合、または 15 分の延長時間が経過した場合、スイッチは ISSU プロセスを中止します。タイマーの延長時間が 1 分経過するごとに、手動介入を要求する警告メッセージが表示されます。

ロールバック タイマーを長時間に設定し（デフォルトの 45 分など）、スタンバイ スーパーバイザ エンジンが 7 分後にホット スタンバイ ステートに移行した場合、38 分間（45 から 7 を引いた値）以内なら必要に応じてロールバックを行うことができます。

ロールバック タイマーを設定するには、**issu set rollback-timer** を使用します。

例

次の例では、ロールバック タイマーを停止して、ISSU プロセスを続行させる方法を示します。

```
Switch# issu acceptversion 2
Switch#
```

関連コマンド

コマンド	説明
issu abortversion	進行中の ISSU アップグレードまたはダウングレード プロセスを中止し、スイッチをプロセス開始前の状態に戻します。
issu commitversion	新しい Cisco IOS ソフトウェア イメージを新しいスタンバイ スーパーバイザ エンジンにロードします。
issu loadversion	ISSU プロセスを開始します。
issu runversion	アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替え、新たにアクティブとなったスーパーバイザ エンジンで、指定した新規イメージを実行します。
issu set rollback-timer	In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）ロールバック タイマーの値を設定します。
show issu state	ISSU プロセスの実行中に ISSU の状態、および現在起動されているイメージの名前を表示します。

issu changeversion

自動 ISSU アップグレード プロシージャを開始するか、または自動アップグレードをあとで開始するようにスケジューリングするには、**issu changeversion** EXEC コマンドを使用します。

issu changeversion [*active-slot*] **new-image** [*standby-slot standby-image*] [**at** *hh:mm* | **in** *hh:mm*] [*quick*]

構文の説明

new-image	アップグレード IOS XE バンドルの URL を指定します。
active-slot	アクティブ スイッチのスロット番号を定義します。
standby-slot	スタンバイ スイッチのスロット番号を定義します。
standby-image	スタンバイ イメージの URL を指定します。
at *hh:mm*	ISSU アップグレードをあとで開始するようにスケジューリングします。次の 24 時間の中でアップグレードを実行する正確な時間（*hh*:*mm*、24 時間形式）を指定します。
in *hh:mm*	ISSU アップグレードをあとで開始するようにスケジューリングします。アップグレードを実行するまでの時間と分（*hh*:*mm* 形式）を指定します（最大 99:59）。
quick	スイッチオーバーが実行されたときに、古いイメージではなく新しいイメージを使用してスタンバイ スーパーバイザ エンジンを起動し、アップグレードを高速化します。

デフォルト

なし

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更内容
3.1.0SG	このコマンドは Catalyst 4500 シリーズ スイッチで初めてサポートされるようになりました。

使用上のガイドライン

issu changeversion コマンドを使用すると、単一ステップの完全な ISSU アップグレード サイクルを開始できます。このコマンドでは、ユーザが介入しなくても、4 つすべての標準コマンド（**issu loadversion**、**issu runversion**、**issu acceptversion**、および **issu commitversion**）のロジックが実行されます。

また、**issu changeversion** コマンドを使用すると、アップグレード プロセスをあとで開始するようにスケジューリングできます。これにより、障害が発生する可能性を最小限に抑えながら、多数のシステムで段階的に順番にアップグレードを実行できます。

標準の ISSU アップグレード プロシージャと同様に、**issu changeversion** コマンドで開始した実行中のアップグレード プロシージャを **issu abortversion** コマンドで中止できます。システムで問題が検出されるか、またはアップグレード中にシステムに異常が検出されると、アップグレードが自動的に中止される可能性があります。

例

次の例では、**issu changeversion** コマンドを使用して、自動 ISSU アップグレードを開始する方法を示します。

```
Switch# issu changeversion 5 bootflash:cat4500e-universalk9.SSA.03.01.00.SG.150-1.XO.bin 6
slavebootflash:cat4500e-universalk9.SSA.03.01.00.SG.150-1.XO.bin
Switch#
```

次の例では、**issu changeversion** コマンドと quick オプションを使用して、自動 ISSU アップグレードを開始する方法を示します。この例では、オプションの standby-slot および standby-image パラメータは指定していません。

```
Switch# issu changeversion 5 bootflash:cat4500e-universalk9.SSA.03.01.00.SG.150-1.XO.bin
quick
Switch#
```

次の例では、**issu changeversion** コマンドと in オプションを使用して、自動 ISSU アップグレードを 2 時間 45 分後に実行するようにスケジューリングする方法を示します。この例では、オプションの standby-slot および standby-image パラメータは指定していません。

```
Switch# issu changeversion 5 bootflash:cat4500e-universalk9.SSA.03.01.00.SG.150-1.XO.bin
in 02:45
Switch#
```

関連コマンド

コマンド	説明
issu acceptversion	ロールバック タイマーを停止し、ISSU プロセスの実行中に新規 Cisco IOS XE ソフトウェア バンドルが自動的に中止されないようにします。
issu commitversion	新規 Cisco IOS XE ソフトウェア バンドルを新しいスタンバイ スーパーバイザ エンジンにロードします。
issu loadversion	ISSU プロセスを開始します。
issu runversion	アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替え、新たにアクティブとなったスーパーバイザ エンジンで、指定した新規イメージを実行します。

issu commitversion

新規 Cisco IOS ソフトウェア イメージを新しいスタンバイ スーパーバイザ エンジンにロードするには、**issu commitversion** コマンドを使用します。

issu commitversion *standby-slot* [*standby-image-new*]

構文の説明

standby-slot	現在のアクティブ スーパーバイザ エンジンのスロット番号を指定します。
standby-image-new	（任意）現在のアクティブ スーパーバイザ エンジンに格納された新規イメージの名前です。

デフォルト

デフォルトでは、イネーブルです。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

issu commitversion コマンドを使用すると、スタンバイ スーパーバイザ エンジンのファイル システムに新規 Cisco IOS ソフトウェア イメージが格納されているかどうか、および両方のスーパーバイザ エンジンが Run Version（RV; 実行バージョン）ステートであるかどうかが検証されます。これらの条件を満たす場合、次のアクションが実行されます。

- スタンバイ スーパーバイザ エンジンがリセットされ、Cisco IOS ソフトウェアの新規バージョンを使用して起動されます。
- スタンバイ スーパーバイザ エンジンが Stateful Switchover（SSO; ステートフル スイッチオーバー）モードに移行し、互換性のあるすべてのクライアントおよびアプリケーションに対して完全にステートフルになります。
- スーパーバイザ エンジンが最終ステート（初期ステートと同じ）に移行します。

issu commitversion コマンドを入力すると、In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）プロセスが完了します。新しい ISSU プロセスを開始することなく、このプロセスを中止したり、元の状態に戻したりすることはできません。

issu acceptversion コマンドを入力することなく、**issu commitversion** コマンドを入力すると、**issu acceptversion** コマンドと **issu commitversion** コマンドの両方を入力した場合と同様の結果が得られます。延長時間中に現在のステートで実行するつもりがなく、新規ソフトウェア バージョンに満足している場合は、**issu commitversion** コマンドを使用してください。

例

次の例では、スタンバイ スーパーバイザ エンジンをリセットして、新規 Cisco IOS ソフトウェア バージョンをリロードするように設定する方法を示します。

```
Switch# issu commitversion 1
Switch#
```

関連コマンド

コマンド	説明
issu acceptversion	ロールバック タイマーを停止し、ISSU プロセス中に新しい Cisco IOS ソフトウェア イメージが自動的に停止されないようにします。
issu commitversion	新しい Cisco IOS ソフトウェア イメージを新しいスタンバイ スーパーバイザ エンジンにロードします。
issu loadversion	ISSU プロセスを開始します。
issu runversion	アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替え、新たにアクティブとなったスーパーバイザ エンジンで、指定した新規イメージを実行します。
show issu state	ISSU プロセスの実行中に ISSU の状態、および現在起動されているイメージの名前を表示します。

issu loadversion

ISSU プロセスを開始するには、**issu loadversion** コマンドを使用します。

issu loadversion *active-slot active-image-new standby-slot standby-image-new* [**force**]

構文の説明

active-slot	現在のアクティブ スーパーバイザ エンジンのスロット番号を指定します。
active-image-new	現在のアクティブ スーパーバイザ エンジンに格納された新規イメージの名前を指定します。
standby-slot	ネットワーク デバイスのスタンバイ スロットを指定します。
standby-image-new	スタンバイ スーパーバイザ エンジンに格納された新規イメージの名前を指定します。
force	（任意）新規 Cisco IOS ソフトウェア バージョンに互換性がないことが検出された場合に、自動ロールバックを無効にします。

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

特権 EXEC モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

issu loadversion コマンドを実行すると、スタンバイ スーパーバイザ エンジンはリセットされ、このコマンドで指定した新規 Cisco IOS ソフトウェア イメージで起動されます。古いイメージと新しいイメージが両方とも ISSU 対応であり、ISSU と互換性があり、コンフィギュレーションの不一致が存在しない場合は、スタンバイ スーパーバイザ エンジンは Stateful Switchover（SSO; ステートフル スイッチオーバー）モードに移行し、両方のスーパーバイザ エンジンが Load Version（LV; ロード バージョン）ステートに移行します。

issu loadversion コマンドを入力してから、Cisco IOS ソフトウェアがスタンバイ スーパーバイザ エンジンにロードされ、スタンバイ スーパーバイザ エンジンが SSO モードに移行するまでには、数秒かかります。

例

次の例では、ISSU プロセスを開始する方法を示します。

```
Switch# issu loadversion 1 bootflash:new-image 2 slavebootflash:new-image
Switch#
```

関連コマンド

コマンド	説明
issu abortversion	進行中の ISSU アップグレードまたはダウングレード プロセスを中止し、スイッチをプロセス開始前の状態に戻します。
issu acceptversion	ロールバック タイマーを停止し、ISSU プロセス中に新しい Cisco IOS ソフトウェア イメージが自動的に停止されないようにします。
issu commitversion	新しい Cisco IOS ソフトウェア イメージを新しいスタンバイ スーパーバイザ エンジンにロードします。
issu runversion	アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替え、新たにアクティブとなったスーパーバイザ エンジンで、指定した新規イメージを実行します。
show issu state	ISSU プロセスの実行中に ISSU の状態、および現在起動されているイメージの名前を表示します。

issu runversion

アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替え、新たにアクティブとなったスーパーバイザ エンジンで、**issu loadversion** コマンドで指定した新規イメージを実行するには、**issu runversion** コマンドを使用します。

issu runversion *standby-slot* [*standby-image-new*]

構文の説明

standby-slot	ネットワーク デバイスのスタンバイ スロットを指定します。
standby-image-new	（任意）スタンバイ スーパーバイザ エンジンに格納された新規イメージの名前を指定します。

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 モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

issu runversion コマンドを実行すると、現在のアクティブ スーパーバイザ エンジンがスタンバイ スーパーバイザ エンジンに切り替わります。実際のスタンバイ スーパーバイザ エンジンは古いイメージ バージョンによって起動され、スイッチがリセットされます。スタンバイ スーパーバイザ エンジンがスタンバイ ステートに移行するとすぐ、ロールバック タイマーが開始します。

例

次の例では、アクティブ スーパーバイザ エンジンをスタンバイ スーパーバイザ エンジンに強制的に切り替える方法を示します。

```
Switch# issu runversion 2
Switch#
```

関連コマンド

コマンド	説明
issu abortversion	進行中の ISSU アップグレードまたはダウングレード プロセスを中止し、スイッチをプロセス開始前の状態に戻します。
issu acceptversion	ロールバック タイマーを停止し、ISSU プロセス中に新しい Cisco IOS ソフトウェア イメージが自動的に停止されないようにします。
issu commitversion	新しい Cisco IOS ソフトウェア イメージを新しいスタンバイ スーパーバイザ エンジンにロードします。
issu loadversion	ISSU プロセスを開始します。
show issu state	ISSU プロセスの実行中に ISSU の状態、および現在起動されているイメージの名前を表示します。

issu set rollback-timer

In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）ロールバック タイマーの値を設定するには、**issu set rollback-timer** コマンドを使用します。

issu set rollback-timer *seconds*

構文の説明

seconds	ロールバック タイマーの値を秒単位で指定します。有効なタイマー値の範囲は 0 ～ 7200 秒（2 時間）です。0 秒に設定すると、ロールバック タイマーはディセーブルになります。

デフォルト

ロールバック タイマーの値は 2700 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 モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ロールバック タイマーの値を設定するには、**issu set rollback-timer** コマンドを使用します。このコマンドは、スーパーバイザ エンジンが初期ステートの場合にのみイネーブルにできます。

例

次の例では、ロールバック タイマーの値を 3600 秒（1 時間）に設定する方法を示します。

```
Switch# configure terminal
Switch(config)# issu set rollback-timer 3600
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
issu acceptversion	ロールバック タイマーを停止し、ISSU プロセス中に新しい Cisco IOS ソフトウェア イメージが自動的に停止されないようにします。
issu set rollback-timer	In Service Software Upgrade（ISSU; インサービス ソフトウェア アップグレード）ロールバック タイマーの値を設定します。

l2protocol-tunnel

インターフェイスでプロトコル トンネリングをイネーブルにするには、**l2protocol-tunnel** コマンドを使用します。Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、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。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には、このコマンドの **no** 形式を使用します。

l2protocol-tunnel [**cdp** | **stp** | **vtp**]

no l2protocol-tunnel [**cdp** | **stp** | **vtp**]

構文の説明

cdp	（任意）CDP のトンネリングをイネーブルにします。
stp	（任意）STP のトンネリングをイネーブルにします。
vtp	（任意）VTP のトンネリングをイネーブルにします。

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。

コマンド 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	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

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）。

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

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

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する方法を示します。

```
Switch(config-if)# l2protocol-tunnel cdp
Switch(config-if)#
```

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; サービス クラス）値を設定します。
l2protocol-tunnel drop-threshold	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 1 秒あたりのレイヤ 2 プロトコル パケットの最大レートに対してドロップしきい値を設定します。
l2protocol-tunnel shutdown-threshold	プロトコル トンネリングのカプセル化レートを設定します。

l2protocol-tunnel cos

すべてのトンネリング レイヤ 2 プロトコル パケットの Class of Service（CoS; サービス クラス）値を設定するには、**l2protocol-tunnel cos** コマンドを使用します。デフォルト値の 0 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。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 モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが、Catalyst 4500 シリーズ スイッチに初めて追加されました。

使用上のガイドライン

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

NVRAM（不揮発性 RAM）に値が保存されます。

例

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

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

関連コマンド

コマンド	説明
l2protocol-tunnel	インターフェイスでプロトコル トンネリングをイネーブルにします。
l2protocol-tunnel drop-threshold	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 1 秒あたりのレイヤ 2 プロトコル パケットの最大レートに対してドロップしきい値を設定します。
l2protocol-tunnel shutdown-threshold	プロトコル トンネリングのカプセル化レートを設定します。

l2protocol-tunnel drop-threshold

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 1 秒あたりのレイヤ 2 プロトコル パケットの最大レートに対してドロップしきい値を設定するには、**l2protocol-tunnel drop-threshold** コマンドを使用します。Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、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）のパケットに対してドロップしきい値を設定できます。インターフェイスでドロップしきい値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。

l2protocol-tunnel drop-threshold [**cdp** | **stp** | **vtp**] *value*

no l2protocol-tunnel drop-threshold [**cdp** | **stp** | **vtp**] *value*

構文の説明

cdp	（任意）CDP のドロップしきい値を指定します。
stp	（任意）STP のドロップしきい値を指定します。
vtp	（任意）VTP のドロップしきい値を指定します。
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のために受信される 1 秒あたりのパケットのしきい値を指定します。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 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 モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

l2protocol-tunnel drop-threshold コマンドでは、インターフェイスがパケットをドロップするまでにそのインターフェイスで受信される 1 秒あたりのプロトコル パケットの数を制御します。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。

例

次の例では、ドロップしきい値のレートを設定する方法を示します。

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

関連コマンド

コマンド	説明
l2protocol-tunnel	インターフェイスでプロトコル トンネリングをイネーブルにします。
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; サービス クラス）値を設定します。
l2protocol-tunnel shutdown-threshold	プロトコル トンネリングのカプセル化レートを設定します。

l2protocol-tunnel shutdown-threshold

プロトコル トンネリングのカプセル化レートを設定するには、**l2protocol-tunnel shutdown-threshold** コマンドを使用します。Cisco Discovery Protocol（CDP; シスコ検出プロトコル）、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）のパケットに対してカプセル化レートを設定できます。インターフェイスでカプセル化レート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。

l2protocol-tunnel shutdown-threshold [**cdp | stp | vtp**] *value*

no l2protocol-tunnel shutdown-threshold [**cdp | stp | vtp**] *value*

構文の説明

cdp	（任意）CDP のシャットダウンしきい値を指定します。
stp	（任意）STP のシャットダウンしきい値を指定します。
vtp	（任意）VTP のシャットダウンしきい値を指定します。
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のために受信される 1 秒あたりのパケット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 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。

コマンド 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	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

l2-protocol-tunnel shutdown-threshold コマンドでは、インターフェイスがシャットダウンするまでにそのインターフェイスで受信される 1 秒あたりのプロトコル パケットの数を制御します。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** 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** でエラー回復機能生成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** 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。

例

次の例では、最大レートを設定する方法を示します。

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

関連コマンド

コマンド	説明
l2protocol-tunnel	インターフェイスでプロトコル トンネリングをイネーブルにします。
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; サービス クラス）値を設定します。
l2protocol-tunnel drop-threshold	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 1 秒あたりのレイヤ 2 プロトコル パケットの最大レートに対してドロップしきい値を設定します。

lacp port-priority

物理インターフェイスの LACP プライオリティを設定するには、**lacp port-priority** コマンドを使用します。

lacp port-priority *priority*

構文の説明

priority	物理インターフェイスのプライオリティです。有効値の範囲は 1 ～ 65535 です。

デフォルト

プライオリティは 32768 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 モード

コマンド履歴

リリース	変更内容
12.1(13)EW	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine I が搭載されているシステムではサポートされません。

スイッチの各ポートにポート プライオリティを割り当てるには、自動指定するか、または **lacp port-priority** コマンドを入力して指定する必要があります。ポート プライオリティとポート番号を組み合わせて、ポート ID が形成されます。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集約できない場合は、ポート 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。

このコマンドはグローバル コンフィギュレーション コマンドですが、*priority* 値は LACP をイネーブルにした物理インターフェイスを持つポート チャネルでのみサポートされます。このコマンドは LACP をイネーブルにしたインターフェイスでサポートされます。

プライオリティを設定する際、値が大きいほど、プライオリティは低くなります。

例

次の例では、インターフェイスのプライオリティを設定する方法を示します。

```
Switch(config-if)# lacp port-priority 23748
Switch(config-if)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel グループに EtherChannel インターフェイスを割り当てて設定します。
channel-protocol	インターフェイスで LACP または PAgP をイネーブルにします。
lacp system-priority	LACP についてシステムのプライオリティを設定します。
show lacp	LACP 情報を表示します。

lacp system-priority

LACP のシステムのプライオリティを設定するには、**lacp system-priority** コマンドを使用します。

lacp system-priority *priority*

構文の説明

priority	システムのプライオリティです。有効値の範囲は 1 ～ 65535 です。

デフォルト

プライオリティは 32768 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 モード

コマンド履歴

リリース	変更内容
12.1(13)EW	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine I を搭載しているシステムではサポートされません。

LACP が稼動する各スイッチにシステム プライオリティを割り当てるには、自動指定するか、または **lacp system-priority** コマンドを入力して指定する必要があります。システム プライオリティとスイッチの MAC アドレスを組み合わせて、システム ID が形成されます。システム プライオリティは、他のシステムとのネゴシエーションでも使用されます。

このコマンドはグローバル コンフィギュレーション コマンドですが、*priority* 値は LACP をイネーブルにした物理インターフェイスを持つポート チャネルでサポートされます。

プライオリティを設定する際、値が大きいほど、プライオリティは低くなります。

lacp system-priority コマンドは、インターフェイス コンフィギュレーション モードで入力することもできます。このコマンドの入力後、システムはデフォルトでグローバル コンフィギュレーション モードになります。

例

次の例では、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 23748
Switch(config)#
```

関連コマンド

コマンド	説明
channel-group	EtherChannel グループに EtherChannel インターフェイスを割り当てて設定します。
channel-protocol	インターフェイスで LACP または PAgP をイネーブルにします。
lacp system-priority	LACP についてシステムのプライオリティを設定します。
show lacp	LACP 情報を表示します。

logging event link-status global（グローバル コンフィギュレーション）

デフォルトの、スイッチ全体でのグローバルなリンクステータス イベント メッセージング設定を変更するには、**logging event link-status global** コマンドを使用します。リンクステータス イベント メッセージ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。

logging event link-status global

no logging event link-status global

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

グローバルなリンクステータス メッセージ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 モード

コマンド履歴

リリース	変更内容
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

リンクステータス ロギング イベントがインターフェイス レベルで設定されていない場合は、このグローバルなリンクステータス設定が各インターフェイスに適用されます。

例

次の例では、各インターフェイスのリンクステータス メッセージをグローバルにイネーブルにする方法を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# logging event link-status global
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
logging event link-status（インターフェイス コンフィギュレーション）	インターフェイスでリンクステータス イベント メッセージングをイネーブルにします。

logging event link-status（インターフェイス コンフィギュレーション）

インターフェイスでリンクステータス イベント メッセージングをイネーブルにするには、**logging event link-status** コマンドを使用します。リンクステータス イベント メッセージ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。グローバルなリンクステータス設定を適用するには、**logging event link-status use-global** コマンドを使用します。

logging event link-status

no logging event link-status

logging event link-status use-global

デフォルト

グローバルなリンクステータス メッセージ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 モード

コマンド履歴

リリース	変更内容
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

特定のインターフェイスに対し、インターフェイス ステート変更イベントのシステム ロギングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **logging event link-status** コマンドを入力します。

システム内の全インターフェイスに対し、インターフェイス ステート変更イベントのシステム ロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging event link-status global** コマンドを入力します。ステート変更イベントを設定していないすべてのインターフェイスには、グローバル設定が適用されます。

例

次の例では、インターフェイス gi11/1 に対してステート変更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 terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event link-status
Switch(config-if)# end
Switch#
```

次の例では、グローバル設定を無視し、リンクステータス イベントのロギングを無効に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 gi11/1
Switch(config-if)# no logging event link-status
Switch(config-if)# end
```

```
Switch#
```

次の例では、インターフェイス gi11/1 に対してグローバルなリンクステータス イベント設定をイネーブルに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 gi11/1
Switch(config-if)# logging event link-status use-global
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
logging event link-status global（グローバル コンフィギュレーション）	デフォルトの、スイッチ全体でのグローバルなリンクステータス イベント メッセージング設定を変更します。

logging event trunk-status global（グローバル コンフィギュレーション）

トランクステータス イベント メッセージングをグローバルにイネーブルにするには、**logging event trunk-status global** コマンドを使用します。トランクステータス イベント メッセージ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。

logging event trunk-status global

no logging event trunk-status global

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

グローバルなトランクステータス メッセージ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 モード

コマンド履歴

リリース	変更内容
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

トランクステータス ロギング イベントがインターフェイス レベルで設定されていない場合は、グローバルなトランクステータス設定が各インターフェイスに適用されます。

例

次の例では、各インターフェイスのリンクステータス メッセージ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 terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# logging event trunk-status global
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
logging event trunk-status global（グローバル コンフィギュレーション）	インターフェイスでトランクステータス イベント メッセージングをイネーブルにします。

logging event trunk-status（インターフェイス コンフィギュレーション）

インターフェイスでトランクステータス イベント メッセージングをイネーブルにするには、**logging event trunk-status** コマンドを使用します。トランクステータス イベント メッセージ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。グローバルなトランクステータス設定を適用するには、**logging event trunk-status use-global** コマンドを使用します。

logging event trunk-status

no logging event trunk-status

logging event trunk-status use-global

デフォルト

グローバルなトランクステータス メッセージ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 モード

コマンド履歴

リリース	変更内容
12.2(25)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

特定のインターフェイスに対し、インターフェイス ステート変更イベントのシステム ロギングをイネーブルにするには、インターフェイス コンフィギュレーション モードで **logging event trunk-status** コマンドを入力します。

システム内の全インターフェイスに対し、インターフェイス ステート変更イベントのシステム ロギングをイネーブルにするには、グローバル コンフィギュレーション モードで **logging event trunk-status use-global** コマンドを入力します。ステート変更イベントを設定していないすべてのインターフェイスには、グローバル設定が適用されます。

例

次の例では、インターフェイス gi11/1 に対してステート変更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 terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# interface gi11/1
Switch(config-if)# logging event trunk-status
Switch(config-if)# end
Switch#
```

次の例では、グローバル設定を無視し、トランクステータス イベントのロギングを無効に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 gi11/1
Switch(config-if)# no logging event trunk-status
Switch(config-if)# end
```

```
Switch#
```

次の例では、インターフェイス gi11/1 に対してグローバルなトランクステータス イベント設定をイネーブルに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 gi11/1
Switch(config-if)# logging event trunk-status use-global
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
logging event trunk-status global（グローバル コンフィギュレーション）	インターフェイスでトランクステータス イベント メッセージングをイネーブルにします。

mab

ポートで MAC Authorization Bypass（MAB; MAC 認証バイパス）をイネーブルにして設定するには、インターフェイス コンフィギュレーション モードで **mab** コマンドを使用します。MAB 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。

mab [**eap**]

no mab [**eap**]

（注）　**mab** コマンドは、**dot1x system-auth control** コマンドの結果とは完全に無関係です。

構文の説明

eap	（任意）標準の RADIUS Access-Request、Access-Accept カンバセーションではなく、完全な EAP カンバセーションを使用するように指定します。

コマンド デフォルト

ディセーブル

コマンド 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	変更内容
12.2(50)SG	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として MAB を使用するようにポートが設定されている場合、ホストの ID を要求するときの失敗回数が設定数に達するまで、そのポートは通常の dot1X 方式で動作します。オーセンティケータは、ホストの MAC アドレスを学習し、その情報を使用して認証サーバにクエリーを送信することで、この MAC アドレスにアクセスが許可されるかどうかを確認します。

例

次の例では、ポートで MAB をイネーブルにする方法を示します。

```
Switch(config-if)# mab
Switch(config-if)#
```

次の例では、ポートで MAB をイネーブルにして設定する方法を示します。

```
Switch(config-if)# mab eap
Switch(config-if)#
```

次の例では、ポートで MAB をディセーブルにする方法を示します。

```
Switch(config-if)# no mab
Switch(config-if)#
```

関連コマンド

コマンド	説明
show authentication	認証マネージャ情報を表示します。
show mab	MAB 情報を表示します。
show running-config	実行コンフィギュレーション情報を表示します。

mac access-list extended

拡張 MAC アクセス リストを定義するには、**mac access-list extended** コマンドを使用します。MAC 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。

mac access-list extended *name*

no mac access-list extended *name*

構文の説明

name	エントリが属する ACL です。

デフォルト

MAC 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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ACL 名を入力するときには、次の命名規則に従ってください。

- 最大 31 文字で、a ～ z、A ～ Z、0 ～ 9、ダッシュ文字（-）、アンダースコア文字（_）、およびピリオド文字（.）を含むことができます。
- 英文字で始まり、すべてのタイプのすべての ACL で一意である必要があります。
- 大文字と小文字が区別されます。
- 数字は使用できません。
- キーワードは使用できません。避けるべきキーワードは、all、default-action、map、help、および editbuffer です。

mac access-list extended *name* コマンドを入力する場合、[**no**] {**permit** | **deny**} {{*src-mac mask* | **any**} [*dest-mac mask*]} [**protocol-family** {**appletalk** | **arp-non-ipv4** | **decnet** | **ipx** | **ipv6** | **rarp-ipv4** | **rarp-non-ipv4** | **vines** | **xns**}] サブセットを使用して MAC レイヤ アクセス リストのエントリを作成または削除します。

表 2-7 に、**mac access-list extended** サブコマンドの構文の説明を示します。

表 2-7　mac access-list extended サブコマンド

サブコマンド	説明
deny	条件が一致した場合にアクセスを禁止します。
no	（任意）アクセス リストからステートメントを削除します。
permit	条件が一致した場合にアクセスを許可します。
src-mac mask	*source-mac-address source-mac-address-mask* の形式の送信元 MAC アドレスです。
any	任意のプロトコル タイプを指定します。

表 2-7　mac access-list extended サブコマンド （続き）

サブコマンド	説明
dest-mac mask	（任意）*dest-mac-address dest-mac-address-mask* の形式の宛先 MAC アドレスです。
protocol-family	（任意）プロトコル ファミリの名前です。表 2-8 に、特定のプロトコル ファミリにマッピングされるパケットを示します。

表 2-8 に、プロトコル ファミリへのイーサネット パケットのマッピングを示します。

表 2-8　プロトコル ファミリへのイーサネット パケットのマッピング

プロトコル ファミリ	パケット ヘッダー内の Ethertype
Appletalk	0x809B、0x80F3
Arp-Non-Ipv4	0x0806、Arp のプロトコル ヘッダーは非 IP プロトコル ファミリです。
Decnet	0x6000 ～ 0x6009、0x8038 ～ 0x8042
Ipx	0x8137 ～ 0x8138
Ipv6	0x86DD
Rarp-Ipv4	0x8035、Rarp のプロトコル ヘッダーは Ipv4 です。
Rarp-Non-Ipv4	0x8035、Rarp のプロトコル ヘッダーは非 Ipv4 プロトコル ファミリです。
Vines	0x0BAD、0x0BAE、0x0BAF
Xns	0x0600、0x0807

src-mac mask または *dest-mac mask* 値を入力するときには、次の注意事項に従ってください。

- MAC アドレスは、0030.9629.9f84 などのドット付き 16 進表記で 3 つの 4 バイト値として入力します。
- MAC アドレス マスクは、ドット付き 16 進表記で 3 つの 4 バイト値として入力します。1 ビットをワイルドカードとして使用します。たとえば、アドレスを完全に一致させるには、0000.0000.0000 を使用します（0.0.0 として入力できます）。
- 任意指定の *protocol* パラメータについては、EtherType またはキーワードのいずれかを入力できます。
- *protocol* パラメータなしのエントリはどのプロトコルとも一致します。
- アクセス リスト エントリは入力順にスキャンされます。最初に一致したエントリが使用されます。パフォーマンスを高めるには、アクセス リストの冒頭付近に最も一般に使用されるエントリを置きます。
- リストの最後に明示的な **permit any any** エントリを含めなかった場合、アクセス リストの最後には暗示的な **deny any any** エントリが存在します。
- 新しいすべてのエントリは既存のリストの最後に置かれます。リストの中間にエントリを追加することはできません。

例

次の例では、0000.4700.0001 から 0000.4700.0009 へのトラフィックを拒否し、それ以外のすべてのトラフィックを許可する、mac_layer という名前の MAC レイヤ アクセス リストを作成する方法を示します。

```
Switch(config)# mac access-list extended mac_layer
Switch(config-ext-macl)# deny 0000.4700.0001 0.0.0 0000.4700.0009 0.0.0 protocol-family
appletalk
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch#
```

関連コマンド

コマンド	説明
show vlan access-map	VLAN アクセス マップ情報を表示します。

macro apply cisco-desktop

スイッチ ポートを標準デスクトップへ接続するのに適したシスコ推奨機能および設定値をイネーブルにするには、**macro apply cisco-desktop** コマンドを使用します。

macro apply cisco-desktop $AVID *access_vlanid*

構文の説明

$AVID *access_vlanid*	アクセス VLAN ID を指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、表示および適用のみが可能で、変更はできません。

インターフェイスの既存のコンフィギュレーションが対象のマクロ コンフィギュレーションと競合しないことを確認してください。マクロを適用する前に、**default interface** コマンドを使用してインターフェイスのコンフィギュレーションをクリアしてください。

例

次の例では、ポート fa2/1 でシスコ推奨機能および設定値をイネーブルにする方法を示します。

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-desktop $AVID 50
Switch(config-if)#
```

このマクロの内容は次のとおりです。

```
# Basic interface - Enable data VLAN only
# Recommended value for access vlan (AVID) should not be 1
switchport access vlan $AVID [access_vlanid]
switchport mode access
# Enable port security limiting port to a single
# MAC address -- that of desktop
switchport port-security
# Ensure port-security age is greater than one minute
# and use inactivity timer
# "Port-security maximum 1" is the default and will not
# Show up in the config
switchport port-security violation restrict
switchport port-security aging time 2
switchport port-security aging type inactivity
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable
```

関連コマンド

コマンド	説明
macro apply cisco-phone	スイッチ ポートを標準デスクトップおよび Cisco IP Phone に接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-router	スイッチ ポートをルータに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-switch	スイッチ ポートを別のスイッチに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。

macro apply cisco-phone

スイッチ ポートを標準デスクトップおよび Cisco IP Phone に接続するのに適したシスコ推奨機能および設定値をイネーブルにするには、**macro apply cisco-phone** コマンドを使用します。

macro apply cisco-phone $AVID *access_vlanid* **$VVID** *voice_vlanid*

構文の説明

$AVID *access_vlanid*	アクセス VLAN ID を指定します。
$VVID *voice_vlanid*	音声 VLAN ID を指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、表示および適用のみが可能で、変更はできません。

インターフェイスの既存のコンフィギュレーションが対象のマクロ コンフィギュレーションと競合しないことを確認してください。マクロを適用する前に、**default interface** コマンドを使用してインターフェイスのコンフィギュレーションをクリアしてください。

例

次の例では、ポート fa2/1 でシスコ推奨機能および設定値をイネーブルにする方法を示します。

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-phone $AVID 10 $VVID 50
Switch(config-if)#
```

このマクロの内容は次のとおりです。

```
# VoIP enabled interface - Enable data VLAN
# and voice VLAN (VVID)
# Recommended value for access vlan (AVID) should not be 1\
switchport access vlan $AVID [access_vlan_id]
switchport mode access
# Update the Voice VLAN (VVID) value which should be
# different from data VLAN
# Recommended value for voice vlan (VVID) should not be 1
switchport voice vlan $VVID [voice_vlan_id]
# Enable port security limiting port to a 3 MAC
# addressees -- One for desktop and two for phone
switchport port-security
switchport port-security maximum 3
# Ensure port-security age is greater than one minute
# and use inactivity timer
switchport port-security violation restrict
switchport port-security aging time 2
```

```
switchport port-security aging type inactivity
# Enable auto-qos to extend trust to attached Cisco phone
auto qos voip cisco-phone
# Configure port as an edge network port
spanning-tree portfast
spanning-tree bpduguard enable@
```

関連コマンド

コマンド	説明
macro apply cisco-desktop	スイッチ ポートを標準デスクトップに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-router	スイッチ ポートをルータに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-switch	スイッチ ポートを別のスイッチに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。

macro apply cisco-router

スイッチ ポートをルータに接続するのに適したシスコ推奨機能および設定値をイネーブルにするには、**macro apply cisco-router** コマンドを使用します。

macro apply cisco-router $NVID *native_vlanid*

構文の説明

$NVID *native_vlanid*	ネイティブ VLAN ID を指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、表示および適用のみが可能で、変更はできません。

インターフェイスの既存のコンフィギュレーションが対象のマクロ コンフィギュレーションと競合しないことを確認してください。**macro apply cisco-router** コマンドを適用する前に、**default interface** コマンドを使用してインターフェイスのコンフィギュレーションをクリアしてください。

例

次の例では、ポート fa2/1 でシスコ推奨機能および設定値をイネーブルにする方法を示します。

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-router $NVID 80
Switch(config-if)#
```

このマクロの内容は次のとおりです。

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE [vlan_range]
# Hardcode trunk and disable negotiation to
# speed up convergence
# Hardcode speed and duplex to router
switchport mode trunk
switchport nonegotiate
speed 100
duplex full
# Configure qos to trust this interface
auto qos voip trust
qos trust dscp
# Ensure fast access to the network when enabling the interface.
```

```
# Ensure that switch devices cannot become active on the interface.
spanning-tree portfast
spanning-tree bpduguard enable
```

関連コマンド

コマンド	説明
macro apply cisco-desktop	スイッチ ポートを標準デスクトップに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-phone	スイッチ ポートを標準デスクトップおよび Cisco IP Phone に接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-router	スイッチ ポートをルータに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-switch	スイッチ ポートを別のスイッチに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。

macro apply cisco-switch

スイッチ ポートを別のスイッチに接続するのに適したシスコ推奨機能および設定値をイネーブルにするには、**macro apply cisco-switch** コマンドを使用します。

macro apply cisco-switch $NVID *native_vlanid*

構文の説明

$NVID *native_vlanid*	ネイティブ VLAN ID を指定します。

デフォルト

このコマンドには、デフォルト設定はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、表示および適用のみが可能で、変更はできません。

インターフェイスの既存のコンフィギュレーションが対象のマクロ コンフィギュレーションと競合しないことを確認してください。このマクロを適用する前に、**default interface** コマンドを使用してインターフェイスのコンフィギュレーションをクリアしてください。

例

次の例では、ポート fa2/1 でシスコ推奨機能および設定値をイネーブルにする方法を示します。

```
Switch(config)# interface FastEthernet2/1
Switch(config-if)# macro apply cisco-switch $NVID 45
Switch(config-if)#
```

このマクロの内容は次のとおりです。

```
# Access Uplink to Distribution
switchport trunk encapsulation dot1q
# Define unique Native VLAN on trunk ports
# Recommended value for native vlan (NVID) should not be 1
switchport trunk native vlan $NVID [native_vlan_id]
# Update the allowed VLAN range (VRANGE) such that it
# includes data, voice and native VLANs
# switchport trunk allowed vlan $VRANGE
# Hardcode trunk and disable negotiation to
# speed up convergence
switchport mode trunk
switchport nonegotiate
# Configure qos to trust this interface
auto qos voip trust
# 802.1w defines the link as pt-pt for rapid convergence
spanning-tree link-type point-to-point
```

関連コマンド

コマンド	説明
macro apply cisco-desktop	スイッチ ポートを標準デスクトップに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-phone	スイッチ ポートを標準デスクトップおよび Cisco IP Phone に接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。
macro apply cisco-router	スイッチ ポートをルータに接続するのに適した、シスコ推奨の機能および設定をイネーブルにします。

macro global apply cisco-global

システム定義のデフォルト テンプレートをスイッチに適用するには、スイッチ スタックまたはスタンドアロン スイッチに対して **macro global apply cisco-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 cisco-global

構文の説明

このコマンドには、キーワードまたは変数はありません。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、システム定義のデフォルトをスイッチに適用する方法を示します。

```
Switch(config)# macro global apply cisco-global
Changing VTP domain name from gsg-vtp to [smartports] Device mode already VTP TRANSPARENT.
Switch(config)#
```

macro global apply system-cpp

コントロール プレーン ポリシングのデフォルト テンプレートをスイッチに適用するには、スイッチ スタックまたはスタンドアロン スイッチに対して **macro global apply system-cpp** グローバル コンフィギュレーション コマンドを使用します。

macro global apply system-cpp

構文の説明

このコマンドには、キーワードまたは変数はありません。

デフォルト

このコマンドにはデフォルト設定はありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、システム定義のデフォルトをスイッチに適用する方法を示します。

```
Switch (config)# macro global apply system-cpp
Switch (config)#
```

関連コマンド

コマンド	説明
macro global apply cisco-global	システム定義のデフォルト テンプレートをスイッチに適用します。
macro global description	スイッチに適用されたマクロについての説明を入力します。

macro global description

スイッチに適用されたマクロについての説明を入力するには、スイッチ スタックまたはスタンドアロン スイッチに対して **macro global description** グローバル コンフィギュレーション コマンドを使用します。説明を削除するには、このコマンドの no 形式を使用します。

macro global description *text*

no macro global description *text*

構文の説明

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 モード

コマンド履歴

リリース	変更内容
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

コメント テキストまたはマクロ名をスイッチに関連付けるには、*text* 引数を使用します。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。

例

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 global apply cisco-global	システム定義のデフォルト テンプレートをスイッチに適用します。

main-cpu

メイン CPU サブモードを開始し、2 つのスーパーバイザ エンジン上のコンフィギュレーションを手動で同期化するには、**main-cpu** コマンドを使用します。

main-cpu

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

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

冗長モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。（Catalyst 4507R のみ）

使用上のガイドライン

メイン CPU サブモードは、2 つのスーパーバイザ エンジン上のコンフィギュレーションを手動で同期化するために使用します。メイン CPU サブモードで、**auto-sync** コマンドを使用して、NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにします。

（注）　メイン CPU サブモードを開始したあとで、**auto-sync** コマンドを使用して、プライマリ コンフィギュレーションに基づいてプライマリおよびセカンダリのルート プロセッサのコンフィギュレーションを自動的に同期化できます。さらに、メイン CPU に適用可能な冗長コマンドのすべてを使用できます。

例

次の例では、auto-sync standard コマンドを使用してデフォルトの自動同期化機能をイネーブルに戻して、アクティブ スーパーバイザ エンジンの startup-config および config-register コンフィギュレーションをスタンバイ スーパーバイザ エンジンと同期化する方法を示します。ブート変数の更新は自動的に行われ、ディセーブルにはできません。

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)# auto-sync standard
Switch(config-r-mc)# end
Switch# copy running-config startup-config
Switch#
```

関連コマンド

コマンド	説明
auto-sync	NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにします。

match

VLAN アクセス マップ シーケンスの 1 つまたは複数の ACL を選択することにより、match 句を指定するには、**match** サブコマンドを使用します。match 句を削除するには、このコマンドの **no** 形式を使用します。

match {**ip address** {*acl-number* | *acl-name*}} | {**mac address** *acl-name*}

no match {**ip address** {*acl-number* | *acl-name*}} | {**mac address** *acl-name*}

（注） match 句が指定されていない場合は、VLAN アクセス マップ シーケンスのアクションがすべてのパケットに適用されます。すべてのパケットがアクセス マップのシーケンスと照合されます。

構文の説明

ip address *acl-number*	VLAN アクセス マップ シーケンスの IP ACL を 1 つまたは複数選択します。有効値の範囲は 1 ～ 199 および 1300 ～ 2699 です。
ip address *acl-name*	名前を指定して IP ACL を選択します。
mac address *acl-name*	VLAN アクセス マップ シーケンスの MAC ACL を 1 つまたは複数選択します。

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

VLAN アクセス マップ モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

match 句では、トラフィック フィルタリングの IP または MAC ACL を指定します。

IP パケットの場合、MAC シーケンスは有効ではありません。IP パケットに対しては IP match 句によってアクセス制御が行われます。

コンフィギュレーションに関する注意事項および制限事項の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

match コマンドの詳細については、『*Cisco IOS Command Reference*』を参照してください。

例

次の例では、VLAN アクセス マップの match 句を定義する方法を示します。

```
Switch(config)# vlan access-map ganymede 10
Switch(config-access-map)# match ip address 13
Switch(config-access-map)#
```

関連コマンド

コマンド	説明
show vlan access-map	VLAN アクセス マップの内容を表示します。
vlan access-map	VLAN アクセス マップを作成するための VLAN アクセス マップ コマンド モードを開始します。

match（クラスマップ コンフィギュレーション）

クラス マップの一致基準を定義するには、**match** クラスマップ コンフィギュレーション コマンドを使用します。一致基準を削除するには、このコマンドの **no** 形式を使用します。

Supervisor Engine 6-E 以外

match {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list*

no match {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list*

Supervisor Engine 6-E および Catalyst 4900M シャーシ

match {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

no match {**access-group** *acl-index-or-name* | **cos** *cos-list* | [**lp**] **dscp** *dscp-list* | [**lp**] **precedence** *ip-precedence-list* | **qos-group** *value* | **protocol** [**ip** | **ipv6** | **arp**]

構文の説明

access-group *acl-index-or-name*	IP 標準または拡張アクセス コントロール リスト（ACL）または MAC（メディア アクセス制御）ACL の番号または名前です。IP 標準 ACL の場合、ACL インデックス範囲は 1 ～ 99 および 1300 ～ 1999 です。IP 拡張 ACL の場合、ACL インデックス範囲は 100 ～ 199 および 2000 ～ 2699 です。
cos *cos-list*	パケットの照合に使用するレイヤ 2 Class of Service（CoS; サービス クラス）値を最大 4 つまで列挙します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。
[**lp**] **dscp** *dscp-list*	（任意）IP キーワードです。IPv4 パケットのみを照合するように指定します。使用しない場合、IPv4 と IPv6 パケットの両方が照合されます。 パケットの照合に使用する IP Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を最大 8 つまで列挙します。各値はスペースで区切ります。指定できる範囲は 0 ～ 63 です。よく使用する値の場合は、ニーモニック名を入力することもできます。
[**lp**] **precedence** *ip-precedence-list*	（任意）IP キーワードです。IPv4 パケットのみを照合するように指定します。使用しない場合、IPv4 と IPv6 パケットの両方が照合されます。 パケットの照合に使用する IP precedence 値を最大 8 つまで列挙します。各値はスペースで区切ります。指定できる範囲は 0 ～ 7 です。よく使用する値の場合は、ニーモニック名を入力することもできます。
qos-group *value*	入力 QoS 分類のパケットに割り当てられた内部生成 QoS グループ値を指定します。
protocol ip	イーサネット ヘッダー内の IP を指定します。この一致基準は、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。コマンドライン ヘルプ ストリングで表示されますが、サポートされているプロトコル タイプは IP、IPv6、および ARP のみです。

protocol ipv6	イーサネット ヘッダー内の IPv6 を指定します。この一致基準は、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。コマンドライン ヘルプ ストリングで表示されますが、サポートされているプロトコル タイプは IP、IPv6、および ARP のみです。
protocol arp	イーサネット ヘッダー内の ARP を指定します。この一致基準は、Supervisor Engine 6-E および Catalyst 4900M シャーシでサポートされています。コマンドライン ヘルプ ストリングで表示されますが、サポートされているプロトコル タイプは IP、IPv6、および ARP のみです。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E および Catalyst 4900M シャーシのサポートが追加されました。
12.2(46)SG	Supervisor Engine 6-E および Catalyst 4900M シャーシでの **match protocol arp** コマンドのサポートが追加されました。

使用上のガイドライン

match コマンドを入力する前に、まず **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名を指定します。パケットを分類するためにパケットのどのフィールドを調べるのかを指定する場合は、**match** コマンドを使用します。指定した基準にパケットが一致する場合、そのパケットはクラスのメンバと見なされ、トラフィック ポリシーに設定された Quality of Service（QoS）の仕様に従って転送されます。

match ip dscp *dscp-list* コマンドまたは **match ip precedence** *ip-precedence-list* コマンドの場合は、よく使用される値のニーモニック名を入力できます。たとえば、**match ip dscp af11** コマンドを入力できます。このコマンドは、**match ip dscp 10** コマンドを入力した場合と同じ結果になります。また、**match ip precedence critical** コマンドを入力できます。このコマンドは、**match ip precedence 5** コマンドを入力した場合と同じ結果になります。サポートされているニーモニック名のリストについては、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドライン ヘルプ ストリングを参照してください。

IPv6 パケットのみを照合するには、**match protocol ipv6** コマンドを使用する必要があります。IPv4 パケットのみを照合するには、**ip** プレフィクスまたはプロトコル **ip** キーワードのいずれかを使用できます。

ARP パケットのみを照合するには、**match protocol arp** コマンドを使用する必要があります。

match cos *cos-list*、**match ip dscp** *dscp-list*、**match ip precedence** *ip-precedence-list* コマンドをポリシー マップ内のクラス マップに設定できます。

match cos *cos-list* コマンドは、VLAN タグを伝送するイーサネット フレームにのみ適用されます。

match qos-group コマンドは、パケットに割り当てられた特定の QoS グループ値を識別するためにクラスマップによって使用されます。QoS グループ値は、スイッチ ローカルのもので、入力 QoS 分類でパケットと関連しています。

どの一致基準とも一致しないパケットは、デフォルトのトラフィック クラスのメンバーとして分類されます。これを設定するには、**class-default** を **class** ポリシーマップ コンフィギュレーション コマンドのクラス名として指定します。詳細については、「class」（P.2-57）を参照してください。

例

次の例では、クラス マップ class2 を作成する方法を示します。このマップは、DSCP 値 10、11、および 12 を持つすべての着信トラフィックに一致します。

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip dscp 10 11 12
Switch(config-cmap)# exit
Switch#
```

次の例では、クラス マップ class3 を作成する方法を示します。このマップは、IPv4 および IPv6 トラフィックの両方について、IP precedence 値 5、6、および 7 を持つすべての着信トラフィックに一致します。

```
Switch# configure terminal
Switch(config)# class-map class3
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# exit
Switch#
```

次の例では、IP precedence 一致基準を削除し、acl1 を使用してトラフィックを分類する方法を示します。

```
Switch# configure terminal
Switch(config)# class-map class2
Switch(config-cmap)# match ip precedence 5 6 7
Switch(config-cmap)# no match ip precedence
Switch(config-cmap)# match access-group acl1
Switch(config-cmap)# exit
Switch#
```

次の例では、Supervisor Engine 6-E の IPv6 トラフィックのみに適用されるクラスマップを指定する方法を示します。

```
Switch# configure terminal
Switch(config)# class-map match all ipv6 only
Switch(config-cmap)# match dscp af21
Switch(config-cmap)# match protocol ipv6
Switch(config-cmap)# exit
Switch#
```

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の照合に使用するクラスマップを作成し、クラスマップ コンフィギュレーション モードを開始します。
show class-map	クラス マップ情報を表示します。

match flow ip

一意の送信元アドレスまたは宛先アドレスを持つフローを新しいフローとして扱うように一致基準を指定するには、**match flow ip** 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。

match flow ip {**source-address** [**ip destination-address ip protocol L4 source-address L4 destination-address**] | **destination-address**}

no match flow ip {**source-address** [**ip destination-address ip protocol L4 source-address L4 destination-address**] | **destination-address**}

構文の説明

source-address	一意の IP 送信元アドレスを持つフローから新しいフローを生成します。
ip destination-address ip protocol L4 source-address L4 destination-address	（任意）完全なフロー キーワードで構成されます。一意の IP 送信元および宛先アドレス、プロトコル、レイヤ 4 の送信元および宛先アドレスを持つ各フローを新しいフローとして扱います。
destination-address	一意の IP 宛先アドレスを持つフローから新しいフローを生成します。

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

クラスマップ コンフィギュレーション サブモード

コマンド履歴

リリース	変更内容
12.2(25)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)SG	完全なフロー オプションのサポートが追加されました。

使用上のガイドライン

source-address キーワードを指定すると、一意の送信元アドレスを持つ各フローは新しいフローとして扱われます。

destination-address キーワードを指定すると、一意の宛先アドレスを持つ各フローは新しいフローとして扱われます。

クラス マップで使用されるフロー キーワードを設定する場合、ポリシー マップは *フローベース*のポリシー マップと呼ばれます。フローベースのポリシー マップを子として集約ポリシー マップに対応付けるには、**service-policy** コマンドを使用します。

（注）　**match flow** コマンドを Catalyst 4500 シリーズ スイッチで使用できるのは、Supervisor Engine VI（WS-X4516-10GE）が存在する場合のみです。

例

次の例では、送信元アドレスに関連付けたフローベースのクラス マップを作成する方法を示します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# end
Switch#
Switch# show class-map c1
Class Map match-all c1 (id 2)
  Match flow  ip source-address
Switch#
```

次の例では、宛先アドレスに関連付けたフローベースのクラス マップを作成する方法を示します。

```
Switch(config)# class-map match-all c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# end
Switch#

Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow  ip destination-address
Switch#
```

ファスト イーサネット インターフェイス 6/1 上で、送信元アドレス 192.168.10.20 および 192.168.10.21 を持つアクティブなフローが 2 つ存在すると仮定します。次の例では、それぞれのフローを 1 Mbps に維持し、9000 バイトのバースト値を許可する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
FastEthernet6/1

 Service-policy input: p1

   Class-map: c1 (match-all)
     15432182 packets
     Match: flow  ip source-address
     police: Per-interface
       Conform: 64995654 bytes Exceed: 2376965424 bytes

   Class-map: class-default (match-any)
     0 packets
     Match: any
       0 packets
Switch#
```

今度は、ファスト イーサネット インターフェイス 6/1 上で、宛先アドレス 192.168.20.20 および 192.168.20.21 を持つアクティブなフローが 2 つ存在する例を示します。次の例では、それぞれのフローを 1 Mbps に維持し、9000 バイトのバースト値を許可する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip destination-address
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface fastethernet6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory

Switch# show policy-map interface
 FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      2965072 packets
      Match: flow  ip destination-address
      police: Per-interface
        Conform: 6105636 bytes Exceed: 476652528 bytes

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
Switch#
```

ファスト イーサネット インターフェイス 6/1 上で、次のようなアクティブなフローが 2 つ存在すると仮定します。

```
SrcIp          DstIp          IpProt SrcL4Port DstL4Port
-------------------------------------------------------
192.168.10.10  192.168.20.20  20     6789       81
192.168.10.10  192.168.20.20  20     6789       21
```

次のコンフィギュレーションでは、各フローは 1000000 bps にポリシングされ、9000 バイトのバースト値が許可されます。

（注） **match flow ip source-address|destination-address** コマンドを使用すると、これらの 2 つのフローは、送信元アドレスと宛先アドレスが同一であるため、1 つのフローとして統合されます。

```
Switch# conf terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# class-map c1
Switch(config-cmap)# match flow ip source-address ip destination-address ip protocol l4
source-port l4 destination-port
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police 1000000 9000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
```

```
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# service-policy input p1
Switch(config-if)# end
Switch# write memory
Switch# show policy-map interface
FastEthernet6/1

class-map c1
   match flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port
!
 policy-map p1
    class c1
       police 1000000 bps 9000 byte conform-action transmit exceed-action drop
!
interface FastEthernet 6/1
  service-policy input p1

Switch# show class-map c1
 Class Map match-all c1 (id 2)
   Match flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port

Switch# show policy-map p1
  Policy Map p1
    Class c1
      police 1000000 bps 9000 byte conform-action transmit exceed-action drop

Switch# show policy-map interface
 FastEthernet6/1

  Service-policy input: p1

    Class-map: c1 (match-all)
      15432182 packets
      Match: flow  ip source-address ip destination-address ip protocol l4 source-port l4
destination-port
      police: Per-interface
        Conform: 64995654 bytes Exceed: 2376965424 bytes


    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
Switch#
```

関連コマンド

コマンド	説明
service-policy（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ポリシー マップを適用します。
show class-map	クラス マップ情報を表示します。
show policy-map	ポリシー マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

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** 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 モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(46)SG	サポート対象およびサポート対象外のラインカード情報が使用上のガイドラインに追加されました。

使用上のガイドライン

銅メディア ポートで CLI を通じて Auto MDIX をサポートするラインカードは、WS-X4124-RJ45、WS-X4148-RJ45（ハードウェア リビジョン 3.0 以上）、WS-X4232-GB-RJ45（ハードウェア リビジョン 3.0 以上）、WS-X4920-GE-RJ45、および WS-4648-RJ45V+E です（ポートでインライン パワーがディセーブルになっている場合の Auto MDIX サポート）。

ポートの自動ネゴシエーションがイネーブルになっているときに Auto MDIX をデフォルトでサポートし、**mdix** CLI コマンドを使用してもオフにできないラインカードは、WS-X4448-GB-RJ45、WS-X4548-GB-RJ45、WS-X4424-GB-RJ45、および WS-X4412-2GB-T です。

デフォルトでも、CLI コマンドを使用しても、Auto MDIX 機能をサポートできないラインカードは、WS-X4548-GB-RJ45V、WS-X4524-GB-RJ45V、WS-X4506-GB-T、WS-X4148-RJ、WS-X4248-RJ21V、WS-X4248-RJ45V、WS-X4224-RJ45V、および WS-X4232-GB-RJ です。

インターフェイスの Auto MDIX をイネーブルにする場合は、機能が正常に動作するように、インターフェイス速度も自動ネゴシエーションされるように設定する必要があります。

Auto MDIX が（速度の自動ネゴシエーションとともに）接続するインターフェイスの一方または両方でイネーブルの場合は、ケーブル タイプ（ストレートまたはクロス）が不正でもリンクがアップします。

例

次の例では、ポートで Auto MDIX をイネーブルにする方法を示します。

```
Switch# configure terminal
Switch(config)# interface FastEthernet6/3
Switch(config-if)# speed auto
Switch(config-if)# mdix auto
Switch(config-if)# end
```

関連コマンド

コマンド	説明
speed	インターフェイス速度を設定します。
show interfaces	特定のインターフェイスのトラフィックを表示します。
show interfaces capabilities	スイッチ上の 1 つのインターフェイスまたはすべてのインターフェイスのインターフェイス機能を表示します。
show interfaces status	インターフェイスのステータスを表示します。

media-type

デュアルモード対応のポート用のコネクタを選択するには、**media-type** コマンドを使用します。

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

構文の説明

rj45	RJ-45 コネクタを使用します。
sfp	SFP コネクタを使用します。

デフォルト

sfp

コマンド 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	変更内容
12.2(20)EWA	このコマンドが、WS-X4306-GB-T モジュールおよび WS-X4948 シャーシに追加されました。

使用上のガイドライン

このコマンドは、WS-X4306-GB-T モジュール上の全ポートおよび WS-X4948 シャーシ上のポート 1/45 ～ 48 でサポートされています。

show interface capabilities コマンドを入力すると、Multiple Media Types フィールドが表示されます。このフィールドには、ポートがデュアルモード対応でない場合は **no** の値が表示され、ポートがデュアルモード対応の場合はメディア タイプ（**sfp** および **rj45**）が表示されます。

例

次の例では、WS-X4948 シャーシ上のポート 5/45 が RJ-45 コネクタを使用するように設定する方法を示します。

```
Switch(config)# interface gigabitethernet 5/45
Switch(config-if)# media-type rj45
```

mode

冗長モードを設定するには、**mode** コマンドを使用します。

mode {**rpr** | **sso**}

構文の説明

rpr	RPR モードを指定します。
sso	SSO モードを指定します。

デフォルト

Supervisor Engine II+、Supervisor Engine IV、および Supervisor Engine V が搭載された Catalyst 4500 シリーズ スイッチのデフォルト設定は次のとおりです。

- スーパーバイザ エンジンが Cisco IOS Release 12.2(20)EWA を使用している場合は、SSO です。
- スーパーバイザ エンジンが Cisco IOS Release 12.1(12c)EW ～ 12.2(18)EW、および 12.1(*xx*)E を使用している場合は、RPR です。

（注） 現在のスーパーバイザ エンジンを Cisco IOS Release 12.2(18)EW またはそれ以前のリリースから 12.2(20)EWA にアップグレードし、RPR モードがスタートアップ コンフィギュレーションに保存されている場合、両方のスーパーバイザ エンジンはソフトウェアのアップグレード後も継続して RPR モードで動作します。SSO モードを使用するには、手動で冗長モードを SSO に変更する必要があります。

コマンド モード

冗長コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(20)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

RPR モードおよび SSO モードは、Supervisor Engine 2 を搭載した Catalyst 4500 シリーズ スイッチではサポートされません。

mode コマンドは、冗長コンフィギュレーション モードでのみ入力できます。

システムを RPR モードまたは SSO モードに設定する場合は、次の注意事項に従ってください。

- RPR モードおよび SSO モードをサポートするには、使用する Cisco IOS イメージおよびスーパーバイザ エンジンが同じである必要があります。Cisco IOS リリースとスーパーバイザ エンジンの機能が異なる場合、冗長性が作用しない可能性があります。
- スイッチオーバー時にオンライン状態でないモジュールはいずれもリセットされ、スイッチオーバー時にリロードされます。
- ステートフル スイッチオーバーまでの 60 秒間に、モジュールの OIR を実行すると、モジュールはステートフル スイッチオーバー中にリセットされ、ポート ステートが再開されます。
- スイッチオーバーが発生すると、FIB テーブルはクリアされます。ルーテッド トラフィックは、ルート テーブルが再コンバージェンスするまで中断されます。

冗長スーパーバイザ エンジンはモードが変更されると必ずリロードを行い、現在のモードで動作を開始します。

例

次の例では、冗長モードを SSO に設定する方法を示します。

```
Switch(config)# redundancy
Switch(config-red)# mode sso
Switch(config-red)#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。
redundancy force-switchover	アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンに強制的に切り替えます。
show redundancy	冗長ファシリティ情報を表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。

monitor session

インターフェイスまたは VLAN で SPAN セッションをイネーブルにするには、**monitor session** コマンドを使用します。SPAN セッションから 1 つまたは複数の送信元または宛先インターフェイスを削除したり、SPAN セッションから送信元 VLAN 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。

monitor session *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** {**interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** {**input** {**error** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**}} | **output** {**error** {**rx**} | **forward** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**} | **adj-same-if** {**rx**} | **all** {**rx**} | **bridged** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **control-packet** {**rx**} | **mtu-exceeded** {**rx**} | **routed** {**forward** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **received** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4**{**rx**} | **rx**} | **rx**] | **rpf-failure** {**rx**} | **unknown-sa** {**rx**}]}]} [**,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [**,** | **-**]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

no monitor session *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** {**interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** {**input** {**error** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**}} | **output** {**error** {**rx**} | **forward** {**rx**} | **log** {**rx**} | **punt** {**rx**} | **rx**} | **adj-same-if** {**rx**} | **all** {**rx**} | **bridged** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **control-packet** {**rx**} | **mtu-exceeded** {**rx**} | **routed** {**forward** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4** {**rx**} | **rx**} | **received** {**1** {**rx**} | **2** {**rx**} | **3** {**rx**} | **4**{**rx**} | **rx**} | **rx**] | **rpf-failure** {**rx**} | **unknown-sa** {**rx**}]}]} [**,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [**,** | **-**]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

Supervisor Engine 6-E および Catalyst 4900M シャーシ

monitor session *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** { **interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** { **input** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} } | **output** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} | **all** {**rx**} | **control-packet** {**rx**} | **esmp** {**rx**} | **l2-forward** { **adj-same-if** {**rx**} | **bridge-cpu** {**rx**} | **ip-option** {**rx**} | **ipv6-scope-check-fail** {**rx**} | **l2-src-index-check-fail** {**rx**} | **mcast-rpf-fail** {**rx**} | **non-arpa** {**rx**} | **router-cpu** {**rx**} | **ttl-expired** {**rx**} | **ucast-rpf-fail** {**rx**} | **rx**} | **l3-forward** { **forward** {**rx**} | **glean** {**rx**} | **receive** {**rx**} | **rx**} **mtu-exceeded** {**rx**} | **unknown-port-vlan-mapping** {**rx**} | **unknown-sa** {**rx**}]} [**,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [**,** | **-**]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

no monitor session *session* {**destination interface** {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number*} [**encapsulation** {**isl** | **dot1q**}] [**ingress** [**vlan** *vlan_id*] [**learning**]]} | {**remote vlan** *vlan_id*} | {**source** {**cpu**{**both** | **queue** | **rx** | **tx**} |

interface {**FastEthernet** *interface-number* | **GigabitEthernet** *interface-number* | **Port-channel** *interface-number*}} | [**vlan** *vlan_id*] |{**remote vlan** *vlan_id*} | {**cpu** [**queue** *queue_id* | **acl** {**input** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} } | **output** {**copy** {**rx**} | **error** {**rx**} | **forward** {**rx**} | **punt** {**rx**} | **rx**} | **all** {**rx**} | **control-packet** {**rx**} | **esmp** {**rx**} | **l2-forward** { **adj-same-if** {rx} | **bridge-cpu** {**rx**} | **ip-option** {**rx**} | **ipv6-scope-check-fail** {**rx**} | **l2-src-index-check-fail** {**rx**} | **mcast-rpf-fail** {**rx**} | **non-arpa** {**rx**} | **router-cpu** {**rx**} | **ttl-expired** {**rx**} | **ucast-rpf-fail** {**rx**} | **rx**} | **l3-forward** {**forward** {**rx**} | **glean** {**rx**} | **receive** {**rx**} | **rx**} **mtu-exceeded** {**rx**} | **unknown-port-vlan-mapping** {**rx**} | **unknown-sa** {**rx**}]} [**,** | **-** | **rx** | **tx** | **both**]} | {**filter** {**ip access-group** [**name** | **id**]}{**vlan** *vlan_id* [**,** | **-**]} | {**packet-type** {**good** | **bad**}} | {**address-type** {**unicast** | **multicast** | **broadcast**} [**rx** | **tx** | **both**]}

構文の説明

session	SPAN セッションの番号です。有効値の範囲は 1 ～ 6 です。
destination	SPAN 宛先を指定します。
interface	インターフェイスを指定します。
FastEthernet *interface-number*	ファスト イーサネットのモジュールおよびポート番号を指定します。有効値の範囲は 1 ～ 6 です。
GigabitEthernet *interface-number*	ギガビット イーサネットのモジュールおよびポート番号を指定します。有効値の範囲は 1 ～ 6 です。
encapsulation	（任意）宛先ポートのカプセル化タイプを指定します。
isl	（任意）ISL カプセル化を指定します。
dot1q	（任意）dot1q カプセル化を指定します。
ingress	（任意）入力オプションがイネーブルであるかどうかを示します。
vlan *vlan_id*	（任意）VLAN を指定します。有効値の範囲は 1 ～ 4094 です。
learning	（任意）入力をイネーブルにした宛先ポート上でホスト ラーニングをイネーブルにします。
remote vlan *vlan_id*	スイッチの RSPAN 送信元または宛先セッションを指定します。
source	SPAN 送信元を指定します。
Port-channel *interface-number*	ポート チャネル インターフェイスを指定します。有効値の範囲は 1 ～ 64 です。
cpu	CPU で送受信されたトラフィックをセッションの宛先にコピーします。
queue *queue_id*	（任意）特定の CPU サブキューで受信されたトラフィックのみをセッションの宛先にコピーするように指定します。有効値の範囲は 1 ～ 64 です。また、all、control-packet、esmp、mtu-exceeded、unknown-port-vlan-mapping、unknown-sa、acl input、acl input copy、acl input error、acl input forward、acl input punt、acl output、acl output copy、acl output error、acl output forward、acl output punt、l2-forward、adj-same-if、bridge-cpu、ip-option、ipv6-scope-check-fail、l2-src-index-check-fail、mcast-rpf-fail、non-arpa、router-cpu、ttl-expired、ucast-rpf-fail、l3-forward、forward、glean、receive の名前を使用して指定することもできます。
acl	（任意）入力および出力 ACL を指定します。有効値の範囲は 14 ～ 20 です。
input	入力 ACL を指定します。有効値の範囲は 14 ～ 16 です。
error	ACL ソフトウェア エラーを指定します。

log/copy	ACL ロギングのパケットを指定します。
punt	オーバーフローによってパントされるパケットを指定します。
rx	受信トラフィックのモニタリングのみを指定します。
output	出力 ACL を指定します。有効値の範囲は 17 ～ 20 です。
l2-forward	（任意）レイヤ 2 またはレイヤ 3 例外パケットです。
bridge-cpu	CPU にブリッジングされるパケットを指定します。
ip-option	IP オプションを含むパケットを指定します。
ipv6-scope-check-fail	スコープチェック障害の IPv6 パケットを指定します。
l2-src-index-check-fail	SRC MAC および SRC IP アドレスが不一致の IP パケットを指定します。
mcast-rpf-fail	IPv4/IPv6 マルチキャスト RPF 障害を指定します。
non-arpa	非 ARPA カプセル化のパケットを指定します。
router-cpu	ソフトウェアによってルーティングされるパケットを指定します。
ttl-expired	IPv4 ルーテッド パケット超過 TTL を指定します。
adj-same-if	着信インターフェイスにルーティングされたパケットを指定します。
bridged	レイヤ 2 ブリッジド パケットを指定します。
1	最高プライオリティのパケットを指定します。
2	高プライオリティのパケットを指定します。
3	中プライオリティのパケットを指定します。
4	低プライオリティのパケットを指定します。
ucast-rpf-fail	IPv4/IPv6 ユニキャスト RPF 障害を指定します。
all	（任意）すべてのキューです。
l3-forward	（任意）レイヤ 3 パケットです。
forward	特別なレイヤ 3 転送トンネル カプセル化を指定します。
glean	特別なレイヤ 3 転送グリーニングを指定します。
receive	ポートにアドレス指定されたパケットを指定します。
control-packet	（任意）レイヤ 2 制御パケットです。
esmp	（任意）ESMP パケットです。
mtu-exceeded	（任意）出力レイヤ 3 インターフェイス MTU 超過です。
routed	レイヤ 3 ルーテッド パケットを指定します。
received	ポートにアドレス指定されたパケットを指定します。
rpf-failure	マルチキャスト RPF 失敗パケットを指定します。
unknown-port-vlan-mapping	（任意）ポート VLAN マッピングが欠落しているパケットです。
unknown-sa	（任意）送信元 IP アドレスが欠落しているパケットです。
,	（任意）SPAN VLAN の別の範囲を指定する記号です。有効値の範囲は 1 ～ 4094 です。
-	（任意）SPAN VLAN の範囲を指定する記号です。
both	（任意）受信および送信トラフィックをモニタおよびフィルタリングします。
rx	（任意）受信トラフィックのみをモニタおよびフィルタリングします。
tx	（任意）送信トラフィックのみをモニタおよびフィルタリングします。
filter	SPAN 送信元トラフィックを特定の VLAN に限定します。

ip access-group	（任意）IP アクセス グループ フィルタを名前または番号で指定します。
name	（任意）IP アクセス リスト名を指定します。
id	（任意）IP アクセス リスト番号を指定します。（任意）IP アクセス リスト名を指定します。IP アクセス リストの有効値の範囲は 1 ～ 199 です。IP 拡張アクセス リストの有効値の範囲は 1300 ～ 2699 です。
vlan *vlan_id*	（任意）フィルタリングする VLAN を指定します。この番号には、1 つの値または範囲を入力します。有効値の範囲は 1 ～ 4094 です。
packet-type	SPAN 送信元トラフィックを特定のタイプのパケットに限定します。
good	良好なパケット タイプを指定します。
bad	不良なパケット タイプを指定します。
address-type unicast | **multicast** | **broadcast**	SPAN 送信元トラフィックを特定のアドレス タイプのパケットに限定します。有効なタイプは、unicast、multicast、および broadcast です。

デフォルト

トランキング インターフェイスでは、送受信されたトラフィックに加え、すべての VLAN、パケット タイプ、およびアドレス タイプがモニタされます。

パケットは宛先ポートからタグなしで送信されます。入力およびラーニングはディセーブルです。

宛先ポートでは、すべてのパケットが「そのまま」許可および転送されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(11b)EW	単一ユーザ セッション内でのさまざまな方向のサポートおよび拡張 VLAN アドレッシングのサポートが追加されました。
12.1(19)EW	入力パケット、カプセル化の指定、パケット タイプとアドレス タイプのフィルタリング、および CPU 送信元識別強化のサポートが追加されました。
12.1(20)EW	入力をイネーブルにした宛先ポートでのリモート SPAN およびホスト ラーニングのサポートが追加されました。
12.2(20)EW	IP アクセス グループ フィルタのサポートが追加されました。
12.2(40)SG	Supervisor Engine 6-E および Catlyst 4900M シャーシの CPU キュー オプションのサポートが追加されました。

使用上のガイドライン

1 つの SPAN セッションでは、1 つの SPAN 宛先だけがサポートされます。すでに宛先インターフェイスが設定されているセッションに別の宛先インターフェイスを追加しようとすると、エラーとなります。SPAN 宛先を別のインターフェイスに変更する前に、SPAN 宛先インターフェイスを削除してください。

Cisco IOS Release 12.1(12c)EW 以降では、単一ユーザ セッション内で異なる方向からの送信元を設定できます。

（注）　Cisco IOS Release 12.1(12c)EW 以降では、SPAN は入力送信元を含む 2 つのセッションおよび出力送信元を含む 4 つのセッションに制限されます。双方向送信元は、入力および出力の両方の送信元をサポートします。

特定の SPAN セッションでは、VLAN または個々のインターフェイスをモニタできます。特定のインターフェイスと特定の VLAN の両方をモニタする SPAN セッションはありません。SPAN セッションに送信元インターフェイスで設定してから、送信元 VLAN を同じ SPAN セッションに追加しようとすると、エラーとなります。SPAN セッションに送信元 VLAN を設定してから、送信元インターフェイスをそのセッションに追加しようとした場合も、同様にエラー メッセージが表示されます。別のタイプの送信元に切り替える前に、SPAN セッションのあらゆる送信元をクリアしてください。CPU 送信元は、送信元インターフェイスおよび送信元 VLAN と組み合わせることができます。

設定されたカプセル化タイプがタグなし（デフォルト）または 802.1Q の場合は、宛先ポートに **ingress** オプションを設定するときに、入力 VLAN を指定する必要があります。カプセル化タイプが ISL の場合は、入力 VLAN を指定する必要はありません。

デフォルトでは、入力をイネーブルにした場合、宛先ポートではホスト ラーニングが実行されません。**learning** キーワードを入力すると、宛先ポートでホスト ラーニングが実行され、トラフィックが宛先ポートから学習されたホストに転送されます。

モニタ対象のトランキング インターフェイス上で **filter** キーワードを入力した場合、指定した VLAN セット上のトラフィックだけがモニタされます。ポート チャネル インターフェイスを設定している場合、それらのインターフェイスが **interface** オプションのリストに表示されます。VLAN インターフェイスはサポートされていません。ただし、**monitor session** *session* **source vlan** *vlan-id* コマンドを入力することにより、特定の VLAN にまたがることができます。

パケット タイプ フィルタは、受信方向でのみサポートされます。受信と送信タイプのフィルタ、および複数タイプのフィルタを同時に指定できます（たとえば、**good** および **unicast** を使用して、エラーのないユニキャスト フレームのみを識別できます）。VLAN フィルタと同様に、タイプを指定しない場合は、すべてのパケット タイプが識別されます。

queue 識別子を使用すると、指定した CPU キューで送受信されたトラフィックのみを識別できます。キューは番号または名前で指定できます。便宜上、キューの名前には番号付きキューを複数含めることができます。

例

次の例では、SPAN セッションに IP アクセス グループ 100 を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# monitor session 1 filter ip access-group 100
Switch(config)# end
Switch(config)#
```

次の例では、送信元インターフェイスを SPAN セッションに追加する方法を示します。

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3
Switch(config)# end
Switch(config)#
Switch(config)#
Switch(config)#
```

次の例では、SPAN セッション内でさまざまな方向の送信元を設定する方法を示します。

```
Switch# configure terminal
Switch(config)# monitor session 1 source interface fa2/3 rx
Switch(config)# monitor session 1 source interface fa2/2 tx
Switch(config)# end
```

次の例では、送信元インターフェイスを SPAN セッションから削除する方法を示します。

```
Switch# configure terminal
Switch(config)# no monitor session 1 source interface fa2/3
Switch(config)# end
```

次の例では、SPAN トラフィックを VLAN 100 ～ 304 に制限する方法を示します。

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

次の例では、RSPAN VLAN 20 を宛先として設定する方法を示します。

```
Switch# configure terminal
Switch(config)# monitor session 2 destination remote vlan 20
Switch(config)# end
```

次の例では、Supervisor Engine 6-E の SPAN 送信元として CPU のキュー名とキュー番号範囲を使用する方法を示します。

```
Switch# configure terminal
Switch(config)# monitor session 2 source cpu queue control-packet rx
Switch(config)# monitor session 3 source cpu queue 10 rx
Switch(config)# end
```

（注）　Supervisor Engine 6-E の場合、制御パケットがキュー 10 にマッピングされます。

関連コマンド

コマンド	説明
show monitor	SPAN セッションに関する情報を表示します。

mtu

パケットの最大サイズ、つまり Maximum Transmission Unit（MTU; 最大伝送ユニット）を調整して、インターフェイスでジャンボ フレームをイネーブルにするには、**mtu** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mtu *bytes*

no mtu

構文の説明

bytes	バイト サイズです。有効値の範囲は 1500 ～ 9198 です。

デフォルト

デフォルト設定は次のとおりです。

- ジャンボ フレームはディセーブルです。
- すべてのポートで 1500 バイトです。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

ジャンボ フレームは、非ブロッキング ギガビット イーサネット ポート、Switch Virtual Interface（SVI; スイッチ仮想インターフェイス）、および EtherChannel でサポートされます。スタブベース ポートでは、ジャンボ フレームを使用できません。

ベビー ジャイアント機能では、グローバルな **system mtu** *size* コマンドを使用して、グローバルなベビー ジャイアント MTU を設定します。また、この機能により、すべてのスタブベース ポート インターフェイスで、1552 バイトまでのイーサネット ペイロード サイズをサポートできるようになります。

ジャンボ フレームをサポートできるインターフェイスでは、**system mtu** コマンドおよびインターフェイス単位の **mtu** コマンドが両方とも動作しますが、インターフェイス単位の **mtu** コマンドが優先されます。

例

次の例では、1800 バイトの MTU を指定する方法を示します。

```
Switch(config)# interface GigabitEthernet 1/1
Switch(config-if)# mtu 1800
```

関連コマンド

コマンド	説明
system mtu	レイヤ 2 またはレイヤ 3 の最大ペイロード サイズを設定します。

name

MST 領域名を設定するには、**name** コマンドを使用します。デフォルトの名前に戻すには、このコマンドの **no** 形式を使用します。

name *name*

no name *name*

構文の説明

name	MST 領域の名前を指定します。最大 32 文字の任意の文字列です。

デフォルト

MST 領域名は設定されていません。

コマンド モード

MST コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

同じ VLAN マッピングおよびコンフィギュレーション バージョン番号を持つ 2 つ以上の Catalyst 4500 シリーズ スイッチは、領域名が異なっている場合は別個の MST 領域にあると考えられます。

例

次の例では、領域に名前を付ける方法を示します。

```
Switch(config-mst)# name Cisco
Switch(config-mst)#
```

関連コマンド

コマンド	説明
instance	1 つの VLAN または一連の VLAN を MST インスタンスにマッピングします。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show spanning-tree mst	MST プロトコル情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

pagp learn-method

着信パケットの入力インターフェイスを学習するには、**pagp learn-method** 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。

pagp learn-method {**aggregation-port** | **physical-port**}

no pagp learn-method

構文の説明

aggregation-port	ポート チャネル上のアドレスを学習するように指定します。
physical-port	バンドル内の物理ポート上のアドレスを学習するように指定します。

デフォルト

集約ポートはイネーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、バンドル内の物理ポート アドレスの学習をイネーブルにする方法を示します。

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

次の例では、バンドル内の集約ポート アドレスの学習をイネーブルにする方法を示します。

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

関連コマンド

コマンド	説明
show pagp	ポート チャネル情報を表示します。

pagp port-priority

ホット スタンバイ モードでポートを選択するには、**pagp port-priority** 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。

pagp port-priority *priority*

no pagp port-priority

構文の説明

priority	ポート プライオリティ番号です。有効値の範囲は 1 ～ 255 です。

デフォルト

ポート プライオリティは 128 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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

プライオリティが高いほど、ポートがホット スタンバイ モードで選択される可能性が高くなります。

例

次の例では、ポート プライオリティを設定する方法を示します。

```
Switch(config-if)# pagp port-priority 45
Switch(config-if)#
```

関連コマンド

コマンド	説明
pagp learn-method	着信パケットの入力インターフェイスを学習します。
show pagp	ポート チャネル情報を表示します。

passive-interface

インターフェイスでルーティング アップデートの送信をディセーブルにするには、**passive-interface** コマンドを使用します。ルーティング アップデートの送信を再びイネーブルにするには、このコマンドの **no** 形式を使用します。

passive-interface [[**default**] {*interface-type interface-number*}] | {**range** *interface-type interface-number-interface-type interface-number*}

no passive-interface [[**default**] {*interface-type interface-number*}] | {**range** *interface-type interface-number-interface-type interface-number*}

構文の説明

default	（任意）すべてのインターフェイスがパッシブとなります。
interface-type	インターフェイス タイプを指定します。
interface-number	インターフェイス番号を指定します。
range range	設定するサブインターフェイスの範囲を指定します。「使用上のガイドライン」を参照してください。

デフォルト

インターフェイスでルーティング アップデートが送信されます。

コマンド モード

ルータ コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

passive-interface range コマンドを使用できるインターフェイスは、FastEthernet、GigabitEthernet、VLAN、ループバック、ポート チャネル、10 GigabitEthernet、およびトンネルです。VLAN インターフェイスで **passive-interface range** コマンドを使用する場合、このインターフェイスは既存の VLAN SVI である必要があります。VLAN SVI を表示するには、**show running config** コマンドを入力します。表示されない VLAN は、**passive-interface range** コマンドで使用できません。

passive-interface range コマンドで入力した値は、既存のすべての VLAN SVI に適用されます。

マクロを使用するには、事前に **define interface-range** コマンドで範囲を定義しておく必要があります。

passive-interface range コマンドによってポート範囲に加えられたコンフィギュレーションの変更はすべて、個別のパッシブ インターフェイス コマンドとして、実行コンフィギュレーション内で保持されます。

range は次の 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。
- 定義済みのマクロを指定します。

インターフェイスを指定するか、またはインターフェイス範囲マクロの名前を指定できます。インターフェイス範囲は同一のインターフェイス タイプで構成されている必要があり、1 つの範囲内のインターフェイスが複数のモジュールをまたがることはできません。

1 回のコマンドで定義できるインターフェイス範囲は最大で 5 つです。各範囲をカンマで区切って指定します。

```
interface range gigabitethernet 5/1-20, gigabitethernet4/5-20.
```

port-range を入力するときは、次の形式を使用します。

- *interface-type* {*mod*}/{*first-port*} - {*last-port*}

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。マクロの作成後、追加の範囲を入力できます。インターフェイス範囲をすでに入力している場合は、CLI でマクロを入力できません。

range *range* 値では単一インターフェイスを指定できます。この点で、このコマンドは **passive-interface** *interface-number* コマンドと類似しています。

（注）　**range** キーワードがサポートされるのは、OSPF、EIGRP、RIP、および ISIS ルータ モードのみです。

インターフェイス上でルーティング アップデートの送信をディセーブルにした場合でも、特定のサブネットは引き続き他のインターフェイスにアドバタイズされ、このインターフェイス上の他のルータからのアップデートは引き続き受信および処理されます。

default キーワードを使用すると、デフォルトですべてのインターフェイスがパッシブとなります。この場合、隣接情報を必要とする個別のインターフェイスを設定するには、**no passive-interface** コマンドを使用します。**default** キーワードは、Internet Service Provider（ISP; インターネット サービス プロバイダー）や大規模な企業ネットワークなど、多数のディストリビューション ルータに 200 以上ものインターフェイスが搭載されるような環境で役立ちます。

Open Shortest Path First（OSPF）プロトコルの場合、指定したルータ インターフェイスでは、OSPF ルーティング情報の送信も受信も行われません。指定したインターフェイス アドレスは、OSPF ドメイン内のスタブ ネットワークとして表示されます。

Intermediate System-to-Intermediate System（IS-IS）プロトコルの場合、このコマンドでは IS-IS に対し、指定したインターフェイスでは実際に IS-IS を実行せずに、このインターフェイスの IP アドレスをアドバタイズするように指示します。IS-IS に対してこのコマンドの **no** 形式を使用すると、指定したアドレスの IP アドレスのアドバタイズがディセーブルになります。

（注）　IS-IS の場合は、1 つ以上のアクティブ インターフェイスを維持する必要があり、このインターフェイスを **ip router isis** コマンドを使用して設定します。

Enhanced Interior Gateway Routing Protocol（EIGRP）は、パッシブと設定されたインターフェイスではディセーブルになりますが、その場合もルートのアドバタイズは行います。

例

次の例では、ネットワーク 10.108.0.0 で、インターフェイス GigabitEthernet 1/1 以外のすべてのインターフェイスに対して EIGRP アップデートを送信する方法を示します。

```
Switch(config)# interface gigabitethernet 1/1
Switch(config-if)# router eigrp 109
Switch(config-router)# network 10.108.0.0
Switch(config-router)# passive-interface gigabitethernet 1/1
Switch(config-router)#
```

次のコンフィギュレーションでは、インターフェイス Ethernet 1 およびインターフェイス serial 0 上で IS-IS をイネーブルにし、リンクステート Protocol Data Unit（PDU; プロトコル データ ユニット）でインターフェイス Ethernet 0 の IP アドレスをアドバタイズしています。

```
Switch(config-if)# router isis Finance
Switch(config-router)# passive-interface Ethernet 0
Switch(config-router)# interface Ethernet 1
Switch(config-router)# ip router isis Finance
Switch(config-router)# interface serial 0
Switch(config-router)# ip router isis Finance
Switch(config-router)#
```

次の例では、すべてのインターフェイスをパッシブに設定してから、インターフェイス ethernet0 をアクティブにする方法を示します。

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface default
Switch(config-router)# no passive-interface ethernet0
Switch(config-router)# network 10.108.0.1 0.0.0.255 area 0
Switch(config-router)#
```

次のコンフィギュレーションでは、モジュール 0 のイーサネット ポート 3 ～ 4、およびモジュール 1 のギガビット イーサネット ポート 4 ～ 7 をパッシブに設定しています。

```
Switch(config-if)# router ospf 100
Switch(config-router)# passive-interface range ethernet0/3-4,gigabitethernet1/4-7
Switch(config-router)#
```

permit

DHCP バインディングと一致した ARP パケットを許可するには、**permit** コマンドを使用します。指定した ACE をアクセス 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 {[**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 要求の照合条件を指定します。**request** を指定しないと、すべての ARP パケットに対して照合が実行されます。
ip	送信元 IP アドレスを指定します。
any	任意の IP アドレスまたは MAC アドレスを許可するように指定します。
host *sender-ip*	特定の送信元 IP アドレスだけを許可するように指定します。
sender-ip sender-ip-mask	特定の範囲の送信元 IP アドレスを許可するように指定します。
mac	送信元 MAC アドレスを指定します。
host *sender-mac*	特定の送信元 MAC アドレスだけを許可するように指定します。
sender-mac sender-mac-mask	特定の範囲の送信元 MAC アドレスを許可するように指定します。
response	ARP 応答の一致条件を指定します。
ip	ARP 応答の IP アドレス値を指定します。
host *target-ip*	（任意）特定の宛先 IP アドレスだけを許可するように指定します。
target-ip target-ip-mask	（任意）特定の範囲の宛先 IP アドレスを許可するように指定します。
mac	ARP 応答の MAC アドレス値を指定します。
host *target-mac*	（任意）特定の宛先 MAC アドレスだけを許可するように指定します。
target-mac target-mac-mask	（任意）特定の範囲の宛先 MAC アドレスを許可するように指定します。
log	（任意）Access Control Entry（ACE; アクセス コントロール エントリ）に一致するパケットを記録します。

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

arp-nacl コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

permit 句を追加すると、一部の一致基準に基づいて ARP パケットを転送したり、ドロップしたりできます。

例

次の例に示すホストの MAC アドレスは 0000.0000.abcd、IP アドレスは 1.1.1.1 です。この例では、このホストからの要求および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
Switch# show arp access-list

ARP access list static-hosts
    permit ip host 1.1.1.1 mac host 0000.0000.abcd
Switch#
```

関連コマンド

コマンド	説明
arp access-list	ARP アクセス リストを定義したり、定義済みリストの最後に句を追加したりします。
deny	DHCP バインディングと一致した ARP パケットを拒否します。
ip arp inspection filter vlan	DAI がイネーブルの場合にスタティック IP が設定されたホストからの ARP を許可したり、ARP アクセス リストを定義して VLAN に適用したりします。

police

トラフィック ポリシング機能を設定するには、**police** QoS 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。コンフィギュレーションからトラフィック ポリシング機能を削除するには、このコマンドの **no** 形式を使用します。

police {*bps* | *kbps* | *mbps* |*gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

no police {*bps* | *kbps* | *mbps* |*gbps*} [*burst-normal*] [*burst-max*] **conform-action** *action* **exceed-action** *action* [**violate-action** *action*]

構文の説明

bps	平均レート（ビット/秒）です。有効値の範囲は 32,000 ～ 32,000,000,000 です。
kbps	平均レート（キロバイト/秒）です。有効値の範囲は 32 ～ 32,000,000 です。
mbps	平均レート（メガビット/秒）です。有効値の範囲は 1 ～ 32,000 です。
gbps	平均レート（ギガビット/秒）です。有効値の範囲は 1 ～ 32 です。
burst-normal	（任意）通常バースト サイズ（バイト）です。有効値の範囲は 64 ～ 2,596,929,536 です。設定レートの 4 倍までのバースト値をサポートできます。
burst-max	（任意）超過バースト サイズ（バイト）です。有効値の範囲は 64 ～ 2,596,929,536 です。設定レートの 4 倍までのバースト値をサポートできます。
conform-action	レート制限に適合したパケットに対して実行するアクションです。
exceed-action	レート制限を超過したパケットに対して実行するアクションです。
violate-action	（任意）通常および最大バースト サイズに違反したパケットに対して実行するアクションです。
action	パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 • **drop**：パケットをドロップします。 • **set-cos-transmit** new-ios : Class of Service（CoS; サービス クラス）値を新しい値に設定して、パケットを送信します。指定できる範囲は 0 ～ 7 です。 • **set-dscp-transmit** *value* : IP Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定して、新しい IP DSCP 値設定でパケットを送信します。 • **set-prec-transmit** *value* : IP precedence を設定して、新しい IP precedence 値設定でパケットを送信します。 • **transmit**：パケットを送信します。パケットは変更されません。

デフォルト

このコマンドは、デフォルトではディセーブルです。

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 モード（マークされたパケットに適用される単一のアクションを指定する場合）

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（マークされたパケットに適用される複数のアクションを指定する場合）

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

police コマンドは、サービスレベル アグリーメントへの準拠に基づいて、異なる Quality of Service（QoS）値を持つパケットをマークするために使用します。

トラフィック ポリシングは、インターフェイスを通過するトラフィックに対しては実行されません。

複数のアクションの指定

police コマンドでは、複数のポリシング アクションを指定できます。**police** コマンドの設定時に複数のポリシング アクションを指定する場合は、次の点に注意してください。

- 同時に最大 4 つのアクションを指定できます。
- **conform-action** *transmit* と **conform-action** *drop* など、矛盾したアクションを指定することはできません。

police コマンドとトラフィック ポリシング機能の使用

police コマンドは、トラフィック ポリシング機能とともに使用することができます。トラフィック ポリシング機能は、トークン バケット アルゴリズムで動作します。トークン バケット アルゴリズムには、1 トークン バケット アルゴリズムと 2 トークン バケット アルゴリズムの 2 種類があります。1 トークン バケット システムは、**violate-action** オプションを指定しなかった場合に使用され、2 トークン バケット システムは、**violate-action** オプションを指定した場合に使用されます。

1 トークン バケットを使用するトークン バケット アルゴリズム

1 トークン バケット アルゴリズムは、**violate-action** オプションを Command-Line Interface（CLI; コマンドライン インターフェイス）の **police** コマンドで指定しなかった場合に使用されます。

適合バケットは、最初はフル サイズに設定されています（フル サイズは、通常バースト サイズとして指定されているバイト数です）。

指定サイズのパケット（たとえば、「B」バイト）が特定の時間（時間「T」）に到着する場合、次のようなアクションが発生します。

- 適合バケットでトークンが更新されます。前にパケットが到着したのが T1 で、現在の時間が T の場合、バケットはトークン到着レートに基づいて（T - T1）相当のビット数で更新されます。トークン到着レートは、次のように計算されます。

  （パケット間の時間 <T - T1> × ポリサー レート）/8 バイト

- 適合バケット B のバイト数が 0 以上の場合、パケットが適合し、そのパケットに対して適合アクションが実行されます。パケットが適合した場合、B バイトが適合バケットから削除されて、そのパケットに対する適合アクションが完了します。
- 適合バケット B のバイト数（制限されているパケット サイズを引いたもの）が 0 未満の場合、超過アクションが実行されます。

2 トークン バケットを使用するトークン バケット アルゴリズム（RFC 2697 を参照）

2 トークン バケット アルゴリズムは、**violate-action** を CLI の **police** コマンドで指定した場合に使用されます。

適合バケットは、最初はフル サイズになっています（フル サイズは、通常バースト サイズとして指定されているバイト数です）。

超過バケットは、最初はフル サイズになっています（フル超過サイズは、最大バースト サイズとして指定されているバイト数です）。

適合および超過トークン バケットのいずれのトークンも、トークン到着レートまたは Committed Information Rate（CIR; 認定情報レート）に基づいて更新されます。

指定サイズのパケット（たとえば、「B」バイト）が特定の時間（時間「T」）に到着する場合、次のようなアクションが発生します。

- 適合バケットでトークンが更新されます。前にパケットが到着したのが T1 で、今回の到着時間が T の場合、バケットはトークン到着レートに基づいて T - T1 相当のビット数で更新されます。補充トークンが適合バケットに配置されます。トークンが適合バケットでオーバーフローした場合、オーバーフロー トークンが超過バケットに配置されます。

  トークン到着レートは、次のように計算されます。

  （パケット間の時間 <T - T1> × ポリサー レート）/8 バイト

- 適合バケット B のバイト数が 0 以上の場合、パケットが適合し、そのパケットに対して適合アクションが実行されます。パケットが適合した場合、B バイトが適合バケットから削除されて、適合アクションが実行されます。超過バケットはこのシナリオでは影響を受けません。
- 適合バケット B のバイト数が 0 未満の場合、超過トークン バケットのバイト数がパケットによってチェックされます。超過バケット B のバイト数が 0 以上の場合、超過アクションが実行され、B バイトが超過トークン バケットから削除されます。適合バケットから削除されるバイトはありません。
- 超過バケット B のバイト数が 0 未満の場合、パケットがレートに違反していて、違反アクションが実行されます。そのパケットに対するアクションが完了します。

例

1 トークン バケットを使用するトークン バケット アルゴリズム

次の例では、（**class-map** コマンドを使用して）トラフィック クラスを定義し、（**policy-map** コマンドを使用して）トラフィック クラスからの一致基準をサービス ポリシーに設定されているトラフィック ポリシング コンフィギュレーションに関連付ける方法を示します。ここで、**service-policy** コマンドはこのサービス ポリシーをインターフェイスに対応付けるために使用されます。

この特定の例では、トラフィック ポリシングは平均レート 8000 ビット/秒で設定され、ギガビット イーサネット インターフェイス 6/1 から発信される全パケットに対して通常バースト サイズが 1000 バイトとなります。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 conform-action transmit exceed-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

この例では、初期トークン バケットはフル サイズの 1000 バイトで開始されます。450 バイトのパケットが到着すると、十分なバイト数が適合トークン バケットで利用可能であるため、パケットが適合します。パケットによって適合アクション（送信）が実行され、450 バイトが適合トークン バケットから削除されます（550 バイトが残ります）。

次のパケットが 0.25 秒後に到着すると、250 バイトがトークン バケットに追加され（(0.25 × 8000) /8）、トークン バケットには 800 バイトが残ります。次のパケットが 900 バイトの場合、パケットが超過して超過アクション（ドロップ）が実行されます。トークン バケットから取り出されるバイトはありません。

2 トークン バケットを使用するトークン バケット アルゴリズムの例（RFC 2697 を参照）

この特定の例では、トラフィック ポリシングは平均レート 8000 ビット/秒で設定され、ギガビット イーサネット インターフェイス 6/1 から発信される全パケットに対して通常バースト サイズが 1000 バイト、超過バースト サイズが 1000 バイトとなります。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map access-match
Switch(config-cmap)# match access-group 1
Switch(config-cmap)# exit
Switch(config)# policy-map police-setting
Switch(config-pmap)# class access-match
Switch(config-pmap-c)# police 8000 1000 1000 conform-action transmit exceed-action set-qos-transmit 1
violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output police-setting
Switch(config-if)# end
```

この例では、初期トークン バケットはフル サイズの 1000 バイトで開始されます。450 バイトのパケットが到着すると、十分なバイト数が適合トークン バケットで利用可能であるため、パケットが適合します。パケットによって適合アクション（送信）が実行され、450 バイトが適合トークン バケットから削除されます（550 バイトが残ります）。

次のパケットが 0.25 秒後に到着すると、250 バイトが適合トークン バケットに追加され（(0.25 × 8000）/8）、適合トークン バケットには 800 バイトが残ります。次のパケットが 900 バイトの場合、適合トークン バケットで利用可能なのが 800 バイトだけなので、パケットが適合しません。

次に、フル サイズの 1000 バイト（超過バースト サイズとして指定済み）で開始される超過トークン バケットの利用可能バイトがチェックされます。超過トークン バケットで十分なバイト数が利用可能であるため、超過アクション（QoS 送信値を 1 に設定）が実行され、900 バイトが超過バケットから取り出されます（超過トークン バケットには 100 バイトが残ります）。

次のパケットが 0.40 秒後に到着すると、400 バイトがトークン バケットに追加されます（(0.40 × 8000）/8）。したがって、適合トークン バケットは現在 1000 バイト（適合バケットで利用可能な最大トークン数）で、200 バイトが適合トークン バケットからオーバーフローしています（適合トークン バケットの容量を満たすために必要なのは 200 バイトだけであるため）。これらのオーバーフロー バイトは、超過トークン バケットに置かれ、超過トークン バケットは 300 バイトになります。

1000 バイトのパケットが到着した場合、十分なバイト数が適合トークン バケットで利用可能であるため、パケットが適合します。パケットによって適合アクション（送信）が実行され、1000 バイトが適合トークン バケットから削除されます（0 バイトが残ります）。

次のパケットが 0.20 秒後に到着すると、200 バイトがトークン バケットに追加されます（(20 × 8000) /8）。したがって、適合バケットは 200 バイトになります。400 バイトのパケットが到着した場合、適合バケットで利用可能なのが 200 バイトだけなので、パケットが適合しません。同様に、超過バケットで利用可能なのが 300 バイトだけなので、パケットは超過しません。したがって、パケットは違反となり、違反アクション（ドロップ）が実行されます。

関連コマンド

コマンド	説明
police（パーセント）	インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定します。
police（2 レート）	Committed Information Rate（CIR; 認定情報レート）および Peak Information Rate（PIR; 最大情報レート）の 2 レートを使用したトラフィック ポリシングを設定します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。
show policy-map	ポリシー マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

police（パーセント）

インターフェイスで利用可能な帯域幅の割合に基づいてトラフィック ポリシングを設定するには、QoS 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 **police** コマンドを使用します。コンフィギュレーションからトラフィック ポリシ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。

police cir percent *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percentage*] [**be** *peak-burst-inmsec*]

no police cir percent *percent* [**bc** *conform-burst-in-msec*] [**pir percent** *percentage*] [**be** *peak-burst-inmsec*]

構文の説明

cir	認定情報レートです。CIR がトラフィック ポリシングに使用されることを示します。
percent	帯域幅の割合を使用して CIR を計算するように指定します。
percent	帯域幅の割合を指定します。有効な範囲は 1 ～ 100 の数字です。
bc	（任意）最初のトークン バケットでトラフィック ポリシングに使用される適合バースト（bc）サイズです。
conform-burst-in-msec	（任意）bc 値をミリ秒単位で指定します。有効な範囲は 1 ～ 2000 の数字です。
pir	（任意）Peak Information Rate（PIR; 最大情報レート）です。PIR がトラフィック ポリシングに使用されることを示します。
percent	（任意）帯域幅の割合を使用して PIR を計算するように指定します。
percent	（任意）帯域幅の割合を指定します。有効な範囲は 1 ～ 100 の数字です。
be	（任意）2 番目のトークン バケットでトラフィック ポリシングに使用されるピーク バースト（be）サイズです。
peak-burst-in-msec	（任意）be サイズをミリ秒単位で指定します。有効な範囲は 1 ～ 2000 の数字です。
action	パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 • **drop**：パケットをドロップします。 • **set-cos-transmit** new-ios：Class of Service（CoS; サービス クラス）値を新しい値に設定して、パケットを送信します。指定できる範囲は 0 ～ 7 です。 • **set-dscp-transmit** *value*：IP Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定して、新しい IP DSCP 値設定でパケットを送信します。 • **set-prec-transmit** *value*：IP precedence を設定して、新しい IP precedence 値設定でパケットを送信します。 • **transmit**：パケットを送信します。パケットは変更されません。

コマンド デフォルト

このコマンドは、デフォルトではディセーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドでは、インターフェイスで利用可能な最大帯域幅の割合に基づいて CIR および PIR を計算します。ポリシー マップがインターフェイスに対応付けられている場合、ビット/秒（bps）単位の等価 CIR および PIR 値が、インターフェイス帯域幅とこのコマンドで入力したパーセント値に基づいて計算されます。**show policy-map interface** コマンドを使用して、計算された bps レートを確認できます。

計算された CIR および PIR の bps レートは、32,000 ～ 32,000,000,000 bps の範囲内でなければなりません。レートがこの範囲外の場合、関連ポリシー マップをインターフェイスに対応付けることができません。インターフェイス帯域幅が変更された場合（帯域幅が追加された場合など）、改訂された帯域幅に基づいて CIR および PIR の bps 値が再計算されます。ポリシー マップをインターフェイスに対応付けたあとに CIR および PIR の割合が変更された場合、CIR および PIR の bps 値が再計算されます。

また、このコマンドでは、適合バースト サイズとピーク バースト サイズの値をミリ秒単位で指定することもできます。帯域幅を割合として計算する場合は、適合バースト サイズとピーク バースト サイズをミリ秒単位で指定する必要があります。

例

次の例では、ギガビット インターフェイス 6/2 で帯域幅の割合に基づいて CIR および PIR を使用したトラフィック ポリシングを設定する方法を示します。この例では、CIR に 20%、PIR に 40% が指定されています。さらに、任意指定の bc 値と be 値（それぞれ 300 ms および 400 ms）が指定されています。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class-map class1
Switch(config-pmap-c)# police cir percent 20 bc 3 ms pir percent 40 be 4 ms
Switch(config-pmap-c)# exit
Switch(config-pmap-c)# interface gigabitethernet 6/2
Switch(config-if)# service-policy output policy
Switch(config-if)# end
```

police rate

シングルまたはデュアル レート ポリサーを設定するには、ポリシーマップ コンフィギュレーション モードで **police rate** コマンドを使用します。コンフィギュレーションからトラフィック ポリシ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。

バイト/秒の構文

police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**pack-burst** *peak-burst-in-bytes* **bytes**]

no police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**pack-burst** *peak-burst-in-bytes* **bytes**]

割合の構文

police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate** *percent* **percentage**] [**pack-burst** *ms* **ms**]

no police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate** *percent* **percentage**] [**pack-burst** *ms* **ms**]

構文の説明

units	トラフィック ポリシング レートをビット/秒単位で指定します。有効な範囲は 32,000 ～ 32,000,000,000 です。
bps	（任意）ビット/秒（bps）を使用して、トラフィックがポリシングされるレートを決定します。 **（注）** レートを指定しなかった場合、トラフィックは bps でポリシングされます。
burst *burst-in-bytes* **bytes**	（任意）バイト単位のバースト レートをトラフィック ポリシングに使用するように指定します。有効な範囲は 64 ～ 2,596,929,536 です。
peak-rate *peak-rate-in-bps* **bps**	（任意）最大レートのピーク バースト値をバイト単位で指定します。有効な範囲は 32,000 ～ 32,000,000,000 です。
peak-burst *peak-burst-in-bytes* **bytes**	（任意）バイト単位のピーク バースト値をトラフィック ポリシングに使用するように指定します。ポリシング レートを bps で指定した場合、値の有効な範囲は 64 ～ 2,596,929,536 です。
percent	（任意）インターフェイス帯域幅の割合を使用して、トラフィックがポリシングされるレートを決定します。
percentage	（任意）帯域幅の割合です。有効な範囲は 1 ～ 100 の数字です。
burst *ms* **ms**	（任意）ミリ秒単位のバースト レートをトラフィック ポリシングに使用します。有効な範囲は 1 ～ 2,000 の数字です。
peak-rate percent *percentage*	（任意）インターフェイス帯域幅の割合を使用して PIR を決定します。有効な範囲は 1 ～ 100 の数字です。
peak-burst *ms* **ms**	（任意）ミリ秒単位のピーク バースト レートをトラフィック ポリシングに使用します。有効な範囲は 1 ～ 2,000 の数字です。

コマンド デフォルト

このコマンドは、デフォルトではディセーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

pps、bps、またはインターフェイス帯域幅の割合に基づいてトラフィックを制限するには、**police rate** コマンドを使用します。

レートを指定せずに **police rate** コマンドを発行すると、宛先指定されたトラフィックは bps に基づいてポリシングされます。

例

次の例では、平均レート 1,500,000 bps にトラフィックを制限するようにクラスのポリシングを設定する方法を示します。

```
Switch(config)# class-map c1
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# police rate 1500000  burst 500000
Switch(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
show policy-map	ポリシー マップ情報を表示します。

police（2 レート）

Committed Information Rate（CIR; 認定情報レート）および Peak Information Rate（PIR; 最大情報レート）の 2 レートを使用したトラフィック ポリシングを設定するには、ポリシーマップ コンフィギュレーション モードで **police** コマンドを使用します。コンフィギュレーションから 2 レート トラフィック ポリシ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。

police cir *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

no police cir *cir* [**bc** *conform-burst*] **pir** *pir* [**be** *peak-burst*] [**conform-action** *action* [**exceed-action** *action* [**violate-action** *action*]]]

構文の説明

cir	最初のトークン バケットが更新される Committed Information Rate（CIR; 認定情報レート）です。
cir	CIR 値をビット/秒単位で指定します。値は 32,000 ～ 32,000,000,000 の数字です。
bc	（任意）最初のトークン バケットでポリシングに使用される適合バースト（bc）サイズです。
conform-burst	（任意）bc 値をバイト単位で指定します。値は 64 ～ 2,596,929,536 の数字です。
pir	2 番目のトークン バケットが更新される Peak Information Rate（PIR; 最大情報レート）です。
pir	PIR 値をビット/秒単位で指定します。値は 32,000 ～ 32,000,000,000 の数字です。
be	（任意）2 番目のトークン バケットでポリシングに使用されるピーク バースト（be）サイズです。
peak-burst	（任意）ピーク バースト（be）サイズをバイト単位で指定します。値は 64 ～ 2,596,929,536 の数字です。
conform-action	（任意）CIR および PIR に適合するパケットに対して実行するアクションです。
exceed-action	（任意）PIR に適合するものの CIR には適合しないパケットに対して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です。
action	（任意）パケットに対して実行するアクションです。次のいずれかのキーワードを指定します。 • **drop**：パケットをドロップします。 • **set-cos-transmit** new-ios：Class of Service（CoS; サービス クラス）値を新しい値に設定して、パケットを送信します。指定できる範囲は 0 ～ 7 です。 • **set-dscp-transmit** *new-dscp*：IP Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定して、新しい IP DSCP 値設定でパケットを送信します。 • **set-prec-transmit** *new-prec*：IP precedence を設定して、新しい IP precedence 値設定でパケットを送信します。 • **transmit**：変更なしでパケットを送信します。

コマンド デフォルト

このコマンドは、デフォルトではディセーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン　RFC 2698「Two Rate Three Color Marker」を参照してください。

2 レート トラフィック ポリシングでは、2 つの独立したレートでのトラフィックのポリシングに 2 つのトークン バケット（Tc と Tp）を使用します。2 つのトークン バケットに関して次の点に注意してください。

- Tc トークン バケットは、パケットが 2 レート ポリサーで到着するたびに CIR 値で更新されます。Tc トークン バケットには、適合バースト（Bc）値まで含めることができます。
- Tp トークン バケットは、パケットが 2 レート ポリサーで到着するたびに PIR 値で更新されます。Tp トークン バケットには、ピーク バースト（Be）値まで含めることができます。

トークン バケットの更新

次のシナリオは、トークン バケットの更新方法について説明したものです。

B バイトのパケットが時間 t に到着します。前のパケットは時間 t1 に到着しています。時間 t での CIR と PIR トークン バケットは、それぞれ Tc(t) および Tp(t) で表されます。これらの値をこのシナリオで使用する場合、トークン バケットは次のように更新されます。

$$Tc(t) = \min(CIR \times (t-t1) + Tc(t1), Bc)$$

$$Tp(t) = \min(PIR \times (t-t1) + Tp(t1), Be)$$

トラフィックのマーキング

2 レート ポリサーは、指定レートに適合しているか、超過しているか、または違反しているとしてパケットをマークします。次のポイント（B バイトのパケットを使用）は、パケットがどのようにマークされるかを示しています。

- B > Tp(t) の場合、パケットは指定レートに違反しているとマークされます。
- B > Tc(t) の場合、パケットは指定レートを超過しているとマークされ、Tp(t) トークン バケットは Tp(t) = Tp(t) - B として更新されます。

これ以外の場合、パケットは指定レートに適合しているとマークされ、Tc(t) および Tp(t) のトークン バケットが次のように更新されます。

$$Tp(t) = Tp(t) – B$$

$$Tc(t) = Tc(t) – B$$

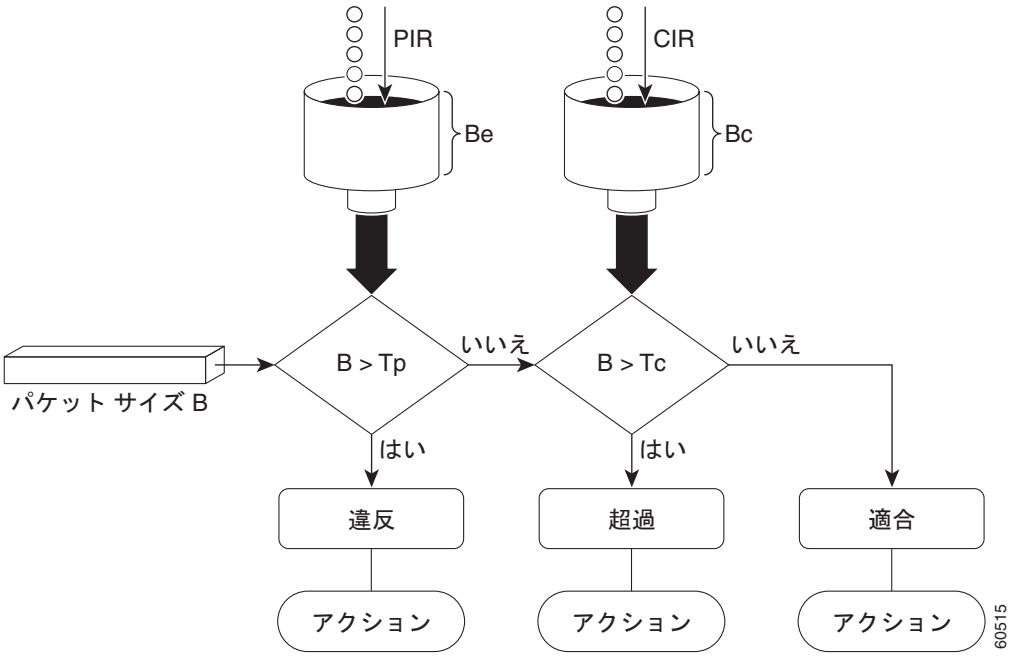
たとえば、CIR が 100 kbps、PIR が 200 kbps で、250 kbps のレートのデータ ストリームが 2 レート ポリサーで到着した場合、パケットは次のようにマークされます。

- 100 kbps は、レートに適合しているとマークされます。
- 100 kbps は、レートを超過しているとマークされます。
- 50 kbps は、レートに違反しているとマークされます。

パケットのマーキングとアクションの割り当てのフローチャート

図 2-1 のフローチャートは、2 レート ポリサーによるパケットのマーキング方法と、パケットへの対応アクション（違反、超過、または適合）の割り当て方法を示したものです。

図 2-1　　2 レート ポリサーでのパケットのマーキングとアクションの割り当て



例

次の例では、平均認定レート 500 kbps、最大レート 1 Mbps にトラフィックを制限するようにクラスの 2 レート トラフィック ポリシングを設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# class-map police
Switch(config-cmap)# match access-group 101
Switch(config-cmap)# policy-map policy1
Switch(config-pmap)# class police
Switch(config-pmap-c)# police cir 500000 bc 10000 pir 1000000 be 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch(config-pmap-c)# interface gigabitethernet 6/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# end
Switch# show policy-map policy1

 Policy Map policy1
  Class police
   police cir 500000 conform-burst 10000 pir 1000000 peak-burst 10000 conform-action
transmit exceed-action set-prec-transmit 2 violate-action drop
Switch#
```

平均認定レート（500 kbps）に適合しているとマークされたトラフィックはそのまま送信されます。500 kbps を超過しているものの 1 Mbps は超過していないとマークされたトラフィックは、IP precedence 2 でマークされてから送信されます。1 Mbps を超過しているとマークされたトラフィックはすべてドロップされます。バースト パラメータは 10000 バイトに設定されています。

次の例では、1.25 Mbps のトラフィックがポリサー クラスに送信（提供）されます。

```
Switch# show policy-map interface gigabitethernet 6/1

 GigabitEthernet6/1

  Service-policy output: policy1

   Class-map: police (match all)
    148803 packets, 36605538 bytes
    30 second offered rate 1249000 bps, drop rate 249000 bps
    Match: access-group 101
    police:
     cir 500000 bps, conform-burst 10000, pir 1000000, peak-burst 100000
     conformed 59538 packets, 14646348 bytes; action: transmit
     exceeded 59538 packets, 14646348 bytes; action: set-prec-transmit 2
     violated 29731 packets, 7313826 bytes; action: drop
     conformed 499000 bps, exceed 500000 bps violate 249000 bps

   Class-map: class-default (match-any)
    19 packets, 1990 bytes
    30 seconds offered rate 0 bps, drop rate 0 bps
    Match: any
Switch#
```

2 レート ポリサーにより、500 kbps のトラフィックが指定レートに適合とマークされ、500 kbps のトラフィックが指定レートを超過とマークされ、250 kbps のトラフィックが指定レートに違反とマークされます。レートに適合しているとマークされたパケットはそのまま送信され、レートを超過しているとマークされたパケットは IP precedence 2 でマークされてから送信されます。レートに違反しているとマークされたパケットはドロップされます。

policy-map

複数のポートに対応付け可能なポリシー 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、ポリシーマップ コンフィギュレーション モードを開始するには、**policy-map** グローバル コンフィギュレーション コマンドを使用します。既存のポリシー マップを削除して、グローバル コンフィギュレーション モードに戻るには、このコマンドの **no** 形式を使用します。

policy-map *policy-map-name*

no policy-map *policy-map-name*

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。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E および Catalyst 4900M シャーシのサポートが追加されました。

使用上のガイドライン

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** コマンドを入力すると、スイッチがポリシーマップ コンフィギュレーション モードになります。そのポリシー マップのクラス ポリシーを設定または変更し、分類されたトラフィックの処理方法を決定できます。

これらのコンフィギュレーション コマンドは、ポリシーマップ コンフィギュレーション モードで利用できます。

- **class**：指定されたクラス マップの分類一致条件を定義します。詳細については、「class」（P.2-57）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**：すでに定義済みのポリシー マップを削除します。

グローバル コンフィギュレーション モードに戻る場合は、**exit** コマンドを使用します。特権 EXEC モードに戻るには、**end** コマンドを使用します。

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。

例

次の例では、*policy1* という名前のポリシー マップを作成する方法を示します。入力方向に適用した場合、*class1* で定義されたすべての着信トラフィックの照合を行い、IP DSCP を 10 に設定し、平均レート 1 Mbps、バースト 20 KB でトラフィックをポリシングします。プロファイルを超過するトラフィックは、ポリシング設定 DSCP マップから取得した DSCP 値がマークされてから送信されます。このポリサー アクションは、Supervisor Engine 6-E および Catalyst 4900M シャーシ以外のすべての Catalyst 4500 Supervisor に適用可能です。

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

次の例では、Supervisor Engine 6-E で「policymap2」というポリシー マップに複数のクラスを設定する方法を示します。

```
Switch# configure terminal
Switch(config)# policy-map policymap2
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 100000 20000 exceed-action
Switch(config-pmap-c)# set-dscp-transmit cs3
Switch(config-pmap-c)# set-cos-transmit 3
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class2
Switch(config-pmap-c)# police cir 32000 pir 64000 conform-action transmit exceed-action
Switch(config-pmap-c)# set-dscp-transmit cs3 violate-action drop
Switch(config-pmap-c)# exit
Switch(config-pmap)# class class3
Switch(config-pmap-c)# set dscp cs3
Switch(config-pmap-c)# exit
Switch#
```

次の例では、「policymap2」というポリシー マップを削除する方法を示します。

```
Switch# configure terminal
Switch(config)# no policy-map policymap2
Switch#
```

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	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
class-map	名前を指定したクラスとパケットの照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（インターフェイス コンフィギュレーション）	ポリシー マップをインターフェイスに対応付けたり、インターフェイスが属する VLAN で異なる QoS ポリシーを適用したりします。
show policy-map	ポリシー マップ情報を表示します。

port-channel load-balance

バンドル内のポート間に負荷分散方式を設定するには、**port-channel load-balance** コマンドを使用します。負荷分散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。

port-channel load-balance *method*

no port-channel load-balance

構文の説明

method	負荷分散方式を指定します。詳細については、「使用上のガイドライン」を参照してください。

デフォルト

送信元 XOR 宛先 IP アドレス上での負荷分散がイネーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

負荷分散方式では、次の値が有効です。

- **dst-ip**：宛先 IP アドレス上での負荷分散
- **dst-mac**：宛先 MAC アドレス上での負荷分散
- **dst-port**：宛先 TCP/UDP ポート上での負荷分散
- **src-dst-ip**：送信元 XOR 宛先 IP アドレス上での負荷分散
- **src-dst-mac**：送信元 XOR 宛先 MAC アドレス上での負荷分散
- **src-dst-port**：送信元 XOR 宛先 TCP/UDP ポート上での負荷分散
- **src-ip**：送信元 IP アドレス上での負荷分散
- **src-mac**：送信元 MAC アドレス上での負荷分散
- **src-port**：送信元ポート上での負荷分散

例

次の例では、負荷分散方式を宛先 IP アドレスに設定する方法を示します。

```
Switch(config)# port-channel load-balance dst-ip
Switch(config)#
```

次の例では、負荷分散方式を送信元 XOR 宛先 IP アドレスに設定する方法を示します。

```
Switch(config)# port-channel load-balance src-dst-port
Switch(config)#
```

関連コマンド

コマンド	説明
interface port-channel	ポートチャネル インターフェイスへのアクセスまたはポートチャネル インターフェイスの作成を行います。
show etherchannel	チャネルの EtherChannel 情報を表示します。

port-security mac-address

インターフェイスで特定の VLAN または VLAN 範囲に対してセキュア アドレスを設定するには、**port-security mac-address** コマンドを使用します。

port-security mac-address *mac_address*

構文の説明

mac_address	セキュアにする必要がある MAC アドレスです。

コマンド モード

VLAN 範囲インターフェイス サブモード

コマンド履歴

リリース	変更内容
12.2(25)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

レイヤ 2 インターフェイスは、複数の VLAN の一部であることがあります（一般的なトランク ポートの場合など）。**vlan** コマンドとともに **port-security mac-address** コマンドを使用すると、異なる VLAN 上の異なるアドレスを指定できます。

例

次の例では、ギガビット イーサネット インターフェイス 1/1 で VLAN 2 ～ 3 に対してセキュア アドレス 1.1.1 を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security mac-address 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

関連コマンド

コマンド	説明
port-security mac-address sticky	インターフェイスで特定の VLAN または VLAN 範囲に対してスティッキ アドレスを設定します。
port-security maximum	インターフェイスで特定の VLAN または VLAN 範囲に対してアドレスの最大数を設定します。

port-security mac-address sticky

インターフェイスで特定の VLAN または VLAN 範囲に対してスティッキ アドレスを設定するには、**port-security mac-address sticky** コマンドを使用します。

port-security mac-address sticky *mac_address*

構文の説明

mac_address	セキュアにする必要がある MAC アドレスです。

コマンド モード

VLAN 範囲インターフェイス サブモード

コマンド履歴

リリース	変更内容
12.2(25)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

port-security mac-address sticky コマンドを設定するには、事前にインターフェイスでスティッキ機能をイネーブルにしておく必要があります。

使用上のガイドライン

レイヤ 2 インターフェイスは、複数の VLAN の一部であることがあります（一般的なトランク ポートの場合など）。**vlan** コマンドとともに **port-security mac-address sticky** コマンドを使用すると、異なる VLAN 上の異なるスティッキ アドレスを指定できます。

port-security mac-address sticky コマンドを設定するには、事前にインターフェイスでスティッキ機能をイネーブルにしておく必要があります。

スティッキ MAC アドレスとは、スイッチの再起動やリンク フラップが発生しても維持されるアドレスのことです。

例

次の例では、ギガビット イーサネット インターフェイス 1/1 で VLAN 2 ～ 3 に対してスティッキ アドレス 1.1.1 を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security mac-address sticky 1.1.1
Switch(config-if-vlan-range)# end
Switch#
```

関連コマンド

コマンド	説明
port-security mac-address	インターフェイスで特定の VLAN または VLAN 範囲に対してセキュア アドレスを設定します。
port-security maximum	インターフェイスで特定の VLAN または VLAN 範囲に対してアドレスの最大数を設定します。

port-security maximum

インターフェイスで特定の VLAN または VLAN 範囲に対してアドレスの最大数を設定するには、**port-security maximum** コマンドを使用します。

port-security maximum *max_value*

構文の説明

max_value	MAC アドレスの最大数です。

コマンド モード

VLAN 範囲インターフェイス サブモード

コマンド履歴

リリース	変更内容
12.2(25)EWA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

レイヤ 2 インターフェイスは、複数の VLAN の一部であることがあります（一般的なトランク ポートの場合など）。**vlan** コマンドとともに **port-security maximum** コマンドを使用すると、異なる VLAN 上のセキュア アドレスの最大数を指定できます。

ポート上の特定の VLAN に最大数が設定されていない場合は、ポートに設定された最大数がその VLAN に使用されます。この場合、この VLAN で設定できるセキュア アドレスの最大数は、ポートに設定された最大数に制限されます。

各 VLAN には、ポートに設定された最大数より大きな値を設定できます。また、すべての VLAN に設定された最大数の合計が、ポートに設定された最大数を超えてもかまいません。どちらの場合も、各 VLAN に設定できるセキュア MAC アドレス数の上限は、VLAN に設定された最大数とポートに設定された最大数のうち、少ないほうの数となります。

例

次の例では、ギガビット イーサネット インターフェイス 1/1 で VLAN 2 ～ 3 に対してアドレスの最大数を 5 に設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface g1/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan 2-3
Switch(config-if-vlan-range)# port-security maximum 5
Switch(config-if-vlan-range)# exit
Switch#
```

関連コマンド

コマンド	説明
port-security mac-address	インターフェイスで特定の VLAN または VLAN 範囲に対してセキュア アドレスを設定します。
port-security mac-address sticky	インターフェイスで特定の VLAN または VLAN 範囲に対してスティッキ アドレスを設定します。

power dc input

スイッチに DC 電源入力パラメータを設定するには、**power dc input** コマンドを使用します。デフォルトの電源設定に戻すには、このコマンドの **no** 形式を使用します。

power dc input *watts*

no power dc input

構文の説明

dc input	両方の電源装置スロットに外部 DC 電源を指定します。
watts	外部 DC 電源の合計容量をワット（W）で設定します。有効値の範囲は 300 ～ 8500 です。

デフォルト

DC 電源入力は 2500 W 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 モード

コマンド履歴

リリース	変更内容
12.1(11)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(13)EW	**dc input** のサポートが追加されました。

使用上のガイドライン

使用しているインターフェイスが Power over Ethernet に対応していない場合には、次のメッセージが表示されます。

```
Power over Ethernet not supported on interface Admin
```

例

次の例では、外部 DC 電源の合計容量を 5000 W に設定する方法を示します。

```
Switch(config)# power dc input 5000
Switch(config)#
```

関連コマンド

コマンド	説明
show power	電力ステータスに関する情報を表示します。

power inline

インライン パワー対応インターフェイスのインライン パワー ステートを設定するには、**power inline** 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。

power inline {**auto** [**max** *milliwatt*] | **never** | **static** [**max** *milliwatt*] | **consumption** *milliwatt*}

no power inline

構文の説明

auto	インライン パワー対応インターフェイスの Power over Ethernet ステートを自動モードに設定します。
max *milliwatt*	（任意）装置が消費可能な最大電力を設定します。従来のモジュールの場合、有効な範囲は 2000 ～ 15400 ミリワット（mW）です。 WS-X4648-RJ45V-E の場合、最大電力は 20000 です。 WS-X4648-RJ45V+E の場合、最大電力は 30000 です。
never	インライン パワー対応インターフェイスで検出と電力の両方をディセーブルにします。
static	電力をスタティックに配分します。
consumption *milliwatt*	インターフェイスごとの電力配分を設定します。従来のモジュールの場合、有効な範囲は 4000 ～ 15400 です。デフォルト以外の値を設定した場合は、電力配分の自動調整がディセーブルになります。

デフォルト

デフォルト設定は次のとおりです。

- Power over Ethernet に自動モードが設定されています。
- 最大ミリワット モードは 15400 に設定されています。WS-X4648-RJ45V-E の場合、最大ミリワットは 20000 に設定されています。WS-X4648-RJ45V+E の場合、最大ミリワットは 30000 に設定されています。
- デフォルトの配分は 15400 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 モード

コマンド履歴

リリース	変更内容
12.1(11)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(19)EW	スタティックな電力配分のサポートが追加されました。
12.1(20)EW	Power over Ethernet のサポートが追加されました。
12.2(44)SG	WS-X4648-RJ45V-E および WS-X4648-RJ45V+E 用に 15400 を超える最大ワットがサポートされました。

使用上のガイドライン

使用しているインターフェイスが Power over Ethernet に対応していない場合には、次のメッセージが表示されます。

```
Power over Ethernet not supported on interface Admin
```

例

次の例では、インライン パワー対応インターフェイスのインライン パワー検出および電力を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline auto
Switch(config-if)# end
Switch#
```

次の例では、インライン パワー対応インターフェイスのインライン パワー検出および電力をディセーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline never
Switch(config-if)# end
Switch#
```

次の例では、ファスト イーサネット インターフェイス 4/1 で永続的な Power over Ethernet 配分を 8000 mW に設定する方法を示します。この場合、検出されたデバイスにおいて 802.3af クラスで指定された電力設定、または受電デバイスから受信した任意の CDP パケットによって指定された電力設定は無視されます。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 4/1
Switch(config-if)# power inline consumption 8000
Switch(config-if)# end
Switch#
```

次の例では、ギガビット イーサネット インターフェイス 2/1 で Power over Ethernet の事前配分を 16500 mW に設定する方法を示します。この場合、検出されたデバイスにおいて 802.3af クラスで指定された電力設定、または受電デバイスから受信した任意の CDP パケットによって指定された電力設定は無視されます。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface gigabitethernet 2/1
Switch(config-if)# power inline static max 16500
Switch(config-if)# end
Switch#
```

関連コマンド

コマンド	説明
show power	電力ステータスに関する情報を表示します。

power inline consumption

1 つのインターフェイスに配分され、スイッチのすべてのインライン パワー対応インターフェイスに適用されるデフォルト電力を設定するには、**power inline consumption** 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。

power inline consumption default *milliwatts*

no power inline consumption default

構文の説明

default	スイッチでデフォルト配分を使用するように指定します。
milliwatts	デフォルトの電力配分をミリワット単位で設定します。有効な範囲は 4000 ～ 15400 です。デフォルト以外の値を設定した場合は、電力配分の自動調整がディセーブルになります。

デフォルト

ミリワット モードは 15400 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 モード

コマンド履歴

リリース	変更内容
12.1(11)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(20)EW	Power over Ethernet のサポートが追加されました。

使用上のガイドライン

使用しているインターフェイスが Power over Ethernet に対応していない場合には、次のメッセージが表示されます。

```
Power over Ethernet not supported on interface Admin
```

例

次の例では、受電デバイスから受信した CDP パケットの種類に関係なく、8000 mW を使用するように Power over Ethernet 配分を設定する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline consumption default 8000
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
power inline	インライン パワー対応インターフェイスのインライン パワー ステートを設定します。
show power	電力ステータスに関する情報を表示します。

power inline police

特定のインターフェイスで PoE ポリシングを設定するには、**power inline police** コマンドを使用します。インターフェイスで PoE ポリシ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。

power inline police [**action**] [**errdisable** | **log**]

no power inline police [**action**] [**errdisable** | **log**]

構文の説明

action	（任意）PoE ポリシング障害が発生した場合（デバイスの消費電力が配分電力を超える）場合にポートで実行するアクションを指定します。
errdisable	（任意）インターフェイスで PoE ポリシングをイネーブルにし、PoE ポリシング障害が発生した場合にポートを errdisable ステートにします。
log	（任意）インターフェイスで PoE ポリシングをイネーブルにし、PoE ポリシング障害が発生した場合にポートをシャットダウンおよび再起動し、エラー メッセージをロギングします。

デフォルト

PoE ポリシ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 モード

コマンド履歴

リリース	変更内容
12.2(50)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

PoE ポリシング障害が原因でポートが errdisable ステートになった場合、インターフェイスで **shut** コマンド、**no shut** コマンドの順に入力して、ポートを再び稼動させてください。

また、インライン パワー errdisable 自動回復を設定して、errdisable 自動回復タイマーが切れたときに errdisable ステートのインターフェイスが自動的に回復されるようにすることもできます。

例

次の例では、PoE ポリシングをイネーブルにし、ポリシング アクションを設定する方法を示します。

```
Switch(config)# int gigabitEthernet 2/1
Switch(config-if)# power inline police
Switch(config-if)# do show power inline police gigabitEthernet 2/1
Available:421(w)  Used:39(w)  Remaining:382(w)

Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1     auto   on         errdisable ok         17.4   7.6


Switch(config-if)# power inline police action log
Available:421(w)  Used:39(w)  Remaining:382(w)
```

```
Interface Admin  Oper       Admin      Oper       Cutoff Oper
          State  State      Police     Police     Power  Power
--------- ------ ---------- ---------- ---------- ------ -----
Gi2/1     auto   on         log        ok         17.4   9.6
```

関連コマンド

コマンド	説明
show power inline police	インターフェイス、モジュール、またはシャーシの PoE ポリシング ステータスを表示します。
errdisable recovery	errdisable 自動回復をイネーブルにします。ポートは、errdisable 自動回復タイマーが切れると、errdisable ステートに移行してから自動的に再起動されます。

power redundancy-mode

シャーシの電源設定を行うには、**power redundancy-mode** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **default** 形式を使用します。

power redundancy-mode {**redundant** | **combined**}

default power redundancy-mode

構文の説明

redundant	スイッチを冗長電源管理モードに設定します。
combined	スイッチを複合電源管理モードに設定します。

デフォルト

冗長電源管理モード

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。 （Catalyst 4500 シリーズ スイッチのみ：4503、4506、および 4507）

使用上のガイドライン

2 つの電源装置は、同じタイプで同じワット数である必要があります。

注意　スイッチに搭載されている電源装置のタイプやワット数が異なる場合、スイッチは電源装置の一方を認識しません。冗長モードに設定したスイッチには、電源冗長がありません。複合モードに設定したスイッチでは、1 つの電源装置だけが使用されます。

冗長モードでは、単一の電源装置からスイッチのコンフィギュレーションをサポートするのに十分な電力を供給する必要があります。

表 2-9 に、シャーシおよび Power over Ethernet で利用可能な最大電力を電源装置ごとに示します。

表 2-9　利用可能な電力

電源モジュール	冗長モード（W）	複合モード（W）
1000 W AC	システム[1] = 1000 インライン = 0	システム = 1667 インライン = 0
2800 W AC	システム = 1360 インライン = 1400	システム = 2473 インライン = 2333

1. システム電力は、スーパーバイザ エンジン、すべてのモジュール、およびファン トレイの電力で構成されます。

例

次の例では、電源管理モードを複合モードに設定する方法を示します。

```
Switch(config)# power redundancy-mode combined
Switch(config)#
```

関連コマンド

コマンド	説明
show power	電力ステータスに関する情報を表示します。

priority

完全優先キュー（Low Latency Queueing（LLQ; 低遅延キューイング））をイネーブルにして、物理ポートに対応付けられているポリシー マップに属するトラフィックのクラスにプライオリティを指定するには、**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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

priority

no priority

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

完全優先キューはディセーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

物理ポートに対応付けられているポリシー マップ内でのみ **priority** コマンドを使用します。このコマンドは、class-level クラスでのみ使用でき、class-default クラスでは使用できません。

このコマンドでは、LLQ を設定し、完全優先キューイングを提供します。完全優先キューイングを使用すると、他のキューにあるパケットが送信される前に、音声などの遅延の影響を受けやすいデータを送信できます。優先キューは、空になるまで最初に処理されます。

bandwidth、**dbl**、および **shape** ポリシーマップ クラス コンフィギュレーション コマンドと **priority** ポリシーマップ クラス コンフィギュレーション コマンドを同じポリシー マップ内の同一クラスで使用することはできません。ただし、これらのコマンドを同じポリシー マップで使用することはできます。

priority ポリシー マップ クラス コンフィギュレーション コマンドとともに、police または set クラス コンフィギュレーション コマンドを使用できます。

優先キューイング クラスでレート制限をしていない場合、bandwidth コマンドは使用できず、代わりに bandwidth remaining percent コマンドを使用できます。

例

次の例では、*policy1* というポリシー マップ用の LLQ 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)# policy-map policy1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
```

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
bandwidth	物理ポートに適用されているポリシー マップに属するクラスに割り当てる最小帯域幅を指定または変更します。
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
dbl	このクラスに一致するトラフィックに対してダイナミック バッファ制限をイネーブルにします。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。
shape（クラスベース キューイング）	物理ポートに適用されているポリシー マップに含まれるトラフィック クラスのトラフィック シェーピングをイネーブルにします。
show policy-map	ポリシー マップ情報を表示します。

private-vlan

プライベート VLAN を設定し、プライベート VLAN とセカンダリ VLAN 間のアソシエーションを設定するには、**private-vlan** 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。

private-vlan {**isolated** | **community** | **primary**}

private-vlan association *secondary-vlan-list* [{**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}]

no private-vlan {**isolated** | **community** | **primary**}

no private-vlan association

構文の説明

isolated	VLAN を独立プライベート VLAN として指定します。
community	VLAN をコミュニティ プライベート VLAN として指定します。
primary	VLAN をプライマリ プライベート VLAN として指定します。
association	セカンダリ VLAN とプライマリ VLAN とのアソシエーションを作成します。
secondary-vlan-list	セカンダリ VLAN の番号を指定します。
add	（任意）セカンダリ VLAN をプライマリ VLAN に関連付けます。
remove	（任意）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。

デフォルト

プライベート VLAN は設定されていません。

コマンド モード

VLAN コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(12c)EW	拡張アドレッシングのサポートが追加されました。
12.2(20)EW	コミュニティ VLAN のサポートが追加されました。

使用上のガイドライン

VLAN 1 または VLAN 1001 ～ 1005 をプライベート VLAN として設定することはできません。

VTP では、プライベート VLAN はサポートされません。プライベート VLAN ポートを使用するデバイスごとに、プライベート VLAN を設定する必要があります。

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 の範囲です。

secondary_vlan_list パラメータには、複数のコミュニティ VLAN ID を含めることができます。

secondary_vlan_list パラメータには、1 つの独立 VLAN ID だけを含めることができます。プライベート VLAN は、VLAN 番号ペアの共通のセットを特徴とするプライベート ポートのセットとして定義されます。各ペアは、少なくとも 2 つの特別な単方向 VLAN から構成され、スイッチと通信するために独立ポートまたはポートのコミュニティによって使用されます。

独立 VLAN は、混合ポートと通信するために独立ポートによって使用される VLAN です。独立 VLAN トラフィックは同じ VLAN 上の他のすべてのプライベート ポートでブロックされ、対応するプライマリ VLAN に割り当てられた標準トランキング ポートおよび混合ポートによってのみ受信できます。

コミュニティ VLAN は、対応するプライマリ VLAN 上でコミュニティ ポート間のトラフィックおよびコミュニティ ポートから混合ポートへのトラフィックを伝送する VLAN です。コミュニティ VLAN をプライベート VLAN トランク上で使用することはできません。

混合ポートは、プライマリ VLAN に割り当てられたプライベート ポートです。

プライマリ VLAN は、トラフィックをスイッチからプライベート ポート上のカスタマー エンド ステーションへ伝送する VLAN です。

独立 *vlan-id* 値は 1 つしか指定できません。一方、コミュニティ VLAN は複数指定できます。独立 VLAN およびコミュニティ VLAN は、1 つの VLAN にだけ関連付けることができます。関連付けられた VLAN リストには、プライマリ VLAN が含まれていてはなりません。同様に、すでにプライマリ VLAN に関連付けられている VLAN は、プライマリ VLAN として設定できません。

config-VLAN サブモードを終了するまで、**private-vlan** コマンドは作用しません。

プライマリ VLAN またはセカンダリ VLAN を削除すると、その VLAN に関連付けされたポートは非アクティブになります。

コンフィギュレーションに関する注意事項の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』を参照してください。

例

次の例では、VLAN 202 をプライマリ VLAN として設定し、そのコンフィギュレーションを確認する方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# end
Switch# show vlan private-vlan
Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
```

次の例では、VLAN 303 をコミュニティ VLAN として設定し、そのコンフィギュレーションを確認する方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 303
Switch(config-vlan)# private-vlan community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
```

次の例では、VLAN 440 を独立 VLAN として設定し、そのコンフィギュレーションを確認する方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 440
```

```
Switch(config-vlan)# private-vlan isolated
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
```

次の例では、プライマリ VLAN 14、独立 VLAN 19、およびコミュニティ VLAN 20 ～ 21 間のプライベート VLAN 関係を作成する方法を示します。

```
Switch(config)# vlan 19
Switch(config-vlan) # private-vlan isolated
Switch(config)# vlan 14
Switch(config-vlan)# private-vlan primary
Switch(config-vlan)# private-vlan association 19
```

次の例では、プライベート VLAN 関係を削除し、プライマリ VLAN を削除する方法を示します。関連付けられたセカンダリ VLAN は削除されません。

```
Switch(config-vlan)# no private-vlan 14
Switch(config-vlan)#
```

次の例では、コミュニティ VLAN 303 ～ 307、309、および独立 VLAN 440 をプライマリ VLAN 202 に関連付け、そのコンフィギュレーションを確認する方法を示します。

```
Switch# configure terminal
Switch(config)# vlan 202
Switch(config-vlan)# private-vlan association 303-307,309,440
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202     303       community
202     304       community
202     305       community
202     306       community
202     307       community
202     309       community
202     440       isolated
        308       community
```

（注） セカンダリ VLAN 308 には、プライマリ VLAN が関連付けられていません。

次の例では、独立 VLAN をプライベート VLAN アソシエーションから削除する方法を示します。

```
Switch(config)# vlan 14
Switch(config-vlan)# private-vlan association remove 18
Switch(config-vlan)#
```

次の例では、インターフェイス FastEthernet 5/1 を PVLAN ホスト ポートとして設定し、その設定を確認する方法を示します。

```
Switch# configure terminal
Switch(config)# interface fastethernet 5/1
Switch(config-if)# switchport mode private-vlan host
Switch(config-if)# switchport private-vlan host-association 202 440
Switch(config-if)# end
Switch# show interfaces fastethernet 5/1 switchport
```

```
Name: Fa5/1
Switchport: Enabled
Administrative Mode: private-vlan host
Operational Mode: private-vlan host
Administrative Trunking Encapsulation: negotiate
Operational Trunking Encapsulation: native
Negotiation of Trunking: Off
Access Mode VLAN: 1 (default)
Trunking Native Mode VLAN: 1 (default)
Voice VLAN: none
Appliance trust: none
Administrative Private Vlan
  Host Association: 202 (VLAN0202) 440 (VLAN0440)
  Promiscuous Mapping: none
  Trunk encapsulation : dot1q
  Trunk vlans:
Operational private-vlan(s):
  202 (VLAN0202) 440 (VLAN0440)
Trunking VLANs Enabled: ALL
Pruning VLANs Enabled: 2-1001
Capture Mode Disabled
Capture VLANs Allowed: ALL
```

関連コマンド

コマンド	説明
show vlan	VLAN 情報を表示します。
show vlan private-vlan	プライベート VLAN 情報を表示します。

private-vlan mapping

プライマリ VLAN とセカンダリ VLAN が同じプライマリ VLAN SVI を共有するように、これらの間のマッピングを作成するには、**private-vlan mapping** コマンドを使用します。すべての PVLAN マッピングを SVI から削除するには、このコマンドの **no** 形式を使用します。

private-vlan mapping *primary-vlan-id* {[*secondary-vlan-list* | {**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}]}

no private-vlan mapping

構文の説明

primary-vlan-id	PVLAN 関係のプライマリ VLAN の VLAN ID です。
secondary-vlan-list	（任意）プライマリ VLAN にマッピングするセカンダリ VLAN の VLAN ID です。
add	（任意）セカンダリ VLAN をプライマリ VLAN 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 間のマッピングを削除します。

デフォルト

すべての PVLAN マッピングが削除されます。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

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 PVLAN ID またはハイフンで連結した PVLAN ID の範囲です。

このコマンドは、プライマリ VLAN のインターフェイス コンフィギュレーション モードで有効です。

プライマリ VLAN の SVI は、レイヤ 3 で作成されます。

セカンダリ VLAN で受信されたトラフィックは、プライマリ VLAN の SVI によってルーティングされます。

既存のセカンダリ VLAN の SVI は機能せず、このコマンドが入力されたあとはダウンしていると見なされます。

セカンダリ SVI は、1 つのプライマリ SVI だけにマッピングできます。設定された PVLAN アソシエーションがこのコマンドで指定されたものと異なる場合（指定された *primary-vlan-id* がセカンダリ VLAN として設定されている場合）、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 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、マッピングのコンフィギュレーションは作用しません。

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(config)# interface vlan 18
Switch(config-if)# private-vlan mapping 18 20
Switch(config-if)#
```

次の例では、PVLAN 303 ～ 307、309、および 440 からのセカンダリ VLAN 入力トラフィックのルーティングを許可し、そのコンフィギュレーションを確認する方法を示します。

```
Switch# config terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            isolated
vlan202   304            isolated
vlan202   305            isolated
vlan202   306            isolated
vlan202   307            isolated
vlan202   309            isolated
vlan202   440            isolated
Switch#
```

次の例では、追加する VLAN がすでに VLAN 18 の SVI にマッピングされている場合に表示されるメッセージを示します。まず、VLAN 18 の SVI からマッピングを削除する必要があります。

```
Switch(config)# interface vlan 19
Switch(config-if)# private-vlan mapping 19 add 21
    Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Switch(config-if)#
```

次の例では、VLAN 19 の SVI からすべての PVLAN マッピングを削除する方法を示します。

```
Switch(config)# interface vlan 19
Switch(config-if)# no private-vlan mapping
Switch(config-if)#


Switch# configure terminal
Switch(config)# interface vlan 202
Switch(config-if)# private-vlan mapping add 303-307,309,440
Switch(config-if)# end
Switch# show interfaces private-vlan mapping
Interface Secondary VLAN Type
--------- -------------- -----------------
vlan202   303            community
vlan202   304            community
vlan202   305            community
vlan202   306            community
vlan202   307            community
vlan202   309            community
vlan202   440            isolated

Switch#
```

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN SVI の PVLAN のマッピング情報を表示します。
show vlan	VLAN 情報を表示します。
show vlan private-vlan	プライベート VLAN 情報を表示します。

private-vlan synchronize

セカンダリ VLAN をプライマリ VLAN として同じインスタンスにマッピングするには、**private-vlan synchronize** コマンドを使用します。

private-vlan synchronize

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

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

MST コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

MST コンフィギュレーション サブモードを終了するときに VLAN を関連プライマリ VLAN として同じインスタンスにマッピングしないと、警告メッセージが表示され、関連プライマリ VLAN として同じインスタンスにマッピングされていないセカンダリ VLAN のリストが示されます。**private-vlan synchronize** コマンドを使用すると、すべてのセカンダリ VLAN が関連プライマリ VLAN として同じインスタンスに自動的にマッピングされます。

例

次の例では、PVLAN 同期を初期化する方法を示します。

```
Switch(config-mst)# private-vlan synchronize
Switch(config-mst)#
```

次の例では、プライマリ VLAN 2 およびセカンダリ VLAN 3 が VLAN 2 に関連付けられ、すべての VLAN が CIST インスタンス 1 にマッピングされていると仮定します。この例では、プライマリ VLAN 2 だけのマッピングを変更しようとした場合の出力も示します。

```
Switch(config)# spanning-tree mst configuration
Switch(config-mst)# instance 1 vlan 2
Switch(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
->3
Switch(config)#
```

関連コマンド

コマンド	説明
show spanning-tree mst	MST プロトコル情報を表示します。

profile

プロファイル call-home コンフィギュレーション サブモードを開始するには、call-home コンフィギュレーション モードで **profile** コマンドを使用します。

profile *profile_name*

構文の説明

profile_name	プロファイル名を指定します。

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

cfg-call-home

コマンド履歴

リリース	変更内容
12.2(52)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

call-home モードで **profile** *profile_name* コマンドを入力すると、プロンプトが Switch(cfg-call-home-profile)# に変わり、次のプロファイル 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。

- **active**
- **destination address**
- **destination message-size-limit bytes**
- **destination preferred-msg-format**
- **destination transport-method**
- **end**
- **exit**
- **subscribe-to-alert-group all**
- **subscribe-to-alert-group configuration**
- **subscribe-to-alert-group diagnostic**
- **subscribe-to-alert-group environment**
- **subscribe-to-alert-group inventory**
- **subscribe-to-alert-group syslog**

例

次の例では、ユーザ定義の call-home プロファイルを作成および設定する方法を示します。

```
Switch(config)# call-home
Switch(cfg-call-home)# profile cisco
Switch(cfg-call-home-profile)# destination transport-method http
Switch(cfg-call-home-profile)# destination address http
https://172.17.46.17/its/service/oddce/services/DDCEService
Switch(cfg-call-home-profile)# subscribe-to-alert-group configuration
Switch(cfg-call-home-profile)# subscribe-to-alert-group diagnostic severity normal
Switch(cfg-call-home-profile)# subscribe-to-alert-group environment severity notification
Switch(cfg-call-home-profile)# subscribe-to-alert-group syslog severity notification
pattern "UPDOWN"
Switch(cfg-call-home-profile)# subscribe-to-alert-group inventory periodic daily 21:12
```

関連コマンド

コマンド	説明
destination address	Call Home メッセージの送信先となる宛先電子メール アドレスまたは URL を設定します。
destination message-size-limit bytes	宛先プロファイルの最大宛先メッセージ サイズを設定します。
destination preferred-msg-format	優先するメッセージ形式を設定します。
destination transport-method	メッセージの転送形式をイネーブルにします。
subscribe-to-alert-group all	使用可能なすべてのアラート グループに加入します。
subscribe-to-alert-group configuration	宛先プロファイルをコンフィギュレーション アラート グループに加入させます。
subscribe-to-alert-group diagnostic	宛先プロファイルを診断アラート グループに加入させます。
subscribe-to-alert-group environment	宛先プロファイルを環境アラート グループに加入させます。
subscribe-to-alert-group inventory	宛先プロファイルを目録アラート グループに加入させます。
subscribe-to-alert-group syslog	宛先プロファイルを Syslog アラート グループに加入させます。

qos（グローバル コンフィギュレーション モード）

スイッチで QoS 機能をグローバルにイネーブルにするには、**qos** コマンドを使用します。QoS 機能をグローバルに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。

qos

no qos

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

QoS 機能はディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。Supervisor Engine 6-E および Catalyst 4900M シャーシでは、QoS は常に設定なしでイネーブルになっています。

QoS 機能をグローバルにイネーブルにすると、QoS がディセーブルになっているインターフェイスを除くすべてのインターフェイスでイネーブルになります。QoS 機能をグローバルにディセーブルにすると、すべてのトラフィックが QoS パススルー モードで渡されます。

例

次の例では、スイッチで QoS 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)# qos
Switch(config)#
```

関連コマンド

コマンド	説明
qos（インターフェイス コンフィギュレーション モード）	インターフェイスで QoS 機能をイネーブルにします。
show qos	QoS 情報を表示します。

qos（インターフェイス コンフィギュレーション モード）

インターフェイスで QoS 機能をイネーブルにするには、**qos** コマンドを使用します。インターフェイスで QoS 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

qos

no qos

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

QoS はイネーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。Supervisor Engine 6-E および Catalyst 4900M シャーシでは、サービス ポリシーを対応付けることにより、スーパーバイザ エンジンで QoS が暗黙的にイネーブルになり、サービス ポリシーの対応付けを解除すると、スーパーバイザ エンジンで QoS が暗黙的にディセーブルになります。

QoS 機能をグローバルにディセーブルにすると、すべてのインターフェイスで QoS 機能がディセーブルになります。

例

次の例では、インターフェイスで QoS 機能をイネーブルにする方法を示します。

```
Switch(config-if)# qos
Switch(config-if)#
```

関連コマンド

コマンド	説明
qos（グローバル コンフィギュレーション モード）	スイッチで QoS 機能をイネーブルにします。
qos（インターフェイス コンフィギュレーション モード）	インターフェイスで QoS 機能をイネーブルにします。
show qos	QoS 情報を表示します。

qos account layer2 encapsulation

QoS 機能で考慮される追加バイトを指定するには、**qos account layer2 encapsulation** コマンドを使用します。追加バイトの使用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。

qos account layer2 encapsulation {**arpa** | **dot1q** | **isl** | **length** *len*}

no qos account layer2 encapsulation {**arpa** | **dot1q** | **isl** | **length** *len*}

構文の説明

arpa	イーサネット ARPA カプセル化パケット長を指定します（18 バイト）。
dot1q	802.1Q カプセル化パケット長を指定します（22 バイト）。
isl	ISL カプセル化パケット長を指定します（48 バイト）。
length *len*	考慮する追加パケット長を指定します。有効な範囲は 0 ～ 64 バイトです。

デフォルト

Supervisor Engine 6-E 以外では、IP パケットの IP ヘッダー内の指定の長さ、および非 IP パケットのイーサネット ヘッダー内の指定の長さのみが考慮されます。

Supervisor Engine 6-E および Catalyst 4900M シャーシでは、IP および非 IP パケットのどちらの場合も、イーサネット ヘッダー内の指定の長さが考慮されます。レイヤ 2 の長さには、VLAN タグのオーバーヘッドも含まれます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

Catalyst 4500 シリーズ スイッチでは、Supervisor Engine 6-E 以外のスーパーバイザの場合、**qos account layer2 encapsulation** コマンドを使用すると、ポリシング機能で IP パケットをポリシングするときに、IP パケット長だけでなく、設定した長さも考慮されます。

共有およびシェーピングには、常にイーサネット ARPA 長が使用されます。

Supervisor Engine 6-E および Catalyst 4900M シャーシのスーパーバイザでは、シェーピングおよび共有には、20 バイトの IPv6 オーバーヘッドが常時ポリシング用に追加されるイーサネット ARPA 長が常に使用されます。ただし、VLAN タグのオーバーヘッドを含むレイヤ 2 の長さのみが考慮されます。

（注）　指定の長さは、受信時のカプセル化タイプに関係なく、すべての IP パケットをポリシングするときに考慮されます。**qos account layer2 encapsulation isl** を設定した場合は、ISL カプセル化を使用して受信される IP パケットだけでなく、すべての IP パケットをポリシングするときに、48 バイトの固定長が考慮されます。

共有およびシェーピングには、レイヤ 2 ヘッダーで指定された長さが使用されます。

例

次の例では、IP パケットをポリシングするときに、追加の 18 バイトを考慮する方法を示します。

```
Switch# config terminal
Switch(conf)# qos account layer2 encapsulation length 18
Switch (conf)# end
Switch#
```

次の例では、QoS 機能でレイヤ 2 カプセル化の考慮をディセーブルにする方法を示します。

```
Switch# config terminal
Switch(config)# no qos account layer2 encapsulation
Switch (config)# end
Switch #
```

関連コマンド

コマンド	説明
show interfaces	特定のインターフェイスのトラフィックを表示します。
switchport	レイヤ 2 スイッチ インターフェイスのスイッチング特性を変更します。
switchport block	不明なマルチキャスト パケットまたはユニキャスト パケットが転送されるのを防ぎます。

qos aggregate-policer

名前付き集約ポリサーを定義するには、**qos aggregate-policer** コマンドを使用します。名前付き集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

qos aggregate-policer *name rate burst* [**conform-action** {**transmit** | **drop**} | **exceed-action** {**transmit** | **drop** | **policed-dscp-transmit**}]

no qos aggregate-policer *name*

構文の説明

name	集約ポリサーの名前です。
rate	最大ビット/秒です。有効値の範囲は 32000 ～ 32000000000 です。
burst	バースト バイトです。有効値の範囲は 1000 ～ 512000000 です。
conform-action	（任意）レートを超えない場合に実行するアクションを指定します。
transmit	（任意）パッケージを送信します。
drop	（任意）パケットをドロップします。
exceed-action	（任意）QoS 値を超えた場合のアクションを指定します。
policed-dscp-transmit	（任意）ポリシング済み DSCP マップ単位で DSCP を送信します。

デフォルト

デフォルト設定は次のとおりです。

- conform-action：transmit
- exceed-action：drop

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

このポリサーは、異なるポリシー マップ クラスおよび異なるインターフェイスで共有できます。

Catalyst 4506 スイッチでは、最大 1000 個の集約入力ポリサーおよび 1000 個の出力ポリサーがサポートされています。

qos aggregate-policer コマンドを使用すると、集約フローおよびその集約のポリシング規則を設定できます。レートおよびバースト パラメータを入力すると、平均レートの範囲は 32 Kbps ～ 32 Gbps となり、バースト サイズの範囲は 1 KB ～ 512 MB となります。

レートは、サフィクスを付けずにビット/秒単位で入力できます。また、表 2-10 に記載されているサフィクスを使用することもできます。

表 2-10　レート サフィクス

サフィクス	説明
k	1000 bps
m	1,000,000 bps
g	1,000,000,000 bps

バーストは、サフィクスを付けずにバイト単位で入力できます。また、表 2-11 に記載されているサフィクスを使用することもできます。

表 2-11　バースト サフィクス

サフィクス	説明
k	1000 バイト
m	1,000,000 バイト
g	1,000,000,000 バイト

（注）　ハードウェアの精度によって、レート値が制限されます。そのため、設定したバーストは実際に使用される値と異なる場合があります。

既存の集約レート制限を変更すると、使用中の場合には NVRAM およびスイッチのエントリが変更されます。

集約ポリサー名を入力するときには、次の命名規則に従ってください。

- 最大 31 文字で、a ～ z、A ～ Z、0 ～ 9、ダッシュ（-）、アンダースコア（_）、およびピリオド（.）を含むことができます。
- 英文字で始まり、すべてのタイプのすべての ACL で一意である必要があります。
- 集約ポリサー名の大文字と小文字は区別されます。
- 数字は使用できません。
- キーワードは使用できません。避けるべきキーワードは、**all**、**default-action**、**map**、**help**、および **editbuffer** です。

集約ポリサーは、1 つまたは複数のインターフェイスに適用できます。ただし、あるインターフェイスの入力方向と、別のインターフェイスの出力方向に同じポリサーを適用すると、スイッチング エンジン上で 2 つの異なる同等の集約ポリサーを作成したことになります。各ポリサーでは、同じポリシング パラメータが使用されます。一方のパラメータは 1 つのインターフェイスの入力トラフィックのポリシングに使用され、もう一方のパラメータは別のインターフェイスの出力トラフィックのポリシングに使用されます。集約ポリサーを複数のインターフェイスに同じ方向で適用した場合、スイッチング エンジン上に作成されるそのポリサーのインスタンスは 1 つだけです。

集約ポリサーは物理インターフェイスまたは VLAN に適用できます。同じ集約ポリサーを物理インターフェイスおよび VLAN に適用した場合、スイッチング エンジン上で 2 つの異なる同等の集約ポリサーを作成したことになります。各ポリサーでは、同じポリシング パラメータが使用されます。一方のパラメータは設定された物理インターフェイス上のトラフィックのポリシングに使用され、もう一方のパラメータは設定された VLAN 上のトラフィックのポリシングに使用されます。集約ポリサーを複数のポートのみ、または複数の VLAN のみに適用した場合、スイッチング エンジン上に作成されるそのポリサーのインスタンスは 1 つだけです。

1 つの集約ポリサーを複数のポートおよび VLAN に異なる方向で適用した場合、同等の 4 つの集約ポリサー（入力方向でポリサーを共有するすべてのポート用、出力方向でポリサーを共有するすべてのポート用、入力方向でポリサーを共有するすべての VLAN 用、および出力方向でポリサーを共有するすべての VLAN 用の集約ポリサー）を作成したことになります。

例

次の例では、QoS 集約ポリサーが最大 100,000 ビット / 秒のレートおよび 10,000 バイトの通常バースト サイズを許可し、これらのレートを超過しない場合にはパケットを送信し、これらのレートを超過した場合にはパケットをドロップするよう設定する方法を示します。

```
Switch(config)# qos aggregate-policer micro-one 100000 10000 conform-action transmit exceed-action drop
Switch(config)#
```

関連コマンド

コマンド	説明
show qos aggregate policer	QoS 集約ポリサー情報を表示します。

qos control-packets

制御パケットでレイヤ 2 制御パケット QoS モードをイネーブルにするには、**qos control-packets** コマンドを使用します。制御パケットでレイヤ 2 制御パケット QoS モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

qos control-packets {**bpdu-range** | **cdp-vtp** | **sstp** | **lldp**}

no qos control-packets {**bpdu-range** | **cdp-vtp** | **sstp** | **lldp**}

構文の説明

bpdu-range	BPDU 範囲パケットで QoS をイネーブルにするように指定します。
cdp-vtp	CDP および VTP パケットで QoS をイネーブルにするように指定します。
sstp	SSTP パケットで QoS をイネーブルにするように指定します。
lldp	LLDP パケットで QoS をイネーブルにするように指定します。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(46)SG	**lldp** キーワードのサポートが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

表 2-12 に、関連コマンドの入力時にレイヤ 2 制御パケット QoS が作用するアドレス範囲を示します。

表 2-12　パケット タイプと作用対象のアドレス範囲

機能がイネーブルになるパケットのタイプ	アドレス範囲
BPDU 範囲	0180.C200.0000 BPDU 0180.C200.0002 OAM, LACP 0180.C200.0003 Eapol
CDP-VTP	0100.0CCC.CCCC
SSTP	0100.0CCC.CCCD
LLDP	0180.C200.000E

（注） どの制御パケット タイプも指定せずに **qos control-packet** を入力した場合、すべてのパケット タイプに対して機能がイネーブルになります。

レイヤ 2 制御パケット QoS をイネーブルにする場合、必要なレイヤ 2 パケットを照合し、それらを必要に応じてポリシングするポリシーを設定する必要があります。この機能が特定のパケット タイプに対してイネーブルであり、MACL が存在しない場合、必要な制御パケットを照合する MACL が自動的に生成されます。これらの MACL と一致する対応クラス マップも自動的に生成されます。次に、制御パケットのポリシングを行うためにこれらのクラス マップをポリシー マップで使用して、他のポリシー マップと同様にこれらをポート単位、VLAN 単位、またはポート単位/VLAN 単位で適用できます。さらに、独自の MACL/クラス マップを定義して、制御パケットを照合することもできます。唯一の制限事項として、ユーザ定義のクラス マップはプレフィクス「system-control-packet-」で開始する必要があります。

例

次の例では、BDPU パケットに対して QoS をイネーブルにする方法を示します。

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets bpdu-range
Switch(config)#
```

次の例では、CDP および VTP パケットに対して QoS をイネーブルにする方法を示します。

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets cdp-vtp
Switch(config)#
```

次の例では、SSTP パケットに対して QoS をイネーブルにする方法を示します。

```
Switch#enable
Switch#configuration terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)#qos control-packets sstp
Switch(config)#
```

次の例では、LLDP パケットに対して QoS をイネーブルにする方法を示します。

```
Switch# enable
Switch# configuration terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# qos control-packets lldp
Switch(config)#
```

関連コマンド

コマンド	説明
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。
show running-config	スイッチの実行コンフィギュレーションを表示します。

qos cos

インターフェイスのデフォルト CoS 値を定義するには、**qos cos** コマンドを使用します。以前の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。

qos cos *cos_value*

no qos cos *cos_value*

構文の説明

cos_value	インターフェイスのデフォルト CoS 値です。有効値の範囲は 0 ～ 7 です。

デフォルト

Supervisor Engine 6-E 以外のスーパーバイザでは、デフォルト CoS 値は 0 です。

Supervisor Engine 6-E および Catalyst 4900M シャーシのスーパーバイザでは、デフォルト CoS は暗黙的に 1 に設定されています。

（注） CoS 無効化は設定されません。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

CoS 値は、物理 LAN ポートでのみ設定できます。

例

次の例では、デフォルト QoS CoS 値を 6 に設定する方法を示します。

```
Switch(config-if)# qos cos 6
Switch(config-if)#
```

関連コマンド

コマンド	説明
show qos	QoS 情報を表示します。

qos dbl

スイッチで Dynamic Buffer Limiting（DBL; ダイナミック バッファ制限）をグローバルにイネーブルにするには、**qos dbl** コマンドを使用します。DBL 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。

qos dbl [**buffers** {**aggressive-flow** *buffers*} | **credits** {**aggressive-flow** *credits* | **maximum** *max*} | **dscp-based** {*value* | *value range*} | **exceed-action** {**ecn** | **probability** *percent*} | **flow** {**include** [**layer4-ports**] [**vlan**]}]

no qos dbl [**buffers** {**aggressive-flow** *buffers*} | **credits** {**aggressive-flow** *credits* | **maximum** *max*} | **dscp-based** {*value* | *value range*} | **exceed-action** {**ecn** | **probability** *percent*} | **flow** {**include** [**layer4-ports**] [**vlan**]}]

構文の説明

buffers	（任意）集約フローのバッファ制限を指定します。
aggressive-flow	（任意）集約フローを指定します。
buffers	（任意）集約フローのバッファ数です。有効値の範囲は 0 ～ 255 です。
credits	（任意）集約フローおよびすべてのフローのクレジット制限を指定します。
credits	（任意）集約フローのクレジット数です。有効値の範囲は 0 ～ 15 です。
maximum	（任意）すべてのフローの最大クレジットを指定します。
max	（任意）すべてのフローのクレジット数です。有効値の範囲は 0 ～ 15 です。
dscp-based	（任意）内部 DSCP のリストに属するパケットを指定します。
value	（任意）単一の DSCP 値です。有効値の範囲は 0 ～ 63 です。
value range	（任意）DSCP 値の範囲です。有効値の範囲は 0 ～ 63 です。カンマ区切りで最大 8 つの DSCP 値を指定できます。
exceed-action	（任意）制限を超えた場合のパケット マーキングを指定します。
ecn	（任意）明示的輻輳通知を指定します。
probability	（任意）パケット マーキングの確率を指定します。
percent	（任意）確率値です。有効値の範囲は 0 ～ 100 です。
flow	（任意）制限するフローを指定します。
include	（任意）レイヤ 4 ポートおよび VLAN をフローに追加できるようにします。
layer4-ports	（任意）フローにレイヤ 4 ポートを含めます。
vlan	（任意）フローに VLAN を含めます。

デフォルト

Supervisor Engine 6-E 以外のスーパーバイザでは、デフォルト設定は次のとおりです。

- QoS DBL はディセーブルです。
- aggressive-flow buffers は 2 に設定されています。
- aggressive-flow credits は 2 に設定され、制限は 10 です。
- レイヤ 4 ポートは追加されます。
- VLAN は追加されます。
- 15 個までのクレジットが許可されます。
- 15% のドロップ確率が設定されています。
- DSCP 値が含まれます。

Supervisor Engine 6-E および Catalyst 4900M シャーシのスーパーバイザでは、デフォルトの dbl 値は暗黙的に設定されており、変更できません。設定は次のとおりです。

- 7 個までのクレジットが許可されます。
- aggressive-flow credits は 4 に設定されています。
- aggressive-flow buffers は 4 に設定されています。
- 6% のドロップ確率が設定されています。
- レイヤ 2 パケットのハッシュ関数では、送信元および宛先 MAC アドレスと送信 VLAN ID が使用されます。
- IPv4 および IPv6 パケットのハッシュ関数では、送信元および宛先 IP アドレス、送信元および宛先レイヤ 4 ポート、送信 VLAN ID 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 モード

QoS ポリシーマップ クラス コンフィギュレーション

コマンド履歴

リリース	変更内容
12.1(13)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(37)SG	DSCP ベースのフロー管理のサポートが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

例

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

```
Switch(config)# qos dbl
Global DBL enabled
Switch(config)#
```

次の例では、QoS 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 DBL をイネーブルにする方法を示します。

```
Switch(config)# class-map c1
Switch(config-cmap)# policy-map p1
Switch(config-pmap)# class c1
Switch(config-pmap-c)# dbl
Switch(config-pmap-c)#
```

次の例では、DSCP 値 1 ～ 10 の DBL を選択的にイネーブルにする方法を示します。

```
Switch# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# qos dbl dscp-based 1-10
Switch(config)# end
Switch# show qos dbl
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion
    DBL exceed-action probability: 15%
    DBL max credits: 15
```

```
    DBL aggressive credit limit: 10
    DBL aggressive buffer limit: 2 packets
    DBL DSCPs with default drop probability:
         1-10
```

次の例では、DSCP 値 1 ～ 10 の DBL を選択的にディセーブルにする方法を示します。

```
Switch# configure t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# no qos dbl dscp-based 1-5, 7
Switch(config)# end
Switch# show qos dbl
    DBL flow includes vlan
    DBL flow includes layer4-ports
    DBL does not use ecn to indicate congestion DBL exceed-action probability: 15% DBL max
    credits: 15 DBL aggressive credit limit: 10 DBL aggressive buffer limit: 2 packets DBL
    DSCPs with default drop probability:
         0,6,8-63
```

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

関連コマンド

コマンド	説明
show qos dbl	QoS Dynamic Buffer Limiting（DBL; ダイナミック バッファ制限）情報を表示します。

qos dscp

インターフェイスのデフォルト CoS 値を定義するには、**qos dscp** コマンドを使用します。以前の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。

qos dscp *dscp_value*

no qos dscp *dscp_value*

構文の説明

dscp_value	インターフェイスのデフォルト DSCP 値です。有効値の範囲は 0 ～ 63 です。

デフォルト

Supervisor Engine 6-E 以外のスーパーバイザでは、デフォルト DSCP 値は 0 です。

Supervisor Engine 6-E および Catalyst 4900M シャーシのスーパーバイザでは、ポート DSCP 値は常に 0 に設定されています。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

例

次の例では、デフォルト QoS DSCP 値を 6 に設定する方法を示します。

```
Switch(config-if)# qos dscp 6
Switch(config-if)#
```

関連コマンド

コマンド	説明
show qos interface	インターフェイスの QoS 情報を表示します。

qos map cos

信頼できるインターフェイスの入力 CoS/DSCP マッピングを定義するには、**qos map cos to dscp** コマンドを使用します。以前の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。

（注）　テーブルから単一のエントリを削除することはできません。

qos map cos *cos_values* **to dscp** *dscp1*

no qos map cos to dscp

構文の説明

cos_values	CoS 値です。最大 8 つの CoS 値をスペースで区切って列挙します。
to dscp	マッピングを定義し、DSCP 値を指定します。
dscp1	CoS 値にマッピングする DSCP 値です。有効値の範囲は 0 ～ 63 です。

デフォルト

次の表に、デフォルトの CoS/DSCP コンフィギュレーション設定を示します。

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。Supervisor Engine 6-E および Catalyst 4900M シャーシでは、この制限されたマッピング機能の代わりに、ポリシー マップ内でパケットのさまざまなマーキング フィールドの設定をサポートしています。詳細については、**set** コマンドを参照してください。

CoS/DSCP マップは、（CoS を信頼するように設定されたインターフェイス上で）パケット CoS を内部 DSCP 値にマッピングするために使用されます。このマップは、8 つの CoS 値（0 ～ 7）およびこれに対応する DSCP 値のテーブルです。スイッチには 1 つのマップがあります。

例

次の例では、CoS 0 の入力 CoS/DSCP マッピングを設定する方法を示します。

```
Switch(config)# qos map cos 0 to dscp 20
Switch(config)#
```

次の例では、CoS/DSCP マッピング テーブル全体をクリアする方法を示します。

```
Switch(config)# no qos map cos 0 to dscp 20
Switch(config)#
```

関連コマンド

コマンド	説明
qos map dscp	選択した送信キューに DSCP 値をマッピングしたり、DSCP/CoS 値をマッピングしたりします。
qos map dscp policed	マークダウンされた DSCP 値へのポリシング済み DSCP 値のマッピングを設定します。
show qos	QoS 情報を表示します。
tablemap（Cisco IOS のマニュアルを参照）	BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

qos map dscp

選択した送信キューに DSCP 値をマッピングしたり、DSCP/CoS 値をマッピングしたりするには、**qos map 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。

qos map dscp *dscp-values* **to tx-queue** *queue-id*

no qos map dscp *dscp-values* **to cos** *cos-value*

構文の説明

dscp-values	キュー ID にマッピングする DSCP 値のリストです。有効値の範囲は 0 ～ 63 です。
to	マッピングを定義します。
tx-queue	送信キューを指定します。
queue-id	送信キューです。有効値の範囲は 1 ～ 4 です。
cos	CoS 値を指定します。
cos-value	サービス クラスです。有効値の範囲は 1 ～ 7 です。

デフォルト

次の表に、デフォルトの DSCP/CoS コンフィギュレーション設定を示します。

DSCP	0 ～ 7	8 ～ 15	16 ～ 23	24 ～ 31	32 ～ 39	40 ～ 47	48 ～ 55	56 ～ 63
CoS	0	1	2	3	4	5	6	7

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。Supervisor Engine 6-E および Catalyst 4900M シャーシでは、このコマンドの代わりに、**tablemap** コマンドを使用して QoS マーキングを行います。詳細については、**tablemap** コマンドを参照してください。

DSCP/CoS マップを使用して、最終 DSCP 分類を最終 CoS にマッピングします。CoS マップは、トランク インターフェイス上の送信済みパケットの ISL ヘッダーまたは 802.1Q タグに書き込まれます。CoS マップには、64 個の DSCP 値およびこれに対応する CoS 値のテーブルが含まれます。スイッチには 1 つのマップがあります。CoS 値については最大 8 つの DSCP 値をスペースで区切って入力できます。

DSCP/ 送信キュー マップは、最終 DSCP 分類を送信キューにマッピングするために使用されます。送信キューについては最大 8 つの DSCP 値をスペースで区切って入力できます。

例

次の例では、出力 DSCP/CoS マッピングを設定する方法を示します。

```
Switch(config)# qos map dscp 20 25 to cos 3
Switch(config)#
```

次の例では、出力 DSCP/送信キューを設定する方法を示します。

```
Switch(config)# qos map dscp 20 25 to tx-queue 1
Switch(config)#
```

関連コマンド

コマンド	説明
qos map cos	信頼できるインターフェイスの入力 CoS/DSCP マッピングを定義します。
show qos interface	キューイング情報を表示します。
show qos	QoS 情報を表示します。
tablemap（Cisco IOS のマニュアルを参照）	BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。
tx-queue	インターフェイスの送信キュー パラメータを設定します。

qos map dscp policed

マークダウンされた DSCP 値へのポリシング済み DSCP 値のマッピングを設定するには、**qos map dscp policed** コマンドを使用します。以前の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。

qos map dscp policed *dscp_list* **to dscp** *policed_dscp*

no qos map dscp policed

構文の説明

dscp_list	DSCP 値です。有効値の範囲は 0 ～ 63 です。
to dscp	マッピングを定義します。
policed_dscp	マークダウンされた DSCP 値です。有効値の範囲は 0 ～ 63 です。

デフォルト

DSCP 値のマッ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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。DSCP の明示的 QoS マーキング、優先順位、および CoS フィールドをサポートする Supervisor Engine 6-E および Catalyst 4900M シャーシでは、さまざまなポリサー タイプがサポートされています。詳細については、**police** コマンドを参照してください。

DSCP/ポリシング済み DSCP マップでは、アウトオブプロファイル フローに適用される、マークダウンされた DSCP 値を判別します。スイッチには 1 つのマップがあります。

最大 8 つの DSCP 値をスペースで区切って入力できます。

ポリシング済み DSCP 値は、1 つだけ入力できます。

（注） シーケンス外のパケットを避けるため、DSCP/ポリシング済み DSCP マップを設定して、マークダウンされたパケットがインプロファイル トラフィックと同じキューに留まるようにします。

例

次の例では、複数の DSCP を単一のポリシング済み DSCP 値にマッピングする方法を示します。

```
Switch(config)# qos map dscp policed 20 25 43 to dscp 4
Switch(config)#
```

関連コマンド

コマンド	説明
qos map cos	信頼できるインターフェイスの入力 CoS/DSCP マッピングを定義します。
qos map dscp	選択した送信キューに DSCP 値をマッピングしたり、DSCP/CoS 値をマッピングしたりします。
show qos	QoS 情報を表示します。

qos rewrite ip dscp

IP パケットの DSCP 書き換えをイネーブルにするには、**qos rewrite ip dscp** コマンドを使用します。IP DSCP 書き換え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。

qos rewrite ip dscp

no qos rewrite ip dscp

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

IP DSCP 書き換えはイネーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

IP DSCP 書き換えをディセーブルにして QoS をグローバルにイネーブルにすると、次のイベントが発生します。

- IP パケットの ToS バイトが修正されません。
- キューイングには、マークおよびマークダウンされた DSCP 値が使用されます。
- 送信キューおよびレイヤ 2 CoS の決定には、（インターフェイスまたは VLAN ポリシー上の信頼できるコンフィギュレーションに基づいて）内部的に生成された DSCP が使用されます。IP パケット ヘッダーにある DSCP 値は書き換えられません。

QoS をディセーブルにした場合、着信パケットの CoS および DSCP 値は保持され、書き換えは行われません。

例

次の例では、IP DSCP 書き換えをディセーブルにする方法を示します。

```
Switch(config)# no qos rewrite ip dscp
Switch(config)#
```

関連コマンド

コマンド	説明
qos（グローバル コンフィギュレーション モード）	スイッチで QoS 機能をイネーブルにします。
show qos	QoS 情報を表示します。

qos trust

インターフェイスの信頼状態（インターフェイスに到達したパケットが正しい CoS、ToS、および DSCP 分類を伝送していると信頼できるかどうかなど）を設定するには、**qos trust** コマンドを使用します。インターフェイスを非信頼状態に設定するには、このコマンドの **no** 形式を使用します。

qos trust {**cos** | *device cisco-phone* | **dscp** | **extend** [**cos** *priority*]}

no qos trust {**cos** | *device cisco-phone* | **dscp** | **extend** [**cos** *priority*]}

構文の説明

cos	着信フレームの CoS ビットを信頼し、CoS ビットから内部 DSCP 値を取得するように指定します。
device cisco-phone	Cisco IP Phone をポートに対して信頼できるデバイスとして指定します。
dscp	着信パケットの ToS ビットに DSCP 値が含まれることを指定します。
extend	PC から着信した Port VLAN ID（PVID; ポート VLAN ID）パケットに対する信頼拡張を指定します。
cos *priority*	（任意）PVID パケットに設定される CoS プライオリティの値を指定します。有効値の範囲は 0 ～ 7 です。

デフォルト

デフォルト設定は次のとおりです。

- グローバル QoS がイネーブルの場合、信頼はポート上でディセーブルになります。
- グローバル QoS がディセーブルの場合、信頼 DSCP はポート上でイネーブルになります。
- CoS プライオリティ レベルは 0 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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.1(11)EW	音声の信頼拡張のサポートが追加されました。
12.1(19)EW	デバイス Cisco IP Phone の信頼サポートが追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

信頼状態を設定できるのは、物理 LAN インターフェイスのみです。

デフォルトでは、QoS がイネーブルの場合、インターフェイスの信頼状態は非信頼です。QoS がインターフェイス上でディセーブルになると、信頼状態は信頼 DSCP にリセットされます。

インターフェイスの信頼状態が **qos trust cos** である場合、送信 CoS は常に着信パケット CoS（または、パケットにタグがない場合にはインターフェイスのデフォルト CoS）です。

インターフェイスの信頼状態が **qos trust dscp** ではない場合、セキュリティおよび QoS ACL 分類では、常にインターフェイス DSCP が使用され、着信パケットの DSCP は使用されません。

EtherChannel に含まれるポート（ポート チャネル）には、信頼境界を設定しないでください。

例

次の例では、インターフェイスの信頼状態を CoS に設定する方法を示します。

```
Switch(config-if)# qos trust cos
Switch(config-if)#
```

次の例では、インターフェイスの信頼状態を DSCP に設定する方法を示します。

```
Switch(config-if)# qos trust dscp
Switch(config-if)#
```

次の例では、PVID CoS レベルを 6 に設定する方法を示します。

```
Switch(config-if)# qos trust extend cos 6
Switch(config-if)#
```

次の例では、Cisco Phone を信頼できるデバイスとして設定する方法を示します。

```
Switch(config-if)# qos trust device cisco-phone
Switch(config-if)#
```

関連コマンド

コマンド	説明
qos cos	インターフェイスのデフォルト CoS 値を定義します。
qos vlan-based	レイヤ 2 インターフェイスの VLAN 単位の QoS を定義します。
show qos interface	インターフェイスの QoS 情報を表示します。

qos vlan-based

レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにするには、**qos vlan-based** コマンドを使用します。レイヤ 2 インターフェイスの VLAN 単位の QoS 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。

qos vlan-based

no qos vlan-based

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

VLAN 単位の QoS はディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。Supervisor Engine 6-E および Catalyst 4900M シャーシでは、インターフェイスおよび VLAN レベルでのさまざまな QoS マーキングおよびポリシング アクションが適切にマージされます。詳細については、『*Catalyst 4500 Series Switch Configuration Guide*』を参照してください。

VLAN ベースのモードでは、レイヤ 2 インターフェイスに対応付けられたポリシー マップは無視され、QoS は対応する VLAN インターフェイスに対応付けられたポリシー マップによって機能します。

VLAN 単位の QoS は、レイヤ 2 インターフェイス上でだけ設定できます。

レイヤ 2 インターフェイスに入力 QoS ポリシーが対応付けられていない場合、ポートが VLAN ベースで設定されていなくても、（パケットが着信する）VLAN に対応付けられた入力 QoS ポリシーがあればそれが使用されます。

このデフォルトが望ましくない場合には、レイヤ 2 インターフェイスにプレースホルダの入力 QoS ポリシーを対応付けます。

同様に、レイヤ 2 インターフェイスに出力 QoS ポリシーが対応付けられていない場合、ポートが VLAN ベースで設定されていなくても、（パケットを送信する）VLAN に対応付けられた出力 QoS ポリシーがあればそれが使用されます。

このデフォルトが望ましくない場合には、レイヤ 2 インターフェイスにプレースホルダの出力 QoS ポリシーを対応付けます。

レイヤ 3 インターフェイスは常にインターフェイスベースのモードです。レイヤ 3 VLAN インターフェイスは常に VLAN ベースのモードです。

例

次の例では、レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにする方法を示します。

```
Switch(config-if)# qos vlan-based
Switch(config-if)#
```

関連コマンド

コマンド	説明
qos cos	インターフェイスのデフォルト CoS 値を定義します。
show qos interface	インターフェイスの QoS 情報を表示します。

queue-limit

ポリシー マップに設定されたクラス ポリシー用のキューに保持できるパケットの最大数を指定または変更するには、**queue-limit** コマンドを使用します。クラスからキューのパケット制限を削除するには、このコマンドの **no** 形式を使用します。

queue-limit *number-of-packets*

no queue-limit *number-of-packets*

構文の説明

number-of-packets	このクラスのキューに蓄積できるパケットの数です。有効な範囲は 16 ～ 8184 です。この数は 8 の倍数にする必要があります。

デフォルト

デフォルトでは、Catalyst 4500 スイッチ上の物理インターフェイスごとに、シャーシ内のスロットの数およびラインカード上のポートの数に基づくデフォルトのキューが用意されています。

コマンド モード

QoS ポリシーマップ クラス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(44)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

この Class-Based Queuing（CBQ; クラスベースド キューイング）コマンドは、Catalyst 4500 スーパーバイザでの MQC サポートの一環として Supervisor 6-E にのみ適用されます。

デフォルトでは、Catalyst 4500 スイッチ上の物理インターフェイスごとに、デフォルトのキューが用意されています。このキューのサイズは、シャーシ内のスロットの数および各スロットのラインカード上のポートの数に基づきます。スイッチでは 512K のキュー エントリがサポートされ、このうち 100K は共通の共有可能プールとして確保されます。残りの 412K のエントリはスロット間で均等に配分されます。さらに、各スロットに配分されたキュー エントリはそれぞれのポート間で均等に分けられます。

CBQ を使用すると、クラス マップが定義されているクラスごとにキューが作成されます。クラスの一致基準を満たすパケットは、送信されるまで、そのクラス用に確保されたキューに蓄積されます。これは、均等化キューイング プロセスによってキューが処理されている場合に行われます。クラスに対して定義した最大パケットしきい値に到達した場合、クラスのキューにさらにパケットがキューイングされると、テール ドロップが発生します。または、クラス ポリシーに DBL が設定されている場合は、パケットのドロップが有効になります。

（注） queue-limit コマンドを出力 QoS ポリシーマップの class-default クラスで設定している場合を除いて、帯域幅、シェーピング、またはプライオリティなどのスケジューリング処理を最初に設定しないと、queue-limit コマンドはサポートされません。

例

次の例では、*acl203* というクラス用のポリシーを含む *policy11* というポリシーマップを設定する方法を示します。このクラスのポリシーは、確保されているキューの最大パケット制限が 40 になるように設定されています。

```
Switch# configure terminal
Switch (config)# policy-map policy11
Switch (config-pmap)# class acl203
Switch (config-pmap-c)# bandwidth 2000
Switch (config-pmap-c)# queue-limit 40
Switch (config-pmap-c)# end
Switch#
```

関連コマンド

コマンド	説明
bandwidth	物理ポートに適用されているポリシー マップに属するクラスに割り当てる最小帯域幅を指定または変更します。
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
shape（クラスベース キューイング）	物理ポートに適用されているポリシー マップに含まれるトラフィック クラスのトラフィック シェーピングをイネーブルにします。

redundancy

冗長コンフィギュレーション モードを開始するには、グローバル コンフィギュレーション モードで **redundancy** コマンドを使用します。

redundancy

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

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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが、Catalyst 4500 シリーズ スイッチに追加されました（Catalyst 4507R および 4510R のみ）。

使用上のガイドライン

冗長コンフィギュレーション モードは、メイン CPU サブモードを開始するために使用します。

メイン CPU サブモードを開始するには、冗長コンフィギュレーション モードで **main-cpu** コマンドを使用します。

メイン CPU サブモードは、2 つのスーパーバイザ エンジン上のコンフィギュレーションを手動で同期化するために使用します。

メイン CPU サブモードで、**auto-sync** コマンドを使用して、NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにします。

冗長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。冗長をディセーブルにしてから、再び冗長をイネーブルにすると、スイッチはデフォルトの冗長設定に戻ります。

冗長コンフィギュレーション モードを終了するには、**exit** コマンドを使用します。

例

次の例では、冗長モードを開始する方法を示します。

```
Switch(config)# redundancy
Switch(config-red)#
```

次の例では、メイン CPU サブモードを開始する方法を示します。

```
Switch(config)# redundancy
Switch(config-red)# main-cpu
Switch(config-r-mc)#
```

関連コマンド

コマンド	説明
auto-sync	NVRAM 内のコンフィギュレーション ファイルの自動同期化をイネーブルにします。
main-cpu	メイン CPU サブモードを開始し、2 つのスーパーバイザ エンジン上のコンフィギュレーションを手動で同期化します。

redundancy config-sync mismatched-commands

アクティブ スーパーバイザとスタンバイ スーパーバイザが異なるバージョンの IOS を実行していると、一部の CLI の互換性がなくなります。このようなコマンドがアクティブ スーパーバイザ エンジンの実行コンフィギュレーション内にすでに存在し、スタンバイ スーパーバイザ エンジンの起動時にこれらのコマンドに対する構文チェックが失敗した場合は、**redundancy config-sync mismatched-commands** コマンドを使用します。このコマンドを使用すると、アクティブ スーパーバイザ エンジンが Mismatched Command List（MCL）に移動され、スタンバイ スーパーバイザ エンジンがリセットされます。

redundancy config-sync {ignore | validate} mismatched-commands

構文の説明

ignore	Mismatched Command List を無視します。
validate	修正した実行コンフィギュレーションに基づいて Mismatched Command List を再確認します。

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 モード

コマンド履歴

リリース	変更内容
12.2(31)SGA	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(44)SG	コマンド構文が issu config-sync から redundancy config-sync に更新されました。

使用上のガイドライン

次に、不一致コマンドのログ エントリの例を示します。

```
00:06:31: Config Sync: Bulk-sync failure due to Servicing Incompatibility. Please check
full list of mismatched commands via:
  show redundancy config-sync failures mcl
00:06:31: Config Sync: Starting lines from MCL file:
interface GigabitEthernet7/7
 ! <submode> "interface"
- ip address 11.0.0.1 255.0.0.0
 ! </submode> "interface"
```

すべての不一致コマンドを表示するには、**show redundancy config-sync failures mcl** コマンドを使用します。

MCL を消去するには、次の手順を実行します。

ステップ 1　アクティブ スーパーバイザ エンジンの実行コンフィギュレーションからすべての不一致コマンドを削除します。

ステップ 2　**redundancy config-sync validate mismatched-commands** コマンドを使用して、修正した実行コンフィギュレーションに基づいて MCL を再確認します。

ステップ 3　スタンバイ スーパーバイザ エンジンをリロードします。

次の手順に従って、MCL を無視することもできます。

ステップ 1　**redundancy config-sync ignore mismatched-commands** コマンドを入力します。

ステップ 2　スタンバイ スーパーバイザ エンジンをリロードします。システムは SSO モードに移行します。

（注）　不一致コマンドを無視する場合、アクティブ スーパーバイザ エンジンおよびスタンバイ スーパーバイザ エンジンの*同期していない*コンフィギュレーションは存在したままです。

ステップ 3　無視した MCL は **show redundancy config-sync ignored mcl** コマンドで確認できます。

例

次の例では、MCL から削除したエントリを確認する方法を示します。

```
Switch# redundancy config-sync validate mismatched-commands
Switch#
```

関連コマンド

コマンド	説明
show redundancy config-sync	ISSU コンフィギュレーション同期障害情報または無視された Mismatched Command List（MCL）を表示します。

redundancy force-switchover

スーパーバイザ エンジンをアクティブからスタンバイに強制的に切り替えるには、**redundancy force-switchover** コマンドを使用します。

redundancy force-switchover

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

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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました（Catalyst 4507R のみ）。

使用上のガイドライン

このコマンドを使用する前に、『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』の「Performing a Software Upgrade」を参照して、さらに詳しい情報を入手してください。

redundancy force-switchover コマンドでは、冗長スーパーバイザ エンジンの手動切り替えを行います。冗長スーパーバイザ エンジンは、Cisco IOS イメージを実行する新しいアクティブ スーパーバイザ エンジンになります。モジュールはリセットされます。

以前のアクティブ スーパーバイザ エンジンが新しいイメージで再起動され、スタンバイ スーパーバイザ エンジンになります。

例

次の例では、アクティブ スーパーバイザ エンジンからスタンバイ スーパーバイザ エンジンに手動で切り替える方法を示します。

```
Switch# redundancy force-switchover
Switch#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。
show redundancy	冗長ファシリティ情報を表示します。

redundancy reload

スーパーバイザ エンジンの一方または両方を強制的にリロードするには、**redundancy reload** コマンドを使用します。

redundancy reload {**peer** | **shelf**}

構文の説明

peer	ピア ユニットをリロードします。
shelf	両方のスーパーバイザ エンジンを再起動します。

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 モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました（Catalyst 4507R のみ）。

使用上のガイドライン

このコマンドを使用する前に、『*Catalyst 4500 Series Switch Cisco IOS Software Configuration Guide*』の「Performing a Software Upgrade」を参照して、さらに詳しい情報を入手してください。

redundancy reload shelf コマンドでは、両方のスーパーバイザ エンジンを再起動します。モジュールはリセットされます。

例

次の例では、一方または両方のスーパーバイザ エンジンを手動でリロードする方法を示します。

```
Switch# redundancy reload shelf
Switch#
```

関連コマンド

コマンド	説明
redundancy	冗長コンフィギュレーション モードを開始します。
show redundancy	冗長ファシリティ情報を表示します。

remote login module

特定のモジュールにリモートから接続するには、**remote login module** コンフィギュレーション コマンドを使用します。

remote login module *mod*

構文の説明

mod	コマンドのターゲット モジュール。

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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドが適用されるのは、Catalyst 4500 シリーズ スイッチのアクセス ゲートウェイ モジュールのみです。

mod の有効値は、使用するシャーシによって異なります。たとえば、Catalyst 4506 シャーシを使用する場合、モジュールに指定できる値は 2 ～ 6 です。4507R シャーシを使用する場合、有効値の範囲は 3 ～ 7 です。

remote login module *mod* コマンドを実行すると、プロンプトが Gateway# に変わります。

remote login module コマンドは、**session module** *mod* および **attach module** *mod* コマンドと同じです。

例

次の例では、アクセス ゲートウェイ モジュールにリモートからログインする方法を示します。

```
Switch# remote login module 5
Attaching console to module 5
Type 'exit' at the remote prompt to end the session

Gateway>
```

関連コマンド

コマンド	説明
attach module	特定のモジュールにリモートから接続します。
session module	仮想コンソールを使用して、スタンバイ スーパーバイザ エンジンにログインします。

remote-span

VLAN を RSPAN VLAN に変換するには、**remote-span** コマンドを使用します。RSPAN VLAN を VLAN に変換するには、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 はディセーブルにされています。

コマンド モード

VLAN コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(20)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、VLAN を RSPAN VLAN に変換する方法を示します。

```
Switch# config terminal
Switch(config)# vlan 20
Switch(config-vlan)# remote-span
Switch(config-vlan)# end
Switch#
```

関連コマンド

コマンド	説明
monitor session	インターフェイスまたは VLAN で SPAN セッションをイネーブルにします。

renew ip dhcp snooping database

DHCP 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** コマンドを使用します。

renew ip dhcp snooping database [**validation none**] [**url**]

構文の説明

validation none	（任意）URL で指定されたファイルの内容に関連付けられたチェックサムを検証しないように指定します。
url	（任意）読み込みの実行元ファイルを指定します。

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 モード

コマンド履歴

リリース	変更内容
12.1(19)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

URL を指定しない場合は、設定された URL からのファイル読み込みが試行されます。

例

次の例では、CRC チェックを省略して、DHCP 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
Switch#
```

関連コマンド

コマンド	説明
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 binding	DHCP バインディング コンフィギュレーションを設定および生成し、再起動後もバインディングを復元します。
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 上で DHCP スヌーピングをイネーブルにします。
ip dhcp snooping vlan	VLAN または VLAN のグループ上で 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 エントリを表示します。

reset

新たに設定しようとしている VLAN データベースを放棄し、引き続き VLAN コンフィギュレーション モードを使用して、現在実装されている VLAN データベースと同じになるように、新たに設定しようとしているデータベースをリセットするには、**reset** コマンドを使用します。

reset

構文の説明

このコマンドには、引数またはキーワードはありません。

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

VLAN コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

例

次の例では、新たに設定しようとしている VLAN データベースを現在の VLAN データベースにリセットする方法を示します。

```
Switch(vlan-config)# reset
RESET completed.
Switch(vlan-config)#
```

revision

MST コンフィギュレーション リビジョン番号を設定するには、**revision** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

revision *version*

no revision

構文の説明

version	コンフィギュレーション リビジョン番号です。有効値の範囲は 0 ～ 65535 です。

デフォルト

リビジョン番号は 0 に設定されています。

コマンド モード

MST コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(12c)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

コンフィギュレーションは同じであるが、リビジョン番号が異なる 2 つの Catalyst 4500 シリーズ スイッチは、それぞれ 2 つの異なる領域に属すると見なされます。

注意　**revision** コマンドを使用して MST コンフィギュレーション リビジョン番号を設定する場合には注意が必要です。設定を間違えると、スイッチは異なる領域に置かれてしまいます。

例

次の例では、コンフィギュレーション リビジョン番号を設定する方法を示します。

```
Switch(config-mst)# revision 5
Switch(config-mst)#
```

関連コマンド

コマンド	説明
instance	1 つの VLAN または一連の VLAN を MST インスタンスにマッピングします。
name	MST 領域名を設定します。
show spanning-tree mst	MST プロトコル情報を表示します。
spanning-tree mst configuration	MST コンフィギュレーション サブモードを開始します。

service-policy（インターフェイス コンフィギュレーション）

ポリシー マップをインターフェイスに対応付けたり、インターフェイスが属する VLAN で異なる QoS ポリシーを適用したりするには、**service-policy** コマンドを使用します。ポリシー マップをインターフェイスから削除するには、このコマンドの **no** 形式を使用します。

service-policy {**input** | **output**} *policy-map name*

no service-policy {**input** | **output**} *policy-map name*

構文の説明

input	入力ポリシー マップを指定します。
output	出力ポリシー マップを指定します。
policy-map name	以前に設定されたポリシー マップの名前です。

デフォルト

ポリシー マップは、インターフェイスや VLAN に対応付けられません。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(25)EWA	VLAN への異なる QoS ポリシーの適用のサポートが追加されました。

使用上のガイドライン

レイヤ 2 インターフェイスは、複数の VLAN の一部であることがあります（一般的なトランク ポートの場合など）。**vlan-range** コマンドとともに **service-policy** コマンドを使用すると、異なる VLAN 上の異なる QoS ポリシーを指定できます。

（注）　この機能は、レイヤ 2 インターフェイスに限定されています。

Supervisor Engine 6-E 以外

ポリシー マップをインターフェイスと VLAN 範囲に同時に適用することはできません。

サービス ポリシーを VLAN に対応付けるには、VLAN の SVI が作成されていて、ポリシーが SVI に適用されていなければなりません。

Supervisor Engine 6-E および Catalyst 4900M シャーシ

サービス ポリシーをインターフェイスと VLAN 範囲に同時に適用できます。ただし、これが許可されるのは、インターフェイス ポリシーにキューイング アクションのみが含まれていて、VLAN には非キューイング アクション（QoS マーキング/ポリシング）のみが含まれている場合のみです。

サービス ポリシーを VLAN に対応付けるには、VLAN コンフィギュレーション モードを使用する必要があります。

例

次の例では、ポリシー マップをファスト イーサネット インターフェイス 5/20 に対応付ける方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# interface fastethernet 5/20
Switch(config-if)# service-policy input pmap1
Switch(config-if)# end
```

次の例では、VLAN 20 および 400 のトラフィックに対してポリシー マップ p1 を適用し、VLAN 300 ～ 301 のトラフィックに対してポリシー マップ p2 を適用する方法を示します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# switchport trunk encapsulation dot1q
Switch(config-if)# switchport mode trunk
Switch(config-if)# vlan-range 20,400
Switch(config-if-vlan-range)# service-policy input p1
Switch(config-if-vlan-range)# exit
Switch(config-if)# vlan-range 300-301
Switch(config-if-vlan-range)# service-policy output p2
Switch(config-if-vlan-range)# end
Switch# show policy-map interface gigabitEthernet 6/1 vlan 20
 GigabitEthernet6/1 vlan 20

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

Switch# show policy-map interface gigabitEthernet 6/1
 GigabitEthernet6/1 vlan 20

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 300

  Service-policy output: p2

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 301

  Service-policy output: p2

    Class-map: class-default (match-any)
      0 packets
```

```
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes

 GigabitEthernet6/1 vlan 400

  Service-policy input: p1

    Class-map: class-default (match-any)
      0 packets
      Match: any
        0 packets
      police: Per-interface
        Conform: 0 bytes Exceed: 0 bytes
```

次の例では、Supervisor Engine 6-E 以外で SVI を使用して VLAN にポリシー マップを対応付ける方法を示します。

```
Switch# configure terminal
Switch(config)#interface vlan 10
Switch(config-if)#service-policy out policy-vlan
Switch(config-if)#end
Switch#
```

次の例では、Supervisor Engine 6-E を使用して VLAN にポリシー マップを対応付ける方法を示します。

```
Switch# configure terminal
Switch(config)#vlan configuration 20
Switch(config-vlan-config)#service-policy out policy-vlan
Switch(config-vlan-config)#end
Switch#
```

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の照合に使用するクラス マップを作成し、クラスマップ コンフィギュレーション モードを開始します。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（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ポリシー マップを適用します。
show policy-map interface vlan	インターフェイス上の特定の VLAN に適用されている QoS ポリシーマップ情報を表示します。

service-policy（ポリシーマップ クラス）

Quality of Service（QoS）であるサービス ポリシーをポリシー マップ（階層型サービス ポリシー）内に作成するには、**service-policy** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。ポリシー マップ内のサービス ポリシー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。

service-policy *policy-map-name*

no service-policy *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

サービス ポリシー マップは定義されていません。

コマンド モード

ポリシーマップ クラス コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E および Catalyst 4900M シャーシのサポートが追加されました。

使用上のガイドライン

物理ポートに対応付けられている階層ポリシー マップ内でのみ **service-policy** コマンドを使用します。このコマンドは、階層のレベル 2 にあるポリシー マップで有効です。

親ポリシー マップでマーキングおよびポリシング アクションを指定し、子ポリシー マップでキューイング アクションを指定することにより、階層を作成できます。

ポリシーマップ クラス コンフィギュレーション モードでこのコマンドを入力した場合、**exit** コマンドを使用してポリシーマップ コンフィギュレーション モードに戻ります。特権 EXEC モードに戻るには、**end** コマンドを使用します。

例

次の例では、「parent」というサービス ポリシーで階層型サービス ポリシーを作成する方法を示します。

```
Switch# configure terminal
Switch(config)# policy-map child
Switch(config-pmap)# class voice
Switch(config-pmap-c)# priority
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# policy-map parent
Switch(config-pmap)# class class1
Switch(config-pmap-c)# police 32k
Switch(config-pmap-c)# service-policy child
Switch#
```

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
bandwidth	名前で参照可能なシグナリング クラス構造を作成します。
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
dbl	トラフィックのクラスが使用する送信キュー上で、アクティブ キュー管理をイネーブルにします。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
priority	完全優先キュー（Low-Latency Queueing（LLQ; 低遅延キューイング））をイネーブルにして、物理ポートに適用されているポリシー マップに属するトラフィックのクラスにプライオリティを指定します。
random-detect（Cisco IOS のマニュアルを参照）	Weighted Random Early Detection（WRED; 重み付けランダム早期検出）または Distributed WRED（DWRED; 分散 WRED）をイネーブルにします。
shape（クラスベース キューイング）	物理ポートに適用されているポリシー マップに含まれるトラフィック クラスのトラフィック シェーピングをイネーブルにします。
show policy-map	ポリシー マップ情報を表示します。

service-policy input（コントロールプレーン）

集約コントロール プレーン サービスのポリシー マップをコントロール プレーンに対応付けるには、**service-policy input** コマンドを使用します。コントロール プレーンからサービス ポリシーを削除するには、このコマンドの **no** 形式を使用します。

service-policy input *policy-map-name*

構文の説明

input	コントロール プレーンに着信するパケットに指定のサービス ポリシーを適用します。
policy-map-name	対応付けるサービス ポリシー マップ（**policy-map** コマンドによって作成）の名前です。

デフォルト

サービス ポリシーは指定されていません。

コマンド モード

コントロール プレーン コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このリリースでは、コントロール プレーンで許可されるポリシーマップは system-cpp-policy のみです。これは、起動時にすでにコントロール プレーンに対応付けられています。何らかのエラー条件が原因で対応付けられていない場合は、**global macro system-cpp** コマンドを使用してコントロール プレーンに対応付けることを推奨します。システムによって作成された system-cpp-policy には、システムによって事前定義された各クラスが含まれています。これらの定義済みクラスでは、ポリシング パラメータを変更することはできますが、それ以外の変更をクラスに加えることは避けるべきです。

独自のクラスマップを定義して、system-cpp-policy ポリシーマップの末尾に追加できます。

例

次の例では、送信元アドレス 10.1.1.1 および 10.1.1.2 を持つ信頼できるホストを設定し、制約を設けずに Telnet パケットをコントロール プレーンに転送する方法を示します。残りのすべての Telnet パケットは、指定のレートでポリシングされるようにします。

```
Switch(config)# access-list 140 deny tcp host 10.1.1.1 any eq telnet
! Allow 10.1.1.2 trusted host traffic.
Switch(config)# access-list 140 deny tcp host 10.1.1.2 any eq telnet
! Rate limit all other Telnet traffic.
Switch(config)# access-list 140 permit tcp any any eq telnet
! Define class-map "telnet-class."
Switch(config)# class-map telnet-class
Switch(config-cmap)# match access-group 140
Switch(config-cmap)# exit
Switch(config)# policy-map control-plane-policy
Switch(config-pmap)# class telnet-class
Switch(config-pmap-c)# police 80000 conform transmit exceed drop
Switch(config-pmap-c)# exit
```

```
Switch(config-pmap)# exit
! Define aggregate control plane service for the active Route Processor.
Switch(config)# control-plane
Switch(config-cp)# service-policy input control-plane-policy
Switch(config-cp)# exit
```

関連コマンド

コマンド	説明
control-plane	コントロール プレーン コンフィギュレーション モードを開始します。
macro global apply system-cpp	コントロール プレーン ポリシングのデフォルト テンプレートをスイッチに適用します。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
show policy-map control-plane	1 つまたはすべてのクラスについて、コントロール プレーンのポリシー マップのコンフィギュレーションを表示します。

session module

（注）　このコマンドは SSO モードでのみサポートされ、RPR モードでは動作しません。

仮想コンソールを使用してスタンバイ スーパーバイザ エンジンにログインするには、**session module** コンフィギュレーション コマンドを使用します。

session module *mod*

構文の説明

mod	コマンドのターゲット モジュール。

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 モード

コマンド履歴

リリース	変更内容
12.2(31)SG	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

Catalyst 4500 シリーズ スイッチに 2 つのスーパーバイザ エンジンを搭載して、冗長構成にできます。スイッチの電源を入れると、一方のスーパーバイザ エンジンがアクティブになり、スイッチオーバーが発生するまでアクティブな状態で維持されます。もう一方のスーパーバイザ エンジンは、スタンバイ モードのままです。

各スーパーバイザ エンジンには、独自のコンソール ポートがあります。スタンバイ スーパーバイザ エンジンにアクセスできるのは、スタンバイ スーパーバイザ エンジンのコンソール ポートからのみです。したがって、スタンバイ スーパーバイザに対するアクセス、モニタ、またはデバッグを行うには、スタンバイ コンソールに接続する必要があります。

スタンバイ スーパーバイザ エンジンの仮想コンソールを使用すると、スタンバイ コンソールへの物理的な接続がなくても、アクティブ スーパーバイザ エンジンからスタンバイ コンソールにアクセスできます。仮想コンソールでは、EOBC 上で IPC を行ってスタンバイ スーパーバイザ エンジンと通信します。これにより、アクティブ スーパーバイザ エンジン上でスタンバイ コンソールをエミュレートします。アクティブ スタンバイ コンソール セッションは、一度に 1 つしかアクティブにできません。

スタンバイ スーパーバイザ エンジンの仮想コンソールを使用すると、アクティブ スーパーバイザ エンジンにログインしたユーザは、スタンバイ スーパーバイザ エンジンに対して show コマンドをリモートから実行でき、この結果をアクティブ スーパーバイザ エンジン上で表示できます。仮想コンソールを使用できるのは、アクティブ スーパーバイザ エンジンからのみです。

アクティブ スーパーバイザ エンジンからスタンバイ仮想コンソールにアクセスするには、アクティブ スーパーバイザ エンジン上で **attach module**、**session module**、または **remote login** コマンドを使用します。これらのコマンドを実行してスタンバイ コンソールにアクセスするには、特権 EXEC モード（レベル 15）である必要があります。

（注）　**session module** コマンドは、**attach module** *mod* および **remote login module** *mod* コマンドと同じです。

スタンバイ仮想コンソールにアクセスすると、端末プロンプトは自動的に [<hostname>-standby-console#] に変わります。hostname はスイッチに設定した名前です。仮想コンソールを終了すると、このプロンプトは元のプロンプトに戻ります。

仮想コンソールを終了するには、**exit** または **quit** コマンドを使用します。ログインしているアクティブ スーパーバイザ エンジンの端末で、非アクティブな時間が、設定されているアイドル時間を超過すると、アクティブ スーパーバイザ エンジンの端末から自動的にログアウトされます。この場合は、仮想コンソール セッションも終了します。仮想コンソール セッションは、スタンバイ エンジンが再起動された場合も自動的に終了します。スタンバイ エンジンの起動後は、新しい仮想コンソール セッションを作成する必要があります。

スタンバイ仮想コンソールには、次の制限事項が適用されます。

仮想コンソールで実行したすべてのコマンドは、完了するまで中止できません。auto-more 機能はなく、**terminal length 0** コマンドを実行した場合と同様の動作となります。また、インタラクティブ性もありません。したがって、実行中のコマンドは、アクティブ スーパーバイザ エンジンからどのようなキー シーケンスを入力しても中断または中止することができません。このため、コマンドの出力量が多い場合、仮想コンソールはこの出力をスーパーバイザの画面上に表示します。

仮想コンソールは非インタラクティブです。仮想コンソールはコマンドのインタラクティブ性を検出しないので、ユーザとの対話が必要なコマンドでは、RPC タイマーによってコマンドが打ち切られるまで、仮想コンソールは待機を続けます。

仮想コンソール タイマーは 60 秒に設定されています。60 秒経過すると、仮想コンソールにプロンプトが表示されます。この期間中は、キーボードからコマンドを打ち切ることはできません。続行するには、タイマーが満了するまで待つ必要があります。

仮想コンソールを使用して、スタンバイ スーパーバイザ エンジン上で表示されているデバッグ メッセージおよび Syslog メッセージを表示することはできません。仮想コンソールには、仮想コンソールから実行したコマンドの出力だけが表示されます。実際のスタンバイ コンソールに表示されるその他の情報は、仮想コンソールには表示されません。

例

仮想コンソールを使用してスタンバイ スーパーバイザ エンジンにログインするには、次のようにします。

```
Switch# session module 2
Connecting to standby virtual console
Type "exit" or "quit" to end this session

Switch-standby-console# exit
Switch#
```

スタンバイ コンソールがイネーブルにされていない場合は、次のメッセージが表示されます。

```
Switch-standby-console#
Standby console disabled.
Valid commands are: exit, logout
```

関連コマンド

コマンド	説明
attach module	特定のモジュールにリモートから接続します。
remote login module	特定のモジュールにリモートから接続します。

set

パケットに Class of Service（CoS; サービス クラス）、Differentiated Services Code Point（DSCP; DiffServ コード ポイント）、または IP precedence を設定することで IP トラフィックをマークするには、**set** ポリシーマップ クラス コンフィギュレーション コマンドを使用します。トラフィック分類を削除するには、このコマンドの **no** 形式を使用します。

set {**cos** *new-cos* | [**ip**] {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos group** *value*}

no set cos *new-cos* | **ip** {**dscp** *new-dscp* | **precedence** *new-precedence*} | **qos group** *value*}

構文の説明

cos *new-cos*	分類されたトラフィックに割り当てられる新しい CoS 値です。指定できる範囲は 0 ～ 7 です。
ip dscp *new-dscp*	分類されたトラフィックに割り当てられる新しい DSCP 値です。指定できる範囲は 0 ～ 63 です。よく使用する値の場合は、ニーモニック名を入力することもできます。指定する値では、IPv4/IPv6 パケット ヘッダー内に Type of Service（ToS; タイプ オブ サービス）トラフィック クラス バイトを設定します。
ip precedence *new-precedence*	分類されたトラフィックに割り当てられる新しい IP precedence 値です。指定できる範囲は 0 ～ 7 です。よく使用する値の場合は、ニーモニック名を入力することもできます。指定する値では、IP ヘッダー内に precedence ビットを設定します。
qos group *value*	インターフェイスに対する入力で分類済みパケットに割り当てられた内部 QoS グループです。

デフォルト

パケットでのマーキングはイネーブルではありません。

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 モード

コマンド履歴

リリース	変更内容
12.1(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E および Catalyst 4900M シャーシのサポートが追加されました。

使用上のガイドライン

set コマンドは、class-level クラスでのみ使用できます。

set dscp *new-dscp* および **set precedence** *new-precedence* コマンドは、**set ip dscp** *new-dscp* および **set ip precedence** *new-precedence* コマンドと同じです。

set dscp *new-dscp* コマンドまたは **set precedence** *new-precedence* コマンドについては、よく使用する値にニーモニック名を入力できます。たとえば、**set dscp af11** コマンドを入力できます。これは **set dscp 10** コマンドの入力と同じです。**set precedence critical** コマンドを入力できます。これは **set precedence 5** コマンドの入力と同じです。サポートされているニーモニックのリストについては、**set dscp ?** または **set precedence ?** コマンドを入力して、コマンドライン ヘルプ ストリングを参照してください。

set cos *new-cos*、**set dscp** *new-dscp*、または **set precedence** *new-precedence* コマンドは、インターフェイスまたは VLAN に対応付けられた入力および出力ポリシー マップに設定できます。

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

例

次の例では、*p1* というポリシー マップを作成し、別のトラフィック タイプに割り当てられた CoS 値を設定する方法を示します。「voice」および「video-data」のクラス マップはすでに作成されています。

```
Switch# configure terminal
Switch(config)# policy-map p1
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap)# exit
Switch#
```

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	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
show policy-map	ポリシー マップ情報を表示します。
trust	**class** ポリシーマップ コンフィギュレーション コマンドを使用して分類されたトラフィックの信頼状態を定義します。

set cos

パケットのレイヤ 2 Class of Service（CoS; サービス クラス）値を設定するには、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 **set cos** コマンドを使用します。特定の CoS 値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。

set cos {*cos-value* | *from-field* [**table** *table-map-name*]}

no set cos {*cos-value* | *from-field* [**table** *table-map-name*]}

構文の説明

cos-value	0 ～ 7 の特定の IEEE 802.1Q CoS 値です。
from-field	パケットの CoS 値の設定に使用される特定のパケットマーキング カテゴリです。パケットマーキング値のマッピングと変換用テーブル マップを使用している場合、これがパケットマーキング カテゴリからマップを確立します。パケットマーキング カテゴリ キーワードは次のとおりです。 • **precedence** • **dscp** • **cos** • **qos group**
table	（任意）指定のテーブル マップに設定された値が CoS 値の設定に使用されることを示します。
table-map-name	（任意）CoS 値の指定に使用されるテーブル マップ名です。テーブル マップ名には、最大 64 の英数字を使用できます。

コマンド デフォルト

発信パケットには CoS 値は設定されていません。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6-E および Catalyst 4900M シャーシを使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

set cos コマンドは、インターフェイスまたは VLAN に対応付けられた入力および出力ポリシー マップで使用できます。

このコマンドを使用して、CoS 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- 優先順位
- DiffServ コード ポイント（DSCP）
- Cost of Service（CoS; サービス コスト）
- Quality of Service（QoS）グループ

「from-field」カテゴリを指定したものの **table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値を CoS 値としてコピーすることです。たとえば、**set cos precedence** コマンドを設定する場合、precedence 値がコピーされ、CoS 値として使用されます。

DSCP マーキング カテゴリに対して同じことを行うことができます。つまり、**set cos dscp** コマンドを設定できます。この場合、DSCP 値がコピーされ、CoS 値として使用されます。

（注） **set cos dscp** コマンドを設定する場合、DSCP フィールドの*最初の 3 ビット*（クラス セレクタ ビット）のみが使用されます。

（注） **set cos qos group** コマンドを設定する場合、qos group フィールドの 3 つの最下位ビットのみが使用されます。

例

次の例では、「cos-set」というポリシー マップを設定し、別のトラフィック タイプの別の CoS 値を割り当てる方法を示します。この例では、「voice」および「video-data」のクラス マップがすでに作成されているものと想定しています。

```
Switch# configure terminal
Switch(config)# policy-map cos-set
Switch(config-pmap)# class voice
Switch(config-pmap-c)# set cos 1
Switch(config-pmap-c)# exit
Switch(config-pmap)# class video-data
Switch(config-pmap-c)# set cos 2
Switch(config-pmap-c)# end
Switch#
```

次の例では、「policy-cos」というポリシー マップを設定し、「table-map1」というテーブル マップで定義された値を使用する方法を示します。「table-map1」というテーブル マップは、**table-map**（値マッピング）コマンドで前に作成されたものです。**table-map**（値マッピング）コマンドの詳細については、**table-map**（値マッピング）コマンド ページを参照してください。

この例では、CoS 値の設定は「table-map1」に定義されている precedence 値に基づいています。

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set cos precedence table table-map1
Switch(config-pmap-c)# end
Switch#
```

関連コマンド

コマンド	説明
match（クラスマップ コンフィギュレーション）	クラス マップの一致基準を定義します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。

コマンド	説明
set dscp	Type of Service（ToS; タイプ オブ サービス）バイトに Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定することによってパケットをマークします。
set precedence	パケット ヘッダーに precedence 値を設定します。
show policy-map	ポリシー マップ情報を表示します。

set dscp

Type of Service（ToS; タイプ オブ サービス）バイトに Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定することによってパケットをマークするには、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 **set dscp** コマンドを使用します。以前に設定した DSCP 値を削除するには、このコマンド **no** 形式を使用します。

set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]}

no set [**ip**] **dscp** {*dscp-value* | *from-field* [**table** *table-map-name*]

構文の説明

ip	（任意）IPv4 パケットのみを照合するように指定します。使用しない場合、IPv4 と IPv6 パケットの両方が照合されます。
dscp-value	DSCP 値を設定する 0 ～ 63 の数字です。よく使用する値の場合は、ニーモニック名を使用することもできます。
from-field	パケットの DSCP 値の設定に使用される特定のパケットマーキング カテゴリです。パケットマーキング値のマッピングと変換用テーブル マップを使用している場合、これがパケットマーキング カテゴリからマップを確立します。パケットマーキング カテゴリ キーワードは次のとおりです。 • **cos** • **qos-group** • **dscp** • **precedence**
table	（任意）*from-field* 引数とともに使用します。指定のテーブル マップに設定された値が DSCP 値の設定に使用されることを示します。
table-map-name	（任意）**table** キーワードとともに使用します。DSCP 値の指定に使用されるテーブル マップ名です。名前には、最大 64 の英数字を使用できます。

コマンド デフォルト

ディセーブル

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 モード

コマンド履歴

リリース	変更内容
12.2(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E に設定されたポリシーマップの「from-field」のサポートが追加されました。

使用上のガイドライン　DSCP ビットを設定すると、他の Quality of Service（QoS）機能がビット設定で動作するようになります。

相互に排他的な DSCP と precedence

set dscp コマンドを **set precedence** コマンドとともに使用して*同じ*パケットをマークすることはできません。2 つの値（DSCP および precedence）は相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

このコマンドを使用して、DSCP 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- Class of Service（CoS; サービス クラス）
- QoS グループ
- 優先順位
- DiffServ コード ポイント（DSCP）

「from-field」カテゴリを指定したものの **table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値を DSCP 値としてコピーすることです。たとえば、**set dscp cos** コマンドを設定する場合、CoS 値がコピーされ、DSCP 値として使用されます。

（注）　CoS フィールドは 3 ビット フィールドで、DSCP フィールドは 6 ビット フィールドです。**set dscp cos** コマンドを設定する場合、CoS フィールドの 3 ビットのみが使用されます。

set dscp qos-group コマンドを設定する場合、QoS グループ値がコピーされ、DSCP 値として使用されます。

DSCP の有効値の範囲は 0 ～ 63 の数字です。QoS グループの有効値の範囲は 0 ～ 63 の数字です。

IPv6 環境での DSCP 値の設定

このコマンドを IPv6 環境で使用すると、デフォルトで IP パケットと IPv6 パケットの両方が照合されます。ただし、この機能によって設定される実際のパケットは、この機能を含むクラスマップの一致基準に合致するパケットのみです。

IPv6 パケットのみに対する DSCP 値の設定

IPv6 パケットのみに対して DSCP 値を設定するには、**match protocol ipv6** コマンドも使用する必要があります。このコマンドを使用しないと、DSCP での照合はデフォルトで IPv4 パケットと IPv6 パケットの両方に対して行われます。

IPv4 パケットのみに対する DSCP 値の設定

IPv4 パケットのみに対して DSCP 値を設定するには、分類のために **match** コマンドで **ip** キーワードを使用します。**ip** キーワードを使用しないと、IPv4 パケットと IPv6 パケットの両方が照合されます。

例

パケットマーキング値とテーブル マップ

次の例では、「policy1」というポリシー マップが、「table-map1」というテーブル マップで定義されたパケットマーキング値を使用するために作成されます。このテーブル マップは、**table-map**（値マッピング）コマンドで前に作成されたものです。**table-map**（値マッピング）コマンドの詳細については、table-map（値マッピング）コマンド ページを参照してください。

この例では、DSCP 値は「table-map1」というテーブル マップに定義されている CoS 値に基づいて設定されています。

```
Switch# configure terminal
Switch(config)# policy-map policy1
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set dscp cos table table-map1
Switch(config-pmap-c)# end
Switch#
```

関連コマンド

コマンド	説明
match（クラスマップ コンフィギュレーション）	クラス マップの一致基準を定義します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。
set cos	Class of Service（CoS; サービス クラス）を設定することによって IP トラフィックを設定します。
set precedence	パケット ヘッダーに precedence 値を設定します。
show policy-map	ポリシー マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。
table-map（値マッピング）（Cisco IOS のマニュアルを参照）	BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

set precedence

パケット ヘッダーに precedence 値を設定するには、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 **set precedence** コマンドを使用します。precedence 値を削除するには、このコマンドの **no** 形式を使用します。

set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

no set precedence {*precedence-value* | *from-field* [**table** *table-map-name*]}

構文の説明

precedence-value	パケット ヘッダーに precedence ビットを設定する 0 ～ 7 の数字です。
from-field	パケットの precedence 値の設定に使用される特定のパケットマーキング カテゴリです。パケットマーキング値のマッピングと変換用テーブル マップを使用している場合、この引数値がパケットマーキング カテゴリからマップを確立します。パケットマーキング カテゴリ キーワードは次のとおりです。 • **cos** • **qos-group** • **dscp** • **precedence**
table	（任意）指定のテーブル マップに設定された値が precedence 値の設定に使用されることを示します。
table-map-name	（任意）Class of Service（CoS; サービス クラス）値に基づいて precedence 値を指定するのに使用されるテーブル マップ名です。名前には、最大 64 の英数字を使用できます。

コマンド デフォルト

ディセーブル

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 モード

コマンド履歴

リリース	変更内容
12.2(8a)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。
12.2(40)SG	Supervisor Engine 6-E に設定されたポリシーマップの「from-field」のサポートが追加されました。

使用上のガイドライン

コマンドの互換性

set precedence コマンドを **set dscp** コマンドとともに使用して*同じ*パケットをマークすることはできません。2 つの値（DSCP および precedence）は相互に排他的です。パケットにはどちらか一方の値を設定でき、両方を設定することはできません。

このコマンドを使用して、precedence 値のマッピングと設定に使用される「from-field」パケットマーキング カテゴリを指定できます。「from-field」パケットマーキング カテゴリは次のとおりです。

- CoS
- QoS グループ
- DSCP
- 優先順位

「from-field」カテゴリを指定したものの **table** キーワードと適用可能な *table-map-name* 引数を指定していない場合、デフォルト アクションは、「from-field」カテゴリに関連付けられた値を precedence 値としてコピーすることです。たとえば、**set precedence cos** コマンドを設定する場合、CoS 値がコピーされ、precedence 値として使用されます。

QoS グループマーキング カテゴリに対して同じことを行うことができます。つまり、**set precedence qos-group** コマンドを設定できます。この場合、QoS グループ値がコピーされ、precedence 値として使用されます。

precedence の有効値の範囲は 0 ～ 7 の数字です。QoS グループの有効値の範囲は 0 ～ 63 の数字です。したがって、**set precedence qos-group** コマンドを設定する場合、qos-group の 3 つの最下位ビットのみが precedence にコピーされます。

IPv6 環境での precedence 値

このコマンドを IPv6 環境で使用する場合、IPv4 および IPv6 パケットの両方に値を設定できます。ただし、この機能によって設定される実際のパケットは、この機能を含むクラスマップの一致基準に合致するパケットのみです。

IPv6 パケットのみに対する precedence 値の設定

IPv6 パケットのみに対して precedence 値を設定するには、このアクションに対してパケットを分類しているクラスマップで **match protocol ipv6** コマンドも使用する必要があります。**match protocol ipv6** コマンドを使用しないと、クラスマップによって（他の一致基準に応じて）IPv6 および IPv4 パケットの両方が分類される可能性があり、**set precedence** コマンドも両方のタイプのパケットに対して作用します。

IPv4 パケットのみに対する precedence 値の設定

IPv4 パケットのみに対して precedence 値を設定するには、**match ip precedence** や **match ip dscp** コマンドなど、**ip** キーワードを含むコマンドを使用するか、または他のコマンドとともに **match protocol ip** コマンドをクラス マップに含めます。追加の **ip** キーワードを使用しないと、クラスマップによって（他の一致基準に応じて）IPv6 および IPv4 パケットの両方が照合される可能性があり、**set precedence** コマンドや **set dscp** コマンドも両方のタイプのパケットに対して作用します。

例

次の例では、policy-cos というポリシー マップが、table-map1 というテーブル マップで定義された値を使用するために作成されます。table-map1 というテーブル マップは、**table-map**（値マッピング）コマンドで前に作成されたものです。**table-map**（値マッピング）コマンドの詳細については、**table-map**（値マッピング）コマンド ページを参照してください。

この例では、precedence 値は table-map1 に定義されている CoS 値に基づいて設定されています。

```
Switch# configure terminal
Switch(config)# policy-map policy-cos
Switch(config-pmap)# class class-default
Switch(config-pmap-c)# set precedence cos table table-map1
Switch(config-pmap-c)# end
Switch#
```

関連コマンド

コマンド	説明
match（クラスマップ コンフィギュレーション）	クラス マップの一致基準を定義します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。
set cos	Class of Service（CoS; サービス クラス）を設定することによって IP トラフィックを設定します。
set dscp	Type of Service（ToS; タイプ オブ サービス）バイトに Differentiated Services Code Point（DSCP; DiffServ コード ポイント）値を設定することによってパケットをマークします。
set qos-group	あとでパケットの分類に使用できる Quality of Service（QoS）グループ ID を設定します。
set precedence	パケット ヘッダーに precedence 値を設定します。
show policy-map	ポリシー マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。
table-map（値マッピング）（Cisco IOS のマニュアルを参照）	BGP で学習されたルートを使用して IP ルーティング テーブルが更新されたときに、メトリックおよびタグ値を変更します。

set qos-group

あとでパケットの分類に使用できる Quality of Service（QoS）グループ ID を設定するには、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 **set qos-group** コマンドを使用します。グループ ID を削除するには、このコマンドの **no** 形式を使用します。

set qos-group *group-id*

no set qos-group *group-id*

構文の説明

group-id	0 ～ 63 の範囲のグループ ID 番号です。

コマンド デフォルト

グループ ID は 0 に設定されています。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6-E および Catalyst 4900M シャーシを使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

set qos-group コマンドでは、グループ ID をパケットと関連付けることができます。この関連付けは、入力方向のインターフェイスや VLAN に対応付けられたサービス ポリシーを通じて行われます。グループ ID は、あとで QoS サービス ポリシーをパケットに適用するために出力方向で使用することができます。

例

次の例では、qos-group を 5 に設定する方法を示します。

```
Switch#configure terminal
Switch(config)#policy-map p1
Switch(config-pmap)#class c1
Switch(config-pmap-c)#set qos
Switch(config-pmap-c)#set qos-group 5
Switch(config-pmap-c)#end
Switch#
```

関連コマンド

コマンド	説明
match（クラスマップ コンフィギュレーション）	クラス マップの一致基準を定義します。
policy-map	複数ポートに適用可能なポリシー マップを作成または変更し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。
show policy-map	ポリシー マップ情報を表示します。
show policy-map interface	インターフェイスに対応付けられた入力および出力ポリシーの統計情報およびコンフィギュレーションを表示します。

shape（クラスベース キューイング）

物理ポートに対応付けられたポリシー マップ内でトラフィック クラスのトラフィック シェーピングをイネーブルにするには、**shape average** ポリシーマップ クラス コマンドを使用します。トラフィック シェーピングは、データ伝送レートを制限します。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。

shape average {*rate*} [**bps** | **kbps** | **mbps** | **gbps**]

shape average percent {*percent_value*}

no shape average

構文の説明

rate	トラフィック シェーピングの平均レートを指定します。範囲は 16000 ～ 10000000000 です。ポストフィックス表記法（k、m、g）は任意で、小数点を使用できます。
bps	（任意）レートをビット/秒単位で指定します。
kbps	（任意）レートをキロバイト/秒単位で指定します。
mbps	（任意）レートをメガビット/秒単位で指定します。
gbps	（任意）レートをギガビット/秒単位で指定します。
percent	トラフィック シェーピングの帯域幅の割合を指定します。
percent_value	（任意）トラフィック シェーピングに使用する帯域幅の割合を指定します。有効値の範囲は 1 ～ 100% です。

デフォルト

平均レート トラフィック シェーピングはディセーブルです。

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 モード

コマンド履歴

リリース	変更内容
12.2(40)SG	このコマンドが、Supervisor Engine 6E を使用する Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

物理ポートに対応付けられているポリシー マップ内でのみ **shape** コマンドを使用します。このコマンドは、階層の任意のレベルにあるポリシー マップで有効です。

シェーピングは、指定したプロファイルに適合するようにキュー内のアウトオブプロファイル パケットを遅延させる処理です。シェーピングはポリシングとは別のものです。ポリシングでは設定したしきい値を超えたパケットをドロップしますが、シェーピングではトラフィックがしきい値内に収まるようにパケットをバッファリングします。シェーピングによって、ポリシングに比べてトラフィックの処理が大幅に平滑化されます。

bandwidth、**dbl**、および **shape** ポリシーマップ クラス コンフィギュレーション コマンドと **priority** ポリシーマップ クラス コンフィギュレーション コマンドを同じポリシー マップ内の同一クラスで使用することはできません。ただし、これらのコマンドを同じポリシー マップで使用することはできます。

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

例

次の例では、指定したトラフィック クラスをデータ伝送レート 256 kbps に制限する方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# policy-map policy1
Switch(config-pmap)# class class1
Switch(config-pmap-c)# shape average 256000
Switch(config-pmap-c)# exit
Switch(config-pmap)# exit
Switch(config)# interface gigabitethernet1/1
Switch(config-if)# service-policy output policy1
Switch(config-if)# 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
bandwidth	名前で参照可能なシグナリング クラス構造を作成します。
class	トラフィック ポリシーを作成または変更するクラスの名前を指定します。
dbl	トラフィックのクラスが使用する送信キュー上で、アクティブ キュー管理をイネーブルにします。
policy-map	複数ポートに適用可能なポリシー マップを作成し、サービス ポリシーを指定してポリシーマップ コンフィギュレーション モードを開始します。
service-policy（ポリシーマップ クラス）	ポリシー マップ内に Quality of Service（QoS）ポリシーとしてサービス ポリシーを作成します。
show policy-map	ポリシー マップ情報を表示します。

shape（インターフェイス コンフィギュレーション）

インターフェイスでトラフィック シェーピングを指定するには、**shape** コマンドを使用します。トラフィック シェー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。

shape [**rate**] [**percent**]

no shape [**rate**] [**percent**]

構文の説明

rate	（任意）トラフィック シェーピングの平均レートを指定します。範囲は 16000 ～ 1000000000 です。ポストフィックス表記法（k、m、g）は任意で、小数点を使用できます。
percent	（任意）トラフィック シェーピングの帯域幅の割合を指定します。

デフォルト

デフォルトでは、トラフィック シェーピングは設定されていません。

コマンド モード

インターフェイス送信キュー コンフィギュレーション モード

コマンド履歴

リリース	変更内容
12.2(18)EW	このコマンドが Catalyst 4500 シリーズ スイッチに追加されました。

使用上のガイドライン

このコマンドは、Supervisor Engine 6-E および Catalyst 4900M シャーシではサポートされません。

トラフィック シェーピングはすべてのポート上で使用可能で、帯域幅の上限を設定するものです。

Catalyst 4500 Supervisor Engine II-Plus-10GE（WS-X4013+10GE）、Catalyst 4500 Supervisor Engine V（WS-X4516）、および Catalyst 4500 Supervisor Engine V-10GE（WS-X4516-10GE）上で高いシェープ レートを設定すると、コンテンションが発生した場合、または異常なサイズのパケットが伝送された場合には、トラフィックのシェープ レートが実現されないことがあります。スタブ ASIC の多重ポートおよびバックプレーン ギガポートに接続しているポート上で 7 Mbps を超えるシェープ レートを設定すると、悪条件な環境によっては達成されないことがあります。バックプレーン ギガポートに直接接続しているポートまたはスーパーバイザ エンジンのギガポート上で 50 Mbps を超えるシェープ レートを設定すると、悪条件な環境によっては達成されないことがあります。

次に、バックプレーンに直接接続しているポートの例を示します。

- Supervisor Engine II+、II+10GE、III、IV、V、および V-10GE 上のアップリンク ポート
- WS-X4306-GB モジュール上のポート
- WS-X4232-GB-RJ モジュール上の 2 つの 1000BASE-X ポート
- WS-X4418-GB モジュール上の最初の 2 つのポート
- WS-X4412-2GB-TX モジュール上の 2 つの 1000BASE-X ポート

24 ポート モジュールおよび 48 ポート モジュールのすべてのポートはスタブ ASIC で多重化されています。次に、スタブ ASIC で多重化されているポートの例を示します。

- WS-X4148-RJ45 モジュール上の 10/100 ポート
- WS-X4124-GB-RJ45 モジュール上の 10/100/1000 ポート
- WS-X4448-GB-RJ45 モジュール上の 10/100/1000 ポート

例

次の例では、インターフェイス fa3/1 に最大帯域幅（70%）を設定する方法を示します。

```
Switch(config)# interface fastethernet3/1
Switch(config-if)# tx-queue 3
Switch(config-if-tx-queue)# shape 70m
Switch(config-if-tx-queue)#
```