platform ip features pisa

PISA へのトラフィックをフィルタする Intelligent Traffic Redirect（ITR）機能を設定するには、インターフェイス コンフィギュレーション モードで、**platform ip features pisa** コマンドを使用します。

platform ip features pisa access-group {*ip-acl-name* | *ip-acl-number*} {**input | output**} [**reverse-only**]

シンタックスの説明

access-group *ip-acl-name*	ITR ACL の名前を指定します。
access-group *ip-acl-number*	ITR ACL の番号を指定します。範囲は、1 ～ 199 および 1300 ～ 2699 です。
input	入力トラフィックに ITR ACL を適用します。
output	出力トラフィックに ITR ACL を適用します。
reverse-only	（任意）inspect direction トラフィックにだけ ITR ACL を適用することを指定します。

コマンドのデフォルト

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（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZYA1	この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

platform ip features pisa コマンドを設定しない場合、PISA アクセラレーション機能を設定したインターフェイス上のすべてのトラフィックが PISA に送信されます。

このコマンドは、レイヤ 2 およびレイヤ 3 ポート、レイヤ 2 およびレイヤ 3 トランク、レイヤ 2 およびレイヤ 3 ポートチャネル インターフェイス、マルチ VLAN アクセス ポイント （MVAP）、レイヤ 3 サブインターフェイス、および、SVI だけに適用できます。このコマンドは他のタイプのインターフェイスに入力できません。他のタイプのインターフェイスに設定しようとすると、エラー メッセージが表示されます。

このコマンドをレイヤ 3 インターフェイスに入力すると、このパケットが PISA による双方向の送信を必要とする場合は、ソフトウェアは自動的にリバース ACL（ミラー ACL ともいう）を同一インターフェイスの反対方向にマッピングしようとします。

このコマンドをレイヤ 2 インターフェイスに入力すると、ハードウェア制限によってリバース ACL が出力方向にマップされることが防止されます。レイヤ 2 インターフェイスで、LTL コピーメカニズムがすべてのパケットをキャプチャします。

PISA アクセラレーション機能に必要な PISA アクション

機能	キーワード	入力トラフィックのアクション	出力トラフィックのアクション
NBAR Modular QoS CLI（MQC; モジュラ QoS CLI）	**input, input reverse-only**	修正	検査
	output, **output reverse-only**	検査	修正
NBAR プロトコル検出	**input, input reverse-only**	検査	検査
	output, **output reverse-only**	検査	検査
NBAR タギング	**input, input reverse-only**	なし	なし
	output, **output reverse-only**	なし	修正
フレキシブル パケット マッチング	**input, input reverse-only**	修正	なし
	output, **output reverse-only**	なし	修正
URL フィルタリング	**input, input reverse-only**	修正	修正
	output, **output reverse-only**	修正	修正

インターフェイスに PISA アクセラレーション機能が設定されている場合、ITR ACL は以下のように動作します。

- **input** : ITR ACL は PISA アクセラレーション機能に必要なアクションのために、ACL によって許可された入力（modify-direction）トラフィックを PISA へリダイレクトします。許可されない入力トラフィックは PFC3 によって処理されます。

  ITR 機能によって自動的に適用される場合は、リバース ITR ACL はリバース ACL によって許可された出力（inspect-direction）トラフィックを PISA へリダイレクトし、統計情報、保有ステート、または、その他のタイプの情報を収集します。

- **input reverse-only** : PISA アクセラレーション機能に必要なアクションのために、すべての入力（modify-direction）トラフィックは PISA へ送信されます。ITR ACL は、ACL によって許可された出力（inspect-direction）トラフィックを PISA へリダイレクトし、統計情報、保有ステート、または、その他のタイプの情報を収集します。**reverse-only** キーワードを使用して、出力（inspect-direction）トラフィックだけに対する ITR ACL を設定します。

- **output** : ITR ACL は PISA アクセラレーション機能に必要なアクションのために、ACL によって許可された出力（modify-direction）トラフィックを PISA へリダイレクトします。許可されない出力トラフィックは PFC3 によって処理されます。

  ITR 機能によって自動的に適用される場合は、リバース ITR ACL は PISA アクセラレーション機能に必要なアクションのために、リバース ACL によって許可された入力（inspect-direction）トラフィックを PISA へリダイレクトします。

- **output reverse-only** : PISA アクセラレーション機能に必要なアクションのために、すべての出力（modify-direction）トラフィックは PISA へ送信されます。ITR ACL は PISA アクセラレーション機能に必要なアクションのために、ACL によって許可された入力（inspect-direction）トラフィックを PISA へリダイレクトします。**reverse-only** キーワードを使用して、入力（inspect-direction）トラフィックだけに対して ITR ACL を設定します。

PFC QoS を適用するトラフィックを許可しないように ITR ACL を設定します。

過剰なトラフィックを PISA に送信することを避けるために、ITR が設定されている場合に、VACL キャプチャ、OAL、および、NAM および Intrusion Detection System（IDS）サービス モジュールのトラフィックなどの非 PISA キャプチャ ベース機能がイネーブルでないことを確認します。

ITR が設定されている場合、NetFlow ベースの機能（たとえば、NAT および WCCP）によって処理されるトラフィックは PISA へ送信されない場合があります。

例

次に、出力トラフィックを PISA へリダイレクトする例を示します。

```
Router(config-if)# platform ip features pisa access-group pisa_egress_redirect out
Router(config-if)#
```

関連コマンド

コマンド	説明
show platform software pisa fm interface	インターフェイス単位の Supervisor Engine 32 PISA 固有情報を表示します。
show platform pisa np	Supervisor Engine 32 PISA 固有情報を表示します。
show running-config interface	現在稼動中のコンフィギュレーション ファイルの内容を表示します。

platform ip features sequential

IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングを有効にして、入力 PFC QoS によって加えられた IP precedence または DSCP ポリシングまたはマーキングの変更を適用するには、**platform ip features sequential** 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。

platform ip features sequential [**access-group** {*ip-acl-name* | *ip-acl-number*}]

no platform ip features sequential [**access-group** {*ip-acl-name* | *ip-acl-number*}]

シンタックスの説明

access-group *ip-acl-name*	（任意）再循環パケットの一致条件を指定するために使用される ACL の名前を指定します。
access-group *ip-acl-number*	（任意）再循環パケットの一致条件を指定するために使用される ACL の番号を指定します。有効値は 1 ～ 199 と 1300 ～ 2699 です。

コマンドのデフォルト

IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングは、受信した IP precedence または DSCP 値を使用し、ポリシングまたはマーキングの結果として入力 QoS によって加えられた IP precedence または DSCP の変更を使用しません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

強化出力 QoS フィルタリングにより、IP precedence ベースまたは DSCP ベースの出力 QoS フィルタリングで入力 QoS によって加えられた IP precedence または DSCP ポリシング/マーキングの変更を使用することができます。

強化されていない出力 QoS フィルタリングの動作は、QoS がハードウェアで適用されたときの通常の Catalyst 6500 シリーズ スイッチ動作です。

PFC3 は、出力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイス）上のレイヤ 3 スイッチドおよびルーテッド トラフィックについてだけ、出力 PFC QoS を提供します。

強化出力 QoS フィルタリングは、入力レイヤ 3 インターフェイス（レイヤ 3 インターフェイスとして設定された LAN ポートまたは VLAN インターフェイス）上で設定します。

特定の標準、拡張名前付き、または拡張番号付き IP ACL によってフィルタされたトラフィックについてだけ強化出力 QoS フィルタリングをイネーブルにするには、IP ACL の名前または番号を入力します。

IP ACL の名前または番号を入力しなかった場合、強化出力 QoS フィルタリングはインターフェイス上のすべての IP 入力 IP トラフィックについてイネーブルになります。

（注）

- 強化出力 QoS フィルタリングを設定すると、PFC3 はトラフィックを処理して、入力 PFC QoS を適用します。PFC3 は入力 QoS フィルタリングと Catalyst 6500 シリーズ スイッチ ハードウェア入力 QoS を適用します。PFC3 は、入力インターフェイス上で設定される出力 QoS フィルタリングおよび Catalyst 6500 シリーズ スイッチ ハードウェア出力 QoS を誤って適用します。
- 入力 QoS マーキングによって変更された IP precedence または DSCP のマッチングを行うためにレイヤ 2 機能を使用するインターフェイス上で強化出力 QoS フィルタリングを設定した場合、パケットはリダイレクトまたは破棄されて、出力 QoS によって処理されません。
- 強化出力 QoS フィルタリングをイネーブルにした場合、再帰 ACL、NAT、TCP インターセプトなどの NetFlow ベース機能のハードウェア アクセラレーションはディセーブルになります。

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

例

次に、強化出力 QoS フィルタリングをイネーブルにする例を示します。

```
Router(config-if)# platform ip features sequential
Router(config-if)#
```

次に、強化出力 QoS フィルタリングをディセーブルにする例を示します。

```
Router(config-if)# no platform ip features sequential
Router(config-if)#
```

関連コマンド

コマンド	説明
show running-config interface	現在稼動中のコンフィギュレーション ファイルの内容を表示します。

platform ipv6 acl icmp optimize neighbor-discovery

IPv6 ACL の TCAM サポートを最適化するには、**platform ipv6 acl icmp optimize neighbor-discovery** コマンドを使用します。IPv6 ACL の TCAM サポートの最適化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。

platform ipv6 acl icmp optimize neighbor-discovery

no platform ipv6 acl icmp optimize neighbor-discovery

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

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（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

（注）　Cisco TAC の指導を受けた場合にだけ、このコマンドを使用してください。

IPv6 ACL の TCAM サポートの最適化をイネーブルにすると、TCAM の上部にあるグローバル ICMPv6 neighbor-discovery ACL はすべての ICMP v 6 ネイバ検出パケットを許可するようにプログラムされます。最適化のイネーブル化によって、すべての IP v 6 セキュリティ ACL の末尾への ICMP v 6 ACE の追加が行われなくなり、使用される TCAM リソースの数が削減されます。このコマンドをイネーブルにすると、すべてのインターフェイス上の IP v 6 ACL が再プログラムされます。

（注）　TCAM 上部の ICMPv6 neighbor-discovery ACL は、設定した ICMP ネイバ検出パケットについてセキュリティ ACL に優先しますが、グローバル ICMP ACL と重複する bridge/deny があった場合は無効です。

例

次に、IP v 6 ACL の TCAM サポートを最適化する例を示します。

```
Router(config)# platform ipv6 acl icmp optimize neighbor-discovery
Router(config)#
```

次に、IP v 6 ACL の TCAM サポートの最適化をディセーブルにする例を示します。

```
Router(config)# no platform ipv6 acl icmp optimize neighbor-discovery
Router(config)#
```

platform scp retry interval

SCP の高速リトライをイネーブルにして、高速リトライのインターバルを設定するには、**platform scp retry interval** コマンドを使用します。SCP の高速リトライ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。

platform scp retry interval *timeout-value*

no platform scp retry interval

シンタックスの説明

timeout-value	高速リトライのインターバル。有効値は、200 ～ 2000 ミリ秒です。

コマンドのデフォルト

2000 ミリ秒

コマンド モード

グローバル コンフィギュレーション（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

（注） Cisco TAC の指導を受けた場合にだけ、このコマンドを使用してください。

例

次に、SCP 高速リトライをイネーブルにして、高速リトライのインターバルを設定する例を示します。

```
Router(config)# platform scp retry interval 600
Router(config)#
```

platform vfi dot1q-transparency

802.1Q 透過性モードをイネーブルにするには、**platform vfi dot1q-transparency** コマンドを使用します。802.1Q 透過性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。

platform vfi dot1q-transparency

no platform vfi dot1q-transparency

シンタックスの説明　このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト　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（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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　このコマンドをサポートするのは、OSM モジュールだけです。

802.1Q 透過性により、サービス プロバイダーは、VPLS カスタマーの 802.1p ビットには変更を加えずに、コアベースの QoS ポリシーの MPLS EXP ビットを変更できるようになりました。

EoMPLS の dot1q 透過性機能では、VLAN に適用されたポリシーが Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）ラベル（コア QoS 用）にだけ影響し、VC ラベル EXP ビットと 802.1p ビットを同じにします。一方出力 PE では、802.1p ビットは受信した VC EXP ビットに基づいて書き換えられますが、EXP ビットは入力 802.1p ビットに一致しているため、VPLS カスタマーの 802.1p ビットは変更されません。

グローバル コンフィギュレーション（config）は、Cisco 7600 シリーズ ルータに設定されたすべての Virtual Forwarding Instance（VFI）およびスイッチ仮想インターフェイス（SVI）の EoMPLS VC に適用されます。

インターオペラビリティを実現するには、接続されているすべての PE ルータに EoMPLS の Dot1q 透過性を適用する必要があります。

例　次に、802.1Q 透過性をイネーブルにする例を示します。

```
Router (config)# platform vfi dot1q-transparency
Router (config)#
```

次に、802.1Q 透過性をディセーブルにする例を示します。

```
Router (config)# no platform vfi dot1q-transparency
Router (config)#
```

police (policy map)

インターフェイス単位のポリサーを作成して、それを使用するようにポリシーマップ クラスを設定するには、**police** コマンドを使用します。ポリシーマップ クラスからインターフェイス単位のポリサーを削除するには、このコマンドの **no** 形式を使用します。

police {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

no police {*bits-per-second* [*normal-burst-bytes*] [*extended-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

シンタックスの説明

bits-per-second	CIR ビット/秒。有効値は、32,000 bps ～ 2 Gbps です。
normal-burst-bytes	（任意）CIR トークン バケット サイズ。有効値は 1000 ～ 512,000,000 バイトです。
maximum-burst-bytes	（任意）PIR トークン バケット サイズ。有効値は 1000 ～ 32,000,000 バイトです。
pir ***peak-rate-bps***	（任意）PIR ピーク レートを設定します。有効値は 32,000 bps ～ 2 Gbps です。
conform-action *action*	（任意）*bits-per-second* レートを超えなかった場合に行うアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。
exceed-action *action*	（任意）*bits-per-second* レートを超えた場合に行うアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。
violate-action *action*	（任意）*bits-per-second* レートが *maximum-burst-bytes* レートより大きいときに行うアクションを指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *maximum-burst-bytes* は *normal-burst-bytes* と同じです。
- **conform-action** は **transmit** です。
- **exceed-action** は **drop** です。
- **violate-action** は、**exceed-action** と同じです。
- **pir** ***peak-rate-bps*** は、*normal-burst-bytes* レートと同じです。

コマンド モード

policy-map サブコマンド

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

Supervisor Engine 32 PISA では、ソフトウェアで **police** コマンドがサポートされています。

名前付き集約ポリサーとマイクロフロー ポリサーは、Supervisor Engine 32 PISA ではサポートされていません。

normal-burst-bytes 引数は、CIR トークン バケット サイズを設定します。

maximum-burst-bytes 引数は、PIR トークン バケット サイズを設定します（**flow** キーワードとの併用はサポートされません）。*maximum-burst-bytes* 引数は、*normal-burst-bytes* 設定と同じになるように設定する必要があります。

pir *peak-rate-bps* は、*extended-burst-bytes* に対応します。

action の有効値は次のとおりです。

- **drop**：*bits-per-second* レートを超えないパケットを廃棄します。
- **policed-dscp-transmit**：すべての不適合トラフィックに、マークダウン マップで指定されているとおりマーキングします。
- **set-dscp-transmit** {*dscp-value* | *dscp-bit-pattern* | **default** | **ef**}：一致したトラフィックを新しい DSCP 値でマークします。有効値は次のとおりです。
  - *dscp-value*：DSCP 値を指定します。有効値は 0 ～ 63 です。
  - *dscp-bit-pattern*：DSCP ビット パターンを指定します。有効値は表 2-28 に列挙されています。
  - **default**：パケットとデフォルトの dscp（000000）とのマッチングを行います。
  - **ef**：パケットと EF dscp（101110）とのマッチングを行います。

表 2-28　有効な dscp-bit-pattern 値

キーワード	定義
af11	パケットと AF11 dscp（001010）とのマッチングを行います。
af12	パケットと AF12 dscp（001100）とのマッチングを行います。
af13	パケットと AF13 dscp（001110）とのマッチングを行います。
af21	パケットと AF21 dscp（010010）とのマッチングを行います。
af22	パケットと AF22 dscp（010100）とのマッチングを行います。
af23	パケットと AF23 dscp（010110）とのマッチングを行います。
af31	パケットと AF31 dscp（011010）とのマッチングを行います。
af32	パケットと AF32 dscp（011100）とのマッチングを行います。
af33	パケットと AF33 dscp（011110）とのマッチングを行います。
af41	パケットと AF41 dscp（100010）とのマッチングを行います。
af42	パケットと AF42 dscp（100100）とのマッチングを行います。
af43	パケットと AF43 dscp（100110）とのマッチングを行います。
cs1	パケットと CS1（precedence 1）dscp（001000）とのマッチングを行います。
cs2	パケットと CS2（precedence 2）dscp（010000）とのマッチングを行います。
cs3	パケットと CS3（precedence 3）dscp（011000）とのマッチングを行います。

表 2-28　有効な dscp-bit-pattern 値

キーワード	定義
cs4	パケットと CS4（precedence 4）dscp（100000）とのマッチングを行います。
cs5	パケットと CS5（precedence 5）dscp（101000）とのマッチングを行います。
cs6	パケットと CS6（precedence 6）dscp（110000）とのマッチングを行います。
cs7	パケットと CS7（precedence 7）dscp（111000）とのマッチングを行います。

- **set-mpls-exp-imposition-transmit** *new-mpls-exp*：インポーズされたラベル エントリの MPLS EXP ビットを書き換えて送信します。*new-mpls-exp* 引数は、ポリシー マップによって定義される MPLS EXP ビットを設定するために使用される値を指定します。*new-mpls-exp* の有効値は 0 ～ 7 です。
- **set-mpls-exp-topmost-transmit**：最上部のラベル エントリの MPLS EXP ビットを書き換えて、送信します。*new-mpls-exp* 引数は、ポリシー マップによって定義される MPLS EXP ビットを設定するために使用される値を指定します。*new-mpls-exp* の有効値は 0 ～ 7 です。
- **set-prec-transmit** *new-precedence*：一致したトラフィックを新しい IP precedence 値でマークして送信します。*new-precedence* の有効値は 0 ～ 7 です。
- **transmit**：*bits-per-second* レートを超えないパケットを送信します。

例

次に、ipp5 という名前のクラス マップを使用するポリシー マップ max-pol-ipp5 を作成する例を示します。この例では、受信した IP precedence 値を信頼するように設定し、最大容量に関する集約ポリサーを設定します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)#
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
service-policy	インターフェイスにポリシー マップを対応付けます。
show class-map	クラス マップ情報を表示します。
show policy-map	ポリシー マップに関する情報を表示します。
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 rate

コントロール プレーン宛のトラフィックのトラフィック ポリシングを設定するには、**police rate** コマンドを使用します。設定からトラフィック 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 rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

no police rate *units* **pps** [**burst** *burst-in-packets* **packets**] [**peak-rate** *peak-rate-in-pps* **pps**] [**peak-burst** *peak-burst-in-packets* **packets**]

no police rate *units* **bps** [**burst** *burst-in-bytes* **bytes**] [**peak-rate** *peak-rate-in-bps* **bps**] [**peak-burst** *peak-burst-in-bytes* **bytes**]

no police rate percent *percentage* [**burst** *ms* **ms**] [**peak-rate percent** *percentage*] [**peak-burst** *ms* **ms**]

シンタックスの説明

units	ポリス レート。有効値については、「使用上のガイドライン」を参照してください。
pps	トラフィックを規制するレートをパケット/秒で指定します。
burst *burst-in-packets* **packets**	（任意）トラフィックのポリシングに使用されるバースト レートを指定します。有効値は 1 ～ 512000 パケットです。
peak-rate *peak-rate-in-pps* **pps**	（任意）トラフィックのポリシングに使用される PIR を指定します。有効値は 1 ～ 512,000 パケットです。
peak-burst *peak-burst-in-packets* **packets**	（任意）トラフィックのポリシングに使用されるピーク バースト値を指定します。有効値は 1 ～ 512,000 パケットです。
bps	トラフィックを規制するレートをビット/秒 で指定します。
burst *burst-in-bytes* **bytes**	（任意）トラフィックのポリシングに使用されるバースト レートを指定します。有効値は 1000 ～ 512,000,000 ビットです。
peak-rate *peak-rate-in-bps* **bps**	（任意）ピーク レートとして使用されるピーク バースト値を指定します。有効値は 1000 ～ 512,000,000 ビットです。
peak-burst *peak-burst-in-bytes* **bytes**	（任意）トラフィックのポリシングに使用されるピーク バースト値を指定します。有効値は 1000 ～ 512,000,000 ビットです。
percent *percentage*	（任意）トラフィックを規制するレートを決めるために使用されるインターフェイス帯域幅のパーセントを指定します。有効値は 1 ～ 100 です。
burst *ms* **ms**	（任意）トラフィックのポリシングに使用されるバースト レートを指定します。有効値は 1 ～ 2000 ミリ秒です。

peak-rate percent *percentage*	（任意）PIR を決めるために使用されるインターフェイス帯域幅のパーセントを指定します。有効値は 1 ～ 100 です。
peak-burst *ms* **ms**	（任意）トラフィックのポリシングに使用されるピーク バースト レートを指定します。有効値は 1 ～ 2000 ミリ秒です。

コマンドのデフォルト

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

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

units の有効値は次のとおりです。

- ポリス レートを pps で指定する場合、有効値は 1 ～ 2,000,000 pps です。
- ポリス レートを bps で指定する場合、有効値は 8000 ～ 10,000,000,000 bps です。

pps は、PIR *peak-rate-in-pps* を計算するために使用されます。

コントロール プレーン宛のトラフィックをパケット/秒（pps）、バイト/秒（bps）、またはインターフェイス帯域幅のパーセントで制限するには、**police rate** コマンドを使用します。

police rate コマンドを入力して、レートを指定しなかった場合、コントロール プレーン宛のトラフィックは bps 単位で規制されます。

例

次に、クラスのポリシングを設定して、トラフィックを平均レート 1,500,000 pps に制限する例を示します。

```
Router(config)# class-map telnet-class
Router(config-cmap)# match access-group 140
Router(config-cmap)# exit
Router(config)# policy-map control-plane-policy
Router(config-pmap)# class telnet-class
Router(config-pmap-c)# police rate 1500000 pps bc 500000 packets
Router(config-pmap-c)# exit
```

関連コマンド

コマンド	説明
policy-map	QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスします。
show policy-map	ポリシー マップに関する情報を表示します。

policy-map

QoS ポリシー マップを設定するための QoS ポリシー マップ コンフィギュレーション モードにアクセスするには、**policy-map** コマンドを使用します。ポリシー マップを削除するには、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*

シンタックスの説明

policy-map-name	ポリシー マップ名。**policy-map** サブコマンドの説明については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *extended-burst-bytes* は *burst-bytes* と同じです。
- **conform-action** は transmit です。
- **exceed-action** は drop です。
- **violate-action** は、**exceed-action** と同じです。
- **pir** ***peak-rate-bps*** は標準の（**cir**）レートと同じです。

コマンド モード

グローバル コンフィギュレーション（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

QoS ポリシー マップ コンフィギュレーション モードでは、次のコンフィギュレーション コマンドが利用できます。

- **exit**：QoS クラス マップ コンフィギュレーション モードを終了します。
- **no**：定義済みポリシー マップを削除します。
- **class** *class-map* [*name*]：QoS クラス マップ コンフィギュレーション モードにアクセスして、以前に作成したクラス マップがポリシー マップに含まれるよう指定したり、クラス マップを作成したりします（詳細については、**class-map** コマンドを参照してください）。
- **class** {*class-name* | **class-default**} は、クラス コンフィギュレーション モードにアクセスして、作成または変更するポリシーのクラス名を指定します（詳細については、**class (policy-map)** コマンドを参照してください）。
- **police** [**aggregate** *name*] サブコマンド：マイクロフローまたは集約ポリサーを定義します（詳細については、**police (policy map)** コマンドを参照してください）。構文は次のとおりです。
  - **police** {**aggregate** *name*}
  - **police flow** {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*] [**pir** *peak-rate-bps*]} | [**conform-action** *action*] [**exceed-action** *action*] [**violate-action** *action*]

  - **police flow mask** {**dest-only** | **full-flow** | **src-only**} {*bits-per-second* [*normal-burst-bytes*] [*maximum-burst-bytes*]} [**conform-action** *action*] [**exceed-action** *action*]

- **trust** {**cos** | **dscp** | **ip-precedence**}：指定されたクラス信頼値を設定します。このコマンドで設定された信頼値は、特定のインターフェイス上で設定された信頼値よりも優先します。

表 2-29 に、**class** の構文を示します。

表 2-29　class の構文

サブコマンド	説明
exit	（任意）QoS クラス アクション コンフィギュレーション モードを終了します。
police	（任意）フロー ポリシングを指定します。詳細については、**police (policy map)** コマンドを参照してください。
trust *state*	（任意）ポリシー マップ クラスの信頼状態を設定します。信頼状態は **cos**、**dscp**、および **ip precedence** です。
cos	（任意）受信した CoS またはインターフェイスの CoS から、内部 DSCP 値を設定します。
dscp	（任意）受信した DSCP 値を使用するように QoS を設定します。
ip-precedence	（任意）受信した IP precedence から、DSCP 値を設定します。

policy-map で **exceed-action** を指定しなかった場合は、デフォルトの drop に設定され、violate-action が続きます。

ポリシー マップ クラスでは、PFC QoS は **bandwidth**、**priority**、**queue-limit**、**random-detect**、または **set** キーワードをサポートしません。

例

次に、設定済みのクラスマップ **ipp5** を使用するポリシー マップ **max-pol-ipp5** を作成する例、および信頼状態を受信された IP precedence 値に設定し、最大容量に関する集約ポリサーおよびマイクロフロー ポリサーを設定する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# policy-map max-pol-ipp5
Router(config-pmap)# class ipp5
Router(config-pmap-c)# trust ip-precedence
Router(config-pmap-c)# police 2000000000 2000000 8000000 conform-action set-prec-transmit
6 exceed-action policed-dscp-transmit
Router(config-pmap-c)# police flow 10000000 10000 conform-action set-prec-transmit 6
exceed-action policed-dscp-transmit
Router(config-pmap-c)# end
Router#
```

関連コマンド

コマンド	説明
class-map	QoS クラス マップを設定するための QoS クラス マップ コンフィギュレーション モードにアクセスします。
class (policy-map)	ポリシーを設定する前に、作成または変更するポリシーを持つクラス名を指定するか、デフォルトのクラス（一般に class-default クラスの呼び名で知られている）を指定します。
service-policy	インターフェイスにポリシー マップを対応付けます。

コマンド	説明
show class-map	クラス マップ情報を表示します。
show policy-map	ポリシー マップに関する情報を表示します。
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。

port access-map

ポート アクセス マップを作成するか、またはポート アクセス マップ コマンド モードを開始するには、**port access-map** コマンドを使用します。マッピング シーケンスまたはマップ全体を削除するには、このコマンドの **no** 形式を使用します。

port access-map *name* [*seq#*]

no port access-map *name* [*seq#*]

シンタックスの説明

name	ポート アクセスマップのタグです。
seq#	（任意）マップ シーケンス番号。有効値は 0 ～ 65,535 です。

コマンドのデフォルト

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（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

既存のマップ シーケンスのシーケンス番号を入力すると、ポート アクセスマップ モードが開始します。シーケンス番号を指定しないと、番号が自動的に割り当てられます。各マップ シーケンスには、match 句および action 句をそれぞれ 1 つずつ指定できます。

シーケンス番号を指定しないで **no port access-map name** [*seq#*] コマンドを入力すると、マップ全体が削除されます。

ポート アクセスマップ モードを開始すると、次のコマンドが使用可能になります。

- **action**：パケットの action 句を指定します。**action** コマンドを参照してください。
- **default**：コマンドをデフォルトに設定します。
- **end**：コンフィギュレーション モードを終了します。
- **exit**：ポート アクセスマップ コンフィギュレーション モードを終了します。
- **match**：match 句を指定します。**match** コマンドを参照してください。
- **no**：コマンドを否定するか、またはデフォルトを設定します。

例

次に、ポート アクセスマップ モードを開始する例を示します。

```
Router(config)# port access-map ted
Router(config-port-map)#
```

関連コマンド

コマンド	説明
action	パケットの action 句を設定します。
match	VLAN アクセス マップ シーケンスの ACL を 1 つまたは複数選択して、match 句を指定します。

port-channel load-balance

バンドル内のポートの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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance *method*

no port-channel load-balance

シンタックスの説明

method	負荷分散方式。有効値の一覧については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

method は **src-dst-ip** 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（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

有効な *method* 値は次のとおりです。

- **dst-ip**：宛先 IP アドレス方式での負荷分散
- **dst-mac**：宛先 MAC アドレス方式での負荷分散
- **dst-port**：宛先ポート方式での負荷分散
- **src-dst-ip**：送信元 XOR 宛先 IP アドレス方式での負荷分散
- **src-dst-mac**：送信元 XOR 宛先 MAC アドレス方式での負荷分散
- **src-dst-port**：送信元 XOR 宛先ポート方式での負荷分散
- **src-ip**：送信元 IP アドレス方式での負荷分散
- **src-mac**：送信元 MAC アドレス方式での負荷分散
- **src-port**：送信元ポート方式での負荷分散

port-channel per-module load-balance コマンドを使用すると、モジュール単位でポート チャネル ロードバランスをイネーブルまたはディセーブルにできます。

次に負荷分散方式を **dst-ip** に設定する例を示します。

```
Router(config)# port-channel load-balance dst-ip
Router(config)#
```

次に特定のモジュールの負荷分散方式を設定する例を示します。

```
Router(config)# port-channel load-balance dst-ip module 2
Router(config)#
```

関連コマンド

コマンド	説明
interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
port-channel per-module load-balance	モジュール単位で負荷分散をイネーブルにします。
show etherchannel	チャネルの EtherChannel 情報を表示します。

port-channel load-balance mpls

MPLS パケットに関してバンドル内のポートの負荷分散方式を設定するには、**port-channel load-balance mpls** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel load-balance mpls {**label** | **label-ip**}

no port-channel load-balance mpls

シンタックスの説明

label	パケットを分散するための MPLS ラベルの使用を指定します。詳細については、「使用上のガイドライン」を参照してください。
label-ip	パケットを分散するための MPLS ラベルまたは IP アドレスの使用を指定します。詳細については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

label-ip

コマンド モード

グローバル コンフィギュレーション（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

label を選択する場合、次の点に注意してください。

- MPLS ラベルが 1 つだけの場合、最後の MPLS ラベルが使用されます。
- MPLS ラベルが 2 つ以上ある場合、最後の 2 つの MPLS ラベル（ 5 つめのラベルまで）が使用されます。

label-ip を選択する場合、次の点に注意してください。

- IPv4 でラベルが 3 つ以下の場合、送信元 XOA または宛先 IP アドレスがパケットの分散に使用されます。
- MPLS ラベルが 4 つ以上ある場合、最後の 2 つの MPLS ラベル（5 つめのラベルまで）が使用されます。
- 非 IPv4 パケットの場合、負荷分散方式は **label** 方式と同じです。

例

次に、負荷分散方式を **label-ip** に設定する例を示します。

```
Router(config)# port-channel load-balance mpls label-ip
Router(config)#
```

関連コマンド

コマンド	説明
interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
show etherchannel	チャネルの EtherChannel 情報を表示します。

port-channel min-links

チャネルをアクティブにする前に、EtherChannel にバンドルされていなければならないポートの最小数を指定するには、**port-channel min-links** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel min-links *min-num*

no port-channel min-links

シンタックスの説明

min-num	チャネルをアクティブにする前に、チャネルにバンドルしなければならないポートの最小数。有効値は 2 ～ 8 です。

コマンドのデフォルト

min-num は **1** です。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

このコマンドは、LACP（802.3ad）ポートだけでサポートされます。複数の LACP セカンダリポート チャネルを同一のチャネル グループに含めることができます。このコマンドは、同一グループのすべてのポート チャネルに適用されます。

使用可能なリンクが指定された数より少ない場合、ポート チャネル インターフェイスがアクティブになりません。

show running-config コマンドを使用して、設定を確認します。

例

次に、チャネルをアクティブにする前に、EtherChannel にバンドルしなければならないポートの最小数を指定する例を示します。

```
Router(config-if)# port-channel min-links 3
Router(config-if)#
```

関連コマンド

コマンド	説明
show running-config	モジュールまたはレイヤ 2 VLAN のステータスおよび設定を表示します。

port-channel per-module load-balance

モジュール単位で負荷分散をイネーブルにするには、**port-channel per-module load-balance** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

port-channel per-module load-balance

no port-channel per-module load-balance

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

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（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

port-channel load-balance *method* **module** *slot* コマンドは、DFC システムだけでサポートされています。

port-channel per-module load-balance コマンドを使用すると、モジュール単位でポート チャネル ロードバランスをイネーブルまたはディセーブルにできます。**port-channel per-module load-balance** コマンドを入力したあとに **port-channel load-balance** *method* **module** *slot* コマンドを入力して、特定のモジュールのロードバランス方式を指定できます。

例

次に、モジュール単位でロード バランスをイネーブルにする例を示します。

```
Router(config)# port-channel per-module load-balance
Router(config)#
```

関連コマンド

コマンド	説明
interface port-channel	ポート チャネル仮想インターフェイスを作成し、インターフェイス コンフィギュレーション モードを開始します。
port-channel load-balance module	特定のモジュールで負荷分散をイネーブルにします。
show etherchannel	チャネルの EtherChannel 情報を表示します。

power enable

モジュールに電源を投入するには、**power enable** コマンドを使用します。モジュールの電源を切断するには、このコマンドの **no** 形式を使用します。

power enable {**module** *slot*}

no power enable {**module** *slot*}

シンタックスの説明

module *slot*	モジュールのスロット番号を指定します。有効値については、「使用上のガイドライン」を参照してください。

コマンドのデフォルト

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（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

no power enable module *slot* コマンドを入力してモジュールの電源を切断した場合、そのモジュールの設定は保存されません。

no power enable module *slot* コマンドを入力して空のスロットの電源を切断した場合、その設定は保存されます。

slot 引数はモジュール番号を指定します。*slot* 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、13 スロット シャーシを使用している場合、モジュール番号の有効値は 1 ～ 13 です。

例

次に、電源が切断されているモジュールに電源を投入する例を示します。

```
Router(config)# power enable module 5
Router(config)#
```

次に、モジュールの電源を切断する例を示します。

```
Router(config)# no power enable module 5
Router(config)#
```

関連コマンド

コマンド	説明
show power	パワー ステータスに関する情報を表示します。

power inline

インターフェイスのインライン パワーの管理モードを設定するには、**power inline** コマンドを使用します。

power inline {**auto** [**max** *max-milliwatts*]} | **never** | {**static** [**max** *max-milliwatts*]}

シンタックスの説明

auto	デバイス検出プロトコルをオンにして、検出されたデバイスに電力を供給します。
max *max-milliwatts*	（任意）ポートに接続されているデバイスが消費できる最大電力量を指定します。有効値は、4000 ～ 16800 ミリワットです。
never	デバイス検出プロトコルをオフにして、デバイスへの電力供給を停止します。
static	システムの電力プールからポートに電力を割り当てます。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- **auto**
- *max-milli-watts* は、15,400 ミリワットです。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。
12.2(18)ZYA	このコマンドは、*max-milliwatts* が 15400 から 16800 へ変更されました。

使用上のガイドライン

power inline コマンドを使用してインライン パワー サポートを設定する場合、次の点に注意してください。

- インライン パワー デバイスの自動検出およびポート インライン パワーの自動割り当てを設定するには、**auto** キーワードを入力します。
- インライン パワー デバイスの自動検出を設定し、固定インライン パワー割り当てを維持するには、**static** キーワードを入力します。
- ポートに割り当てる最大電力を指定するには、**auto** または **static** キーワードのいずれかを入力し、そのあとに **max** キーワードおよび電力レベル（ミリワット）を入力します。
- **auto** キーワードが入力され、ポート上で CDP がイネーブルである場合、CDP をサポートするインライン パワー デバイスは、異なる電力レベルをネゴシエーションできます。
- インライン パワー デバイスの自動検出をディセーブルにするには、**never** キーワードを入力します。

例

次に、インターフェイスのインライン パワーをオフ モードに設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline never
```

次に、システムの電力プールからポートに電力を割り当てる例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# switchport
Router(config-if)# power inline static max 15000
```

関連コマンド

コマンド	説明
show power	パワー ステータスに関する情報を表示します。

power redundancy-mode

電源装置の冗長モードを設定するには、**power redundancy-mode** コマンドを使用します。

power redundancy-mode {**combined** | **redundant**}

シンタックスの説明

combined	非冗長モードを指定します（電源装置の出力が合計されます）。
redundant	冗長モードを指定します（いずれかの電源装置でシステムを稼動できます）。

コマンドのデフォルト

redundant

コマンド モード

グローバル コンフィギュレーション（config）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	このコマンドのサポートが追加されました。

例

次に、電源装置を非冗長モードに設定する例を示します。

```
Router(config)# power redundancy-mode combined
Router(config)#
```

次に、電源装置を冗長モードに設定する例を示します。

```
Router(config)# power redundancy-mode redundant
Router(config)#
```

関連コマンド

コマンド	説明
show power	パワー ステータスに関する情報を表示します。

priority-queue cos-map

受信および送信完全優先キューに CoS 値をマッピングするには、**priority-queue cos-map** コマンドを使用します。デフォルト マッピングに戻すには、このコマンドの **no** 形式を使用します。

priority-queue cos-map *queue-id cos1* [*cos2* [*cos3* [*cos4* [*cos5* [*cos6* [*cos7* [*cos8*]]]]]]]

シンタックスの説明

queue-id	キュー番号。有効値は **1** です。
cos1	CoS 値。有効値は 0 ～ 7 です。
...cos8	（任意）CoS 値。有効値は、0 ～ 7 です。

コマンドのデフォルト

デフォルト マッピングはキュー 1 で、次の受信および送信完全優先キューで CoS 5 にマッピングされます。

- 1p1q4t 受信キュー
- 1p1q0t 受信キュー
- 1p1q8t 受信キュー
- 1p2q2t 送信キュー
- 1p3q8t 送信キュー
- 1p7q8t 送信キュー
- 1p3q1t 送信キュー
- 1p2q1t 送信キュー

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

完全優先キューに CoS 値をマッピングする場合、次の点に注意してください。

- キュー番号は、常に **1** です。
- キューにマッピングする、最大 8 つの CoS 値を入力できます。

例

次に、ギガビット イーサネット ポート 1/1 の完全優先キューに、CoS 値 7 をマッピングする例を示します。

```
Router(config-if)# priority-queue cos-map 1 7
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

priority-queue queue-limit

インターフェイス上にプライオリティ キュー サイズを設定するには、**priority-queue queue-limit** コマンドを使用します。

priority-queue queue-limit *weight*

シンタックスの説明

weight	プライオリティ キュー サイズの重み。有効値は、1 ～ 100% です。

コマンドのデフォルト

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：15
- グローバル QoS がディセーブルの場合：0

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

このコマンドをサポートするモジュールのリストについては、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*』*Release 12.2ZY*を参照してください。

例

次に、プライオリティ キューに使用可能なバッファ スペースを割り当てる例を示します。

```
Router(config-if)# priority-queue queue-limit 15
Router(config-if)#
```

関連コマンド

コマンド	説明
show queueing interface	キューイング情報を表示します。

private-vlan

PVLAN、および PVLAN とセカンダリ VLAN 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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

private-vlan {**isolated** | **community** | **primary**}

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

no private-vlan {**isolated** | **community** | **primary**}

no private-vlan association

シンタックスの説明

isolated	VLAN を隔離 PVLAN として指定します。
community	VLAN をコミュニティ PVLAN として指定します。
primary	VLAN をプライマリ PVLAN として指定します。
association	セカンダリ VLAN とプライマリ VLAN とのアソシエーションを作成します。
secondary-vlan-list	セカンダリ VLAN の番号
add	セカンダリ VLAN をプライマリ VLAN に対応付けます。
remove	セカンダリ VLAN とプライマリ VLAN とのアソシエーションをクリアします。

コマンドのデフォルト

PVLAN は設定されていません。

コマンド モード

config-VLAN サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

PVLAN をポート セキュリティ ポートには設定できません。

ポートセキュリティが設定されたポートで **pvlan** コマンドを入力すると、次のエラー メッセージが表示されます。

```
Command rejected: Gix/y is Port Security enabled port.
```

12 個のポートからなるグループ（1 ～ 12、13 ～ 24、25 ～ 36、および 37 ～ 48）内のポートの 1 つがトランクや SPAN の宛先、または混合モード プライベート VLAN ポートの場合は、ポートを隔離 VLAN ポートまたはコミュニティ VLAN ポートとして設定しないでください。1 つのポートがトランクや SPAN の宛先、または混合モード プライベート VLAN ポートの場合は、12 ポート中の他のポートの隔離 VLAN またはコミュニティ VLAN 設定は非アクティブになります。ポートを再度アクティブにするには、隔離 VLAN またはコミュニティ VLAN のポート設定を削除し、**shutdown** および **no shutdown** コマンドを入力します。

注意　PVLAN（プライマリまたはセカンダリ）上の config-vlan モードで **shutdown** コマンドを入力して、次に **no shutdown** コマンドを入力すると、PVLAN タイプおよびアソシエーション情報が削除されます。VLAN が PVLAN になるよう再設定する必要があります。

（注）　この制限事項は WS-X6548-RJ-45 および WS-X6548-RJ-21 を除くイーサネット 10-Mb、10/100-Mb、および 100-Mb モジュールに適用されます。

VLAN 1 または VLAN 1001 ～ 1005 を PVLAN として設定することはできません。

VTP は PVLAN をサポートしません。PVLAN ポートを使用するデバイスごとに、PVLAN を設定する必要があります。

secondary-vlan-list 引数には、スペースを挿入できません。複数のカンマ区切り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 PVLAN ID のハイフンで連結した範囲です。*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 引数には、1 つの隔離 VLAN ID だけを含めることができます。PVLAN 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 ポートのセットです。各ペアは、少なくとも 2 つの特別単一方向 VLAN で構成され、ルータと通信するために隔離ポートとポートのコミュニティの一方または両方によって使用されます。

隔離 VLAN は、混合モード ポートと通信するために隔離ポートによって使用される VLAN です。隔離 VLAN のトラフィックは、同じ VLAN 内のその他のすべてのプライベート ポート上でブロックされます。このトラフィックを受信できるのは、対応するプライマリ VLAN に割り当てられた標準トランキング ポートおよび混合モード ポートだけです。

混合モード ポートは、プライマリ VLAN に割り当てられたプライベート ポートとして定義されます。

プライマリ VLAN は、トラフィックをルータからプライベート 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 として定義されます。

コミュニティ VLAN は、コミュニティ ポート間で、およびコミュニティ ポートから対応するプライマリ VLAN 上の混合モード ポートに、トラフィックを伝送する VLAN として定義されます。

複数のコミュニティ VLAN が許可される場合、隔離された *vlan-id* は 1 つだけ指定できます。隔離 VLAN およびコミュニティ VLAN は、1 つの VLAN にだけ対応付けることができます。対応付けられた 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 に対応付けられた VLAN は、プライマリ VLAN として設定できません。

コンフィギュレーション VLAN サブモードを終了しないと、**private-vlan** コマンドは有効になりません。

プライマリまたはセカンダリ VLAN を削除する場合、VLAN と対応付けられるポートは非アクティブとなります。

設定に関する注意事項については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide*、*Release 12.2ZY*』を参照してください。

例

次に、プライマリ VLAN 14、隔離 VLAN 19、およびコミュニティ VLAN 20 ～ 21 間の PVLAN 関係を作成する例を示します。

```
Router(config) # vlan 19
Router(config-vlan) # private-vlan isolated
Router(config) # vlan 20
Router(config-vlan) # private-vlan community
Router(config-vlan) # private-vlan community
Router(config) # vlan 14
Router(config-vlan) # private-vlan primary
Router(config-vlan) # private-vlan association 19-21
```

次に、隔離 VLAN およびコミュニティ VLAN 20 を PVLAN アソシエーションから削除する例を示します。

```
Router(config) # vlan 14
Router(config-vlan) # private-vlan association remove 18,20
Router(config-vlan) #
```

次に、PVLAN 関係を削除し、プライマリ VLAN を削除する例を示します。対応付けられたセカンダリ VLAN は削除されません。

```
Router(config-vlan) # no private-vlan 14
Router(config-vlan) #
```

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	PVLAN 情報を表示します。

private-vlan mapping

プライマリ VLAN とセカンダリ VLAN のマッピングを作成して、両方の VLAN で同じプライマリ VLAN SVI を共有できるようにするには、**private-vlan mapping** コマンドを使用します。SVI からすべての PVLAN マッピングを削除するには、このコマンドの **no** 形式を使用します。

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

no private-vlan mapping

シンタックスの説明

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
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 との間のマッピングを削除します。

コマンドのデフォルト

PVLAN SVI マッピングは設定されていません。

コマンド モード

インターフェイス コンフィギュレーション（config-if）

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

private-vlan mapping コマンドは、PISA 上のソフトウェアでスイッチングされるトラフィックに影響します。

secondary-vlan-list 引数にはスペースを挿入できません。複数のカンマ区切り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 PVLAN ID のハイフンで連結した範囲です。

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 にだけマッピングできます。プライマリ VLAN をセカンダリ VLAN として設定した場合、このコマンドで指定されたすべての SVI はダウン状態になります。

有効なレイヤ 2 アソシエーションのない 2 つの VLAN 間のマッピングを設定しても、マッピング設定は有効になりません。

例

次に、VLAN 20 のインターフェイスを VLAN 18 の SVI にマッピングする例を示します。

```
Router(config)# interface vlan 18
Router(config-if)# private-vlan mapping 18 20
Router(config-if)#
```

次に、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て、設定を確認する例を示します。

```
Router# configure terminal
Router(config)# interface vlan 202
Router(config-if)# private-vlan mapping add 303-307,309,440
Router(config-if)# end
Router# 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
Router#
```

次に、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エラーメッセージの例を示します。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。

```
Router(config)# interface vlan 19
Router(config-if)# private-vlan mapping 19 add 21
    Command rejected: The interface for VLAN 21 is already mapped as s secondary.
Router(config-if)#
```

次に、VLAN 19 の SVI からすべての PVLAN マッピングを削除する例を示します。

```
Router(config)# interface vlan 19
Router(config-if)# no private-vlan mapping
Router(config-if)#
```

関連コマンド

コマンド	説明
show interfaces private-vlan mapping	VLAN SVI の PVLAN マッピングに関する情報を表示します。
show vlan	VLAN 情報を表示します。
show vlan private-vlan	PVLAN 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

シンタックスの説明

このコマンドには、キーワードまたは引数はありません。

コマンドのデフォルト

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 サブモード

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

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、対応付けられたプライマリ VLAN と同じインスタンスに VLAN をマッピングしていないと、警告メッセージにより、対応付けられたプライマリ VLAN と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 のリストが表示されます。**private-vlan synchronize** コマンドは、すべてのセカンダリ VLAN を対応付けられたプライマリ VLAN と同じインスタンスに自動的にマッピングします。

例

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 に対応付けられ、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。また、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。

```
Router(config)# spanning-tree mst configuration
Router(config-mst)# instance 1 vlan 2
Router(config-mst)# exit
These secondary vlans are not mapped to the same instance as their primary:
-> 3
```

次に、PVLAN 同期を初期化する例を示します。

```
Router(config-mst)# private-vlan synchronize
Router(config-mst)#
```

関連コマンド

コマンド	説明
show	MST の設定を確認します。
show spanning-tree mst	MST プロトコルに関する情報を表示します。

process-min-time percent

他のプロセスに対して CPU を解放する前に OSPF が必要とするプロセス時間の最小の割合を指定するには、**process-min-time percent** 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。

process-min-time percent *percent*

no process-min-time

シンタックスの説明

percent	他のプロセスに対して CPU を解放する前に使用される CPU プロセス時間の割合。有効値は、1 ～ 100 です。

コマンドのデフォルト

percent は、**25** です。

コマンド モード

ルータ コンフィギュレーション

コマンドの履歴

リリース	変更内容
12.2(18)ZY	この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

（注）　Cisco TAC の指導を受けた場合にだけ、このコマンドを使用してください。

このコマンドは、OSPFv2 および OSPFv3 でサポートされます。

process-min-time コマンドを使用して、プロセスの最大時間から起算する最小の割合を設定します。割合が超過すると、CPU 制御はプライオリティが高い方のプロセスに割り当てられる可能性があります。

process-max-time コマンドを使用して、プロセスの最大時間を設定します。**process-max-time** コマンドとともに **process-min-time** コマンドを使用してください。

例

次に、CPU を解放する前に使用される CPU プロセス時間の割合を設定する例を示します。

```
Router> configure terminal
Router(configure)# router ospf
Router(config-router)# process-min-time percent 35
Router(config-router)#
```

次に、デフォルト設定に戻す例を示します。

```
Router> configure terminal
Router(configure)# router rip
Router(config-router)# no process-min-time
Router(config-router)#
```

関連コマンド

コマンド	説明
process-max-time	プロセスが別のプロセスに自発的に移行する時間を設定します。