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。有効値については、表 2-8 を参照してください。
number	モジュールおよびポート番号

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	変更箇所
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 2-8 に、*type* の有効値を示します。

表 2-8　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

次に、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 モードを開始する例を示します。

```
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（仮想スイッチ）

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** グローバル コンフィギュレーション モード コマンドを使用します。

interface [*interface switch-num/slot/port.subinterface*}

構文の説明

interface	設定するインターフェイスを指定します。有効な値については、表 2-9 を参照してください。
switch-num	スイッチ ID を指定します。
slot	スロット番号を指定します。
port	ポート番号を指定します。
.subinterface	ポート サブインターフェイス番号を指定します。

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	変更箇所
Cisco IOS XE 3.4.0SG および 15.1(2)SG	Catalyst 4500 シリーズ スイッチでサポートが開始されました。

使用上のガイドライン

表 2-9 に、*type* の有効値を示します。

表 2-9　type の有効値

キーワード	定義
fastethernet	ファスト イーサネット 802.3
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。
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。
tunnel	トンネル インターフェイス

例

次に、スイッチ 1、モジュール 2、ポート 4 の GigabitEthernet インターフェイスでインターフェイス コンフィギュレーション モードを開始する例を示します。

```
Router(config)# interface gigabitethernet 1/2/4
Router(config)#
```

関連コマンド

コマンド	説明
show interfaces（仮想スイッチ）	特定のインターフェイスが認識するトラフィックを表示します。

interface port-channel

ポートチャネル インターフェイスにアクセスまたは作成するには、**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がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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

コマンドを複数のポートで同時に実行するには、**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。有効値は 1 ～ 4094 です。
port-range	ポート範囲。*port-range* の有効値のリストについては、「使用上のガイドライン」の項を参照してください。
macro *name*	マクロ名を指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.1(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。

ポート範囲に対して行われるすべての設定変更は NVRAM に保存されますが、**interface range** コマンドで作成されたポート範囲は NVRAM には保存されません。

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。マクロを作成した後、範囲を追加できます。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)#
```

次に、ポート範囲マクロを実行する例を示します。

```
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	変更箇所
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 インターフェイスを新規に作成するたびにメッセージが表示されるため、入力した VLAN 番号が正しいかどうかを確認できます。

no interface vlan *vlan-id* コマンドを入力して SVI を削除した場合、関連付けられたインターフェイスは強制的に管理上のダウン ステートになり、削除とマークされます。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復元しますが、以前の設定の大半は失われます。

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 admission proxy http refresh-all

スイッチのシステム ディレクトリで、カスタマイズされた WebAuth のログイン ページが前のログイン ページと同じ名前で表示されるようにするには、**ip admission proxy http refresh-all** コマンドを使用します。

ip admission proxy http [success | failure | refresh-all | login [expired | page]]

構文の説明

success	成功した認証プロキシ。
failure	失敗した認証プロキシ。
refresh-all	すべてのカスタム html ページを更新します。
login expired	期限切れの Web ページを指定します。
login page	カスタマイズしたログイン Web ページを指定します。

デフォルト

このコマンドを入力しない場合、同じ名前のファイルを持つカスタマイズされた Web ベースの認証ページ ファイルのいずれかが変更されていると、新しいファイルではなく、古いログイン ページが表示されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.0(2)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

カスタマイズされた Web ベースの認証ページがシステム ディレクトリで変更されたときには、必ずこのコマンドを入力する必要があります。

例

次に、このコマンドを入力する例を示します。

```
Switch# config terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip admission proxy http [success | failure | refresh-all | login]
Switch(config)# end
Switch#
```

<新しい HTML ページが表示されます。>

ip arp inspection filter vlan

DAI がイネーブルの場合に、スタティック IP に設定されたホストからの ARP を許可し、ARP アクセス リストを定義して、これを VLAN に適用するには、**ip arp inspection filter vlan** コマンドを使用します。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 リストを静的に適用する必要があることを指定します。

デフォルト

VLAN には、定義された ARP ACL が適用されていません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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）

インターフェイス上で着信 ARP 要求および応答のレートを制限し、DoS 攻撃の場合に DAI によりすべてのシステム リソースが消費され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 パケットのレートに上限がないことを指定します。
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。設定できる間隔の範囲は 1 ～ 15 秒です。

デフォルト

信頼できないインターフェイスでは、レートは 15 パケット/秒に設定します。このネットワークが毎秒 15 の新しいホストに接続される 1 つのホストを持つスイッチド ネットワークであると想定しています。

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。

バースト間隔は、デフォルトで 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	変更箇所
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 ポートでは、集約を反映するためにより高いレートを設定する必要があります。着信パケットのレートがユーザ設定のレートを超えると、インターフェイスは errdisable ステートになります。errdisable-timeout 機能は、ポートを errordisable ステートから有効に戻すのに使用することができます。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 ポートの着信 ARP パケットのレートは、すべてのチャネル メンバからの着信パケットのレートの合計と同じです。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。0 の値は、このバッファからエントリがロギングされないことを意味します。
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	変更箇所
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。これらパケットは、すべての VLAN で共有されるログ バッファで登録されます。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、最大 45 のエントリを保持できるようにロギング バッファを設定する方法を示します。

```
Switch# config 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

ポート単位で設定可能な信頼状態を設定して、着信 ARP パケットが検査される一連のインターフェイスを決定するには、**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がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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** をイネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、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 本体のターゲット MAC アドレスと比較します。このチェックは、ARP 応答に対して実行されます。 **（注）** **dst-mac** をイネーブルにすると、異なる MAC アドレスを持つパケットは無効パケットとして分類され、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。アドレスには 0.0.0.0、255.255.255.255、およびすべての IP マルチキャスト アドレスが含まれます。 送信元 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	変更箇所
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 単位でダイナミック ARP インスペクション（DAI）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 で ARP インスペクション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	変更箇所
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	変更箇所
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 と **dhcp-bindings** キーワードは、組み合わせて使用します。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。次の 2 つのオプションを使用できます。

- **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

次に、**logging** キーワードを指定して、ACL に一致したときにパケットをログに追加するように VLAN 1 に ARP インスペクションを設定する例を示します。

```
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 TCP/UDP ポート、宛先 TCP/UDP ポート、またはその両方のポートが、送信元および宛先 IP アドレスに加えてハッシュに含めることができるように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。このポートが含まれていないデフォルト状態に戻すには、このコマンドの **no** 形式を使用します。

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 ポートを含める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。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	変更箇所
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

オリジナル アルゴリズム、トンネル アルゴリズム、およびユニバーサル アルゴリズムは、ハードウェア経由で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によって処理されます。**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 device tracking maximum

レイヤ 2 ポートで IP ポート セキュリティ バインディングのトラッキングをイネーブルにするには、**ip device tracking maximum** コマンドを使用します。信頼できないレイヤ 2 インターフェイスで IP ポート セキュリティをディセーブルにするには、このコマンドの **no 形式**を使用します。

ip device tracking maximum {*number*}

no ip device tracking maximum {*number*}

構文の説明

number	ポートの IP デバイス トラッキング テーブルに作成するバインディングの数を指定します。有効な値は 0 ～ 2048 です。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(37)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、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポート セキュリティをイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastethernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

設定を確認するには、**show ip verify source** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip verify source	信頼できないレイヤ 2 インターフェイスで IP ソース ガードをイネーブルにします。
show ip verify source	特定のインターフェイス上の IP ソース ガード設定とフィルタを表示します。

ip dhcp snooping

DHCP スヌーピングをグローバルにイネーブルにするには、**ip dhcp snooping** 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	変更箇所
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

DHCP バインディングの設定を確立および生成して、再起動後にバインディングを復元するには、**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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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る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 は無期限として定義されています。
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

タイムアウト値は 300 秒（5 分）に設定されます。

書き込み遅延値は 300 秒に設定されます。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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

スイッチがネットワークベースの URL（TFTP や FTP など）に設定された URL にバインディングを初めて書き込む前に、この URL に空のファイルを作成しておく必要があります。

（注） NVRAM およびブートフラッシュの保存容量は限られているので、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。フラッシュにデータベース ファイルを保存する場合は、エージェントによって新しく更新されると新しいファイルが作成されます（フラッシュがすぐにいっぱいになります）。さらに、フラッシュで使用されるファイル システムの性質上、ファイル数が多くなるとアクセスが非常に遅くなります。TFTP からアクセス可能なリモート ロケーションにファイルが格納されている場合、RPR/SSO スタンバイ スーパーバイザ エンジンはスイッチオーバーが発生したときにバインディング 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 に対するリモート 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	変更箇所
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 circuit-id string	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 の DHCP パケットは、信頼できないスヌーピング ポート上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	変更箇所
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 レートの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。

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	変更箇所
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。

コマンド	説明
show ip dhcp snooping	DHCP スヌーピング設定を表示します。
show ip dhcp snooping binding	DHCP スヌーピング バインディング エントリを表示します。

ip dhcp snooping trust

インターフェイスを DHCP スヌーピングの目的として信頼できると設定するには、**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	変更箇所
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 上で 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。有効値は 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	変更箇所
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

グローバル スヌーピングおよび VLAN スヌーピングがどちらもイネーブルの場合にのみ、VLAN 上で DHCP スヌーピングがイネーブルになります。

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)#
```

次に、VLAN 上で DHCP スヌーピングをディセーブルにする例を示します。

```
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 circuit-id string	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 circuit-id string

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 circuit-id string** 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** [**override**] **string** *string*

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

構文の説明

number	単一の VLAN または VLAN 範囲を指定します。有効値は 1 ～ 4094 です。
override	（任意）上書き文字列を指定します。
string *string*	回線 ID にユーザ定義の文字列を指定します。スペースを含まない 3 ～ 63 文字の範囲の ASCII 文字で指定します。

デフォルト

DHCP スヌーピングのオプション 82 がディセーブルの場合、VLAN-mod-port。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(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(54)SG	**override** オプションが追加されました。

使用上のガイドライン

DHCP オプション 82 の回線 ID サブ オプションは、DHCP スヌーピングが DHCP オプション 82 を使用してグローバルにイネーブルであり、また VLAN 上でイネーブルである場合に限りサポートされます。

このコマンドを使用すると、サーキット ID となる ASCII 文字列を設定できます。vlan-mod-port フォーマット タイプを無効にし、その代わりに回線 ID を使用して、サブスクライバ情報を定義する場合、**override** キーワードを使用します。

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
```

次の例では、オプション 82 サーキット ID 上書きサブオプションを設定する方法を示します。

```
Switch(config-if)# ip dhcp snooping vlan 250 information option format-type circuit-id
override string testcustomer
```

設定を確認するには、show ip dhcp snooping ユーザ EXEC コマンドを入力します。

（注）　リモート ID 設定を含むグローバル コマンド出力だけを表示するには、**show ip dhcp snooping** ユーザ EXEC コマンドを使用します。サーキット ID として設定したインターフェイス単位または VLAN 単位の文字列は表示されません。

関連コマンド

コマンド	説明
ip dhcp snooping	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。有効値は 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	変更箇所
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; スイッチ仮想インターフェイス）、または EtherChannel グループに属するポートに対して IGMP フィルタを適用することはできません。

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

例

次の例では、IGMP プロファイル 22 を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	設定されているすべての 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。有効値は 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	変更箇所
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

次に、インターフェイスが加入できる IGMP グループの数を 25 に制限する例を示します。

```
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	変更箇所
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 つだけです。

例

次の例では、IP マルチキャスト アドレスの範囲を指定した IGMP プロファイル 40 の設定方法を示します。

```
Switch # config 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	設定されているすべての 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

スイッチで 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」の項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	変更箇所
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。IGMP スヌーピングの学習方式として CGMP をサポートするようにデフォルト設定を変更した場合は、有効なクエリーの間隔は 1 ～ 300 秒です。

LAN では、IGMP ホスト クエリー メッセージを送信するスイッチだけが指定スイッチになります。IGMP バージョン 1 の場合､指定スイッチは LAN で稼動するマルチキャスト 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。

タイムアウト期間中（**ip igmp query-timeout** コマンドで制御）にクエリーを受信しないと、スイッチがクエリアになります。

（注）　タイムアウト期間を変更すると、マルチキャスト転送能力が著しく低下することがあります。

例

次に、指定したスイッチが IGMP ホスト クエリーのメッセージを送信する頻度を変更する例を示します。

```
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た後、ルータがインターフェイスのクエリアとして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、インターネット グループ管理プロトコル（IGMP）経由で学習されたレシーバ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）トポロジ変更設定を指定します。
flood	（任意）トポロジが変更されるとき、ネットワークにスパニング ツリー テーブルをフラッディングするように指定します。
query	（任意）TCN クエリーの設定を指定します。
count *count*	（任意）スパニング ツリー テーブルがフラッディングされる頻度を指定します。有効値は 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	変更箇所
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。

ip igmp snooping command コマンドは、マルチキャスト ルータではデフォルトでディセーブルになります。

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

例

次に、IGMP スヌーピングをイネーブルにする例を示します。

```
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、トポロジ変更が 9 回発生した後に、ネットワークへのスパニング ツリー テーブル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、ネットワークへのスパニング ツリー テーブル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 デバイスに転送するには、このコマンドの **no** 形式を使用します。

ip igmp snooping report-suppression

no 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	変更箇所
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。有効値は 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	変更箇所
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。

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

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、VLAN 上で 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 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	変更箇所
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

次に、VLAN 200 インターフェイス上で IGMP 明示的ホスト トラッキングをディセーブルにし、設定を確認する例を示します。

```
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。

コマンド	説明
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	変更箇所
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。

特定の VLAN の MAC グループごとに 1 つのレシーバがある場合にだけ、即時脱退機能を使用します。

即時脱退機能をサポートするのは、IGMP バージョン 2 が稼動しているホストだけです。

例

次の例では、VLAN 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。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。

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	変更箇所
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

このコマンドは、VLAN インターフェイス コンフィギュレーション モードだけで使用してください。

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として設定するには、**ip igmp snooping vlan static** コマンドを使用します。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。

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。
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がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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	変更箇所
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	変更箇所
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 multicast multipath

等コスト マルチパス（ECMP）を介した IP マルチキャスト トラフィックのロード分割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 **ip multicast multipath** 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。

ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash** {**basic** | **next-hop-based**}]

no ip multicast [**vrf** *vrf-name*] **multipath** [**s-g-hash** {**basic** | **next-hop-based**}]

構文の説明

vrf *vrf-name*	（任意）*vrf-name* 引数で指定したマルチキャスト バーチャル プライベート ネットワーク（MVPN）ルーティングおよび転送（MVRF）インスタンスに関連付けられた IP マルチキャスト トラフィックに対する ECMP マルチキャスト ロード分割をイネーブルにします。
s-g-hash basic | **next-hop-based**	（任意）ソース アドレスとグループ アドレス、またはソース アドレスとグループ アドレスとネクスト ホップ アドレスに基づいた ECMP マルチキャスト ロード分割をイネーブルにします。 **basic** キーワードを指定すると、ソース アドレスとグループ アドレスに基づいた単純なハッシュがイネーブルになります。このアルゴリズムは、基本 S-G ハッシュ アルゴリズムと呼ばれます。 **next-hop-based** キーワードを指定すると、ソース アドレス、グループ アドレス、およびネクスト ホップ アドレスに基づく複雑なハッシュがイネーブルになります。このアルゴリズムはネクスト ホップ ベースの S-G ハッシュ アルゴリズムと呼ばれます。

コマンド デフォルト

複数の等コスト パスが存在する場合、マルチキャスト トラフィックはこれらのパス間でロード分割されません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(53)SG	**s-g-hash** キーワードが、Catalyst 4500 スイッチで導入されました。

使用上のガイドライン

ip multicast multipath コマンドは、双方向プロトコル独立型マルチキャスト（PIM）では動作しません。

複数の等コスト パス間で IP マルチキャスト トラフィックのロード分割をイネーブルにするには、**ip multicast multipath** コマンドを使用します。

ソースから 2 つ以上の等コスト パスが使用できる場合は、ユニキャスト トラフィックはそれらのパスの間でロード分割されます。一方、マルチキャスト トラフィックは、デフォルトでは、複数の等コスト パスの間でロード分割されることはありません。一般的に、マルチキャスト トラフィックは、Reverse Path Forwarding（RPF）ネイバーから伝送されます。PIM 仕様によると、複数のネイバーが同じメトリックを持つ場合、このネイバーは最も大きい IP アドレスを持っていなければなりません。

ip multicast multipath コマンドでロード分割を設定すると、システムは、S ハッシュ アルゴリズムを使用して、ソース アドレスに基づいて、複数の等コスト パスの間でマルチキャスト トラフィックを分割します。**ip multicast multipath** コマンドを設定していて、複数の等コスト パスが存在する場合、マルチキャスト トラフィックを伝送するパスは、ソース IP アドレスに基づいて選択されます。異なる複数のソースからのマルチキャスト トラフィックが、異なる複数の等コスト パスの間でロード分割されます。同一ソースから異なる複数のマルチキャスト グループに送信されたマルチキャスト トラフィックについては、複数の等コスト パスの間でロード スプリットは行われません。

（注）　**ip multicast multipath** コマンドは、トラフィックのロード バランシングではなくロード分割を行います。ソースからのトラフィックは、そのトラフィックがその他のソースからのトラフィックよりはるかに多い場合でも、1 つのパスしか使用しません。

ip multicast multipath コマンドが **s-g-hash** キーワードで設定されており、複数の等コスト パスが存在する場合、ソース アドレスとグループ アドレス、またはソース アドレスとグループ アドレスとネクスト ホップ アドレスに基づいて、等コスト パスの間でロード分割が発生します。IP マルチキャスト トラフィックのロード分割にオプションの **s-g-hash** キーワードを指定する場合は、次のキーワードのいずれかを指定することによって、等コスト パスの計算に使用するアルゴリズムを選択しなければなりません。

- **basic**：基本 S-G ハッシュ アルゴリズムは、ハッシュ値の計算にランダム化を一切使用しないため、予測可能です。ただし、基本 S-G ハッシュ アルゴリズムは、特定のソースとグループについて、どのルータ上でそのハッシュが計算されたかに関係なく常に同じハッシュが選択されるため、局在化する傾向があります。
- **next-hop-based** : ネクスト ホップ ベースの S-G ハッシュ アルゴリズムは、ランダム化はハッシュ値を決定するには使用されないため、予測可能です。S ハッシュ アルゴリズムや基本 S-G ハッシュ アルゴリズムと違って、ネクスト ホップ ベースのハッシュ メカニズムは局在化の傾向がありません。

例

次の例は、S ハッシュ アルゴリズムを使用した、ソース アドレスに基づく ECMP マルチキャスト ロード分割をルータ上でイネーブルにする方法を示します。

```
Switch(config)# ip multicast multipath
```

次に、S-G ハッシュ アルゴリズムを使用する、送信元に基づいた ECMP マルチキャスト ロード分割を、ルータ上でイネーブルにする例を示します。

```
Switch(config)# ip multicast multipath s-g-hash basic
```

次に、ネクスト ホップ ベースの S-G ハッシュ アルゴリズムを使用する、送信元、グループ、およびネクスト ホップ アドレスに基づいた ECMP マルチキャスト ロード分割を、ルータ上でイネーブルにする例を示します。

```
Switch(config)# ip multicast multipath s-g-hash next-hop-based
```

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。

推測された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	変更箇所
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コマンドが拡張されました。

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 サービス カードを取り付ける必要があります。

NetFlow 統計情報機能は、一連のトラフィック統計情報をキャプチャします。これらのトラフィック統計情報には、ネットワーク分析、計画、アカウンティング、課金、および DoS 攻撃の識別に使用できる、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、入力および出力識別子、およびその他のルーティング情報が含まれています。

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 infer-fields コマンドを **ip route-cache flow** コマンドの後に入力すると、既存のキャッシュを消去できます。逆も同様です。この処理は、予測フィールドが存在する場合も、また存在しない場合も、キャッシュ内で同時にフローが発生することを避けるために実行します。

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 モードに比べて、メモリおよび CPU リソースを多く消費します。NetFlow をイネーブルにする前に、スイッチで必要なリソースを把握することが必要です。

例

次に、スイッチ上で NetFlow スイッチングをイネーブルにする例を示します。

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

（注） このコマンドは、個々のインターフェイスでは機能しません。

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がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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 エントリだけを追加するために使用します。

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。正常に削除されるようにするには、すべての必須パラメータが一致する必要があります。

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 送信元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	変更箇所
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 でのみ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した ARP エントリは、スティッキ ARP エントリです。(**show arp** コマンドを使用して、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 インターフェイス上の ARP エントリには期限がないため、MAC アドレスが変更された場合は、PVLAN インターフェイス上の 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がありません。

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	変更箇所
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 スイッチでは、スイッチングされたすべての IPv4 パケットの IPv4 ヘッダーにある次のフィールドの有効性を確認します。

- 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 ヘッダー検証に失敗すると、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、無効な IP ヘッダーを持つパケットはブリッジングされますが、ルーティングが意図されていてもルーティングされません。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** | **tracking**} [**port-security**]

no ip verify source {**vlan dhcp-snooping** | **tracking**} [**port-security**]

構文の説明

vlan dhcp-snooping	信頼できないレイヤ 2 DHCP スヌーピング インターフェイスで IP ソース ガードをイネーブルにします。
tracking	ポートでスタティック IP アドレス ラーニングを学習するために IP ポート セキュリティをイネーブルにします。
port-security	（任意）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 送信元ガードはディセーブルです。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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、ポート単位で VLAN 10 ～ 20 で IP ソース ガードをイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip dhcp snooping
Switch(config)# ip dhcp snooping vlan 10 20
Switch(config)# interface 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#
```

次の例では、レイヤ 2 アクセス ポートで IP-MAC フィルタを使用して IP ポート セキュリティをイネーブルにする方法を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# ip device tracking
Switch(config)# interface fastEthernet 4/3
Switch(config-if)# switchport mode access
Switch(config-if)# switchport access vlan 1
Switch(config-if)# ip device tracking maximum 5
Switch(config-if)# switchport port-security
Switch(config-if)# switchport port-security maximum 5
Switch(config-if)# ip verify source tracking port-security
Switch(config-if)# end
```

設定を確認するには、**show ip verify source** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
ip device tracking maximum	レイヤ 2 ポートで IP ポート セキュリティ バインディングのトラッキングをイネーブルにします。
ip dhcp snooping	DHCP スヌーピングをグローバルにイネーブルにします。
ip dhcp snooping 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 ガード設定とフィルタを表示します。

ip verify unicast source reachable-via

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が受信されたインターフェイスに到達可能か確認します。
allow-default	デフォルトのルートが送信元アドレスに一致するかどうかを確認します。

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	変更箇所
12.2(40)SG	Catalyst 4900M シャーシと、Supervisor Engine 6-E を搭載した Catalyst 4500 でサポートが開始されました。

使用上のガイドライン

基本的な RX モードでは、ユニキャスト RPF で送信元アドレスが到達したインターフェイスに到達可能である必要があります。たとえば、ロード バランシング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 エンドのルータの入力インターフェイスだけに適用されます。

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。ユニキャスト RPF を適用するのは、もともと対称か、または対称に設定されている場合だけにしてください。

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。

ip wccp

サービス グループに参加できるように、指定した Web キャッシュ通信プロトコル（WCCP）サービスのサポート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 **ip wccp** コマンドを使用します。サービス グループをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip wccp {**web-cache** | *service-number*} [**accelerated**] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0** | **7**] *password*]

no ip wccp {**web-cache** | *service-number*}[**accelerated**] [**group-address** *multicast-address*] [**redirect-list** *access-list*] [**group-list** *access-list*] [**password** [**0** | **7**] *password*]

構文の説明

web-cache	Web キャッシュ サービスを指定します。 **（注）** Web キャッシュは、1 つのサービスとしてカウントされます。サービスの最大数（*service-number* 引数で割り当てられたサービスを含む）は 8 です。
service-number	ダイナミック サービス ID。このサービスの定義は、キャッシュによって示されます。ダイナミック サービス番号の範囲は 0 ～ 254 です。サービスの最大数（**web-cache** キーワードで指定する Web キャッシュ サービスを含む）は 8 です。 **（注）** シスコのキャッシュ エンジンがサービス グループで使用される場合、リバース プロキシ サービスは、値 99 で指定されます。
accelerated	（任意）このオプションは、ハードウェア アクセラレーション ルータにだけ適用されます。このキーワードは、キャッシュ エンジンで接続が確立されるのを防ぐためにサービス グループを設定します。ただし、ルータのリダイレクトにハードウェア アクセラレーションを利用できる方法でキャッシュ エンジンが設定されている場合を除きます。
group-address *multicast-address*	（任意）WCCP サービス グループと通信するマルチキャスト IP アドレス。マルチキャスト アドレスは、リダイレクトされたメッセージを受信するキャッシュ エンジンを決定するためにルータで使用されます。
redirect-list *access-list*	（任意）このサービス グループにリダイレクトされるトラフィックを制御するアクセス リスト。*access-list* 引数は、アクセス リストを指定する 64 文字以下の文字列（名前または番号）で設定する必要があります。
group-list *access-list*	（任意）サービス グループへの参加を許可するキャッシュ エンジンを決定するアクセス リスト。*access-list* 引数には、標準または拡張アクセス リストの番号または名前を指定します。
password [**0** | **7**] *password*	（任意）サービス グループから受信したメッセージに対する Message Digest アルゴリズム 5（MD5）認証。認証で受け入れられなかったメッセージは廃棄されます。暗号化タイプには 0 ～ 7 のタイプを指定できます。0 は暗号化されないことを、7 は独自の暗号化を示します。*password* 引数の長さは最大 8 文字です。

コマンド デフォルト

WCCP サービスがルータでイネーブルになっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(31)SG	Catalyst 4500 シリーズ スイッチでサポートが開始されました。
15.0(2)SG/3.2(0)SG	Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E にサポートが拡張されました。
15.0(2)SG1	**redirect-list** キーワードのサポートが追加されました。
IOS XE 3.3.0 SG (15.1(1)SG)	Supervisor Engine 7-E および Supervisor Engine 7L-E にサポートが拡張されました。

使用上のガイドライン

このコマンドは、指定したサービス番号または Web キャッシュ サービス名に対するサポートをイネーブルまたはディセーブルにするようにルータに指示します。サービス番号には 0 ～ 254 を指定できます。サービス番号または名前がイネーブルになると、ルータはサービス グループの確立に参加できます。

no ip wccp コマンドを入力すると、ルータはサービス グループへの参加を終了し、他のインターフェイスがサービスに設定されていない場合はスペースの割り当てを解除し、他のサービスが設定されていない場合は WCCP タスクを終了します。

web-cache キーワードおよび *service-number* 引数の後に続くキーワードはオプションで、任意の順序で指定できますが、1 度しか指定できません。次の項では、このコマンドのさまざまな形式の使用方法について、概要を説明します。

ip wccp {web-cache | *service-number*} group-address *multicast-address*

WCCP グループ アドレスは、協調ルータと Web キャッシュが WCCP プロトコル メッセージの交換に使用するマルチキャスト アドレスを設定するために設定できます。このようなアドレスを使用する場合、IP マルチキャスト ルーティングをイネーブルにして、設定されたグループ（マルチキャスト）アドレスを使用するメッセージが正常に受信されるようにする必要があります。

このオプションは、このグループ アドレスで受信した「Here I Am」メッセージに対する「I See You」応答を結合するために、指定されたマルチキャスト IP アドレスを使用するようにルータに指示します。応答はグループ アドレスにも送信されます。デフォルトではグループ アドレスは設定されていないため、すべての「Here I Am」メッセージにユニキャスト応答が返されます。

ip wccp {web-cache | *service-number*} redirect-list *access-list*

このオプションは、サービス名で指定されたサービス グループの Web キャッシュにリダイレクトされるトラフィックを制御するのに、アクセス リストを使用するようにルータに指示します。*access-list* 引数には、標準または拡張アクセス リストの番号または名前を指定します。アクセス リストは、リダイレクトを許可されるトラフィックを指定します。デフォルトでは、リダイレクト リストは設定されていません（すべてのトラフィックがリダイレクトされます）。

WCCP では、次のプロトコルとポートが、いかなるアクセス リストによってもフィルタリングされないようにする必要があります。

- ユーザ データグラム プロトコル（UDP）（プロトコル タイプ 17）ポート 2048。このポートはシグナリングの制御に使用されます。このタイプのトラフィックをブロックすることで、WCCP によるルータとキャッシュ エンジン間の接続の確立が阻止されます。

ip wccp {web-cache | *service-number*} group-list *access-list*

このオプションは、指定されたサービス グループへの参加を許可されるキャッシュ エンジンを制御するのに、アクセス リストを使用するようにルータに指示します。*access-list* 引数には、標準または拡張アクセス リストの番号、または任意のタイプの名前付きアクセス リストの名前を指定します。アク

セス リストは、サービス グループへの参加を許可されるキャッシュ エンジンを指定します。デフォルトでは、グループ リストは設定されていないため、すべてのキャッシュ エンジンがサービス グループに参加する可能性があります。

（注）　**ip wccp** {**web-cache** | *service-number*} **group-list** コマンドの構文は、**ip wccp** {**web-cache** | *service-number*} **group-listen** コマンドと似ていますが、これらはまったく別のコマンドです。**ip wccp group-listen** コマンドは、キャッシュ クラスタからのマルチキャスト通知を受信するようインターフェイスを設定するために使用する、インターフェイス コンフィギュレーション コマンドです。『*Cisco IOS IP Application Services Command Reference*』の **ip wccp group-listen** コマンドの説明を参照してください。

ip wccp {web-cache | *service-number*} password *password*

このオプションは、サービス名で指定されたサービス グループから受信したメッセージに対して MD5 認証を適用するようルータに指示します。ルータにパスワードを設定するには、コマンドのこの形式を使用します。また、各 Web キャッシュに対して同じパスワードを個別に設定する必要があります。パスワードは最大 8 文字まで入力できます。ルータで認証がイネーブルになっているとき、認証されないメッセージは廃棄されます。デフォルトは認証パスワードは設定されておらず、認証はディセーブルになっています。

例

次に、マルチキャスト アドレス 239.0.0.0 を使用して、WCCP 逆プロキシ サービスを実行するようにルータを設定する例を示します。

```
Router(config)# ip multicast-routing
Router(config)# ip wccp 99 group-address 239.0.0.0
Router(config)# interface gigabitethernet 3/1
Router(config-if)# ip wccp 99 group-listen
```

次に、宛先が 10.168.196.51 以外の Web 関連パケットを Web キャッシュにリダイレクトするようにルータを設定する例を示します。

```
Router(config)# access-list 100 deny ip any host 10.168.196.51
Router(config)# access-list 100 permit ip any any
Router(config)# ip wccp web-cache redirect-list 100
Router(config)# interface gigabitethernet 3/2
Router(config-if)# ip wccp web-cache redirect out
```

関連コマンド

コマンド	説明
ip wccp check services all	すべての WCCP サービスをイネーブルにします。
ip wccp version	ルータで使用する WCCP のバージョンを指定します。
show ip wccp	WCCP に関連するグローバル統計情報を表示します。

ip wccp check services all

すべての Web キャッシュ通信プロトコル（WCCP）サービス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 **ip wccp check services all** コマンドを使用します。すべてのサービスをディセーブルにするには、このコマンドの **no** 形式を使用します。

ip wccp check services all

no ip wccp check services all

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

WCCP サービスがルータでイネーブルになっていません。

コマンド モード

グローバル コンフィギュレーション（config）

コマンド履歴

リリース	変更箇所
12.2(31)SG	Catalyst 4500 シリーズ スイッチでサポートが開始されました。
IOS XE 3.2(0)SG (15.0(2)SG)	Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E にサポートが拡張されました。
IOS XE 3.3.0 SG (15.1(1)SG)	Supervisor Engine 7-E および Supervisor Engine 7L-E にサポートが拡張されました。

使用上のガイドライン

ip wccp check services all コマンドを使用すると、一致についてすべての設定済みサービスをチェックし、必要に応じてそのサービスについてリダイレクションを実行するように WCCP を設定できます。パケットのリダイレクト先キャッシュは、リダイレクト ACL のアクセス コントロール リスト（ACL）と、サービスのプライオリティ値によって制御できます。

複数の WCCP サービスとのインターフェイスを設定することができます。1 つのインターフェイスに複数の WCCP サービスを設定する場合、サービスの優先順位は、他の設定済みサービスのプライオリティと比較した、そのサービスの相対的なプライオリティによって変わります。各 WCCP サービスには、定義の一部にプライオリティ値があります。

WCCP サービスをリダイレクト ACL を使用して設定する場合、IP パケットに一致するサービスが見つかるまで、プライオリティ順にサービスがチェックされます。パケットに一致するサービスがない場合、パケットはリダイレクトされません。サービスがパケットに一致し、サービスにリダイレクト ACL が設定されている場合、IP パケットは ACL に対してチェックされます。ACL によってパケットが拒否される場合、**ip wccp check services all** コマンドを設定していないと、低いプライオリティのサービスにパケットは渡されません。**ip wccp check services all** コマンドを設定すると、インターフェイスに設定されている残りの低いプライオリティのサービスに対して、引き続きパケットのマッチングが試行されます。

（注） WCCP サービス グループのプライオリティは、Web キャッシュ装置によって決まります。WCCP サービス グループのプライオリティは、Cisco IOS ソフトウェアで設定できません。

（注）　**ip wccp check services all** コマンドは、すべてのサービスに適用され、単一のサービスには関連付けられないグローバル WCCP コマンドです。

例

次に、すべての WCCP サービスを設定する例を示します。

```
Router(config)# ip wccp check services all
```

関連コマンド

コマンド	説明
ip wccp	サービス グループに参加できるように、指定した WCCP サービスのサポートをイネーブルにします。
ip wccp group-listen	Web キャッシュ通信プロトコル（WCCP）の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにするように、ルータ上のインターフェイスを設定します。
ip wccp redirect	Web キャッシュ通信プロトコル（WCCP）を使用して、受信インターフェイスまたは発信インターフェイスでパケットのリダイレクションをイネーブルにします。
ip wccp redirect exclude in	インターフェイスで受信したパケットを、リダイレクトのチェックから除外するようにインターフェイスを設定します。
ip wccp version	ルータで使用する WCCP のバージョンを指定します。

ip wccp group-listen

Web キャッシュ通信プロトコル（WCCP）の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにするようにルータ上のインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **ip wccp group-listen** コマンドを使用します。WCCP の IP マルチキャスト パケットの受信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 wccp {**web-cache** | *service-number*} **group-listen**

no ip wccp {**web-cache** | *service-number*} **group-listen**

構文の説明

web-cache	Web キャッシュ サービス。
service-number	WCCP サービス番号。有効値は 0 ～ 254 です。

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

インターフェイス コンフィギュレーション（config-if）

コマンド履歴

リリース	変更箇所
12.2(31)SG	Catalyst 4500 シリーズ スイッチでサポートが開始されました。
IOS XE 3.2(0)SG (15.0(2)SG)	Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E にサポートが拡張されました。
IOS XE 3.3.0 SG (15.1(1)SG)	Supervisor Engine 7-E および Supervisor Engine 7L-E にサポートが拡張されました。

使用上のガイドライン

IP マルチキャストを使用するとき、サービス グループのメンバであるルータでは、次の設定が必要です。

- WCCP サービス グループで使用する IP マルチキャスト アドレスを設定します。
- **ip wccp** {**web-cache** | *service-number*} **group-listen** インターフェイス コンフィギュレーション コマンドを使用して、ルータで IP マルチキャスト アドレスを受信するインターフェイスを設定します。

例

次に、マルチキャスト アドレスが 224.1.1.100 である Web キャッシュに対してマルチキャスト パケットをイネーブルにする例を示します。

```
Switch# configure terminal
Switch(config)# ip wccp web-cache group-address 224.1.1.100
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp web-cache group-listen
```

関連コマンド

コマンド	説明
ip wccp	サービス グループに参加できるように、WCCP サービスのサポートをイネーブルにします。
ip wccp check services all	すべての Web キャッシュ通信プロトコル（WCCP）サービスをイネーブルにします。
ip wccp redirect	インターフェイスでの WCCP リダイレクションをイネーブルにします。
ip wccp redirect	Web キャッシュ通信プロトコル（WCCP）を使用して、受信インターフェイスまたは発信インターフェイスでパケットのリダイレクションをイネーブルにします。
ip wccp redirect exclude in	インターフェイスで受信したパケットを、リダイレクトのチェックから除外するようにインターフェイスを設定します。
ip wccp version	ルータで使用する WCCP のバージョンを指定します。

ip wccp redirect

Web キャッシュ通信プロトコル（WCCP）を使用して、受信インターフェイスまたは発信インターフェイスでパケット リダイレクション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 **ip wccp redirect** コマンドを使用します。WCCP リダイレク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 wccp {**web-cache** | *service-number*} **redirect** {**in** | **out**}

no ip wccp {**web-cache** | *service-number*} **redirect** {**in** | **out**}

構文の説明

web-cache	Web キャッシュ サービスをイネーブルにします。
service-number	キャッシュ エンジン サービス グループの識別番号。有効値は 0 ～ 254 です。 キャッシュ エンジン クラスタでシスコ製キャッシュ エンジンが使用されている場合、リバース プロキシ サービスは、値 99 で指定されます。
in	着信インターフェイスでパケット リダイレクションを指定します。
out	発信インターフェイスでパケット リダイレクションを指定します。

コマンド デフォルト

インターフェイスでのリダイレクションの確認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（config-if）

コマンド履歴

リリース	変更箇所
12.2(31)SG	Catalyst 4500 シリーズ スイッチでサポートが開始されました。
IOS XE 3.2(0)SG (15.0(2)SG)	Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E にサポートが拡張されました。
15.0(2)SG1	**web-cache** キーワードおよび **service-number** キーワードが、Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E でサポートされました。
IOS XE 3.3.0 SG (15.1(1)SG)	Supervisor Engine 7-E および Supervisor Engine 7L-E にサポートが拡張されました。

使用上のガイドライン

ip wccp {web-cache | service-number} redirect in コマンドを使用すると、着信ネットワーク トラフィックを受信するインターフェイスに WCCP リダイレクションを設定できます。コマンドがインターフェイスに適用されると、そのインターフェイスに到着したすべてのパケットが、指定された WCCP サービスで定義された基準と比較されます。パケットが条件を満たしていれば、リダイレクトされます。

同様に、**ip wccp {web-cache | service-number} redirect out** コマンドでは、発信インターフェイスでの WCCP リダイレクション チェックを設定することができます。

ヒント　**ip wccp {web-cache | service-number} redirect {out | in}** コンフィギュレーション コマンドと、**ip wccp redirect exclude in** コンフィギュレーション コマンドを混同しないよう注意してください。

例

次に、イーサネット インターフェイス 3/1 上の逆プロキシ パケットのリダイレクションがチェックされ、シスコのキャッシュ エンジンにリダイレクトされるセッションを設定する例を示します。

```
Switch(config)# ip wccp 99
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp 99 redirect out
```

次に、ギガビット イーサネット インターフェイス 3/1 に到着した HTTP トラフィックをキャッシュ エンジンにリダイレクトするセッションを設定する例を示します。

```
Switch(config)# ip wccp web-cache
Switch(config)# interface gigabitethernet 3/1
Switch(config-if)# ip wccp web-cache redirect in
```

関連コマンド

コマンド	説明
ip wccp check services all	Web キャッシュ通信プロトコル（WCCP）の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにするように、ルータ上のインターフェイスを設定します。
ip wccp group-listen	Web キャッシュ通信プロトコル（WCCP）の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにするように、ルータ上のインターフェイスを設定します。
ip wccp redirect exclude in	インターフェイスでのリダイレクトの除外をイネーブルにします。
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
show ip wccp	WCCP のグローバル設定と統計情報を表示します。

ip wccp redirect exclude in

インターフェイスで受信したパケットを、リダイレクトのためのチェックから除外するようにインターフェイスを設定するには、インターフェイス コンフィギュレーション モードで **ip wccp redirect exclude in** コマンドを使用します。リダイレクション チェックからパケットを除外するためのルータ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。

ip wccp redirect exclude in

no ip wccp redirect exclude in

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

リダイレクトの除外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（config-if）

コマンド履歴

リリース	変更箇所
12.2(31)SG	Catalyst 4500 シリーズ スイッチでサポートが開始されました。
IOS XE 3.2(0)SG (15.0(2)SG)	Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E にサポートが拡張されました。
IOS XE 3.3.0 SG (15.1(1)SG)	Supervisor Engine 7-E および Supervisor Engine 7L-E にサポートが拡張されました。

使用上のガイドライン

このコンフィギュレーション コマンドは、リダイレクション チェックから受信パケットを除外するようにインターフェイスに指示します。このコマンドは、すべてのサービスに対してグローバルであり、リダイレクションから除外するすべての着信インターフェイスに適用されることに注意してください。

このコマンドは、キャッシュ エンジンからインターネットへのパケットのフローを高速化し、Web キャッシュ通信プロトコル（WCCP）v2 パケット リターン機能を使用できるようにするために使用することを目的としています。

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 3/1 に着信したパケットは、WCCP 出力リダイレクション チェックから除外されます。

```
Router (config)# interface gigabitethernet 3/1
Router (config-if)# ip wccp redirect exclude in
```

関連コマンド

コマンド	説明
ip wccp	サービス グループに参加できるように、WCCP サービスのサポートをイネーブルにします。
ip wccp redirect	Web キャッシュ通信プロトコル（WCCP）を使用して、受信インターフェイスまたは発信インターフェイスでパケットのリダイレクションをイネーブルにします。
ip wccp redirect out	発信方向のインターフェイスにリダイレクションを設定します。
ip wccp check services all	Web キャッシュ通信プロトコル（WCCP）の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにするように、ルータ上のインターフェイスを設定します。
ip wccp group-listen	Web キャッシュ通信プロトコル（WCCP）の IP マルチキャスト パケットの受信をイネーブルまたはディセーブルにするように、ルータ上のインターフェイスを設定します。
ip wccp redirect exclude in	インターフェイスでのリダイレクトの除外をイネーブルにします。
show ip interface	IP 用に設定されたインターフェイスが使用可能かどうかのステータスを表示します。
show ip wccp	WCCP のグローバル設定と統計情報を表示します。

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 の範囲は 1 ～ 1001 および 1006 ～ 4094 です。

デフォルト

スイッチ上で、MLD スヌーピングはグローバルにディセーブルです。

すべての VLAN で MLD スヌーピングはイネーブルです。ただし、VLAN スヌーピングが実行される前に、MLD スヌーピングをグローバルにイネーブルにする必要があります。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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 設定は、MLD スヌーピングがディセーブルのインターフェイス上のグローバル コンフィギュレーションを上書きします。

MLD スヌーピングがグローバルにディセーブルである場合、VLAN 上で MLD スヌーピングをイネーブルにできません。MLD スヌーピングがグローバルにイネーブルである場合、個々の VLAN 上で MLD スヌーピングをディセーブルにできます。

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）マルチキャスト リスナー検出（MLD）スヌーピング設定を表示します。

ipv6 mld snooping last-listener-query-count

クライアントが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。クエリー回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*] **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 の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	整数の範囲は 1 ～ 7 です。

コマンド デフォルト

デフォルトのグローバル カウントは 2 です。

デフォルトの VLAN カウントは 0 です（グローバル カウントを使用します）。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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する MASQ の数が決定します。

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 の数が設定されていない（デフォルトの 0 に設定されている）場合は、グローバルな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）マルチキャスト リスナー検出（MLD）スヌーピング設定を表示します。
show ipv6 mld snooping querier	スイッチまたは VLAN で最後に受信された IP version 6（IPv6）MLD スヌーピング クエリアに関連する情報を表示します。

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 の範囲は 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	変更箇所
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前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 で最後に受信された IP version 6（IPv6）MLD スヌーピング クエリアに関連する情報を表示します。

ipv6 mld snooping listener-message-suppression

IP version 6（IPv6）マルチキャスト リスナー検出（MLD）スヌーピング リスナー メッセージ抑制をイネーブルにするには、**ipv6 mld snooping listener-message-suppression** 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	変更箇所
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 の範囲は 1 ～ 1001 および 1006 ～ 4094 です。
integer_value	ロバストネス値の範囲は 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	変更箇所
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、スイッチが応答しないリスナーを削除する前に待機するクエリー数が決定し、VLAN 値が設定されていない VLAN すべてに適用されます。

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 にロバストネス変数を設定する方法を示します。この値は VLAN のグローバル コンフィギュレーションより優先されます。

```
Switch# 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）マルチキャスト リスナー検出（MLD）トポロジ変更通知（TCN）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、要求したポートだけにマルチキャスト データを転送する前に送信されるクエリー数です。指定できる範囲は 1 ～ 10 です。
query solicit	TCN クエリーの送信請求をイネーブルにします。

コマンド デフォルト

TCN クエリー送信請求はディセーブルです。

イネーブルの場合、デフォルトのフラッディング クエリー カウントは 2 です。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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。このコマンドの **no** 形式を使用すると、設定が削除されます。
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	変更箇所
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 つのレシーバだけが存在する場合、即時脱退処理の機能だけを設定してください。設定は、NVRAM に保存されます。

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

設定およびスタティック ポートとグループは、NVRAM に保存されます。

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 GigabitEthernet1/1
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 GigabitEthernet1/1
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	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	変更箇所
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、新しい Cisco IOS ソフトウェア イメージが ISSU プロセス中に自動的に停止し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）現在アクティブなスーパーバイザ エンジン上の新しいイメージの名前。

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	変更箇所
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

新しいイメージに満足し、新しいスーパーバイザ エンジンにコンソールとネットワークの両方から到達可能であることを確認したら、**issu acceptversion** コマンドを実行して、ロールバック タイマーを停止させます。**issu runversion** コマンドを入力してから 45 分以内に **issu acceptversion** コマンドが入力されなかった場合は、全体の ISSU プロセスが以前の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** コマンドを入力した直後に開始されます。

スタンバイ スーパーバイザ エンジンがホット スタンバイ状態になるまでにロールバック タイマーが切れると、タイマーは最長 15 分まで自動的に延長されます。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。介入を必要とする警告メッセージが、タイマーの延長時間の 1 分ごとに表示されます。

ロールバック タイマーが、デフォルトの 45 分などの長時間に設定されているとき、スタンバイ スーパーバイザ エンジンが 7 分でホット スタンバイ状態になった場合は、ロールバックまで 38 分（45 - 7）あることになります。

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 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）現在アクティブなスーパーバイザ エンジン上の新しいイメージの名前。

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	変更箇所
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 コマンドは、スタンバイ スーパーバイザ エンジンのファイル システムに新しい Cisco IOS ソフトウェア イメージが存在し、両方のスーパーバイザ エンジンが実行バージョン（RV）ステートにあることを確認します。これらの条件が満たされると、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 エンジンはリセットされ、Cisco IOS ソフトウェアの新しいバージョンで起動されます。
- スタンバイ スーパーバイザ エンジンがステートフル スイッチオーバー（SSO）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、インサービス ソフトウェア アップグレード（ISSU）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。現在の状態のまま長時間実行しない予定で、新しいソフトウェア バージョンに満足している場合は、**issu commitversion** コマンドを使用します。

例

次に、スタンバイ スーパーバイザ エンジンをリセットし、新しい Cisco IOS ソフトウェア バージョンでリロードするよう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	現在アクティブなスーパーバイザ 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	ネットワーキング 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）新しい 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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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の両方が、ISSU 対応、ISSU 互換であり、設定の不一致がない場合は、スタンバイ スーパーバイザ エンジンがステートフル スイッチオーバー（SSO）モードに移行し、両方のスーパーバイザ エンジンがロード バージョン（LV）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	ネットワーキング 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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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状態に移行すると、すぐにロールバック タイマーが起動します。

例

次に、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変更する例を示します。

```
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。

コマンド	説明
issu loadversion	ISSU プロセスを開始します。
show issu state	ISSU プロセス中に 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

インサービス ソフトウェア アップグレード（ISSU）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 秒の値を設定すると、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	変更箇所
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 エンジンが初期状態にある場合にのみイネーブルにすることができます。

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; Cisco Discovery Protocol）、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	変更箇所
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 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

次に、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例を示します。

```
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 パケットに対してサービス クラス（CoS）値を設定します。
l2protocol-tunnel drop-threshold	インターフェイスによってドロップされるまでに受信されるレイヤ 2 プロトコル パケットの最大レート（パケット/秒）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 パケットのサービス クラス（CoS）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でデータ用に設定された 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	変更箇所
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 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	インターフェイスによってドロップされるまでに受信されるレイヤ 2 プロトコル パケットの最大レート（パケット/秒）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

インターフェイスによってドロップするまでに受信されるレイヤ 2 プロトコル パケットの最大レート（パケット/秒）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）、スパニング ツリー プロトコル（STP）、または VLAN トランキング プロトコル（VTP）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	変更箇所
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

次に、ドロップしきい値レートを設定する例を示します。

```
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 パケットに対してサービス クラス（CoS）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）、スパニング ツリー プロトコル（STP）、または VLAN トランキング プロトコル（VTP）のパケットに対してカプセル化レートを設定できます。インターフェイスの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	変更箇所
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** コマンドを入力してエラー回復をイネーブルにすると、インターフェイスは errdisable ステートから抜け出し、すべての原因がタイムアウトになったときに動作を再開できます。**l2ptguard** でエラー回復機能がイネーブルにされないと、インターフェイスは、**shutdown** および **no shutdown** インターフェイス コンフィギュレーション コマンドが入力されるまで errdisable ステートのままになります。

例

次に、最大レートを設定する例を示します。

```
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 パケットに対してサービス クラス（CoS）値を設定します。
l2protocol-tunnel drop-threshold	インターフェイスによってドロップされるまでに受信されるレイヤ 2 プロトコル パケットの最大レート（パケット/秒）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	変更箇所
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

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 プライオリティは、ポート ID を作成するためにポート番号とともに使用されます。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 対応物理インターフェイスがあるポート チャネルでのみサポートされています。このコマンドは、LACP 対応インターフェイスでサポートされています。

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	変更箇所
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

LACP を実行している各スイッチに、システム プライオリティを自動的に設定するか、**lacp system-priority** コマンドを入力して割り当てる必要があります。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* の値は、LACP 対応物理インターフェイスがあるポート 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。

また、インターフェイス コンフィギュレーション モードで **lacp system-priority** コマンドを入力することもできます。このコマンドを入力すると、システムが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。

lldp tlv-select power-management

LLDP による電力ネゴシエーションをイネーブルにするには、**lldp tlv-select power-management** インターフェイス コマンドを使用します。

lldp tlv-select power-management

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

POEP ポートでイネーブルにします。

コマンド モード

インターフェイス レベル

コマンド履歴

リリース	変更箇所
12.2(54)SG	Catalyst 4500 シリーズ スイッチで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

LLDP による電力ネゴシエーションを実行しない場合は、この機能をディセーブルにする必要があります。

この機能は非 POEP ポートではサポートされていません。このようなポートでは CLI は抑制され、TLV は交換されません。

例

次に、インターフェイスのギガビット イーサネット 3/1 上で LLDP 電力ネゴシエーションをイネーブルにする例を示します。

```
Switch# config t
Enter configuration commands, one per line.  End with CNTL/Z.
Switch(config)# int gi 3/1
Switch(config-if)# lldp tlv-select power-management
```

関連コマンド

コマンド	説明
lldp run	Cisco IOS Command Reference ライブラリ。

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	変更箇所
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に対してリンクステータス 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	変更箇所
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でインターフェイス state-change 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	変更箇所
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に対してリンクステータス 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	変更箇所
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でインターフェイス state-change 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 認証バイパス（MAB）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	変更箇所
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

ポートにフォールバック方式として MAB が設定されていると、ホストの ID の要求失敗が設定可能な数に到達するまで、ポートは一般的な 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	変更箇所
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。
- 大文字と小文字を区別します。
- 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、MAC 層アクセス リストのエントリを作成または削除するには、次のサブセットを使用します。

[**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**} | <*arbitrary ethertype*> | *name-coded ethertype*].

表 2-10 に、**mac access-list extended** サブコマンドの構文の説明を示します。

表 2-10　mac access-list extended サブコマンド

サブコマンド	説明
any	送信元ホストまたは宛先ホストを指定します。
arbitrary ethertype	（任意）1536 ～ 65535 の範囲で任意の ethertype を指定します（10 進数または 16 進数）
deny	条件が一致した場合にアクセスを禁止します。

表 2-10　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）宛先 MAC アドレスを、*dest-mac-address dest-mac-address-mask* という形式で指定します。
name-coded ethertype	（任意）一般的なプロトコルの定義済みの *name-coded ethertype* を表します。 aarp：AppleTalk ARP amber：DEC-Amber appletalk：AppleTalk/EtherTalk dec-spanning：DEC スパニングツリー decnet-iv：DECnet Phase IV diagnostic：DEC-Diagnostic dsm：DEC-DSM etype-6000：0x6000 etype-8042：0x8042 lat：DEC-LAT lavc-sca：DEC-LAVC-SCA mop-console：DEC-MOP リモート コンソール mop-dump：DEC-MOP ダンプ msdos：DEC-MSDOS mumps：DEC-MUMPS netbios：DEC-NETBIOS protocol-family：イーサネット プロトコル ファミリ vines-echo：VINES Echo vines-ip：VINES IP xns-idp：XNS IDP
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。
protocol-family	（任意）プロトコル ファミリの名前です。表 2-11 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。
src-mac mask	*source-mac-address source-mac-address-mask* の形式の送信元 MAC アドレスです。

表 2-11 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 2-11　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。

表 2-11　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
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。
- 新しいエントリはすべて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 層アクセス 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。

mac-address（仮想スイッチ）

メディア アクセス コントロール（MAC）アドレスを、アクティブ シャーシとスタンバイ シャーシのインターフェイスで共通のルータ MAC アドレスとして使用するように指定するには、**mac-address** 仮想スイッチ コンフィギュレーション サブモード コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac-address {*mac-address* | **use-virtual** | **chassis**}

no mac-address {*mac-address* | **use-virtual** | **chassis**}

構文の説明

mac-address	MAC アドレスを 16 進数形式で指定します。
use-virtual	仮想スイッチ システム（VSS）用に予約される MAC アドレスの範囲を指定します。
chassis	シャーシから取得される MAC アドレスを指定します。

デフォルト

ルータの MAC アドレスは、ドメイン 1 ～ 255 を対象とするシスコの仮想スイッチ固有の MAC アドレス プールから取得されます。

コマンド モード

仮想スイッチ コンフィギュレーション サブモード（config-vs-domain）

コマンド履歴

リリース	変更箇所
Cisco IOS XE 3.4.0SG および 15.1(2)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

仮想スイッチを起動すると、シスコの仮想スイッチ固有の MAC アドレス プールからルータの MAC アドレスが取得されます。ルータ アドレスは、アクティブ シャーシとスタンバイ シャーシの両方のインターフェイスに共通のルータ MAC アドレスとして使用されます。スイッチオーバー間で、この MAC アドレスが新しいアクティブ スイッチ上で維持されます。**mac-address mac-address** コマンドを入力して、使用する MAC アドレスを指定するか、**mac-address use-virtual** コマンドを入力して、VSS 用に予約された MAC アドレス範囲を使用することができます。

VSS 用に予約された MAC アドレス範囲は、最後のオクテットの先頭の 6 ビットと mac-address の前のオクテットの末尾の 2 ビットで符号化されたドメイン ID を持つアドレスの専用プールから取得されます。最初のオクテットの最後の 2 ビットは、プロトコル ID（0 ～ 3）をルータ MAC アドレスに追加することによって取得されたプロトコル mac-address に割り当てられます。

（注） 新しいルータ MAC アドレスを有効にするには、仮想スイッチをリロードします。設定した MAC アドレスが現在の MAC アドレスと異なる場合は、次のメッセージが表示されます。

Console (enable)#

例

次に、使用する MAC アドレスを 16 進数形式で指定する例を示します。

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address 0000.0000.0000
```

```
Router(config-vs-domain)#
```

次に、VSS 用に予約される MAC アドレス範囲を指定する例を示します。

```
Router(config)# switch virtual domain test-mac-address
Router(config-vs-domain)# mac-address use-virtual
Router(config-vs-domain)#
```

関連コマンド

コマンド	説明
switch virtual domain（仮想スイッチ）	スイッチ番号を割り当て、仮想スイッチ ドメイン コンフィギュレーション サブモードを開始します。

mac-address-table aging-time

レイヤ 2 テーブルでエントリのエージング タイムを設定するには、**mac-address-table aging-time** コマンドを使用します。*seconds* の値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。

mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

no mac-address-table aging-time *seconds* [**vlan** *vlan_id*]

構文の説明

seconds	エージング タイム。秒で指定します。有効値は、0 および 10 ～ 1000000 秒です。
vlan *vlan_id*	（任意）単一の VLAN 番号または VLAN の範囲。有効値は 1 ～ 4094 です。

デフォルト

エージング タイムは 300 秒に設定されます。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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

VLAN を入力しない場合、変更はすべてのルーテッド ポート VLAN に適用されます。

エージングをディセーブルにするには、0 秒を入力します。

例

次に、エージング タイムを 400 秒に設定する例を示します。

```
Switch(config)# mac-address-table aging-time 400
Switch(config)#
```

次に、エージングをディセーブルにする例を示します。

```
Switch(config)# mac-address-table aging-time 0
Switch(config)
```

関連コマンド

コマンド	説明
show mac-address-table aging-time	MAC アドレス テーブルのエージング情報を表示します。

mac-address-table dynamic group protocols

「ip」および「other」のプロトコル バケットの両方で MAC アドレス ラーニングをイネーブルにするには、着信パケットがこれらのプロトコル バケットのいずれか一方だけに属している場合でも、**mac-address-table dynamic group protocols** コマンドを使用します。グループ ラーニ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。

mac-address-table dynamic group protocols {**ip** | **other**} {**ip** | **other**}

no mac-address-table dynamic group protocols {**ip** | **other**} {**ip** | **other**}

構文の説明

ip	「ip」プロトコル バケットを指定します。
other	「other」のプロトコル バケットを指定します。

デフォルト

グループ ラーニング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	変更箇所
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

「ip」および「other」のプロトコル バケット内のエントリは、着信トラフィックのプロトコルに応じて作成されます。

mac-address-table dynamic group protocols コマンドを使用すると、「ip」または「other」のプロトコル バケットに属する着信 MAC アドレスが、両方のプロトコル バケットで学習されます。したがって、この MAC アドレス宛てで、いずれかのプロトコル バケットに属するすべてのトラフィックが、フラッディングするせずにその MAC アドレスにユニキャストされます。これによって、あるホストからの着信トラフィックが、送信元ホスト宛てのトラフィックとは異なるプロトコル バケットに属する場合に、ユニキャスト レイヤ 2 フラッディングが発生する可能性が小さくなります。

例

次に、MAC アドレスが「ip」または「other」のプロトコル バケットのいずれかに最初に割り当てられる例を示します。

```
Switch# show mac-address-table dynamic
Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.5000   dynamic other                 GigabitEthernet1/1
   1    0001.0234.6616   dynamic ip                    GigabitEthernet3/1
   1    0003.3178.ec0a   dynamic assigned              GigabitEthernet3/1
   1    0003.4700.24c3   dynamic ip                    GigabitEthernet3/1
   1    0003.4716.f475   dynamic ip                    GigabitEthernet3/1
   1    0003.4748.75c5   dynamic ip                    GigabitEthernet3/1
   1    0003.47f0.d6a3   dynamic ip                    GigabitEthernet3/1
   1    0003.47f6.a91a   dynamic ip                    GigabitEthernet3/1
```

```
   1    0003.ba06.4538   dynamic ip                    GigabitEthernet3/1
   1    0003.fd63.3eb4   dynamic ip                    GigabitEthernet3/1
   1    0004.2326.18a1   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5d.de53   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5e.6ecc   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5e.f60e   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.06f7   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.072f   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.08f6   dynamic ip                    GigabitEthernet3/1
   1    0004.5a5f.090b   dynamic ip                    GigabitEthernet3/1
   1    0004.5a88.b075   dynamic ip                    GigabitEthernet3/1
   1    0004.c1bd.1b40   dynamic ip                    GigabitEthernet3/1
   1    0004.c1d8.b3c0   dynamic ip                    GigabitEthernet3/1
   1    0004.c1d8.bd00   dynamic ip                    GigabitEthernet3/1
   1    0007.e997.74dd   dynamic ip                    GigabitEthernet3/1
   1    0007.e997.7e8f   dynamic ip                    GigabitEthernet3/1
   1    0007.e9ad.5e24   dynamic ip                    GigabitEthernet3/1
   1    000b.5f0a.f1d8   dynamic ip                    GigabitEthernet3/1
   1    000b.fdf3.c498   dynamic ip                    GigabitEthernet3/1
   1    0010.7be8.3794   dynamic assigned              GigabitEthernet3/1
   1    0012.436f.c07f   dynamic ip                    GigabitEthernet3/1
   1    0050.0407.5fe1   dynamic ip                    GigabitEthernet3/1
   1    0050.6901.65af   dynamic ip                    GigabitEthernet3/1
   1    0050.da6c.81cb   dynamic ip                    GigabitEthernet3/1
   1    0050.dad0.af07   dynamic ip                    GigabitEthernet3/1
   1    00a0.ccd7.20ac   dynamic ip                    GigabitEthernet3/1
   1    00b0.64fd.1c23   dynamic ip                    GigabitEthernet3/1
   1    00b0.64fd.2d8f   dynamic assigned              GigabitEthernet3/1
   1    00d0.b775.c8bc   dynamic ip                    GigabitEthernet3/1
   1    00d0.b79e.de1d   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c79.1939   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c7b.d765   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c82.66b7   dynamic ip                    GigabitEthernet3/1
   1    00e0.4c8b.f83e   dynamic ip                    GigabitEthernet3/1
   1    00e0.4cbc.a04f   dynamic ip                    GigabitEthernet3/1
   1    0800.20cf.8977   dynamic ip                    GigabitEthernet3/1
   1    0800.20f2.82e5   dynamic ip                    GigabitEthernet3/1
Switch#
```

次に、「ip」または「other」のバケットのいずれかに属する MAC アドレスを両方のバケットに割り当てる例を示します。

```
Switch(config)# mac-address-table dynamic group protocols ip other
Switch(config)# exit
Switch# show mac address-table dynamic
Unicast Entries
 vlan   mac address     type        protocols               port
-------+---------------+--------+---------------------+--------------------
   1    0000.0000.5000   dynamic ip,other              GigabitEthernet1/1
   1    0001.0234.6616   dynamic ip,other              GigabitEthernet3/1
   1    0003.4700.24c3   dynamic ip,other              GigabitEthernet3/1
   1    0003.4716.f475   dynamic ip,other              GigabitEthernet3/1
   1    0003.4748.75c5   dynamic ip,other              GigabitEthernet3/1
   1    0003.47c4.06c1   dynamic ip,other              GigabitEthernet3/1
   1    0003.47f0.d6a3   dynamic ip,other              GigabitEthernet3/1
   1    0003.47f6.a91a   dynamic ip,other              GigabitEthernet3/1
   1    0003.ba0e.24a1   dynamic ip,other              GigabitEthernet3/1
   1    0003.fd63.3eb4   dynamic ip,other              GigabitEthernet3/1
   1    0004.2326.18a1   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5d.de53   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5d.de55   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5e.6ecc   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5e.f60e   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a5f.08f6   dynamic ip,other              GigabitEthernet3/1
```

```
   1    0004.5a5f.090b   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a64.f813   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a66.1a77   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a6b.56b2   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a6c.6a07   dynamic ip,other              GigabitEthernet3/1
   1    0004.5a88.b075   dynamic ip,other              GigabitEthernet3/1
   1    0004.c1bd.1b40   dynamic ip,other              GigabitEthernet3/1
   1    0004.c1d8.b3c0   dynamic ip,other              GigabitEthernet3/1
   1    0004.c1d8.bd00   dynamic ip,other              GigabitEthernet3/1
   1    0005.dce0.7c0a   dynamic assigned             GigabitEthernet3/1
   1    0007.e997.74dd   dynamic ip,other              GigabitEthernet3/1
   1    0007.e997.7e8f   dynamic ip,other              GigabitEthernet3/1
   1    0007.e9ad.5e24   dynamic ip,other              GigabitEthernet3/1
   1    0007.e9c9.0bc9   dynamic ip,other              GigabitEthernet3/1
   1    000b.5f0a.f1d8   dynamic ip,other              GigabitEthernet3/1
   1    000b.fdf3.c498   dynamic ip,other              GigabitEthernet3/1
   1    0012.436f.c07f   dynamic ip,other              GigabitEthernet3/1
   1    0050.0407.5fe1   dynamic ip,other              GigabitEthernet3/1
   1    0050.6901.65af   dynamic ip,other              GigabitEthernet3/1
   1    0050.da6c.81cb   dynamic ip,other              GigabitEthernet3/1
   1    0050.dad0.af07   dynamic ip,other              GigabitEthernet3/1
   1    00a0.ccd7.20ac   dynamic ip,other              GigabitEthernet3/1
   1    00b0.64fd.1b84   dynamic assigned             GigabitEthernet3/1
   1    00d0.b775.c8bc   dynamic ip,other              GigabitEthernet3/1
   1    00d0.b775.c8ee   dynamic ip,other              GigabitEthernet3/1
   1    00d0.b79e.de1d   dynamic ip,other              GigabitEthernet3/1
   1    00e0.4c79.1939   dynamic ip,other              GigabitEthernet3/1
   1    00e0.4c7b.d765   dynamic ip,other              GigabitEthernet3/1
   1    00e0.4c82.66b7   dynamic ip,other              GigabitEthernet3/1
   1    00e0.4c8b.f83e   dynamic ip,other              GigabitEthernet3/1
   1    00e0.4c8c.0861   dynamic ip,other              GigabitEthernet3/1
   1    0800.20d1.bf09   dynamic ip,other              GigabitEthernet3/1
Switch#
```

mac address-table learning vlan

VLAN で MAC アドレス ラーニングをイネーブルにするには、**mac address-table learning** グローバル コンフィギュレーション コマンドを使用します。VLAN で MAC アドレス ラーニングをディセーブルにして、MAC アドレスを学習できる VLAN を制御するには、このコマンドの **no** 形式を使用します。

mac address-table learning vlan *vlan-id*

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

構文の説明

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

デフォルト

すべての VLAN でイネーブル

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)SG	このコマンドは、Catalyst 4500 シリーズ スイッチの学習機能のディセーブル化をサポートするように変更されました。

使用上のガイドライン

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

MAC アドレス ラーニングは単一の VLAN ID（たとえば、**no mac address-table learning vlan 223** と入力）、または VLAN ID の範囲（たとえば、**no mac address-table learning vlan 1-20, 15** と入力）に対してディセーブルにできます。

MAC アドレス ラーニングをディセーブルにする前に、ネットワーク トポロジとスイッチ システムの設定についてよく理解してください。VLAN で MAC アドレス ラーニングをディセーブルにすると、ネットワークでフラッディングが発生する場合があります。たとえば、スイッチ仮想インターフェイス（SVI）を設定済みの VLAN で MAC アドレス ラーニングをディセーブルにした場合、スイッチはレイヤ 2 ドメインにすべての IP パケットをフラッディングします。3 つ以上のポートを含む VLAN で MAC アドレス ラーニングをディセーブルにした場合、スイッチに着信するすべてのパケットは、その VLAN ドメインでフラッディングします。2 つのポートが含まれる VLAN だけで MAC アドレス ラーニングをディセーブルにします。SVI が設定された VLAN で MAC アドレス ラーニングをディセーブルにする場合は、十分注意してください。

スイッチが内部的に使用する VLAN で MAC アドレス ラーニングはディセーブルにできません。この操作によって、スイッチでエラー メッセージが発生し、**no mac address-table learning vlan** コマンドが拒否されるようになります。使用している内部 VLAN を表示するには、**show vlan internal usage** 特権 EXEC コマンドを入力します。

PVLAN のプライマリまたはセカンダリ VLAN として設定された VLAN で MAC アドレス ラーニングをディセーブルにする場合、MAC アドレスは、その PVLAN に関連付けられた VLAN（プライマリまたはセカンダリ）上で引き続き学習されます。

RSPAN VLAN で MAC アドレス ラーニングはディセーブルにできません。設定すること自体できません。

セキュア ポートを含む VLAN で MAC アドレス ラーニングをディセーブルにする場合、セキュア ポートで MAC アドレス ラーニングはディセーブルになりません。後でインターフェイスのポート セキュリティをディセーブルにすると、ディセーブルになった MAC アドレス ラーニングの状態がイネーブルになります。

特定の VLAN またはすべての VLAN の MAC アドレス ラーニングのステータスを表示するには、**show mac-address-table learning vlan** コマンドを入力します。

例

次の例では、VLAN 2003 で MAC アドレス ラーニングをディセーブルにする方法を示します。

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

関連コマンド

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

mac-address-table notification

スイッチで MAC アドレス通知をイネーブルにするには、**mac-address-table notification** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mac-address-table notification [[**change** [**history-size** *hs_value* | **interval** *intv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage* | **interval** *time*]] | [**learn-fail** [**interval** *time* | **limit** *num_fail*]]

no mac-address-table notification [[**change** [**history-size** *hs_value* | **interval** *intv_value*]] | [**mac-move**] | [**threshold** [**limit** *percentage* | **interval** *time*]] | [**learn-fail** [**interval** *time* | **limit** *num_fail*]]

構文の説明

change	（任意）MAC 変更通知のイネーブル化を指定します。
history-size *hs_value*	（任意）MAC 変更通知の履歴テーブル内の最大エントリ数を設定します。指定できる範囲は 0 ～ 500 エントリです。
interval *intv_value*	（任意）通知トラップ間隔（2 つの連続するトラップ間の間隔）を設定します。指定できる範囲は 0 ～ 2,147,483,647 秒です。
mac-move	（任意）MAC 移動通知のイネーブル化を指定します。
threshold	（任意）MAC しきい値通知のイネーブル化を指定します。
limit *percentage*	（任意）MAT 利用率しきい値を指定します。有効値は 1 ～ 100% です。
interval *time*	（任意）MAC しきい値通知間隔を指定します。有効な値は 120 秒以上です。
learn-fail	（任意）ソフトウェアで学習した MAC アドレスをハードウェアにインストールする際の失敗についての syslog（レベル 6）通知を指定します。デフォルトでは、ディセーブルです。
interval *time*	（任意）ハードウェア MAC ラーニングの失敗通知の syslog 間隔を指定します。デフォルト値は 150 秒です。範囲は 1 ～ 100000 秒です。
limit *num_fail*	（任意）通知間隔で許可されているハードウェア MAC ラーニングの失敗回数を指定します。

デフォルト

MAC アドレス通知機能はディセーブルです。

デフォルトの MAC 変更トラップ間隔の値は 1 秒です。

履歴テーブルのデフォルトのエントリ数は 1 です。

MAC 移動通知はディセーブルです。

MAC しきい値モニタリング機能はディセーブルです。

limit のデフォルトは 50% です。

time のデフォルトは 120 秒です。

ハードウェア MAC ラーニングの失敗の syslog 通知はディセーブルです。

limit のデフォルトは 1000 です。

interval のデフォルトは 150 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	変更箇所
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。
12.2(52)SG	**learn-fail** キーワードが、Supervisor Engine 6-E と Catalyst 4900M で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

MAC 変更通知機能は、**mac-address-table notification change** コマンドを使用してイネーブルにできます。これを実行する場合は、
snmp trap mac-notification change interface コンフィギュレーション コマンドを使用してインターフェイスで MAC 通知トラップをイネーブルにし、**snmp-server enable traps mac-notification** グローバル コンフィギュレーション コマンドを使用してスイッチが MAC 変更トラップを NMS に送信するよう設定する必要があります。

history-size オプションを設定すると、既存の MAC 変更履歴テーブルが削除され、新しいテーブルが作成されます。

例

次の例は、MAC アドレス通知履歴テーブルのサイズを 300 エントリに設定する方法を示しています。

```
Switch(config)# mac-address-table notification change history-size 300
Switch(config)#
```

次の例は、MAC アドレス通知間隔を 1250 秒に設定する方法を示しています。

```
Switch(config)# mac-address-table notification change interval 1250
Switch(config)#
```

次の例は、ハードウェア MAC アドレス ラーニング失敗の syslog 通知をイネーブルにする方法を示しています。

```
Switch(config)# mac address-table notification learn-fail
```

次の例は、ハードウェア MAC アドレス ラーニング失敗の syslog 通知の間隔を 30 秒に設定する方法を示しています。

```
Switch(config)# mac address-table notification learn-fail interval 30
```

関連コマンド

コマンド	説明
clear mac-address-table	レイヤ 2 MAC アドレス テーブルから、グローバル カウンタ エントリをクリアします。
mac-address-table notification	スイッチで MAC アドレス通知をイネーブルにします。
snmp-server enable traps	SNMP 通知をイネーブルにします。
snmp trap mac-notification change	SNMP MAC アドレス通知をイネーブルにします。

mac-address-table static

VLAN インターフェイスのスタティック MAC アドレスを設定するか、または VLAN インターフェイスの MAC アドレスに対するユニキャスト トラフィックをドロップするには、**mac-address-table static** コマンドを使用します。スタティック MAC アドレスの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。

mac-address-table static *mac-addr* {**vlan** *vlan-id*} {**interface** *type* | **drop**}

no mac-address-table static *mac-addr* {**vlan** *vlan-id*} {**interface** *type*} {**drop**}

構文の説明

mac-addr	MAC アドレス。このコマンドの **no** 形式を使用する場合のオプションです。
vlan *vlan-id*	VLAN および有効な VLAN 番号。有効値は 1 ～ 4094 です。
interface *type*	インターフェイスのタイプと番号。有効なオプションは **FastEthernet** と **GigabitEthernet** です。
drop	指定された VLAN 内の設定された MAC アドレスとの間で送受信されるすべてのトラフィックをドロップします。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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

スタティック MAC アドレスを設定すると、ポートに関連付けられます。

指定された出力インターフェイスは、SVI ではなく、レイヤ 2 インターフェイスである必要があります。

プロトコル タイプを入力しない場合、4 つのプロトコル タイプのそれぞれについてエントリが自動的に作成されます。

このコマンドの **no** 形式を入力しても、システム MAC アドレスは削除されません。

MAC アドレスを削除するときには、**interface** *int* の入力は省略できます。ユニキャスト エントリの場合、エントリは自動的に削除されます。マルチキャスト エントリの場合、インターフェイスを指定しないとエントリ全体が削除されます。インターフェイスを指定することにより、削除する選択ポートを指定できます。

例

次に、MAC アドレス テーブルにスタティック エントリを追加する例を示します。

```
Switch(config)# mac-address-table static 0050.3e8d.6400 vlan 100 interface fastethernet5/7
Switch(config)#
```

関連コマンド

コマンド	説明
show mac-address-table static	スタティック MAC アドレス テーブル エントリだけを表示します。

macro apply 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がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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だけが可能です。変更することはできません。

インターフェイスの既存の設定が目的のマクロの設定と競合しないようにします。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設定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がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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だけが可能です。変更することはできません。

インターフェイスの既存の設定が目的のマクロの設定と競合しないようにします。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設定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-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がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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だけが可能です。変更することはできません。

インターフェイスの既存の設定が目的のマクロの設定と競合しないようにします。**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 ポートを他のスイッチ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-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がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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だけが可能です。変更することはできません。

インターフェイスの既存の設定が目的のマクロの設定と競合しないようにします。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設定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 auto device

あるデバイス タイプに対する組み込み関数のパラメータ変更を簡素化するには、**macro auto device** コマンドを使用します。初期パラメータ値に戻すには、このコマンドの **no** 形式を使用します。

macro auto device *device_type* [*params values*]

no macro auto device *device_type* [*params values*]

構文の説明

device_type	デバイス タイプを指定します。 • phone：電話を検出するインターフェイス設定を適用します。 • switch：スイッチを検出するインターフェイス設定を適用します。 • router：ルータを検出するインターフェイス設定を適用します。 • ap：ap を検出するインターフェイス設定を適用します。 • lwap：Lightweight ap を検出するインターフェイス設定を適用します。 • dmp：DMP を検出するインターフェイス設定を適用します。 • ipvsc：IPVSC を検出するインターフェイス設定を適用します。
param name=value	（任意）*parameter=value*：**$** で始まるデフォルト値を置き換えます。それぞれの名前と値のペアをスペースで区切る形式で新しい値を入力します（例：[<name1>=<value1> <name2>=<value2>...]）。デフォルト値は丸カッコ内に表示されます。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)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

macro auto execute コマンドを使用しても **macro auto device** コマンドと同じ効果が得られますが、後者の方が簡単です。

例

次に、アクセス VLAN と音声 VLAN を、デフォルト値からユーザが定義した電話デバイスの値に変更する例を示します。

```
(config)# macro auto device phone ACCESS_VLAN=10 VOICE_VLAN=20
```

関連コマンド

コマンド	説明
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
macro auto sticky	リンク フラップとデバイス取り外しに対し ASP によって適用された設定を削除しないように指定します。
shell trigger	ユーザ定義トリガーを作成します。

macro auto execute（組み込み関数）

組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡すには、**macro auto execute** コンフィギュレーション コマンドを使用します。トリガーのマッピングを解除するには、このコマンドの **no** 形式を使用します。

macro auto execute *event_trigger* **builtin** *shell_function* **[***param name=values***]**

no macro auto execute *event_trigger* **builtin** *shell_function* **[***param name=values***]**

構文の説明

event_trigger	イベント トリガーから組み込みマクロへのマッピングを定義します。 *event trigger* に次の値を指定します。 • CISCO_PHONE_EVENT • CISCO_SWITCH_EVENT • CISCO_ROUTER_EVENT • CISCO_WIRELESS_AP_EVENT • CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT • CISCO_DMP_EVENT • CISCO_IPVSC_EVENT • WORD：ユーザ定義のイベント トリガーを適用します。
shell_function	次の 組み込みマクロ名を指定します。 • CISCO_PHONE_AUTO_SMARTPORT （任意）パラメータ値 $ACCESS_VLAN=(1) および $VOICE_VLAN=(2) を指定します。 • CISCO_SWITCH_AUTO_SMARTPORT （任意）パラメータ値 $NATIVE_VLAN=(1) を指定します。 • CISCO_ROUTER_AUTO_SMARTPORT （任意）パラメータ値 $NATIVE_VLAN=(1) を指定します。 • CISCO_AP_AUTO_SMARTPORT （任意）パラメータ値 $NATIVE_VLAN=(1) を指定します。 • CISCO_LWAP_AUTO_SMARTPORT （任意）パラメータ値 $ACCESS_VLAN=(1) を指定します。 • CISCO_DMP_AUTO_SMARTPORT • CISCO_IP_CAMERA_AUTO_SMARTPORT
param name=value	（任意）関数本体で使用されるパラメータの値を指定します。

デフォルト

Auto Smartports 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

コマンド履歴

リリース	変更箇所
12.2(54)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

スイッチは組み込みイベント トリガーから組み込み関数に自動的にマッピングします。組み込み関数は、ソフトウェア イメージでシステム定義された関数です。

組み込み関数のデフォルト値を、スイッチに固有の値で置き換えるには、**macro auto execute** グローバル コンフィギュレーション コマンドを使用します。

ユーザ定義トリガーを作成し、このコマンドを使用してトリガーを組み込み関数にマッピングすることもできます。

shell trigger グローバル コンフィギュレーション コマンドを入力すると、ユーザ定義のイベント トリガーを作成できます。組み込みおよびユーザ定義のトリガーと関数の内容を表示するには、**show shell** 特権 EXEC コマンドを使用します。

例

次の例では、該当するスイッチに Cisco スイッチと Cisco IP Phone を接続するための 2 つの組み込み Auto Smartports マクロを使用する方法を示します。この例ではトランク インターフェイス用にデフォルトの音声 VLAN、アクセス VLAN、およびネイティブ VLAN を変更します。

```
Switch# configure terminal
Switch(config)#!!! the next command modifies the access and voice vlans
Switch(config)#!!! for the built in Cisco IP phone auto smartport macro
Switch(config)# macro auto execute CISCO_PHONE_EVENT builtin CISCO_PHONE_AUTO_SMARTPORT
ACCESS_VLAN=10 VOICE_VLAN=20
Switch(config)#
Switch(config)#!!! the next command modifies the native vlan
Switch(config)#!!! for the built in switch auto smartport macro
Switch(config)# macro auto execute CISCO_SWITCH_EVENT builtin CISCO_SWITCH_AUTO_SMARTPORT
NATIVE_VLAN=10
Switch(config)#!!! the next example creates a user-defined trigger and maps it to a
builtin functions
Switch(config)# shell trigger myTrigger "user-defined trigger"
Switch(config)# macro auto execute myTrigger builtin CISCO_PHONE_AUTO_SMARTPORT_ACCESSVLAN
voice_vlan
Switch(config)#!!! the next command enables auto smart ports globally
Switch(config)# macro auto global processing fallback CDP

Switch# !!! here's the running configuration of the interface connected
Switch# !!! to another Cisco Switch after the Macro is applied
Switch#
Switch# show running-config interface Gi1/0/1
Building configuration...

Current configuration : 284 bytes
!
interface GigabitEthernet1/0/1
 switchport trunk encapsulation dot1q
 switchport trunk native vlan 10
 switchport mode trunk
 srr-queue bandwidth share 10 10 60 20
 queue-set 2
 priority-queue out
 mls qos trust cos
 auto qos voip trust
 macro description CISCO_SWITCH_EVENT
end
```

関連コマンド

コマンド	説明
macro auto device	あるデバイス タイプに対する組み込み関数のパラメータ変更を簡素化します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
macro auto sticky	リンク フラップとデバイス取り外しに対し ASP によって適用された設定を削除しないように指定します。
shell trigger	ユーザ定義トリガーを作成します。

macro auto execute（リモート定義されたトリガー）

macro auto execute コンフィギュレーション コマンドを使用して、トリガーをリモート定義された関数にマッピングします。トリガーのマッピングを解除するには、このコマンドの **no** 形式を使用します。

macro auto execute *trigger_name* **remote** *url*

no macro auto execute *trigger_name* **remote** *url*

構文の説明

trigger_name	トリガーの名前を指定します。
url	リモート定義された URL を指定します

デフォルト

なし

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)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

このコマンドにより、シェル関数を一か所に集中して格納でき、複数のスイッチ上で ASP によって使用できます。これにより、変更のたびにすべてのスイッチで関数を更新する問題を軽減できます。

リモートで定義された関数のトリガーには URL へのネットワーク接続が必要であり、関数を実行するたびにアクセスされます。

例

次に、リモートで定義された関数 **myfunction** にトリガーをマッピングする例を示します。このファイル名には関数本体が含まれます。

```
Switch(config)# macro auto execute mytrigger remote tftp://dirt/tftpboot/myfunction
```

関連コマンド

コマンド	説明
macro auto device	あるデバイス タイプに対する組み込み関数のパラメータ変更を簡素化します。
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。

コマンド	説明
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
macro auto sticky	リンク フラップとデバイス取り外しに対し ASP によって適用された設定を削除しないように指定します。
shell trigger	ユーザ定義トリガーを作成します。

macro auto execute（ユーザ定義関数）

macro auto execute コンフィギュレーション コマンドを使用して、トリガーをユーザ定義関数にマッピングします。トリガーのマッピングを解除するには、このコマンドの **no** 形式を使用します。

macro auto execute *trigger_name* **[***param_name=value***]** {*function body*}

no macro auto execute *trigger_name* **[***param_name=value***]**

構文の説明

trigger_name	トリガーの名前を指定します。
param name=value	（任意）関数本体で使用されるパラメータの値を指定します。
function_body	CLI によるシェル関数。

デフォルト

なし。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)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

このコマンドで定義された関数には名前がないため、別のトリガーへのマップに使用できません。これは、トリガーをユーザ定義関数にマップする唯一の方法です。コンフィギュレーション モード以外で定義されたシェル関数は、トリガーのマップに使用できません。

例

次の例では、ユーザ定義のイベント トリガーである **Cisco Digital Media Player**（DMP）をユーザ定義のマクロにマッピングする方法を示します。

a. 802.1x または MAB に対応したスイッチ ポートに DMP を接続します。

b. RADIUS サーバ上で、属性と値のペアを **auto-smart-port**=CISCO_DMP_EVENT に設定します。

c. スイッチ上で、イベント トリガー CISCO_DMP_EVENT を作成し、次に示すユーザ定義のマクロ コマンドを入力します。

d. スイッチは、RADIUS サーバからの attribute-value pair=CISCO_DMP_EVENT 応答を受け入れ、このイベント トリガーに関連付けられたマクロを適用します。

```
Switch(config)# shell trigger CISCO_DMP_EVENT Cisco DMP player
Switch(config)# macro auto execute CISCO_DMP_EVENT {
if [[ $LINKUP -eq YES ]]; then
conf t
 interface $INTERFACE
   macro description $TRIGGER
   switchport access vlan 1
   switchport mode access
   switchport port-security
   switchport port-security maximum 1
   switchport port-security violation restrict
```

```
   switchport port-security aging time 2
   switchport port-security aging type inactivity
   spanning-tree portfast
   spanning-tree bpduguard enable
   exit
fi
if [[ $LINKUP -eq NO ]]; then
conf t
interface $INTERFACE
     no macro description $TRIGGER
     no switchport access vlan 1
     if [[ $AUTH_ENABLED -eq NO ]]; then
        no switchport mode access
     fi
     no switchport port-security
     no switchport port-security maximum 1
     no switchport port-security violation restrict
     no switchport port-security aging time 2
     no switchport port-security aging type inactivity
     no spanning-tree portfast
     no spanning-tree bpduguard enable
     exit
fi
}
Switch(config)# end
```

関連コマンド

コマンド	説明
macro auto device	あるデバイス タイプに対する組み込み関数のパラメータ変更を簡素化します。
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
macro auto sticky	リンク フラップとデバイス取り外しに対し ASP によって適用された設定を削除しないように指定します。
shell trigger	ユーザ定義トリガーを作成します。

macro auto global processing

スイッチで Auto SmartPorts マクロをイネーブルにするには、**macro auto global processing** グローバル コンフィギュレーション コマンドを使用します。Auto SmartPorts（ASP）マクロ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。

macro auto global processing [**cdp** | **lldp**]

no macro auto global processing [cdp | **ldp**]

（注）　Release 15.0(2)SG から、**fallback** オプションは非推奨になりました。

構文の説明

cdp	フォールバック モードとして CDP を選択します。
lldp	フォールバック モードとして LLDP を選択します。

デフォルト

Auto Smartports 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

コマンド履歴

リリース	変更箇所
12.2(54)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

スイッチ上で Auto Smartports マクロをグローバルにイネーブルにするには、**macro auto global processing** グローバル コンフィギュレーション コマンドを使用します。特定のポートに対して ASP マクロをディセーブルにするには、ASP をグローバルにイネーブルにする前に、インターフェイス モードで **no macro auto processing** コマンドを使用します。

Auto Smartports マクロは、ポートで検出されたデバイス タイプに基づいてポートを動的に設定します。スイッチがポートで新しいデバイスを検出すると、適切な ASP マクロが適用されます。リンクダウン イベントがポートで発生した場合は、スイッチはそのマクロを削除します。たとえば、ポートに Cisco IP Phone を接続すると、ASP により IP Phone マクロが自動的に適用されます。IP Phone マクロが適用されると、遅延に影響されやすい音声トラフィックを正しく処理できるように QoS（Quality of Service）、セキュリティ機能、および専用の音声 VLAN がイネーブルになります。

ASP はイベント トリガーを使用してデバイスをマクロにマッピングします。最も一般的なイベント トリガーは、接続されているデバイスから受信した Cisco Discovery Protocol（CDP）メッセージに基づいています。Cisco IP Phone、シスコ ワイヤレス アクセス ポイント、Cisco スイッチ、Cisco ルータなどのデバイスが検出されると、CDP イベント トリガーが呼び出されます。それ以外のイベント トリガーでは、MAC 認証バイパス（MAB）や 802.1X 認証メッセージが使用されます。

ポート認証がイネーブルで、RADIUS サーバがイベント トリガーを送信しない場合は、CDP を使用します。

認証に失敗した場合は、LLDP を選択して自動設定を適用します。

認証がポート上でイネーブルの場合、**cdp** キーワードがイネーブルでない限り、スイッチは CDP メッセージと LLDP メッセージを無視します。

802.1X または MAB 認証を使用する場合は、シスコ属性値（AV）のペア **auto-smart-port=***event trigger* をサポートするように、RADIUS サーバを設定します。

CDP を識別するデバイスが複数の機能をアドバタイズする場合、スイッチは、スイッチ、ルータ、アクセスポイント、Lightweight アクセス ポイント、電話機、ホストのプライオリティ順で機能を選択します。

ASP マクロがインターフェイスに適用されていることを確認するには、**show running config** コマンドを使用します。

まだイネーブルになっていない場合は、**macro auto global processing cdp** コマンドおよび **macro auto global processing lldp** コマンドで ASP をグローバルにイネーブルにし、CDP または LLDP にフォールバックをそれぞれ設定します。ただし、**no macro auto global processing [cdp | lldp]** コマンドは、フォールバック メカニズムだけを削除します。このコマンドで ASP をグローバルにディセーブルにすることはできません。ASP をグローバルにディセーブルにできるのは、**no macro auto global processing** コマンドだけです。

cdp キーワードおよび **lldp** キーワードは、インターフェイス レベルでも制御されます。デフォルトでは、CDP がインターフェイスのフォールバック メカニズムです。LLDP を使用する場合は、最初に **no macro auto processing cdpp** コマンドを入力し、次に **acro auto processing lldp** コマンドを入力します。

CDP と LLDP の両方をアクティブにする場合は、それらを順番に有効にする必要があります。たとえば、最初に **macro auto processing cdp** コマンドを入力し、次に **macro auto processing lldp** コマンドを入力します。

例

次の例では、ASP をスイッチでイネーブルにし、Gi1/0/1 でディセーブルにする方法を示します。

```
Switch(config)# interface interface Gi1/0/1
Switch(config-if)# no macro auto processing
Switch(config)# macro auto global processing
```

関連コマンド

コマンド	説明
macro auto device	あるデバイス タイプに対する組み込み関数のパラメータ変更を簡素化します。
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto processing	特定のインターフェイスで ASP マクロをイネーブルにします。
macro auto sticky	ASP によってリンク フラップとデバイス取り外しに適用された設定を、ユーザが削除しないようにします。
shell trigger	ユーザ定義トリガーを作成します。

macro auto mac-address-group

MAC アドレスまたは OUI のグループをトリガーとして設定するには、**macro auto mac-address-group** コマンドを使用します。グループの設定を解除する場合は、このコマンドの **no** 形式を使用します。

macro auto mac-address-group *grp_name*

no macro auto mac-address-group *grp_namel*

構文の説明

grp_name	グループ名を指定します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)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

このコマンドは、モードを config-mac-addr-grp に変更します。このモードでは、MAC アドレスまたは OUI をグループに追加したり、グループから削除することができます。

MAC または OUI のリスト、または OUI の範囲（範囲内に最大 5 つ）を指定できます。

例

次に、**testGroup** をトリガーとして設定する例を示します。

```
Switch(config)# macro auto mac-address-group testGroup
Switch(config-addr-grp-mac)# mac-address list 1111.1111.1111 2222.2222.2222
Switch(config-addr-grp-mac)# exit
Switch(config)# exit
```

関連コマンド

コマンド	説明
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
macro auto sticky	リンク フラップとデバイス取り外しに対し ASP によって適用された設定を削除しないように指定します。
shell trigger	ユーザ定義トリガーを作成します。

macro auto monitor

デバイス分類子をイネーブルにするには、**macro auto monitor** グローバル コンフィギュレーション コマンドを使用します。デバイス分類子をディセーブルにするには、このコマンドの **no** 形式を使用します。

macro auto monitor

no macro auto monitor

構文の説明

このコマンドには、引数またはキーワードはありません。

コマンド デフォルト

デバイス分類子はイネーブルです。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
Release IOS XE 3.3.0 SG (15.1(1)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

デバイス分類子をディセーブルにするには、**no macro auto monitor** グローバル コンフィギュレーション コマンドを使用します。ASP などの機能が使用中のデバイス分類子はディセーブルにできません。

例

次に、スイッチの ASP デバイス分類子をイネーブルにする例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# macro auto monitor
Switch(config)# end
```

関連コマンド

コマンド	説明
show macro auto monitor clients	スイッチのデバイス分類子機能を使用しているクライアントを表示します。
show macro auto monitor device	スイッチに接続されているデバイスとそのプロパティおよび分類を表示します。
show macro auto monitor type	デバイス分類エージェントが認識しているすべてのデバイス タイプを表示します。

macro auto processing

（注）　このコマンドは、Auto SmartPorts（ASP）がグローバルにイネーブルになっている場合にのみ使用します。ASP がグローバルにディセーブルになっている場合は、インターフェイス レベルの制御は効果がありません。

特定のインターフェイスで ASP マクロをイネーブルにするには、**macro auto processing** インターフェイス コンフィギュレーション コマンドを使用します。ASP をグローバルにイネーブルにする前に、特定のインターフェイスで ASP をディセーブルにするには、このコマンドの **no** 形式を使用します。

macro auto processing [fallback cdp] [fallback lldp]

no macro auto processing [fallback cdp] [fallback lldp]

構文の説明

fallback cdp	フォールバック メカニズムとして CDP を指定します。
fallback lldp	フォールバック メカニズムとして LLDP を指定します。

デフォルト

フォールバック メカニズムは CDP です。

コマンド モード

インターフェイス レベルの設定

コマンド履歴

リリース	変更箇所
12.2(54)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

no macro auto processing コマンドは、ASP が適していないすべてのインターフェイス（レイヤ 3 および EtherChannel インターフェイスなど）において、ASP をグローバルにイネーブルにする前に設定する必要があります。

インターフェイス レベルでは、デフォルトのフォールバック メカニズムは CDP です。メカニズムを LLDP に変更するには、**no macro auto processing fallback cdp** コマンドと、続いて **macro auto processing fallback lldp** コマンドを入力してください。

例

次に、インターフェイスでこの機能をイネーブルにする例を示します。

```
Switch(config)# interface Gi3/1
Switch(config-if)# macro auto processing
```

関連コマンド

コマンド	説明
macro auto execute（組み込み関数）	イベント トリガーから組み込みマクロへのマッピングを設定します。
shell trigger	ユーザ定義トリガーを作成します。
show shell functions	ユーザ定義および組み込み関数を含むすべての組み込み関数に含まれる設定を表示します。
show shell triggers	サポートされているすべてのユーザ定義および組み込みトリガーの詳細が表示されます。
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。

macro auto sticky

ASP によってリンク フラップとデバイス取り外しに適用された設定を、ユーザが削除しないように指定するには、**macro auto sticky** コンフィギュレーションを使用します。

macro auto sticky

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スティッキがありません（マクロが削除されます）。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(54)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

このコマンドにより、ある機能によって意図的にリンクがシャットダウンされるとき（電力を節約するために非アクティブなリンクをシャットダウンする EnergyWise など）、ASP 設定が不必要に削除されなくなります。このような機能がイネーブルのとき、ASP マクロが不必要に適用および削除されるのは好ましくありません。したがって、スティッキ機能を設定します。

例

次に、設定が削除されないようにする例を示します。

```
Switch(config)# macro auto sticky
```

関連コマンド

コマンド	説明
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（リモート定義されたトリガー）	リモートで定義された関数にトリガーをマッピングします。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
shell trigger	ユーザ定義トリガーを作成します。

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のスイッチに対して、**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、キーワードや変数はありません。

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	変更箇所
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のスイッチに対して、**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、キーワードや変数はありません。

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	変更箇所
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るマクロ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のスイッチに対して、**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	変更箇所
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

このコマンドは、スイッチにコメント テキストまたはマクロ名を関連付けます。複数のマクロがスイッチに適用されている場合、説明テキストは最後に適用されたマクロの説明になります。

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がありません。

コマンド モード

冗長モード

コマンド履歴

リリース	変更箇所
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 台のスーパーバイザ エンジンの設定を手動で同期させるために使用します。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するには、メイン CPU サブモードから **auto-sync** コマンドを使用します。

（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。また、メイン CPU に適用可能な冗長コマンドをすべて使用できます。

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に照合されます。

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*	IP ACL を名前で選択します。
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がありません。

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	変更箇所
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 コントロールが行われます。

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。

その他の **match** コマンドについては、『*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。

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 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 サービス クラス（CoS）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 DiffServ コード ポイント（DSCP）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。一般的に使用する値に対してはニーモニック名を入力することもできます。
[**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。一般的に使用する値に対してはニーモニック名を入力することもできます。
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。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。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。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	変更箇所
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 シャーシにサポートが拡張されました。
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 QoS（Quality of Service）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のリストを表示するには、**match ip dscp ?** または **match ip precedence ?** コマンドを入力して、コマンドラインのヘルプ ストリングを表示してください。

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** プレフィッ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.2-92）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	変更箇所
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。

ポリシー マップが使用するクラス マップで flow キーワードを設定すると、ポリシー マップは *フローベース ポリシー マップ*と呼ばれます。フロー ベース ポリシー マップを集約ポリシー マップの子として付加するには、**service-policy** コマンドを使用します。

（注）　**match flow** コマンドは、Catalyst 4500 シリーズ スイッチに Supervisor Engine VI（WS-X4516-10GE）が装着されている場合にのみ使用できます。

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）	ポリシー マップをインターフェイスに関連付けます。
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	変更箇所
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	サポートされている、およびサポートされていないラインカードの情報を、使用上のガイドラインに追加。

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（仮想スイッチ）	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	変更箇所
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 フィールドに値が設定されます。このフィールドには、そのポートがデュアル モード対応でない場合は **no** という値が表示され、デュアル モード対応のポートの場合は、メディアのタイプ（**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

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	変更箇所
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 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 と SSO モードをサポートするには、同一の Cisco IOS イメージとスーパーバイザ エンジンを使用する必要があります。Cisco IOS Release 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でないモジュールはリセットされ、スイッチオーバー時にリロードされます。
- ステートフル スイッチオーバーの前に 60 秒以内にモジュールの OIR を実行すると、ステートフル スイッチオーバー時にモジュールがリセットされ、ポート ステートが再起動されます。
- FIB テーブルはスイッチオーバー時にクリアされます。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 capture {access-list | class-map}

コア フィルタとしてアクセス リストまたはクラス マップを指定するには、**monitor capture** {**access-list** | **class-map**} コマンドを使用します。フィルタを削除するには、このコマンドの **no** 形式を使用します。

monitor capture *name* {**access-list** *name* | **class-map** *name*}

no monitor capture *name* {**access-list** *name* | **class-map** *name*}

構文の説明

name	キャプチャ ポイントを指定します。
access-list *name*	アクセス リスト名を指定します。
class-map *name*	クラス マップ名を指定します。

デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

アクセス リストまたはクラス マップは、コンフィギュレーション コマンドで定義します。アクセス リストまたはクラス マップは、**monitor capture** コマンドを入力する前に定義する必要があります。コア フィルタをクラス マップ、アクセス リスト、または明示的なインライン フィルタとして指定することもできます。**monitor capture** コマンドを入力したときにフィルタがすでに指定されていた場合は、古いものが置き換えられます。

例

次に、既存の ACL または class-map を使用して、コア システム フィルタを定義する例を示します。

```
Switch# monitor capture mycap filter access-list myacl

Switch# monitor capture mycap filter class-map mycm
Switch# no monitor capture mycap filter class-map mycm
```

monitor capture [clear | export]

キャプチャ バッファの内容をクリアするか、ファイルにパケットを格納するには、**monitor capture [clear | export** *filename***]** コマンドを使用します。

monitor capture *name* [**clear**] [**export** *filename*]

構文の説明

name	キャプチャ ポイントを指定します。
clear	キャプチャ バッファのすべてのパケットをクリアします。
export *filename*	.pcap ファイルにキャプチャ バッファ内のすべてのパケットを格納します。

デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

clear オプションは、キャプチャ バッファを空にし、**export** オプションは、ファイルにキャプチャ バッファのパケットを格納します。ストレージ先がキャプチャ バッファである場合にのみ、これらのコマンドを使用する必要があります。これらのコマンドは、1 つまたは複数の終了条件を満たしているか、または **stop** コマンドを入力したため、キャプチャ中または停止されているときに使用可能となります。キャプチャが停止してから **clear** コマンドを入力した場合、バッファにパケットがないため、その後の **export**（または **decode**）および **display** コマンドでは何も実行されません。

例

次の例では、キャプチャ ファイルを関連付ける方法または関連付けを解除する方法を示します。

```
Switch# monitor capture mycap export bootflash:mycap.pcap
Switch# monitor capture mycap clear
```

monitor capture [interface | vlan | control-plane]

方向を持つ 1 つ以上の接続ポイントを指定するには、**monitor capture** [**interface** | **vlan** | **control-plane**] コマンドを使用します。接続ポイントを削除するには、このコマンドの **no** 形式を使用します。

monitor capture *name* [{**interface** *name* | **vlan** *num* | **control-plane**} {**in** | **out** | **both**}]

no monitor capture *name* [{**interface** *name* | **vlan** *num* | **control-plane**} {**in** | **out** | **both**}]

構文の説明

name	キャプチャ ポイントを指定します。
interface *name*	インターフェイスを指定します。インターフェイス範囲を使用できます。
vlan *num*	VLAN を指定します。
control-plane	コントロール プレーンを指定します。
input | **output** | **both**	特定のトラフィックの方向。

デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

方向を持つ 1 つ以上の接続ポイントを指定します。インターフェイスの範囲を指定することもできます。このコマンドは、複数の接続ポイントを追加するために、必要に応じて何度でも繰り返し実行できます。

少なくとも 1 つの接続ポイントを規定する必要があります。VLAN では、方向は両方に設定する必要があります。

例

次の例では、接続ポイントを追加する方法を示します。

```
Switch# monitor capture mycap interface gigabitEthernet 3/1 in
```

次の例では、接続ポイントを削除する方法を示します。

```
Switch# no monitor capture mycap interface gigabitEthernet 3/1 in
```

monitor capture file location buffer-size

キャプチャ先を指定するには、**monitor capture** コマンドを使用します。詳細を削除するには、このコマンドの **no** 形式を使用します。

monitor capture *name* **[[file location** *filename* [**buffer-size** <*1-100*>] [**ring** <2-10>] [**size** <*1-100*>]] | [**buffer** [**circular**] **size** <*1-100*>]]

]no monitor capture *name* [**file** | **buffer**]

構文の説明

file location *filename*	場所のファイル名を指定します。
buffer-size <*1-100*>	バッファ サイズを MB 単位で指定します。
ring <2-10>	ファイルの数を指定します。
size <*1-100*>	ファイル サイズを指定します。
buffer [**circular**] **size** <*1-100*>	キャプチャ先がバッファであることを指定します。デフォルトでは、モードはリニアです。 キーワード **circular** は、バッファ モードを循環に設定します。 キーワード **size** は、バッファ サイズを指定します。

デフォルト

デフォルトのバッファ サイズは 1 MB 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	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

キャプチャ先にはストレージ ディスクまたはメモリ バッファのファイルを使用できます。このコマンドは、パケット ストレージに関連するパラメータを指定します。

file オプションは、パケットをファイルに保存する必要があることを指定します。パケット キャプチャの損失を減らすか、回避するために、**buffer-size** オプションを使用できます。キャプチャおよび保存動作には多くの CPU が必要で、キャプチャのスループットが制限されます。

パケットがバッファに最初にキャプチャされる**ロックステップ** モードを開始することで、スループットを向上できます。このモードでは、「duration」パラメータがキャプチャの期間を定義します。バッファがいっぱいになるか、または期間が終了すると、バッファの内容がファイルに書き込まれ、キャプチャのスループットが大幅に向上します。ロックステップ モードは、バッファ サイズを 32MB 以上に指定すると自動的に開始されます。

キャプチャ ファイルのサイズは **size** オプションで制限できます。ファイルの場所は次のいずれにする必要があります。

- 内部ブートフラッシュ（bootflash: ）
- 外部フラッシュ（slot0: ）

- USB（usb0: ）

他のデバイスを指定しないでください。

宛先ファイルは、1 つのファイルではなく、ファイルのリングにすることができます。**ring** オプションはリング内のファイルの数を指定し、**size** はすべてのファイルの合計サイズを指定します。リング ファイル モードでは、ファイル サイズの制限に到達した場合は、最も古いファイルを削除して、新しいパケットのスペースにします。

キャプチャ先がバッファの場合、バッファからパケットをデコードして表示するには、**show** コマンドを使用する必要があります。circular オプションが指定されている場合、キャプチャは明示的に **stop** コマンドを発行するまで続行されます。スペースがバッファにない場合は、新しいパケットを収容するために最も古いパケットが削除されます。**circular** オプションが指定されていない場合は、キャプチャ バッファがいっぱいになると新しいパケットは廃棄されます。

例

次の使用例では、キャプチャ先としてファイルまたはファイルのリングを指定する方法を示します。

```
Switch# monitor capture mycap associate buffer-size 1000000file location
bootflash:mycap.pcap
Switch# monitor capture mycap file location bootflash:mycap.pcap size 40
Switch# monitor capture mycap file location bootflash:mycap.pcap ring 4 size 40
Switch# monitor capture mycap file location bootflash:mycap.pcap buffer-size 8
Switch# monitor capture mycap file location bootflash:mycap.pcap ring 4 size 40
buffer-size 16
Switch# no monitor capture mycap file
```

次の例では、ロックステップ モードのキャプチャを設定する方法を示します。

```
Switch# monitor capture mycap file location bootflash:mycap.pcap buffer-size 64
Switch# no monitor capture mycap file
```

次の例では、循環バッファをキャプチャ先にしてバッファでの操作方法を示します。

```
Switch# monitor capture mycap int gi 3/1 in match ipv4 any any
Switch# monitor capture mycap buffer circular size 1
Switch# monitor capture mycap start
Switch#
Switch# sh monitor capture mycap buffer
  0.000000   10.1.1.164 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000   10.1.1.165 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000   10.1.1.166 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000   10.1.1.167 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000   10.1.1.168 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000   10.1.1.169 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000   10.1.1.170 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000   10.1.1.171 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000   10.1.1.172 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000   10.1.1.173 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10.000000   10.1.1.174 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 11.000000   10.1.1.175 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 12.000000   10.1.1.176 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

Switch# sh monitor capture mycap buffer detailed
Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
    Arrival Time: Apr 12, 2012 10:59:06.255983000 PDT
    Epoch Time: 1334253546.255983000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 256 bytes (2048 bits)
    Capture Length: 256 bytes (2048 bits)
```

```
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
    Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
        Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
…
Switch# sh monitor capture mycap buffer dump
  0.000000   10.1.1.164 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 58 0a 01 01 a4 14 01   ......@.YX......
0020  01 02 4e 21 4e 22 00 da 6e 13 00 01 02 03 04 05   ..N!N"..n.......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 63 24 51 ee   ............c$Q.

  1.000000   10.1.1.165 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
…
Switch# monitor capture mycap clear
Switch# sh monitor capture mycap buffer detailed
…
Switch# monitor capture mycap stop
```

monitor capture limit

キャプチャの制限を指定するには、**monitor capture limit** コマンドを使用します。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。

monitor capture *name* **limit** {**duration** *seconds*] [**packet-length** *size*] [**packets** *num*]

no monitor capture *name* **limit** [**duration**] [**packet-length**] [**packets**]

構文の説明

name	キャプチャ ポイントを指定します。
duration *seconds*	期間を秒で指定します。
packet-length *size*	パケット長を指定します。実際のパケットが長い場合、最初の *size* バイトだけが保存されます。
packets *num*	処理されるパケットの数を指定します。

デフォルト

パケット長を指定しないと、パケット全体が処理されます。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

セッション期間、パケット セグメント長、および保存するパケット数を指定します。

例

次の例では、キャプチャ ファイルの関連付け / 関連付け解除を行う方法を示します。

```
Switch# monitor capture mycap limit duration 10

Switch# monitor capture mycap limit packet-length 128

Switch# monitor capture mycap limit packets 100

Switch# no monitor capture mycap limit duration packet-length packets

Switch# monitor capture mycap limit duration 10 packet-length 128 packets 100

Switch# no monitor capture mycap limit
```

monitor capture mycap match

明示的なインライン コア フィルタを定義するには、**monitor capture mycap match** コマンドを使用します。これを削除するには、このコマンドの **no** 形式を使用します。

```
Switch# [no] monitor capture mycap match {any | mac mac-match-string | ipv4
ipv4-match-string | ipv6 ipv6-match-string}
```

MAC のフィルタを使用するには、次の形式を使用します。

```
Switch# [no] monitor capture mycap match mac {src-mac-addr src-mac-mask | any | host
src-mac-addr} | {dest-mac-addr dest-mac-mask | any | host dest-mac-addr}
```

IPv4/IPv6 のフィルタを使用するには、次の形式のいずれかを使用します。

```
Switch# [no] monitor capture mycap match {ipv4 | ipv6} [src-prefix/length | any | host
src-ip-addr] [dest-prefix/length | any | host dest-ip-addr]
```

```
Switch# [no] monitor capture mycap match {ipv4 | ipv6} proto {tcp | udp}
[src-prefix/length | any | host src-ip-addr] [eq | gt | lt | neq <0-65535>]
[dest-prefix/length | any | host dest-ip-addr] [eq | gt | lt | neq <0-65535>]
```

構文の説明

any	「すべて」のパケットを指定します
mac *mac-match-string*	レイヤ 2 パケットを指定します。
ipv4 *ipv4-match-string*	IPv4 パケットを指定します。
ipv6 *ipv6-match-string*	IPv6 パケットを指定します。
match *name*	キャプチャ ポイントを指定します
src-mac-addr	送信元 MAC アドレスを指定します。
src-mac-mask	送信元 MAC マスクを指定します。
host ***src-mac-addr***	送信元（または宛先）MAC（または IP）アドレスを指定します。
dest-mac-addr	宛先 MAC アドレスを指定します。
dest-mac-mask	宛先 MAC マスクを指定します。
host ***dest-mac-addr***	送信元（または宛先）MAC（または IP）アドレスを指定します。
src-prefix/*length*	送信元プレフィックス/長さを指定します。
host ***src-ip-addr***	ホストの送信元 IP アドレスを指定します。
dest-prefix/length	宛先プレフィックス/長さを指定します。
host ***dest-ip-addr***	送信元（または宛先）MAC（または IP）アドレスを指定します。
proto {**tcp** | **udp**}	使用されるプロトコルを指定します。
{eq | gt | lt | neq} *<0-65535>*	等しい、より大きい、より小さい、等しくないを指定します。

デフォルト

なし

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

クラス マップ、アクセス リスト、または明示的なインライン フィルタとして、コア フィルタを指定できます。このコマンドを入力したときにフィルタがすでに指定されている場合、古いフィルタを置き換えます。

明示的なインライン フィルタは、コア フィルタの指定を簡単にすることを目的としています。特定の状況では、設定を変更するために承認プロセスが必要になり、時間がかかることがあります。明示的なフィルタはこのプロセスを簡略化しますが、アクセス リストとクラス マップに対してより広範に対応していることに注意が必要です。

適切なキーワードを指定して、IPv4、IPv6、MAC、または「任意」のトラフィックをキャプチャできます。トラフィック タイプによって、使用方法は異なります。MAC の場合、アドレスまたはプレフィックスを指定できます。IPv4 または IPv6 の場合、複数のフィールドで照合できます。送信元または宛先ポートでは、複数のオペレータがサポートされます。

例

次の使用例では、明示的なフィルタを設定または削除する方法を示します。

```
Switch# monitor capture mycap match any

Switch# monitor capture mycap match mac any any

Switch# monitor capture mycap match mac host 0000.0a01.0102 host 0000.0a01.0103

Switch# monitor capture mycap match ipv4 any any

Switch# monitor capture mycap match ipv4 host 10.1.1.2 host 20.1.1.2

Switch# monitor capture mycap match ipv4 proto udp 10.1.1.0/24 eq 20001 20.1.1.0/24 eq
20002

Switch# monitor capture mycap match ipv4 proto udp 10.1.1.2/24 eq 20001 any

Switch# no monitor capture mycap match
```

monitor capture start

キャプチャ ポイントを開始または停止するには、**monitor capture** コマンドを使用します。

monitor capture *name* **start** [**capture-filter** *filter-string*] [**display** [**display-filter** *filter-string*]] [**brief** | **detailed** | **dump** | **stop**]

構文の説明

name	キャプチャ ポイントを指定します。
start	Wireshark のセッションを開始し、ライブ トラフィックをキャプチャします。
capture-filter ***filter-string***	キャプチャ フィルタを指定します。
display [**display-filter** *filter-string*]	フィルタをデコードして表示します。任意で、表示フィルタを指定します。
[**brief** | **detailed** | **dump**]	表示モードを指定します。デフォルトは **brief** です。
stop	Wireshark のセッションを停止します。

デフォルト

デフォルトの表示モードは **brief** 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	変更箇所
IOS XE 3.3.0SG/ 15.1(1)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

これらのコマンドは、すべての必須パラメータが指定されていると判断してキャプチャ セッションを開始または停止します。セッションを開始する前に CPU およびメモリなどのリソースが使用可能であることを確認する必要があります。キャプチャおよび表示フィルタは Wireshark の表示フィルタの構文に従う必要があるため、フィルタが正しいことを確認します（たとえば、二重引用符で囲んでフィルタを指定します）。

パケットが格納され、表示されている場合は、表示フィルタを使用しないでください。このモードでは、パケットが格納されていれば表示もされます。表示フィルタを指定しても無視されます。

キャプチャ フィルタが指定されている場合、キャプチャは 65536 パケットに制限されます。このリリースでは、キャプチャ フィルタを使用するとタイムスタンプが不正確になるという制限があります。

例

次の例では、さまざまなモードのキャプチャ セッションを開始または停止する方法を示します。

```
Switch# monitor capture mycap int gi 3/1 in match ipv4 any any
Switch# monitor capture mycap file location bootflash:mycap.pcap
Switch# monitor capture mycap limit packets 100 duration 60

Switch# monitor capture mycap start
Switch#
Switch# monitor capture mycap stop
```

```
Switch# monitor capture mycap start capture-filter "udp.port == 20001"
Switch# monitor capture mycap stop
Switch# monitor capture mycap start capture-filter "udp.port == 20001" display
A file by the same capture file name already exists, overwrite?[confirm]

  0.000000     10.1.1.9 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.10 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.11 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.12 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.13 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.14 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.15 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.16 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.17 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.18 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.19 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.20 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.21 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.22 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.23 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.24 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.25 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.26 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.27 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.28 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.29 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.30 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

Switch# monitor capture mycap start capture-filter "udp.port == 20001" display
display-filter "udp.port == 20002"
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display  filter%
A file by the same capture file name already exists, overwrite?[confirm]

  0.000000    10.1.1.96 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.97 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.98 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000    10.1.1.99 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.100 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.101 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.102 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.103 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.104 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.105 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.106 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.107 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.108 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  0.000000   10.1.1.109 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

Switch#
Switch# monitor capture mycap start capture-filter "udp.port == 20001" display
display-filter "udp.port == 20002" detailed
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display  filter%
A file by the same capture file name already exists, overwrite?[confirm]

Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
    Arrival Time: Dec 31, 1969 17:00:00.000000000 PDT
    Epoch Time: 0.000000000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 256 bytes (2048 bits)
```

```
    Capture Length: 256 bytes (2048 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
    Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
        Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Switch# monitor capture mycap start capture-filter "udp.port == 20001" display dump
A file by the same capture file name already exists, overwrite?[confirm]

  0.000000     10.1.1.6 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 f6 0a 01 01 06 14 01   ......@.Y.......
0020  01 02 4e 21 4e 22 00 da 6e b1 00 01 02 03 04 05   ..N!N"..n.......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 ac 69 6e fd   ............in.

  0.000000     10.1.1.7 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002


Switch#
Switch# monitor capture mycap start display display-filter "udp.port == 20002"
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display  filter%
A file by the same capture file name already exists, overwrite?[confirm]

  0.000000    10.1.1.41 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000    10.1.1.42 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000    10.1.1.43 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000    10.1.1.44 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000    10.1.1.45 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000    10.1.1.46 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.998993    10.1.1.47 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.998993    10.1.1.48 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.998993    10.1.1.49 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.998993    10.1.1.50 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.998993    10.1.1.51 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10.998993    10.1.1.52 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

Switch#
Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump
%Display-filter cannot be specified when capture is associated to a file. Ignoring
display  filter%
A file by the same capture file name already exists, overwrite?[confirm]
```

```
  0.000000   10.1.1.117 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 87 0a 01 01 75 14 01   ......@.Y....u..
0020  01 02 4e 21 4e 22 00 da 6e 42 00 01 02 03 04 05   ..N!N"..nB......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 41 0c b4 5d   ............A..]

  1.000000   10.1.1.118 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002


Switch# no monitor capture mycap file

Switch# monitor capture mycap start display display-filter "udp.port == 20002" dump

  0.000000   10.1.1.160 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002

0000  54 75 d0 3a 85 3f 00 00 00 00 03 01 08 00 45 00   Tu.:.?........E.
0010  00 ee 00 00 00 00 40 11 59 5c 0a 01 01 a0 14 01   ......@.Y\......
0020  01 02 4e 21 4e 22 00 da 6e 17 00 01 02 03 04 05   ..N!N"..n.......
0030  06 07 08 09 0a 0b 0c 0d 0e 0f 10 11 12 13 14 15   ................
0040  16 17 18 19 1a 1b 1c 1d 1e 1f 20 21 22 23 24 25   .......... !"#$%
0050  26 27 28 29 2a 2b 2c 2d 2e 2f 30 31 32 33 34 35   &'()*+,-./012345
0060  36 37 38 39 3a 3b 3c 3d 3e 3f 40 41 42 43 44 45   6789:;<=>?@ABCDE
0070  46 47 48 49 4a 4b 4c 4d 4e 4f 50 51 52 53 54 55   FGHIJKLMNOPQRSTU
0080  56 57 58 59 5a 5b 5c 5d 5e 5f 60 61 62 63 64 65   VWXYZ[\]^_`abcde
0090  66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75   fghijklmnopqrstu
00a0  76 77 78 79 7a 7b 7c 7d 7e 7f 80 81 82 83 84 85   vwxyz{|}~.......
00b0  86 87 88 89 8a 8b 8c 8d 8e 8f 90 91 92 93 94 95   ................
00c0  96 97 98 99 9a 9b 9c 9d 9e 9f a0 a1 a2 a3 a4 a5   ................
00d0  a6 a7 a8 a9 aa ab ac ad ae af b0 b1 b2 b3 b4 b5   ................
00e0  b6 b7 b8 b9 ba bb bc bd be bf c0 c1 c2 c3 c4 c5   ................
00f0  c6 c7 c8 c9 ca cb cc cd ce cf d0 d1 9f 20 8a e5   ............. ..

  1.000000   10.1.1.161 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002


Switch# monitor capture mycap start display display-filter "udp.port == 20002"

  0.000000   10.1.1.173 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  1.000000   10.1.1.174 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  2.000000   10.1.1.175 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  3.000000   10.1.1.176 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  4.000000   10.1.1.177 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  5.000000   10.1.1.178 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  6.000000   10.1.1.179 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  7.000000   10.1.1.180 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  8.000000   10.1.1.181 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
  9.000000   10.1.1.182 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 10.000000   10.1.1.183 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 11.000000   10.1.1.184 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
 12.000000   10.1.1.185 -> 20.1.1.2     UDP Source port: 20001  Destination port: 20002
```

```
Switch# monitor capture mycap start display detailed

Frame 1: 256 bytes on wire (2048 bits), 256 bytes captured (2048 bits)
    Arrival Time: Apr 12, 2012 11:46:54.245974000 PDT
    Epoch Time: 1334256414.245974000 seconds
    [Time delta from previous captured frame: 0.000000000 seconds]
    [Time delta from previous displayed frame: 0.000000000 seconds]
    [Time since reference or first frame: 0.000000000 seconds]
    Frame Number: 1
    Frame Length: 256 bytes (2048 bits)
    Capture Length: 256 bytes (2048 bits)
    [Frame is marked: False]
    [Frame is ignored: False]
    [Protocols in frame: eth:ip:udp:data]
Ethernet II, Src: 00:00:00:00:03:01 (00:00:00:00:03:01), Dst: 54:75:d0:3a:85:3f
(54:75:d0:3a:85:3f)
    Destination: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        Address: 54:75:d0:3a:85:3f (54:75:d0:3a:85:3f)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)
    Source: 00:00:00:00:03:01 (00:00:00:00:03:01)
        Address: 00:00:00:00:03:01 (00:00:00:00:03:01)
        .... ...0 .... .... .... .... = IG bit: Individual address (unicast)
        .... ..0. .... .... .... .... = LG bit: Globally unique address (factory default)

Switch#
```

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/宛先インターフェイス、または SPAN セッションから送信元 VLAN を削除するには、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** {**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 セッション番号。有効値は 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*	スイッチで、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 のサブキューで受信するトラフィックだけをセッションの宛先にコピーするように指定します。有効な値は 1 ～ 64、または次の名前で指定します。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。
acl	（任意）入出力 ACL を指定します。有効な値は 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りパケットがパントされることを指定します。
rx	受信トラフィックだけのモニタリングを指定します。
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 の例外パケット。
bridge-cpu	CPU にブリッジ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る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。
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	ポートを宛先とするパケットを指定します。
control-packet	（任意）レイヤ 2 制御パケット。
esmp	（任意）ESMP パケット。
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	ポートを宛先とするパケットを指定します。
rpf-failure	マルチキャスト RPF 障害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。有効な値は 1 ～ 4094 です。
-	（任意）SPAN VLAN の範囲を指定する記号です。
both	（任意）受信トラフィックと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）受信トラフィックだけをモニタおよびフィルタリングします。
tx	（任意）送信トラフィックだけ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指定されたタイプのパケットに制限します。
good	有効なパケット 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指定されたアドレス タイプのパケットに制限します。有効なタイプは、unicast、multicast、および broadcast です。

デフォルト

受信トラフィックと送信トラフィック、およびすべての VLAN、パケット タイプ、アドレス タイプがトランキング インターフェイスでモニタされます。

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	変更箇所
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 セッションと拡張 VLAN アドレッシング内の異なる方向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、パケットおよびアドレス タイプ フィルタリング、および CPU 送信元のスニッフィング機能拡張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 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 から、SPAN は入力送信元を含む 2 セッションおよび出力送信元を含む 4 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送信元の両方をサポートします。

特定の SPAN セッションは VLAN または個別のインターフェイスのいずれかをモニタできます。特定のインターフェイスと特定の VLAN を両方ともモニタする SPAN セッションを設定することはできません。SPAN セッションを送信元インターフェイスで設定し、送信元 VLAN を同じ SPAN セッションに追加しようとした場合は、エラーになります。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、入力 VLAN を指定する必要はありません。

デフォルトで入力をイネーブルにすると、ホスト ラーニングは宛先ポート上では実行されません。**learning** キーワードを入力すると、ホスト ラーニングが宛先ポートで行われ、学習済みホストへのトラフィックは宛先ポートから送信されます。

モニタされたトランキング インターフェイス上で **filter** キーワードを入力した場合、指定された 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 Rx 方向でだけサポートされます。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、セッションではすべてのパケット タイプがスニッフィングされます。

queue ID は指定された CPU キュー上で送受信されたトラフィックだけのスニッフィングを許可します。キューは、番号または名前のどちらかによって識別されます。キュー名には、便宜上、複数の番号が付けられたキューが含まれることがあります。

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 セッション内で異なる方向で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、宛先として、RSPAN VLAN 20 を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）　**control-packet** は、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

パケットまたは最大伝送ユニット（MTU）の最大サイズを調整することにより、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。有効な値は 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	変更箇所
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。ジャンボ フレームはスタブベース ポートでは使用できません。

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 領域の名前を設定するには、**name** コマンドを使用します。デフォルト名に戻すには、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	変更箇所
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

次に、領域に名前を付ける例を示します。

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

関連コマンド

コマンド	説明
instance	VLAN または VLAN セットを 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。

netflow-lite exporter

エクスポータを定義し、NetFlow-lite エクスポータ サブモードを開始するには、**netflow-lite exporter** コマンドを使用します。エクスポータを削除するには、このコマンドの **no** 形式を使用します。

netflow-lite exporter *exporter*

no netflow-lite exporter *exporter*

構文の説明

exporter	エクスポータを指定します。

デフォルト

なし

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	変更箇所
15.0(2)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

エクスポータの名前は、エクスポータを識別します。最小の完全なエクスポータ設定の必須パラメータは、コレクタの宛先 IP アドレス、使用する（スイッチ上の）送信元 IP アドレス、およびコレクタの UDP 宛先ポートです。指定されていない任意のパラメータはデフォルトの値になります。

エクスポータの名前は、データ ソースのサンプリングを **monitor** コマンドによってアクティブにするときに指定できます。

エクスポータ サブモードでは、NetFlow テンプレートの更新頻度を指定することができます。サンプラ コンフィギュレーション パラメータ、snmp インターフェイス テーブルのマッピングなどの NetFlow パケット サンプリング プロセスに関するメタデータは、定期的にコレクタにエクスポートすることもできます。

任意のパラメータの値を削除すると、デフォルト値に戻ります。

例

次の例では、NetFlow エクスポータを設定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```
Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite  Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address:   5.5.5.6
    Source IP Address:        5.5.5.5
    VRF label:
    DSCP:                     0x20
    TTL:                      128
    COS:                      7
  Transport Protocol Configuration:
    Transport Protocol:       UDP
    Destination Port:         8188
    Source Port:              61670
  Export Protocol Configuration:
    Export Protocol:                  netflow-v9
    Template data timeout:            60
    Options sampler-table timeout:    1800
    Options interface-table timeout:  1800
  Exporter Statistics:
    Packets Exported:         0
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
export-protocol（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのエクスポート プロトコルを指定します。
netflow-lite exporter	エクスポータを定義し、NetFlow-lite エクスポータ サブモードを開始します。
destination（netflow-lite エクスポータ サブモード）	netflow-lite サブモードでの宛先アドレスを指定します。
source（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの送信元レイヤ 3 インターフェイスを指定します。
transport udp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの UDP トランスポート宛先ポートを指定します。
ttl（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの TTL 値を指定します。
cos（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
dscp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
template data timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのテンプレート データ タイムアウトを指定します。
options timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのオプションのタイムアウトを指定します。

netflow-lite monitor

インターフェイスのモニタ インスタンスを定義し、netflow-lite モニタ サブモードを開始するには、**netflow-lite monitor** コマンドを使用します。モニタを削除するには、このコマンドの **no** 形式を使用します。

netflow-lite monitor *sampler-name*

no netflow-lite sampler *sampler-name*

構文の説明

sampler-name	サンプルを指定します。

デフォルト

なし

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	変更箇所
15.0(2)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

単一パケットのサンプリング インスタンスだけがデータ ソースでサポートされます。これらのコマンドは、物理ポート インターフェイス モード、ポート チャネル インターフェイス モード、または config VLAN モードで入力されます。モニタは他のインターフェイスではサポートされていません。物理ポートがポート チャネルのメンバである場合、ポートにモニタを適用しても効果はありません。代わりにポート チャネルにモニタを適用する必要があります。

（注） VLAN のサンプリングは Cisco IOS Release 15.0(2)SG でサポートされません。これは以降のリリースでサポートされます。

必須パラメータは、サンプラおよびエクスポータです。エクスポータがモニタに関連付けられていない場合、サンプルはエクスポートされません。その場合、入力パケット サンプリングはそのターゲット インターフェイスに対して行われません。必須パラメータが欠落している場合、サンプラまたはエクスポータが無効であることを示す警告メッセージが表示されます。

パケット サンプリング メカニズムはランダムな 1/N サンプリングを試みます。内部的には 2 レベルのサンプリングが実行されます。サンプリングの最初のレベルの精度は、特定のインターフェイスに到着したパケットのサイズによって異なります。アルゴリズムの相対的な精度を調整するために **average-packet-size** パラメータを使用できます。

システムによって自動的に入力トラフィックの監視に基づいてインターフェイスでの平均パケット サイズが決定され、最初のレベルのサンプリングでの値が使用されます。

アルゴリズムで使用できるパケット サイズの有効な範囲は 64 ～ 9216 バイトです。64 バイトより小さい数は、平均パケット サイズの自動決定が必要なことを意味します。

例

次の例では、ポートのギガビット インターフェイス 1/3 のモニタを設定する方法を示します。

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite  Monitor-1:
    Active:               TRUE
    Sampler:              sampler1
    Exporter:             exporter1
    Average Packet Size:  0
  Statistics:
    Packets exported:     0
    Packets observed:     0
    Packets dropped:      0
    Average Packet Size observed: 64
    Average Packet Size used: 64
```

同様に、VLAN コンフィギュレーション モードで VLAN のモニタを設定できます。

```
Switch# config terminal
Switch(config)# vlan config 2
Switch(config-vlan-config)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# exit
Switch(config-vlan-config)# exit
Switch# show netflow-lite monitor 1 vlan 2
VlanID-2:
  Netflow-lite  Monitor-1:
    Active:               TRUE
    Sampler:              sampler1
    Exporter:             exporter1
    Average Packet Size:  0
  Statistics:
    Packets exported:     0
    Packets observed:     0
    Packets dropped:      0
    Average Packet Size observed: 64
    Average Packet Size used: 64
```

show netflow-lite sampler 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
sampler（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのインターフェイスでサンプリングをアクティブにします。
average-packet-size（netflow-lite モニタ サブモード）	観測ポイントでの平均パケット サイズを指定します。
exporter（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのエクスポータを割り当てます。

netflow-lite sampler

パケット サンプリング パラメータを再利用可能な名前付きエンティティとして設定し、netflow-lite サンプラ サブモードを開始するには、**netflow-lite sampler** コマンドを使用します。サンプラを削除するには、このコマンドの **no** 形式を使用します。

netflow-lite sampler *name*

no netflow-lite sampler *name*

構文の説明

name	サンプラを指定します。

デフォルト

なし

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	変更箇所
15.0(2)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

サンプラ CLI 構造では、入力パケットのサンプリング レートを設定することができます。パケットのサンプリング レートは 32 ～ 2^15 の範囲で 2 の累乗単位で指定できます。サンプリング レート 1 は最大 2 個の 1 ギガビット ポートだけに対するトラブルシューティングに許可され、rx span と基本的に同じです。エクスポート用の fpga の帯域幅要求が高すぎるため、10GE ポートで設定できません。

必須パラメータは、パケット レートです。

ターゲット インターフェイスで使用中のサンプラを更新できますが、必須パラメータを削除または設定解除できません。

すべての必須パラメータがサンプラを検証するために必要です。指定されていない任意のパラメータはデフォルトの値になります。

例

次の例では、パケットのサンプリング パラメータを再利用可能な名前付きエンティティとして設定して、サンプラを表示する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch#
```

```
Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id :                    1
  Packet Sampling rate:   1 out of 32
  Packet Section Size:    64    bytes
  Packet offset:          16    bytes
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
packet-offset（netflow-lite サンプラ サブモード）	netflow-lite サブモードの開始パケットのオフセットを指定します。
packet-rate（netflow-lite サンプラ サブモード）	netflow-lite サンプラ サブモードでパケットのサンプリング レートを指定します。
packet-section size（netflow-lite サンプラ サブモード）	netflow-lite サブモードでサンプリングされたヘッダー サイズを指定します。

nmsp

スイッチのネットワーク モビリティ サービス プロトコル（NMSP）を設定するには、**nmsp** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

nmsp {**enable** | {**notification interval** {**attachment** | **location**} *interval-seconds*}}

no nmsp {**enable** | {**notification interval** {**attachment** | **location**} *interval-seconds*}}

構文の説明

enable	スイッチで NMSP 機能をイネーブルにします。
notification interval	NMSP 通知間隔を指定します。
attachment	接続通知間隔を指定します。
location	ロケーション通知間隔を指定します。
interval-seconds	スイッチから MSE にロケーション更新または接続更新が送信されるまでの期間（秒）。指定できる範囲は 1 ～ 30 です。デフォルト値は 30 です。

デフォルト

NMSP はディセーブルです。NMSP 接続通知間隔および NMSP ロケーション通知間隔のデフォルトは 30 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	変更箇所
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

暗号化された NMSP ロケーションおよび接続通知をシスコ モビリティ サービス エンジン（MSE）に送信するようにスイッチをイネーブルにするには、**nmsp** グローバル コンフィギュレーション コマンドを使用します。

例

次の例では、スイッチ上で NMSP をイネーブルにし、ロケーション通知時間を 10 秒に設定する方法を示します。

```
Switch(config)# nmsp enable
Switch(config)# nmsp notification interval location 10
Switch(config)#
```

関連コマンド

コマンド	説明
clear nmsp statistics	NMSP 統計カウンタをクリアします。
nmsp attachment suppress	特定のインターフェイスからの接続情報の報告を抑制します。
show nmsp	NMSP 情報を表示します。

nmsp attachment suppress

指定したインターフェイスからの接続情報の報告を抑制するには、**nmsp attachment suppress interface** コマンドを使用します。このコマンドは、スイッチで暗号化ソフトウェア イメージが実行されている場合にだけ利用できます。接続情報を報告するには、このコマンドの **no** 形式を使用します。

nmsp attachment suppress

no nmsp attachment suppress

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

接続情報が報告されます。

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	変更箇所
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

接続通知をシスコ モビリティ サービス エンジン（MSE）に送信しないようにインターフェイスを設定するには、**nmsp attachment suppress** インターフェイス コンフィギュレーション コマンドを使用します。

例

次の例では、アタッチメント情報を MSE に送信しないようにインターフェイスを設定する方法を示します。

```
Switch(config)# switch interface gigabitethernet1/2
Switch(config-if)# nmsp attachment suppress
Switch(config-if)#
```

関連コマンド

コマンド	説明
nmsp	スイッチ上でネットワーク モビリティ サービス プロトコル（NMSP）を設定します。
show nmsp	NMSP 情報を表示します。

options timeout（netflow-lite エクスポータ サブモード）

NetFlow-lite コレクタのオプションのタイムアウトを指定するには、**options timeout** コマンドを使用します。この値を削除するには、このコマンドの **no** 形式を使用します。

options {**sampler-table** | **interface-table**} **timeout** *seconds*

no options {**sampler-table** | **interface-table**} **timeout** *second*

構文の説明

sampler-table	サンプラ設定のエクスポート タイムアウト値を指定します。
interface-table	snmp ifIndex マッピングのエクスポート タイムアウト値を指定します。
seconds	NetFlow-lite コレクタのオプションのタイムアウトを指定します。

デフォルト

1800 秒

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)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

デフォルトのタイムアウト値は 1800 秒（30 分）です。設定されるタイムアウト値は、実際には、コレクタ、およびテンプレートを更新する必要がある頻度によって決まります。

例

次の例では、NetFlow-lite コレクタのオプションのタイムアウトを指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite exporter exporter1
Switch(config-netflow-lite-exporter)# destination 5.5.5.6
Switch(config-netflow-lite-exporter)# source 5.5.5.5
Switch(config-netflow-lite-exporter)# transport udp 8188
Switch(config-netflow-lite-exporter)# ttl 128
Switch(config-netflow-lite-exporter)# cos 7
Switch(config-netflow-lite-exporter)# dscp 32
Switch(config-netflow-lite-exporter)# template data timeout 1
Switch(config-netflow-lite-exporter)# options sampler-table timeout 1
Switch(config-netflow-lite-exporter)# options interface-table timeout 1
Switch(config-netflow-lite-exporter)# export-protocol netflow-v9
Switch(config-netflow-lite-exporter)# exit
Switch(config)#
```

```
Display the exporter
Switch# show netflow-lite exporter exporter1
Netflow-lite  Exporter exporter1:
  Network Protocol Configuration:
    Destination IP address:   5.5.5.6
    Source IP Address:        5.5.5.5
    VRF label:
    DSCP:                     0x20
    TTL:                      128
    COS:                      7
  Transport Protocol Configuration:
    Transport Protocol:       UDP
    Destination Port:         8188
    Source Port:              61670
  Export Protocol Configuration:
    Export Protocol:                  netflow-v9
    Template data timeout:            60
    Options sampler-table timeout:    1800
    Options interface-table timeout:  1800
  Exporter Statistics:
    Packets Exported:         0
```

show netflow-lite exporter 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
cos（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。
source（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの送信元レイヤ 3 インターフェイスを指定します。
transport udp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの UDP トランスポート宛先ポートを指定します。
ttl（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの TTL 値を指定します。
destination（netflow-lite エクスポータ サブモード）	netflow-lite サブモードでの宛先アドレスを指定します。
template data timeout（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのテンプレート データ タイムアウトを指定します。
export-protocol（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタのエクスポート プロトコルを指定します。
dscp（netflow-lite エクスポータ サブモード）	NetFlow-lite コレクタの CoS 値を指定します。

packet-offset（netflow-lite サンプラ サブモード）

netflow-lite サブモードで開始パケットのオフセットを指定するには、**packet-offset** 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。

packet-offset *offset*

no packet-offset *offset*

構文の説明

offset	開始パケットのオフセットをバイトで指定します（最大 48）。

デフォルト

L2 ヘッダーのバイト 0 で開始

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)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

デフォルトのパケット セクションのオフセット値は 0 です。サンプリングされたパケットから抽出されたパケット セクションは、パケットのオフセット 0 で開始されます。

例

次の例では、開始パケットのオフセットを指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id :                    1
  Packet Sampling rate:   1 out of 32
  Packet Section Size:    64    bytes
  Packet offset:          16    bytes
```

show netflow-lite sampler 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
packet-section size（netflow-lite サンプラ サブモード）	netflow-lite サブモードでサンプリングされたヘッダー サイズを指定します。
packet-rate（netflow-lite サンプラ サブモード）	netflow-lite サンプラ サブモードのパケットのサンプリング レートを指定します。

packet-rate（netflow-lite サンプラ サブモード）

netflow-lite サンプラ サブモードでパケットのサンプリング レートを指定するには、**packet rate** コマンドを使用します。パケットのサンプリング レートを削除するには、このコマンドの **no** 形式を使用します。

packet rate *n*

no packet rate *n*

構文の説明

n	パケットのサンプリング レートを指定します。

デフォルト

なし

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)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

パケットのサンプリング レートは 32 ～ 2^15 の範囲で 2 の累乗単位で指定できます。レート 1 は、2 個の 1 ギガビット イーサネット ポートのトラブルシューティングだけに許可されます（rx span に相当）。エクスポートの帯域幅要求が高すぎるため、10 ギガビット イーサネット ポートでレートを 1 に設定できません。

これは必須パラメータです。最大 2 個の 1 ギガビット イーサネット ポートで 1/1 サンプリングを設定できます。1 ギガビットまたは 10 ギガビット イーサネット ポートで設定できる最適なパケットのサンプリング レートは 1/32 です。パケットのサンプリング レートは 2 の累乗単位で設定できます（1/64、1/128 など）。

例

次の例では、netflow-lite サンプラ サブモードでパケットのサンプリング レートを指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch#

Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id :                    1
  Packet Sampling rate:   1 out of 32
  Packet Section Size:    64    bytes
  Packet offset:          16    bytes
```

show netflow-lite sampler 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
packet-section size（netflow-lite サンプラ サブモード）	netflow-lite サブモードでサンプリングされたヘッダー サイズを指定します。
packet-offset（netflow-lite サンプラ サブモード）	netflow-lite サブモードの開始パケットのオフセットを指定します。

packet-section size（netflow-lite サンプラ サブモード）

netflow-lite サブモードでサンプリングされたヘッダー サイズを指定するには、**packet-section size** コマンドを使用します。デフォルトに戻す場合は、このコマンドの **no** 形式を入力します。

packet-section size *bytes*

no packet-section size *bytes*

構文の説明

bytes	サンプリングされたヘッダー サイズを指定します。有効なサイズ範囲は 4 バイト単位で 16 ～ 252 バイトです。

デフォルト

64 バイト

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)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

デフォルトのパケット セクション サイズは、通常、入力 IPv4 パケットのレイヤ 2、レイヤ 3、およびレイヤ 4 ヘッダーをカバーする 64 バイトです。

例

次の例では、サンプリングされたヘッダー サイズを指定する方法を示します。

```
Switch# config terminal
Switch(config)# netflow-lite sampler sampler1
Switch(config-netflow-lite-sampler)# packet-rate 32
Switch(config-netflow-lite-sampler)# packet-section size 128
Switch(config-netflow-lite-sampler)# packet-offset 16
Switch(config-netflow-lite-sampler)# exit
Switch(config)# exit
Switch#

Switch# show netflow-lite sampler sampler1
Netflow-lite Sampler sampler1:
  Id :                    1
  Packet Sampling rate:   1 out of 32
  Packet Section Size:    64    bytes
  Packet offset:          16    bytes
```

show netflow-lite sampler 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
packet-rate（netflow-lite サンプラ サブモード）	netflow-lite サンプラ サブモードでパケットのサンプリング レートを指定します。
packet-offset（netflow-lite サンプラ サブモード）	netflow-lite サブモードの開始パケットのオフセットを指定します。

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	変更箇所
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	変更箇所
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度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	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

インターフェイス上でルーティング 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	変更箇所
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。マクロを作成した後、範囲を追加できます。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 キーワードを指定すると、すべてのインターフェイスがデフォルトでパッシブに設定されます。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、インターネット サービス プロバイダー（ISP）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 要求の照合を要求します。**request** を指定しない場合は、すべての ARP パケットに対して照合が行われます。
ip	送信元 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がありません。

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	変更箇所
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 バインディングとの照合に基づいて 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：サービス クラス（CoS）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 DiffServ コード ポイント（DSCP）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	変更箇所
12.2(40)SG	このコマンドが Catalyst 4900M および Supervisor Engine 6E 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 QoS（Quality of Service）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** オプションをコマンドライン インターフェイス（CLI）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実行されます。

- 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。トークンの到達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）X ポリシング 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、パケットは適合し、パケットで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実行されます。

- 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。リフィル トークンは、適合バケットに置かれます。トークンが適合バケットでオーバーフローになると、超過バケットにオーバーフロー トークンが置かれます。

  トークンの到達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。このシナリオでは、超過バケットには影響ありません。
- 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 バケットでパケットによるバイトがチェックされます。適合バケット 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、超過トークン バケットから B バイトが削除されます。適合バケットから削除されるバイトはありません。
- 適合バケット B のバイト数が 0 未満の場合、パケットはレートに違反しているため、違反アクションが実行されます。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、トークン バケットは 1000 バイトでいっぱいの状態から始まります。450 バイトのパケットを受信すると、適合トークン バケットに使用可能なバイトが十分あるため、パケットは適合しています。パケットにより適合アクション（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（残り 550 バイト）。

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、トークン バケットは 1000 バイトでいっぱいの状態から始まります。450 バイトのパケットを受信すると、適合トークン バケットに使用可能なバイトが十分あるため、パケットは適合しています。パケットにより適合アクション（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（残り 550 バイト）。

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 バケットでは 800 バイトしか使用できないため、パケットは適合していません。

フルの 1000 バイトで始まる超過トークン バケット（超過バースト サイズで指定）に使用可能なバイトがあるかどうかがチェックされます。超過トークン バケットには使用可能なバイトが十分あるため、超過アクション（QoS 送信値を 1 に設定）が実行され、超過バケットから 900 バイトが取られ、超過トークン バケットの残りは 100 バイトになります。

次のパケットが 0.40 秒後に到達し、トークン バケットに 400 バイトが追加されます（(.40 X 8000)/8）。これで、適合トークン バケットには 1000 バイトあり（適合バケットで使用可能な最大トークン数）、200 バイトが適合トークン バケットをオーバーフローします（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 バイトだけのため）。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 バケットに 300 バイト与えられます。

着信パケットが 1000 バイトの場合、適合トークン バケットで使用可能なバイト数が十分あるため、パケットは適合します。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 秒後に到達し、トークン バケットに 200 バイトが追加されます（(.20 X 8000)/8）。これで、適合バケットの中身は 200 バイトになります。着信パケットが 400 バイトの場合、適合バケットでは 200 バイトしか使用できないため、パケットは適合していません。同様に、超過バケットで使用可能なバイト数は 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（割合）	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 つのレート）	認定情報レート（CIR）と最大情報レート（PIR）の 2 つの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 QoS（Quality of Service）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（割合）

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。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：サービス クラス（CoS）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 DiffServ コード ポイント（DSCP）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	変更箇所
12.2(40)SG	このコマンドが Catalyst 4900M および Supervisor Engine 6-E 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後に 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。オプションの bc 値と be 値（それぞれ、300 ms、400 ms）も指定されています。

```
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	変更箇所
12.2(40)SG	このコマンドが、Supervisor Engine 6-E 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 つのレート）

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：サービス クラス（CoS）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 DiffServ コード ポイント（DSCP）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	変更箇所
12.2(40)SG	このコマンドが、Supervisor Engine 6-E 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。

$Tp(t) = Tp(t) – B$

$Tc(t) = Tc(t) – B$

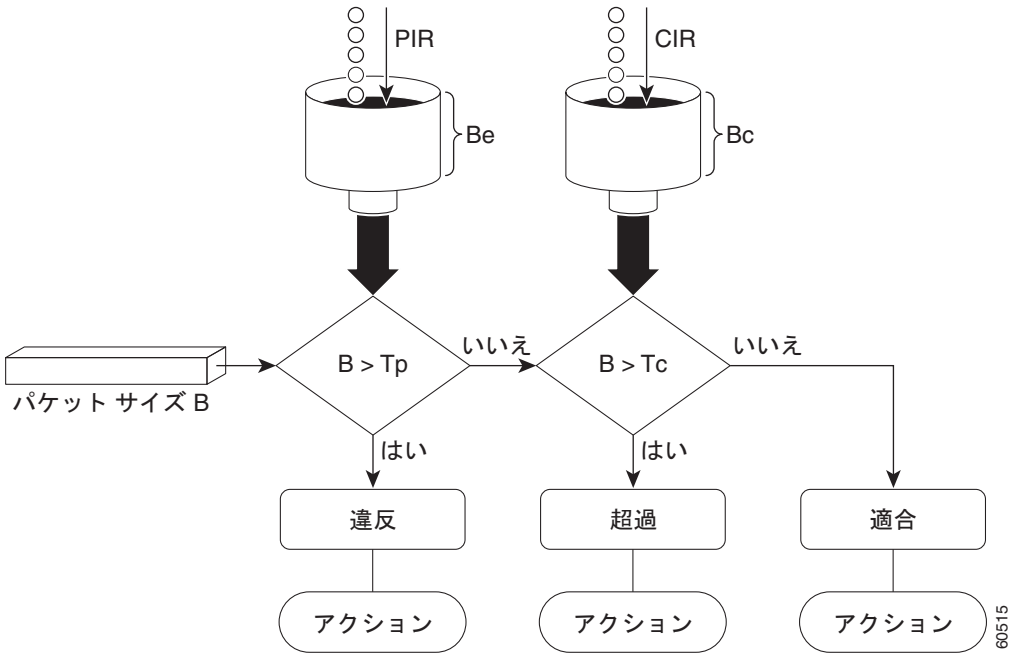
たとえば、CIR が 100 kbps、PIR が 200 kbps で、250 kbps のレートのデータ ストリームが 2 レート ポリサーで到着した場合、パケットは次のようにマークされます。

- 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）に適合するとして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	変更箇所
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拡張されました。

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**：指定したクラス マップの分類一致基準を定義します。詳細については、「class」（P.2-92）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**：定義済みポリシー 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。

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、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」の項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	変更箇所
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-channel standalone-disable

ポート チャネルの EtherChannel スタンドアロン オプションをディセーブルにするには、インターフェイス コンフィギュレーション モードで **port-channel standalone-disable** コマンドを使用します。このオプションをイネーブルにするには、このコマンドの no 形式を使用します。

port-channel standalone-disable

no port-channel standalone-disable

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

スタンドアロン オプション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	変更箇所
15.0(2)SG1	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、ポート チャネル プロトコル タイプが Link Aggregation Control Protocol（LACP）の場合にだけ使用できます。物理ポートが LACP EtherChannel とバンドルできない場合、現在の動作を変更することができます。

例

次の例では、ポート チャネルの EtherChannel スタンドアロン オプションをイネーブルにする方法を示します。

```
Switch(config-if)# no port-channel standalone-disable
```

関連コマンド

コマンド	説明
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	変更箇所
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	変更箇所
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	変更箇所
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 上のセキュア アドレスの最大数はポートに設定された最大値に制限されます。

各 VLAN は、ポートで設定された値よりも大きい最大数を設定できます。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。いずれの場合でも、各 VLAN のセキュア MAC アドレス数は、VLAN の設定最大値とポートの設定最大値の小さい方の数に制限されます。

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

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	変更箇所
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	変更箇所
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 ～ 15399 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	変更箇所
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

inline power consumption コマンドは、IEEE/Cisco 電話の検出および CDP/LLDP 電力ネゴシエーションを使用してポートに割り当てられた電力を上書きします。システムの安全な動作を保証するには、ここで設定した値が接続デバイスの実際の電力要件以下ではないことを確認します。インライン受電装置によって供給される電力が電源装置の機能を超過した場合、電源装置をトリップさせる可能性があります。

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 four-pair forced

（注）　このコマンドは、Supervisor Engine 7-E および Supervoisor Engine 7L-E だけで使用できます。

エンド デバイスが信号およびスペア ペアの両方で PoE に対応しているが、UPOE に必要な CDP または LLDP の拡張をサポートしていない場合に、自動的にスイッチ ポートからの信号およびスペア ペアの両方で電力をイネーブルにするには、**power inline four-pair forced** コマンドを使用します。

power inline four-pair forced

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

なし

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.0(2)SG	このコマンドが、Supervisor Engine 7-E および 7L-E 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

IEEE 802.at はポート単位で最大 30W の電力だけを提供しますが、WS-X4748-UPOE+E モジュールは RJ45 ケーブルのスペア ペア（ワイヤ 4、5、7、8）、および信号ペア（ワイヤ 1、2、3、6）を使用して最大 60W を提供します。スイッチ ポートおよびエンド デバイスが CDP または LLDP を使用して UPOE 対応として相互を識別し、エンド デバイスがスペア ペアの電力のイネーブル化を要求すると、スペア ペアの電力がイネーブルになります。スペア ペアに電源を入れると、エンド デバイスは、CDP または LLDP を使用して、スイッチから最大 60W の電力ネゴシエートできます。

エンド デバイスが信号およびスペア ペアの両方で PoE に対応しているが、UPOE に必要な CDP または LLDP の拡張をサポートしていない場合、次の設定により自動的にスイッチ ポートからの信号およびスペア ペアの両方で電力がイネーブルになります。

例

次の例では、自動的にスイッチのギガビット イーサネット ポート 2/1 からの信号およびスペア ペアの両方の電力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 gigabitethernet 2/1
Switch(config-if)# power inline four-pair forced
Switch(config-if)# shutdown
Switch(config-if)# no shutdown
Switch(config-if)# end
Switch#
```

エンド デバイスがスペア ペアのインライン パワーを供給できないか、またはエンド デバイスが UPOE の CDP または LLDP の拡張をサポートしている場合、このコマンドを入力しないでください。

power inline logging global

PoE 装置がいつ検出されたか、および PoE 装置がいつ削除されたかを示すコンソール メッセージをイネーブルにするには、**power inline logging global** コマンドを使用します。

power inline logging 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

ディセーブル

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
15.0(2)SG2/ XE 3.2.2SG	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

このコマンドを複数の PoE 装置に接続されたスイッチで使用する場合、コンソールのフラッディングの可能性に注意してください。

例

次の例では、各インターフェイスの PoE 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。

PoE イベント ロギングをイネーブルにするには、**logging event poe-status global** コマンドを使用します。

```
Switch# conf terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# power inline logging global
Switch(config)# int gigabitEthernet 5/5
Switch(config-if)# shut
Switch(config-if)#
*Oct 17 12:02:48.407: %ILPOWER-5-IEEE_DISCONNECT: Interface Gi5/5: PD removed
Switch(config-if)# no shut
Switch(config-if)#
*Oct 17 12:02:54.915: %ILPOWER-7-DETECT: Interface Gi5/5: Power Device detected: IEEE PD
```

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。

power inline police

特定のインターフェイスの Power over Ethernet 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	変更箇所
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
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。
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。

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	変更箇所
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

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 2-12 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 2-12　利用可能な電力

電源装置	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。

pppoe intermediate-agent（グローバル）

スイッチで PPPoE 中継エージェント機能をイネーブルにするには、**pppoe intermediate-agent** グローバル コンフィギュレーション コマンドを使用します。この機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

pppoe intermediate-agent

no pppoe intermediate-agent

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

disabled

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	変更箇所
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

スイッチで PPPoE 中継エージェントをグローバルにイネーブルにしてから、インターフェイスまたはインターフェイス VLAN で PPPoE 中継エージェントを使用する必要があります。

例

次の例では、スイッチで PPPoE 中継エージェントをイネーブルにする方法を示します。

```
Switch(config)# pppoe intermediate-agent
```

次の例では、スイッチで PPPoE 中継エージェントをディセーブルにする方法を示します。

```
Switch(config)# no pppoe intermediate-agent
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（グローバル）	スイッチのアクセス ノード識別子、一般的なエラーに関するメッセージ、および ID 文字列を設定します。

pppoe intermediate-agent（インターフェイス）

（注）　このコマンドは、**pppoe intermediate-agent** グローバル コマンドをイネーブルにする場合にだけ有効です。

インターフェイスで PPPoE 中継エージェント機能をイネーブルにするには、**pppoe intermediate-agent** 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。

pppoe intermediate-agent

no pppoe intermediate-agent

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのインターフェイスでディセーブル

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	変更箇所
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

PPPoE 中継エージェントがスイッチおよびインターフェイスの両方でイネーブルになっていれば、インターフェイスで PPPoE 中継エージェントがイネーブルになります。

例

次の例では、インターフェイスで PPPoE 中継エージェントをイネーブルにする方法を示します。

```
Switch(config-if)# pppoe intermediate-agent
```

次の例では、インターフェイスで PPPoE 中継エージェントをディセーブルにする方法を示します。

```
Switch(config-if)# no pppoe intermediate-agent
```

関連コマンド

コマンド	説明
pppoe intermediate-agent format-type（インターフェイス）	インターフェイスの回線 ID またはリモート ID を設定します。
pppoe intermediate-agent limit rate	インターフェイスに着信する PPPoE ディスカバリ パケットのレートを制限します。

コマンド	説明
pppoe intermediate-agent trust	インターフェイスの信頼設定を設定します。
pppoe intermediate-agent vendor-tag strip	PPPoE サーバ（または BRAS）からの PPPoE ディスカバリ パケットでベンダー タグの除去をイネーブルにします。

pppoe intermediate-agent（インターフェイス VLAN 範囲）

（注）　このコマンドは、**pppoe intermediate-agent** グローバル コマンドをイネーブルにする場合にだけ有効です。

インターフェイス VLAN 範囲で PPPoE 中継エージェントをイネーブルにするには、**pppoe intermediate-agent** グローバル 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。

pppoe intermediate-agent

no pppoe intermediate-agent

構文の説明

このコマンドには、引数またはキーワードはありません。

デフォルト

すべてのインターフェイスのすべての VLAN でディセーブル

コマンド モード

インターフェイス VLAN 範囲コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(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

このコマンドは **pppoe intermediate-agent**（インターフェイス コンフィギュレーション モード）コマンドに関係なく有効になりますが、**pppoe intermediate-agent**（グローバル コンフィギュレーション モード）コマンドをイネーブルにする必要があります。

例

次の例では、VLAN の範囲で PPPoE 中継エージェントをイネーブルにする方法を示します。

```
Switch(config-if)# vlan-range 167-368
Switch(config-if-vlan-range)# pppoe intermediate-agent
```

次の例では、単一の VLAN で PPPoE 中継エージェントをディセーブルにする方法を示します。

```
Switch(config-if)# vlan-range 268
Switch(config-if-vlan-range)# no pppoe intermediate-agent
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（インターフェイス）	インターフェイスで PPPoE 中継エージェント機能をイネーブルにします。

pppoe intermediate-agent format-type（グローバル）

スイッチのアクセス ノード識別子、一般的なエラーに関するメッセージ、および ID 文字列を設定するには、**pppoe intermediate-agent format-type（グローバル）**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。

pppoe intermediate-agent format-type access-node-identifier string *string*

pppoe intermediate-agent format-type generic-error-message string *string*

pppoe intermediate-agent format-type identifier-string string *string* **option {sp|sv|pv|spv} delimiter {**,|.|;|/|#**}**

no pppoe intermediate-agent format-type {**access-node-identifier** | **generic-error-message** | **identifier-string**}

構文の説明

access-node-identifier string *string*	アクセス ノード識別子の ASCII 文字列のリテラル値。
generic-error-message string *string*	一般的なエラーに関するメッセージの ASCII 文字列のリテラル値。
identifier-string string *string*	ID 文字列の ASCII 文字列のリテラル値。
option {**sp**|**sv**|**pv**|**spv**}	次のオプションがあります。 **sp** = スロット + ポート **sv** = スロット + VLAN **pv** = ポート + VLAN **spv** = スロット + ポート + VLAN
delimiter {,|.|;|/|#**}**	**option** のスロット / ポート /VLAN 部分間のデリミタ。

デフォルト

access-node-identifier には 0.0.0.0 のデフォルト値があります。

generic-error-message、**identifier-string**、**option**、および **delimiter** にはデフォルト値はありません。

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	変更箇所
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

回線 ID パラメータを自動的に生成するようにスイッチをイネーブルにするには、**access-node-identifier** および **identifier-string** コマンドを使用します。

option と delimiter の設定を解除するには、**identifier-string** コマンドの **no** 形式を使用します。

PPPoE ディスカバリ パケットが大きすぎることを送信者に通知するエラー メッセージを設定するには、**generic-error-message** コマンドを使用します。

例

次の例では、アクセス ノード識別子を設定する方法を示します。

```
Switch(config)# pppoe intermediate-agent format-type access-node-identifier string
switch-abc-123
```

次の例では、一般的なエラーに関するメッセージを解除する方法を示します。

```
Switch(config)# no pppoe intermediate-agent format-type generic-error-message
```

関連コマンド

コマンド	説明
show pppoe intermediate-agent interface	PPPoE 中継エージェント設定および統計情報（パケット カウンタ）を表示します。

pppoe intermediate-agent format-type（インターフェイス）

（注）　このコマンドは、**pppoe intermediate-agent** インターフェイス コンフィギュレーション コマンドをイネーブルにする場合にだけ有効です。

インターフェイスの回線 ID またはリモート ID を設定するには、**pppoe intermediate-agent format-type** コマンドを使用します。パラメータの設定を解除するには、このコマンドの **no** 形式を使用します。

pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

no pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

構文の説明

circuit-id string *string*	回線 ID の ASCII 文字列のリテラル値。
remote-id string *string*	リモート ID の ASCII 文字列のリテラル値。

デフォルト

回線 ID およびリモート ID のデフォルト値はありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(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

インターフェイス固有の回線 ID 値およびリモート ID 値を設定するには、**pppoe intermediate-agent format-type** コマンドを使用します。インターフェイス固有の回線 ID が設定されていない場合、システムの自動生成された回線 ID 値が使用されます。

例

次の例では、インターフェイスのリモート ID を設定する方法を示します。

```
Switch(config-if)# pppoe intermediate-agent format-type remote-id string user5551983
```

次の例では、インターフェイスの回線 ID の設定を解除する方法を示します。

```
Switch(config)# no pppoe intermediate-agent format-type circuit-id
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（インターフェイス）	インターフェイスで PPPoE 中継エージェント機能をイネーブルにします。
pppoe intermediate-agent（インターフェイス VLAN 範囲）	インターフェイス VLAN 範囲の回線 ID またはリモート ID を設定します。

pppoe intermediate-agent format-type（インターフェイス VLAN 範囲）

（注）　このコマンドは、**pppoe intermediate-agent** インターフェイス VLAN 範囲コンフィギュレーション モード コマンドをイネーブルにする場合にだけ有効です。

インターフェイス VLAN 範囲の回線 ID またはリモート ID を設定するには、**pppoe intermediate-agent format-type** interface vlan-range mode コマンドを使用します。パラメータの設定を解除するには、このコマンドの **no** 形式を使用します。

pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

no pppoe intermediate-agent format-type {**circuit-id** | **remote-id**} **string** *string*

構文の説明

circuit-id string *string*	回線 ID に設定される ASCII 文字列のリテラル値。
remote-id string *string*	リモート ID に設定される ASCII 文字列のリテラル値。

デフォルト

回線 ID およびリモート ID のデフォルト値はありません。

コマンド モード

インターフェイス VLAN 範囲コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(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

インターフェイス VLAN 範囲で回線 ID またはリモート ID を設定するには、これらのコマンドを使用します。回線 ID が設定されていない場合、システムの自動生成された回線 ID が使用されます。

例

次の例では、インターフェイス VLAN のリモート ID を設定する方法を示します。

```
Switch(config-if)# vlan-range 268
Switch(config-if-vlan-range)#
pppoe intermediate-agent format-type remote-id string user5551983-cabletv
```

次の例では、インターフェイス VLAN 範囲の回線 ID の設定を解除する方法を示します。

```
Switch(config-if)# vlan-range 167-368
Switch(config-if-vlan-range)# no pppoe intermediate-agent format-type circuit-id
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（インターフェイス VLAN 範囲）	インターフェイス VLAN 範囲で PPPoE 中継エージェントをイネーブルにします。

pppoe intermediate-agent limit rate

インターフェイスに着信する PPPoE ディスカバリ パケットのレートを制限するには、**pppoe intermediate-agent limit rate** 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。

pppoe intermediate-agent limit rate *number*

no pppoe intermediate-agent limit rate *number*

構文の説明

number	このインターフェイスで受信した PPPoE ディスカバリ パケットのしきい値レートをパケット/秒で指定します。

デフォルト

このコマンドにはデフォルト設定がありません。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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

このコマンドを使用すると、受信した PPPoE ディスカバリ パケットが設定されているレートを超えた場合、インターフェイスは errdisable になります（シャットダウン）。

例

次の例では、インターフェイスのレート制限を設定する方法を示します。

```
Switch(config-if)# pppoe intermediate-agent limit rate 50
```

次の例では、インターフェイスの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 pppoe intermediate-agent limit rate
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（インターフェイス）	インターフェイスで PPPoE 中継エージェント機能をイネーブルにします

pppoe intermediate-agent trust

インターフェイスの信頼設定を設定するには、**pppoe intermediate-agent trust** グローバル コマンドを使用します。信頼パラメータの設定を解除するには、このコマンドの **no** 形式を使用します。

pppoe intermediate-agent trust

no pppoe intermediate-agent 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

すべてのインターフェイスは untrusted。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
12.2(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

PPPoE 中継エージェント機能が機能するために、スイッチに少なくとも 1 つの信頼できるインターフェイスが存在する必要があります。

スイッチを PPPoE サーバ（または BRAS）に接続するインターフェイスを信頼できるインターフェイスに設定します。

例

次の例では、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方法を示します。

```
Switch(config-if)# pppoe intermediate-agent trust
```

次の例では、インターフェイスの信頼設定をディセーブルにする方法を示します。

```
Switch(config-if)# no pppoe intermediate-agent trust
```

関連コマンド

コマンド	説明
pppoe intermediate-agent vendor-tag strip	PPPoE サーバ（または BRAS）からの PPPoE ディスカバリ パケットでベンダー タグの除去をイネーブルにします。

pppoe intermediate-agent vendor-tag strip

（注）　このコマンドは、**pppoe intermediate-agent** インターフェイス コンフィギュレーション コマンドおよび **pppoe intermediate-agent trust** コマンドをイネーブルにする場合にだけ有効です。

PPPoE サーバ（または BRAS）からの PPPoE ディスカバリ パケットでベンダー タグの除去をイネーブルにするには、**pppoe intermediate-agent vendor-tag strip** コマンドを使用します。この設定をディセーブルにするには、このコマンドの **no** 形式を使用します。

pppoe intermediate-agent vendor-tag strip

no pppoe intermediate-agent vendor-tag strip

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

ベンダー タグの除去がオフになります。

コマンド モード

インターフェイス コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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

このコマンドは、信頼できないインターフェイスに影響を与えません。

PPPoE サーバ（または BRAS）からのダウンストリーム PPPoE ディスカバリ パケットのベンダー固有のタグを取り除くには、PPPoE 中継エージェントの信頼できるインターフェイスでこのコマンドを使用します。

例

次の例では、インターフェイスでベンダー タグの除去を設定する方法を示します。

```
Switch(config-if)# pppoe intermediate-agent vendor-tag strip
```

次の例では、インターフェイスでベンダー タグの除去をディセーブルにする方法を示します。

```
Switch(config-if)# no pppoe intermediate-agent vendor-tag strip
```

関連コマンド

コマンド	説明
pppoe intermediate-agent（インターフェイス）	インターフェイスで PPPoE 中継エージェント機能をイネーブルにします。
pppoe intermediate-agent trust	インターフェイスの信頼設定を設定します。

priority

完全プライオリティ 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

完全プライオリティ 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	変更箇所
12.2(40)SG	Supervisor Engine 6E および Catalyst 4900M で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

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、完全プライオリティ キューイングを提供します。完全プライオリティ 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。プライオリティ キューは、空になるまで先に処理されます。

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一のポリシー マップ内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。

プライオリティ 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。
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。
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 QoS（Quality of Service）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** | **twoway-community** | **primary**}

private-vlan association *secondary-vlan-list* [{**add** *secondary-vlan-list*} | {**remove** *secondary-vlan-list*}]

no private-vlan {**isolated** | **community** | **twoway-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。
twoway-community	双方向コミュニティ セカンダリ VLAN に属するホスト ポートとして VLAN を指定します。
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 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。 リストには独立 VLAN を 1 つだけ含めることができます。複数のコミュニティまたは双方向コミュニティの VLAN ID を含めることもできます。
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	変更箇所
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。
15.0(2)SG	双方向コミュニティ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 はプライベート VLAN をサポートしません。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、独立 VLAN ID を 1 つだけ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、無差別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 ポートおよび無差別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 ポートから無差別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。

無差別ポートは、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

次に、VLAN 202 をプライマリ VLAN として設定し、その設定を確認する例を示します。

```
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
```

次に、VLAN 303 をコミュニティ VLAN として設定し、その設定を確認する例を示します。

```
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
```

次に、VLAN 440 を独立 VLAN として設定し、その設定を確認する例を示します。

```
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、VLAN 550 を双方向コミュニティ VLAN 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)# vlan 550
Switch(config-vlan)# private-vlan twoway-community
Switch(config-vlan)# end
Switch# show vlan private-vlan

Primary Secondary Type              Interfaces
------- --------- ----------------- ------------------------------------------
202               primary
        303       community
        440       isolated
         550   twoway-community
```

次の例は、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 に関連付けて設定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 は、プライマリ VLAN と関連付けされません。

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)#
```

次に、ファスト イーサネット インターフェイス 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例を示します。

```
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	変更箇所
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がありません。

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	変更箇所
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** コマンドにより、すべてのセカンダリ VLAN が、関連付けられたプライマリ VLAN として自動的に同じインスタンス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がありません。

コマンド モード

cfg-call-home

コマンド履歴

リリース	変更箇所
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 メッセージが送信される宛先電子メール 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 グループに登録します。
subscribe-to-alert-group configuration	この宛先プロファイルを Configuration アラート グループに登録します。
subscribe-to-alert-group diagnostic	この宛先プロファイルを Diagnostic アラート グループに登録します。
subscribe-to-alert-group environment	この宛先プロファイルを Environment アラート グループに登録します。
subscribe-to-alert-group inventory	この宛先プロファイルを Inventory アラート グループに登録します。
subscribe-to-alert-group syslog	この宛先プロファイルを Syslog アラート グループに登録します。

profile flow

メディア サービス プロキシ（MSP）をイネーブルにするには、**profile flow** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

profile flow

no profile flow

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がありません。

コマンド モード

config

コマンド履歴

リリース	変更箇所
リリース IOS XE 3.4.0SG and IOS 15.1(2)SG)	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

MSP プロファイル フロー コマンドを設定し、MSP プラットフォーム パケット パーサーをアクティブにする必要があります。これは、MSP デバイス ハンドラが MSP フロー パーサーと強固に組み合わされるためです。この CLI をイネーブルにしないと、MSP は IOS センサーに SIP、H323 通知を送信しません。

例

次に、MSP をイネーブルにする例を示します。

```
Switch(config)# profile flow
```

qos account layer-all encapsulation

QoS ポリシング機能で 20 バイトのレイヤ 1 ヘッダー長を考慮するには、**qos account layer-all 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 layer-all encapsulation

no qos account layer-all encapsulation

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

Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E では、ポリサーはポリシング機能でレイヤ 2 ヘッダー長だけを考慮します。これに対し、シェーパはレート計算にヘッダー長および IPG を考慮します。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
15.0(2)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

Supervisor Engine 6-E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948E は、**qos account layer-all encapsulation** コマンドを使用してポリシング機能で 20 バイトのレイヤ 1 ヘッダー（プリアンブル + IPG）とレイヤ 2 ヘッダーを考慮します。このコマンドが設定されている場合、**show policy-map interface** コマンドの出力に表示されたポリサー統計情報（バイト単位）には、レイヤ 1 ヘッダー長も反映されます（パケットあたり 20 バイト）。

例

次の例では、ポリシングに IPG を含める方法を示します。

```
Switch)# config t
Switch(config)# qos account layer-all encapsulation
Switch(config)# end
Switch#
```

関連コマンド

コマンド	説明
show policy-map interface	特定のインターフェイスのポリサー統計情報を表示します。

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 6E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948-E 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が含まれます。

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	変更箇所
12.1(19)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

Supervisor Engine 6E、Supervisor Engine 6L-E、Catalyst 4900M、および Catalyst 4948-E 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 の長さだけが考慮されます。

（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(config)# qos account layer2 encapsulation length 18
Switch (config)# 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 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	変更箇所
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
queue-limit	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。

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	変更箇所
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）コマンドは、Catalyst 4500 Supervisor Engine の MQC サポートの一部として、Supervisor Engine 6-E だけに適用されます。

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がありません。

コマンド モード

グローバル コンフィギュレーション モード

コマンド履歴

リリース	変更箇所
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 台のスーパーバイザ エンジンの設定を手動で同期させるために使用します。

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するには、メイン CPU サブモードから **auto-sync** コマンドを使用します。

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 エンジンを Mismatched Command List（MCL）に移動し、スタンバイ スーパーバイザ エンジンをリセットするには、**redundancy config-sync mismatched-commands** コマンドを使用します。

アクティブとスタンバイのスーパーバイザ エンジンが Cisco IOS の異なるバージョンを実行している場合、一部の CLI の互換性がありません。このようなコマンドがすでにアクティブ 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存在し、スタンバイ スーパーバイザ エンジンの起動中にコマンドの構文チェックが失敗した場合は、アクティブ スーパーバイザ エンジンを Mismatched Command List（MCL）に移動する必要があります。

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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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	コマンド名が **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、すべての不一致コマンドをアクティブ 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削除し、**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 を再確認してから、スタンバイ スーパーバイザ エンジンをリロードします。

redundancy config-sync ignore mismatched-commands コマンドを入力し、スタンバイ スーパーバイザ エンジンをリロードすることで、MCL を無視することもできます。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。

無視した MCL は **show redundancy config-sync ignored mcl** コマンドで確認できます。

コンフィギュレーション ファイル内の非互換性が原因で、SSO モードをアクティブ スーパーバイザ エンジンとスタンバイ スーパーバイザ エンジン間で確立できない場合、Mismatched Command List（MCL）がアクティブ スーパーバイザ エンジンで生成され、スタンバイ スーパーバイザ エンジンは RPR モードに強制的にリロードされます。問題の設定を削除し、まったく同じイメージでスタンバイ スーパーバイザ エンジンを再起動した後、SSO を確立しようとすると、ピア イメージが互換性がないと表示されるため、「C4K_REDUNDANCY-2-IOS_VERSION_CHECK_FAIL and ISSU-3-PEER_IMAGE_INCOMPATIBLE」というメッセージが表示される場合があります。設定上の問題を修正できる場合は、ピアが STANDBY COLD（RPR）ステートの間に、**redundancy config-sync ignore mismatched-commands** EXEC コマンドで互換性のないリストからピア イメージをクリアできます。このアクションは、リロード時にスタンバイ スーパーバイザ エンジンが STANDBY HOT（SSO）ステートで起動できるようにします。

例

次の例では、MCL からのエントリの削除を検証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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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し、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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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 はディセーブルです。

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	変更箇所
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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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。

rep admin vlan

Resilient Ethernet Protocol（REP）が Hardware Flood Layer（HFL; ハードウェア フラッド レイヤ）メッセージを送信するように REP 管理 VLAN を設定するには、**rep admin vlan** グローバル コンフィギュレーション コマンドを使用します。デフォルト設定（VLAN 1 が管理 VLAN）に戻す場合は、このコマンドの **no** 形式を使用します。

rep admin vlan *vlan-id*

no rep admin vlan

構文の説明

vlan-id	VLAN ID の範囲は 1 ～ 4094 です。デフォルトは VLAN 1 のため、設定する範囲は 2 ～ 4094 です。

デフォルト

管理 VLAN は VLAN 1 です。

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(44)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

VLAN がまだ存在していない場合、このコマンドにより VLAN が作成されることはありません。

ロード バランシング時のリンク障害や VLAN ブロッキングの通知のメッセージをソフトウェアでリレーすることによって発生する遅延を回避するために、REP は HFL で通常のマルチキャスト アドレスにパケットをフラッディングします。これらのメッセージは REP セグメントだけではなくネットワーク全体にフラッディングされます。セグメントに属していないスイッチは、これらのメッセージをデータ トラフィックとして扱います。ドメイン全体の管理 VLAN を設定することにより、これらのメッセージのフラッディングを管理できます。

REP 管理 VLAN が設定されていない場合、デフォルトは VLAN 1 になります。

スイッチとセグメントで 1 つの管理 VLAN だけが可能です。

管理 VLAN は RSPAN VLAN になりません。

例

次の例では、VLAN 100 を REP 管理 VLAN として設定する方法を示します。

```
Switch(config)# rep admin vlan 100
```

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

関連コマンド

コマンド	説明
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの詳細 REP 設定およびステータスを表示します。

rep block port

Resilient Ethernet Protocol（REP）VLAN ロード バランシングを設定するには、REP プライマリ エッジ ポートで**rep block port** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

rep block port {id *port-id* | *neighbor_offset* | **preferred}** **vlan** {***vlan-list*** | **all}**

no rep block port {**id** *port-id* | *neighbor_offset* | **preferred**}

構文の説明

id *port-id*	REP イネーブル時に自動的に生成される一意のポート ID を入力することで、VLAN ブロック代替ポートを識別します。REP ポート ID は、16 文字の 16 進数値です。インターフェイスのポート ID を表示するには、**show interface** *interface-id* **rep detail** コマンドを入力します。
neighbor_offset	ネイバーのオフセット番号を入力することで、VLAN ブロック代替ポートを識別します。指定できる範囲は –256 ～ +256 で、値 0 は無効です。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジ ポート（オフセット番号 –1）とダウンストリーム ネイバーを識別します。
preferred	VLAN ブロック代替ポートを、**rep segment** *segment-id* **preferred** インターフェイス コンフィギュレーション コマンドを入力したセグメント ポートとして識別します。 **（注）** **preferred** キーワードを入力しても確実に代替ポートは指定されませんが、他の類似のポートより優先されます。
vlan	ブロックする VLAN を識別します。
vlan-list	ブロックする VLAN について、1 ～ 4094 の範囲の VLAN ID を入力するか、VLAN ID の範囲または連続番号（1-3、22、41-44 など）を入力します。
all	すべての VLAN をブロックするように入力します。

デフォルト

rep preempt segment 特権 EXEC コマンド（手動プリエンプション）を入力した場合のデフォルトのアクションは、プライマリ エッジ ポートで VLAN すべてがブロックされます。この動作は **rep block port** コマンドを設定するまで継続されます。

プライマリ エッジ ポートで代替ポートを判別できない場合は、デフォルトのアクションはプリエンプションなし、および VLAN ロード バランシングなしです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

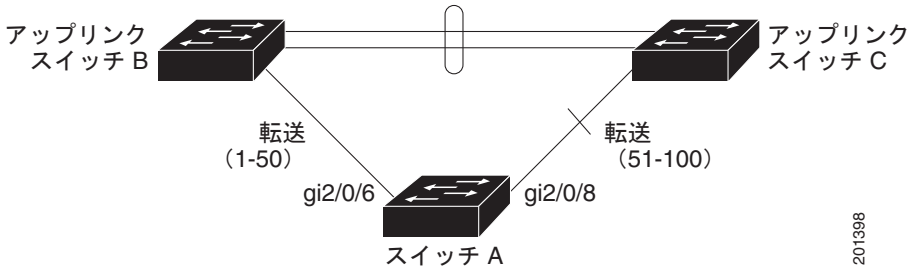
リリース	変更箇所
12.2(44)SG	このコマンドが追加されました。

使用上のガイドライン

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

オフセット番号を入力して代替ポートを選択する場合、オフセット番号はエッジポートのダウンストリーム ネイバー ポートを識別します。プライマリ エッジ ポートはオフセット番号 1 です。1 を超える正数はプライマリ エッジ ポートのダウンストリーム ネイバーを識別します。負の番号は、セカンダリ エッジ ポート（オフセット番号 –1）とダウンストリーム ネイバーを識別します。「REP セグメントのネイバー オフセット番号」図 2-2 を参照してください。

図 2-2　REP セグメントのネイバー オフセット番号



（注） 番号 1 はプライマリ エッジ ポート自体のオフセット番号なので、オフセット番号 1 は入力しないでください。

rep preempt delay *seconds* インターフェイス コンフィギュレーション コマンドを入力することでプリエンプション遅延時間を設定していて、リンク障害とリカバリが発生した場合、別のリンク障害が発生することなく設定したプリエンプション期間が経過すると、VLAN ロード バランシングが開始されます。ロードバランシング設定で指定された代替ポートは、設定された VLAN をブロックし、その他すべてのセグメント ポートのブロックを解除します。プライマリ エッジ ポートで VLAN バランシングの代替ポートを決定できない場合、デフォルトのアクションはプリエンプションなしになります。

セグメント内のポートごとに、一意のポート ID が割り当てられます。ポート ID の形式は、スパニング ツリー アルゴリズムで使用されるものと同様で、MAC アドレス（ネットワーク内で一意）に関連付けられるポート番号（ブリッジ上で一意）となります。ポートのポート ID を判別するには、**show interface** *interface-id* **rep detail** 特権 EXEC コマンドを入力します。

rep block port id *port-id* **vlan** *vlan-list* インターフェイス コンフィギュレーション コマンドは、入力回数の制限はありません。番号、範囲、または連続番号の制限なく、VLAN をブロックできます。

REP プライマリ エッジ ポート上で **rep block port id** *port-id* **vlan** *vlan-list* インターフェイス コンフィギュレーション コマンドを入力して VLAN リストをブロックし、その後同じコマンドを使用して同一のポート上で別の VLAN リストをブロックした場合、最初の VLAN リストが 2 番目の VLAN リストに置き換わることはありません。2 番目の VLAN リストは、最初の VLAN リストに追加されます。

REP プライマリ エッジ ポート上で **rep block port id** *port-id* **vlan** *vlan-list* インターフェイス コンフィギュレーション コマンドを入力して任意のポートで VLAN リストをブロックし、その後同じコマンドを使用して別のポート上で別の VLAN リストをブロックした場合、最初のポート番号および VLAN リストは上書きされます。

例

次の例では、スイッチ B のプライマリ エッジ ポート（ギガビット イーサネット ポート 1/0/1）上で REP VLAN ロード バランシングを設定し、スイッチ A のギガビット イーサネット ポート 1/1 を、VLAN 1 ～ 100 をブロックする代替ポートとして設定する方法を示します。代替ポートは、スイッチ A ポートの **show interface rep detail** コマンドの出力に太字で表示されるポート ID により識別されます。

```
Switch A# show interface gigabitethernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB17800EEE
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 1
Preempt Delay Timer: 35 sec
Load-balancing block port: none
Load-balancing block vlan: none
STCN Propagate to:
PDU/TLV statistics:
LSL PDU rx: 107122, tx: 192493

Switch B# config t
Switch (config)# interface gigabitethernet1/0/1
Switch (config-if)# rep block port id 0080001647FB1780 vlan 1-100
Switch (config-if)# exit
```

次の例では、ネイバー オフセット番号を使用して VLAN ロード バランシングを設定する方法と、**show interfaces rep detail** 特権 EXEC コマンドを入力して設定を確認する方法について示します。

```
Switch# config t
Switch (config)# interface gigabitethernet1/1
Switch (config-if)# rep block port 6 vlan 1-110
Switch (config-if)# end

Switch# show interface GigabitEthernet1/1 rep detail
GigabitEthernet1/1 REP enabled
Segment-id: 2 (Segment)
PortID: 0080001647FB1780
Preferred flag: No
Operational Link Status: TWO_WAY
Current Key: 007F001647FB178009C3
Port Role: Open
Blocked Vlan: <empty>
Admin-vlan: 3
Preempt Delay Timer: 35 sec
Load-balancing block port: 6
Load-balancing block vlan: 1-110
STCN Propagate to: none
LSL PDU rx: 1466780, tx: 3056637
HFL PDU rx: 2, tx: 0
BPA TLV rx: 1, tx: 2119695
BPA (STCN, LSL) TLV rx: 0, tx: 0
BPA (STCN, HFL) TLV rx: 0, tx: 0
EPA-ELECTION TLV rx: 757406, tx: 757400
EPA-COMMAND TLV rx: 1, tx: 1
EPA-INFO TLV rx: 178326, tx: 178323
```

関連コマンド

コマンド	説明
rep preempt delay	ポート障害とリカバリの後から REP VLAN ロード バランシングがトリガーされるまでの待機期間を設定します。
rep preempt segment	手動でセグメント上の REP VLAN ロード バランシングを開始します。
show interfaces rep detail	管理 VLAN を含め、すべてのインターフェイスまたは指定したインターフェイスの REP 詳細設定およびステータスを表示します。

rep lsl-age-timer

REP インターフェイスが REP ネイバーから hello を受信せずに起動し続ける時間の Link Status Layer（LSL）エージング タイマーを設定するには、Resilient Ethernet Protocol（REP）ポートで **rep lsl-age-timer** インターフェイス コンフィギュレーション コマンドを使用します。デフォルト時間に戻すには、このコマンドの **no** 形式を使用します。

rep lsl-age timer *value*

no rep lsl-age timer

構文の説明

value	エージアウト時間（ミリ秒）。指定できる範囲は 120 ～ 10000 ミリ秒（40 ミリ秒単位）です。デフォルト値は 5000 ミリ秒（5 秒）です。

デフォルト

REP リンクは、5000 ms 間ネイバーから hello メッセージを受信しなければ、シャットダウンされます。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(44)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

LSL エージ タイマーの間に少なくとも 2 つの LSL hello が送信されるように、LSL Hello タイマーはエージ タイマーの値を 3 で割った値に設定されます。この期間に hello が受信されない場合、REP リンクはシャットダウンします。

Cisco IOS Release 12.2(52)SE では、LSL エージング タイマーの範囲が 3000 ～ 10000 ミリ秒（500 ミリ秒単位）から 120 ～ 10000 ミリ秒（40 ミリ秒単位）に変更されています。REP ネイバー デバイスで Cisco IOS Release 12.2(52)SE 以降が稼動していない場合、デバイスは以前の範囲を逸脱する値を受け付けないため、時間の範囲を短くする必要があります。

EtherChannel ポート チャネル インターフェイスでは、1000 ミリ秒未満の LSL エージング タイマー値はサポートされていません。ポート チャネルで 1000 ミリ秒未満の値を設定しようとすると、エラー メッセージが表示されてコマンドが拒否されます。

例

次の例では、REP リンクの REP LSL エージ タイマーを 7000 ms に設定する方法を示します。

```
Switch(config)# interface GigabitEthernet1/1
Switch(config-if)# rep lsl-age-timer 7000
Switch(config-if)# exit
```

設定されたエージアウト時間を確認するには、**show interfaces rep detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep [**detail**]	設定済みの LSL エージアウト タイマー値を含め、すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep preempt delay

セグメント ポートの障害および回復の発生後 Resilient Ethernet Protocol（REP）VLAN ロード バランシングがトリガーされるまでの待機時間を設定するには、REP プライマリ エッジ ポートで **rep preempt delay** インターフェイス コンフィギュレーション コマンドを使用します。設定された遅延を削除するには、このコマンドの **no** 形式を使用します。

rep preempt delay *seconds*

no rep preempt delay

構文の説明

seconds	REP プリエンプションを遅延させる秒数を設定します。指定できる範囲は 15 ～ 300 です。

デフォルト

プリエンプション遅延は設定されていません。**rep preempt delay** コマンドを入力しない場合、デフォルトは遅延のない手動プリエンプションとなります。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(44)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

このコマンドは、REP プライマリ エッジ ポート上に入力する必要があります。

リンク障害とリカバリ後に自動的に VLAN ロード バランシングをトリガーする場合、このコマンドを入力してプリエンプション時間遅延を設定する必要があります。

VLAN ロード バランシングが設定されている場合、セグメント ポート障害とリカバリの後、VLAN ロード バランシングが発生する前に REP プライマリ エッジ ポートで遅延タイマーが起動されます。各リンク障害が発生した後にタイマーが再起動することに注意してください。タイマーが満了となると、（**rep block port** インターフェイス コンフィギュレーション コマンドを使用して設定された）VLAN ロード バランシングを実行するように REP プライマリ エッジが代替ポートに通知し、新規トポロジ用のセグメントが準備されます。設定された VLAN リストは代替ポートでブロックされ、他のすべての VLAN はプライマリ エッジ ポートでブロックされます。

EoMPLS トラフィックを伝送するインターフェイス上では、VLAN ロード バランシングを設定しないでください。REP リング間での VLAN ロード バランシングにより、一部の EoMPLS トラフィックが転送されなくなる場合があります。

例

次の例では、プライマリ エッジ ポートで REP プリエンプション時間遅延を 100 秒に設定する方法を示します。

```
Switch(config)# interface gigabitethernet1/0/1
Switch(config-if)# rep preempt delay 100
Switch(config-if)# exit
```

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

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep [**detail**]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep preempt segment

セグメントで Resilient Ethernet Protocol（REP）VLAN ロード バランシングを手動で開始するには、**rep preempt segment** 特権 EXEC コマンドを使用します。

rep preempt segment *segment_id*

構文の説明

segment-id	REP セグメントの ID。指定できる範囲は 1 ～ 1024 です。

デフォルト

デフォルト動作は手動プリエンプションです。

コマンド モード

特権 EXEC

コマンド履歴

リリース	変更箇所
12.2(44)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

rep preempt segment *segment-id* コマンドを入力すると、プリエンプションによってネットワークが中断する可能性があるため、コマンド実行前に確認メッセージが表示されます。

プライマリ エッジ ポートのあるセグメントのスイッチにこのコマンドを入力します。

VLAN ロード バランシングを設定しない場合、このコマンドを入力するとデフォルトの動作になります（プライマリ エッジ ポートですべての VLAN がブロックされます）。

手動でプリエンプションを開始する前に、REP プライマリ エッジ ポートで **rep block port** {**id** *port-id* | *neighbor_offset* | **preferred**} **vlan** {*vlan-list* | **all**} インターフェイス コンフィギュレーション コマンドを入力して、VLAN ロード バランシングを設定します。

このコマンドには、**no** バージョンはありません。

例

次の例では、確認メッセージ付きで、セグメント 100 で REP プリエンプションを手動でトリガーする方法を示します。

```
Switch)# rep preempt segment 100
The command will cause a momentary traffic disruption.
Do you still want to continue? [confirm]
```

関連コマンド

コマンド	説明
rep block port	VLAN ロード バランシングを設定します。
show interfaces rep [detail]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

rep segment

インターフェイスで Resilient Ethernet Protocol（REP）をイネーブルにして、セグメント ID を割り当てるには、**rep segment** インターフェイス コンフィギュレーション コマンドを使用します。インターフェイスで REP をディセーブルにする場合は、このコマンドの **no** 形式を使用します。

rep segment *segment-id* [**edge** [**no-neighbor**] [**primary**]] [**preferred**]

no rep segment

構文の説明

segment-id	セグメント ID をインターフェイスに割り当てます。指定できる範囲は 1 ～ 1024 です。
edge	（任意）2 つの REP エッジ ポートの 1 つとしてインターフェイスを識別します。**primary** キーワードなしで **edge** キーワードを入力すると、ポートがセカンダリ エッジ ポートとして設定されます。
no-neighbor	（任意）セグメント エッジを外部 REP ネイバーなしに設定します。
primary	（任意）エッジ ポートで、ポートがプライマリ エッジ ポートであると指定します。1 セグメント内のプライマリ エッジ ポートは 1 つだけです。別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。
preferred	（任意）ポートを優先代替ポートまたは VLAN ロード バランシングの優先ポートに指定します。 **（注）** ポートを優先に設定しても、代替ポートになるとは限りません。同等に可能性のあるポートよりやや可能性が高くなるだけです。通常、前に障害が発生したポートが、代替ポートとなります。

デフォルト

REP はインターフェイスでディセーブルです。

REP がインターフェイスでイネーブルの場合、デフォルトでは通常のセグメント ポートであるポートに対してイネーブルになります。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(44)SG	このコマンドが追加されました。
15(02)SG	**no-neighbor** キーワードが追加されました。

使用上のガイドライン

REP ポートは、レイヤ 2 トランク ポートである必要があります。非 ES REP ポートは、IEEE 802.1Q トランク ポートまたは ISL トランク ポートのいずれかになります。

REP ポートは次のいずれかのポート タイプとして設定してはいけません。

- SPAN 宛先ポート
- プライベート VLAN ポート

- トンネル ポート
- アクセス ポート

各 REP セグメント上には、プライマリ エッジ ポートと、セカンダリ エッジ ポートとして機能するポートの、2 種類のエッジ ポートを設定しなければいけません。たとえば別のスイッチにあるポートなどの、セグメント内の 2 つのポートをプライマリ エッジ ポートとして指定すると（設定は可能です）、REP によりその内の 1 つがセグメントのプライマリ エッジ ポートとして機能するように選択されます。

REP は EtherChannel でサポートされていますが、EtherChannel に属する個別のポートではサポートされません。

- REP ポートは以下の規則に従います。
  - スイッチ上の REP ポートの数に制限はありませんが、同じ REP セグメントに属することができるスイッチ上のポートは 2 つだけです。
  - セグメント内にスイッチ上の 1 ポートだけが設定されている場合、そのポートがエッジ ポートとなります。
  - 同じセグメント内に属するスイッチに 2 つのポートがある場合、両方のポートがエッジ ポートであるか、両方のポートが通常セグメント ポートであるか、一方が通常ポートでもう一方が非ネイバー エッジ ポートである必要があります。スイッチ上のエッジ ポートと通常セグメント ポートが同じセグメントに属することはできません。
  - スイッチ上の 2 ポートが同じセグメントに属していて、1 つがエッジ ポートとして設定され、もう 1 つが通常セグメント ポートに設定されている場合（設定ミス）、エッジ ポートは通常セグメント ポートとして扱われます。

別のスイッチのポートなど、セグメント内で 2 つのポートをプライマリ エッジ ポートに設定すると、REP がそのうちのいずれかを選択してセグメントのプライマリ エッジ ポートとして機能させます。いずれのポートがプライマリ エッジ ポートかを確認するには、**show rep topology** 特権 EXEC コマンドをセグメント内のポートに入力します。

REP インターフェイスはブロック ステートで起動し、安全にブロック解除可能と通知されるまでブロック ステートのままになります。突然の接続切断を避けるために、これを意識しておく必要があります。

冗長ネットワーク内だけに REP を設定します。冗長性のないネットワークに REP を設定すると、接続が失われます。

近接スイッチ上のポートで REP がサポートされていないネットワークでは、非 REP 側ポートを非ネイバー エッジ ポートとして設定できます。非ネイバー エッジ ポートはエッジ ポートのすべてのプロパティを継承するため、非ネイバー エッジ ポートをその他のいずれのエッジ ポートとしても設定できます。これには、STP または REP トポロジ変更通知をアグリゲーション スイッチに送信することも含まれます。この場合、送信される STP Topology Change Notification（TCN; トポロジ変更通知）は、Multiple Spanning-Tree（MST）STP メッセージです。

例

次の例では、通常の（非エッジ）セグメント ポートで REP をイネーブルにする方法を示します。

```
Switch (config)# interface gigabitethernet1/0/1
Switch (config-if)# rep segment 100
```

次の例では、ポートで REP をイネーブルにして、ポートを REP プライマリ エッジ ポートとして識別する方法を示します。

```
Switch (config)# interface gigabitethernet1/1
Switch (config-if)# rep segment 100 edge primary
```

次に、インターフェイスに外部 REP ネイバーがない場合の同じ設定の例を示します。

```
Switch# configure terminal
Switch (config)# interface gigabitethernet1/1
Switch (config-if)# rep segment 100 edge no-neighbor primary
```

次の例では、ポートで REP をイネーブルにして、ポートを REP セカンダリ エッジ ポートとして識別する方法を示します。

```
Switch (config)# interface GigabitEthernet1/1
Switch (config-if)# rep segment 100 edge
```

設定を確認するには、**show interfaces rep** 特権 EXEC コマンドを入力します。セグメントのいずれのポートがプライマリ エッジ ポートであるか確認するには、**show rep topology** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep [**detail**]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。
show rep topology [**detail**]	プライマリ エッジ ポートとして設定および選択されたポートを含む、セグメント内のすべてのポートに関する情報を表示します。

rep stcn

REP Segment Topology Change Notification（STCN; セグメント トポロジ変更通知）を他のインターフェイス、他のセグメントまたは Spanning Tree Protocol（STP）ネットワークに送信する設定を行うには、Resilient Ethernet Protocol（REP）エッジ ポートで **rep stcn** インターフェイス コンフィギュレーション コマンドを使用します。STCN をインターフェイス、セグメント、または STP ネットワークに送信することをディセーブルにする場合は、このコマンドの **no** 形式を使用します。

rep stcn {**interface** *interface-id* | **segment** *id-list* | **stp**}

no rep stcn {**interface** | **segment** | **stp**}

構文の説明

interface *interface-id*	STCN を受信するように物理インターフェイスまたはポート チャネルを識別します。
segment *id-list*	STCN を受信する 1 REP セグメントまたはセグメントのリストを識別します。有効範囲は 1 ～ 1024 です。一連のセグメント（たとえば 3-5、77、100 など）を設定することもできます。
stp	STCN を STP ネットワークに送信します。

デフォルト

他のインターフェイス、セグメント、または STP ネットワークへの STCN の送信がディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(44)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

このコマンドをセグメント エッジ ポートに入力します。

このコマンドを使用して、ローカル REP セグメントで発生しているトポロジ変更をレイヤ 2 ネットワークの他の部分に通知します。これにより、ネットワークの他部分にあるレイヤ 2 転送テーブル内の廃止エントリが削除され、より高速なネットワーク コンバージェンスが可能になります。

例

次の例では、セグメント 25 ～ 50 に STCN を送信するように REP エッジ ポートを設定する方法を示します。

```
Switch (config)# interface GigabitEthernet1/1
Switch (config-if)# rep stcn segment 25-50
Switch (config-if)# exit
```

設定を確認するには、**show interfaces rep detail** 特権 EXEC コマンドを入力します。

関連コマンド

コマンド	説明
show interfaces rep [**detail**]	すべてのインターフェイスまたは指定したインターフェイスの REP 設定およびステータスを表示します。

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がありません。

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	変更箇所
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	変更箇所
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	VLAN または VLAN セットを MST インスタンスにマッピングします。
name	MST リージョン名を設定します。
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。

sampler（netflow-lite モニタ サブモード）

netflow-lite モニタ サブモードのインターフェイスでサンプリングをアクティブにするには、**sampler** コマンドを使用します。サンプラを削除するには、このコマンドの **no** 形式を使用します。

sampler *sampler-name*

no sampler *sampler-name*

構文の説明

sampler-name	サンプラを指定します。

デフォルト

なし

コマンド モード

netflow-lite エクスポータ サブモード

コマンド履歴

リリース	変更箇所
15.0(2)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

物理ポート インターフェイス モード、ポート チャネル インターフェイス モード、または config VLAN モードでこのコマンドを入力できます。

例

次の例では、ポートのギガビット インターフェイス 1/3 のモニタを設定する方法を示します。

```
Switch# config terminal
Switch(config)# int GigabitEthernet1/3
Switch(config-if)# netflow-lite monitor 1
Switch(config-netflow-lite-monitor)# sampler sampler1
Switch(config-netflow-lite-monitor)# average-packet-size 128
Switch(config-netflow-lite-monitor)# exporter exporter1
Switch(config-netflow-lite-monitor)# exit
Switch(config-if)# exit
Switch(config)# exit
Switch# show netflow-lite monitor 1 interface gi1/3
Interface GigabitEthernet1/3:
  Netflow-lite  Monitor-1:
    Sampler:              sampler1
    Exporter:             exporter1
    Average Packet Size:  128
  Statistics:
    Packets exported:     0
    Packets observed:     0
    Packets dropped:      0
```

show netflow-lite sampler 特権 EXEC コマンドを使用して設定を確認できます。

関連コマンド

コマンド	説明
average-packet-size（netflow-lite モニタ サブモード）	観測ポイントでの平均パケット サイズを指定します。
exporter（netflow-lite モニタ サブモード）	netflow-lite モニタ サブモードのエクスポータを割り当てます。

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	変更箇所
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。

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 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）	ポリシー マップをインターフェイスに関連付けます。
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）

QoS（Quality of Service）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	変更箇所
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	完全プライオリティ キュー（低遅延キューイング（LLQ）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	変更箇所
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、システムで事前に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ないでください。

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がありません。

コマンド モード

特権 EXEC モード

コマンド履歴

リリース	変更箇所
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 スイッチには、冗長性を持たせるため、2 つのスーパーバイザ エンジンを搭載できます。スイッチに電源が入ると、スーパーバイザ エンジンの 1 つ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のままになります。もう 1 つのスーパーバイザ エンジンはスタンバイ モードのままです。

スーパーバイザ エンジンのそれぞれには、自身のコンソール ポートがあります。スタンバイ スーパーバイザ エンジンのコンソール ポート経由でだけ、スタンバイ スーパーバイザ エンジンにアクセスできます。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、モニタリング、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は、スタンバイ コンソールへの物理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るようにします。EOBC で IPC を使用してスタンバイ スーパーバイザ エンジンと通信し、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。一度にアクティブにできるアクティブ スタンバイ コンソール セッションは 1 つだけです。

スタンバイ スーパーバイザ エンジンの仮想コンソールにより、アクティブ スーパーバイザ エンジンにログインしているユーザは、スタンバイ スーパーバイザ エンジン上で show コマンドをリモートで実行し、アクティブ スーパーバイザ エンジンでその結果を表示できます。仮想コンソールは、アクティブ スーパーバイザ エンジンからだけ利用できます。

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）を開始している必要があります。

（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。

exit コマンドまたは **quit** コマンドを入力すると、仮想コンソールは終了します。ログインしたアクティブ スーパーバイザ エンジンの端末の無活動時間が設定されたアイドル時間を超えると、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します。この場合、仮想コンソール セッションも終了します。また、スタンバイが再起動すると、仮想コンソール セッションも自動的に終了します。スタンバイが起動したあとは、別の仮想コンソール セッションを作成する必要があります。

次の制限事項がスタンバイ仮想コンソールに適用されます。

- 仮想コンソールで実行されたコマンドは、すべて最後まで実行されます。auto-more 機能はありません。したがって、**terminal length 0** コマンドの実行時と同じように機能します。また、対話形式ではありません。したがって、アクティブ スーパーバイザ エンジン上でキー シーケンスを入力しても、コマンドの実行を中断できません。コマンドによって大量の出力が発生した場合、仮想コンソールはスーパーバイザ画面に出力を表示します。
- 仮想コンソールは対話形式ではありません。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ため、ユーザとの対話を必要とするコマンドが入力されると、RPC タイマーがコマンドを中断するまで仮想コンソールは待機します。
- 仮想コンソール タイマーは 60 秒に設定されています。60 秒後に仮想コンソールはプロンプトに戻ります。この間、キーボードからコマンドを中断できません。操作を続ける前に、タイマーが期限切れになるのを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。仮想コンソールは、仮想コンソールから実行されたコマンドの出力だけを表示します。実際のスタンバイ コンソールで表示される別の情報は、仮想コンソールでは表示できません。

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、次の操作を実行します。

```
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でない場合、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

パケットにサービス クラス（CoS）、DiffServ コード ポイント（DSCP）、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。一般的に使用する値に対してはニーモニック名を入力することもできます。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。一般的に使用する値に対してはニーモニック名を入力することもできます。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	変更箇所
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、コマンドラインのヘルプ ストリングを表示してください。

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 サービス クラス（CoS）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、これにより「map from」パケットマーキング カテゴリが確立されます。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	変更箇所
12.2(40)SG	Supervisor Engine 6E および Catalyst 4900M で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

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、トラフィック タイプごとに異なる 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 QoS（Quality of Service）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	タイプ オブ サービス（ToS）バイトに DiffServ コード ポイント（DSCP）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、これにより「map from」パケットマーキング カテゴリが確立されます。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。この名前には最大 64 文字までの英数字を指定できます。

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	変更箇所
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 および Catalyst 4900M で **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 QoS（Quality of Service）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。

- サービス クラス（CoS）
- 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 QoS（Quality of Service）ポリシーとしてサービス ポリシーを作成します。
set cos	サービス クラス（CoS）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「map from」パケットマーキング カテゴリを確立します。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）サービス クラス（CoS）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。この名前には最大 64 文字までの英数字を指定できます。

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	変更箇所
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 および Catalyst 4900M で **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 QoS（Quality of Service）ポリシーとしてサービス ポリシーを作成します。
set cos	サービス クラス（CoS）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	タイプ オブ サービス（ToS）バイトに DiffServ コード ポイント（DSCP）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 QoS（Quality of Service）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 QoS（Quality of Service）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	変更箇所
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 QoS（Quality of Service）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	変更箇所
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、ポリシングとは異なります。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。シェーピングでは、ポリシングよりもトラフィック処理を円滑に実行できます。

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一のポリシー マップ内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 QoS（Quality of Service）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	変更箇所
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)#
```

shell trigger

ユーザ定義トリガーを作成するには、**shell trigger** グローバル コンフィギュレーション コマンドを使用します。イベント トリガーを削除する場合は、このコマンドの **no** 形式を使用します。

shell trigger *identifier description*

no shell trigger *identifier description*

構文の説明

identifier	イベント トリガー ID を指定します。この ID を指定する場合は、文字間にスペースやハイフンを入れないでください。
description	イベント トリガーの説明文を指定します。

デフォルト

次のシステム定義のイベント トリガーが用意されています。

- CISCO_PHONE_EVENT
- CISCO_SWITCH_EVENT
- CISCO_ROUTER_EVENT
- CISCO_WIRELESS_AP_EVENT
- CISCO_WIRELESS_LIGHTWEIGHT_AP_EVENT
- DMP
- IPVSC

コマンド モード

グローバル コンフィギュレーション

コマンド履歴

リリース	変更箇所
12.2(50)SE	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

このコマンドを使用して、**macro auto execute** グローバル コンフィギュレーション コマンドで使用されるユーザ定義のイベント トリガーを作成します。

802.1X 認証を使用している場合にダイナミック デバイス検出に対応できるようにするには、Cisco 属性と値（AV）のペア **auto-smart-port=***event trigger* をサポートするように RADIUS 認証サーバを設定します。

このコマンドは、802.1X または MAB がサポートされていれば、主に 802.1X 認証に基づくトリガーに使用し、新しいプラットフォームの文字列またはデバイス ID を個々のマクロまたは関数にマッピングできるようにします。

例

次の例では、RADIUS_MAB_EVENT というユーザ定義のイベント トリガーを作成する方法を示します。

```
Switch# configure terminal
Switch(config)# shell trigger RADIUS_MAB_EVENT MAC_AuthBypass Event
Switch(config)# end
```

関連コマンド

コマンド	説明
macro auto global processing	スイッチ上で Auto Smartports をイネーブルにします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
show shell	イベント トリガーおよびマクロに関する情報を表示します。
macro auto device	あるデバイス タイプに対する組み込み関数のパラメータ変更を簡素化します。
macro auto execute（組み込み関数）	組み込み関数のデフォルト値を変更するか、ユーザ定義トリガーを組み込み関数にマッピングし、パラメータ値を渡します。
macro auto execute（ユーザ定義関数）	ユーザ定義関数にトリガーをマッピングします。
macro auto execute（リモート定義関数）	リモートで定義された関数にトリガーをマッピングします。
macro auto processing	特定のインターフェイスで Auto SmartPorts マクロをイネーブルにします。
macro auto sticky	リンク フラップとデバイス取り外しに対し ASP によって適用された設定を削除しないように指定します。