mls flow

NDE のフロー マスクを設定するには、**mls flow** コマンドを使用します。フロー マスクをデフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls flow {{**ip** | **ipv6**} {**destination** | **destination-source** | **full** | **interface-destination-source** | **interface-full** | **source**}}

no mls flow {**ip** | **ipv6**}

シンタックスの説明

ip	MLS IP パケットのフロー マスクをイネーブルにします。
ipv6	MLS IPv6 パケットのフロー マスクをイネーブルにします。
destination	レイヤ 3 テーブルのキーとして、宛先 IP アドレスを使用します。
destination-source	レイヤ 3 テーブルのキーとして、宛先および送信元 IP アドレスを使用します。
full	レイヤ 3 テーブルのキーとして、送信元および宛先 IP アドレス、IP プロトコル（UDP または TCP）、送信元および宛先ポート番号を使用します。
interface-destination-source	レイヤ 3 テーブルのキーとして、宛先および送信元フロー マスク内のすべての情報と、送信元 VLAN 番号を使用します。
interface-full	レイヤ 3 テーブルのキーとして、フル フロー マスク内のすべての情報、および送信元 VLAN 番号を使用します。
source	送信元フロー マスクだけのすべての情報を使用します。

コマンドのデフォルト

NDE フロー マスクはヌルです。

コマンド モード

グローバル コンフィギュレーション（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

このコマンドは、スーパーバイザ エンジンの統計情報を収集します。

例

次に、MLS IP の拡張アクセス リストに最小限のフロー マスクを設定する例を示します。

```
Router(config)# mls flow ip full
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls ip

インターフェイス上で内部ルータの MLS IP をイネーブルにするには、**mls ip** コマンドを使用します。MLS IP をインターフェイス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。

mls ip

no mls ip

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

マルチキャストはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

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、MLS IP のショートカットをイネーブルにする例を示します。

```
Router(config-if)# mls ip
Router(config-if)#
```

関連コマンド

コマンド	説明
mls rp ip (interface configuration mode)	外部システムが指定インターフェイスで MLS IP をイネーブルにすることができるようにします。
show mls ip multicast	MLS IP 情報を表示します。

mls ip acl port expand

レイヤ 4 に対する ACL 固有機能をイネーブルにするには、**mls ip acl port expand** コマンドを使用します。ACL 固有のレイヤ 4 機能をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip acl port expand

no mls ip acl port expand

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

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、レイヤ 4 ポート上での ACL の論理動作の拡張をイネーブルにする例を示します。

```
Router(config)# mls ip acl port expand
Router(config)#
```

mls ip cef accounting per-prefix

MLS のプレフィクス単位のアカウンティングをイネーブルにするには、**mls ip cef accounting per-prefix** コマンドを使用します。MLS のプレフィクス単位のアカウンティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip cef accounting per-prefix *prefix-entry prefix-entry-mask* [*instance-name*]

no mls ip cef accounting per-prefix

シンタックスの説明

prefix	A.B.C.D のフォーマットのプレフィクス エントリ
prefix-entry-mask	A.B.C.D のフォーマットのプレフィクス エントリ マスク
instance-name	（任意）VPN ルーティング / 転送インスタンス名

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

プレフィクス単位のアカウンティングでは、プレフィクスが使用する隣接カウンタが収集されます。プレフィクスをアカウンティングに使用する場合は、その他のプレフィクスと隣接を共有できません。特定宛先に送信されるパケットのアカウンティングを行うには、プレフィクス単位のアカウンティングを使用します。

例

次の例は、MLS のプレフィクス単位のアカウンティングをイネーブルにする方法を示しています。

```
Router(config)# mls ip cef accounting per-prefix 172.20.52.18 255.255.255.255
Router(config)#
```

次の例は、MLS のプレフィクス単位のアカウンティングをディセーブルにする方法を示しています。

```
Router(config)# no mls ip cef accounting per-prefix
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip accounting per-prefix	統計情報の収集のために設定されたプレフィクスをすべて表示します。

mls ip cef load-sharing

CEF ロードバランスを設定するには、**mls ip cef load-sharing** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip cef load-sharing [**full** [**exclude-port** {**destination** | **source**}]] [**simple**]

no mls ip cef load-sharing

シンタックスの説明

full	（任意）送信元/宛先レイヤ 4 ポートおよび送信元 IP/宛先 IP アドレス（レイヤ 3）を含めるように CEF ロードバランスを設定します。
exclude-port destination	（任意）ロードバランス アルゴリズムから宛先レイヤ 4 ポートおよび送信元 IP/宛先 IP アドレス（レイヤ 3）を除外します。
exclude-port source	（任意）ロードバランス アルゴリズムから送信元レイヤ 4 ポートおよび送信元 IP/宛先 IP アドレス（レイヤ 3）を除外します。
simple	（任意）単一ステージのロード シェアリングに対して CEF ロード バランスを設定します。

コマンドのデフォルト

送信元および宛先 IP アドレスおよびユニバーサル ID

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

mls ip cef load-sharing コマンドは、IPv4、IPv6、および MPLS 転送に影響します。

mls ip cef load-sharing コマンドの構造は、次のとおりです。

- **mls ip cef load-sharing full** : 複数の隣接関係とともにレイヤ 3 およびレイヤ 4 情報を使用します。
- **mls ip cef load-sharing full simple** : 複数の隣接関係なしでレイヤ 3 およびレイヤ 4 情報を使用します。
- **mls ip cef load-sharing simple** : 複数の隣接関係なしでレイヤ 3 情報を使用します。

その他の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、複数の隣接関係とともにレイヤ 3 およびレイヤ 4 ポートを含めるようにロードバランスを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full
Router(config)#
```

次に、ロードバランス アルゴリズムから宛先レイヤ 4 ポートおよび送信元/宛先 IP アドレス（レイヤ 3）を除外するようロード バランスを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full exclude-port destination
Router(config)#
```

次に、ロードバランス アルゴリズムから送信元レイヤ 4 ポートおよび送信元/宛先 IP アドレス（レイヤ 3）を除外するようロード バランスを設定する例を示します。

```
Router(config)# mls ip cef load-sharing full exclude-port source
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls ip cef load-sharing
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

mls ip cef rate-limit

CEF によりパントされたデータ パケットのレートを制限するには、**mls ip cef rate-limit** コマンドを使用します。CEF によりパントされたデータ パケットのレート制限をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip cef rate-limit *pps*

no mls ip cef rate-limit

シンタックスの説明

pps	データ パケットの番号。有効値は 0 ～ 1,000,000 です。

コマンドのデフォルト

レート制限は設定されていません。

コマンド モード

グローバル コンフィギュレーション（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

特定の DoS 攻撃は、ルータのルート処理エンジンをターゲットにしています。PFC で転送できない特定のパケットは、PISA に転送されて処理されます。DoS 攻撃が発生すると、ルート処理エンジンは過負荷になり、ダイナミックなルーティング プロトコルの稼動時にはルーティングが不安定になることがあります。**mls ip cef rate-limit** コマンドを使用すると、PISA に送信されるトラフィック量を制限し、ルート処理エンジンへの denial-of-servic 攻撃を防ぐことができます。

このコマンドは、次のパケットを含めて、CEF によりパントされたすべてのデータ パケットのレートを制限します。

- ローカル インターフェイス IP アドレス宛のデータパケット
- ARP を必要とするデータ パケット

低いレートを設定すると、ローカル インターフェイスの IP アドレス宛のパケット、および ARP を必要とするパケットに影響が及びます。このコマンドは、これらのパケットを通常の標準レートに制限して、異常な着信レートを回避する場合に使用してください。

その他の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、レート制限のイネーブル化および設定を行う例を示します。

```
Router(config)# mls ip cef rate-limit 50000
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

mls ip cef rpf hw-enable-rpf-acl

uRPF ACL がイネーブルの場合に deny ace に一致するパケットのハードウェアの uRPF をイネーブルにするには、**mls ip cef rpf hw-enable-rpf-acl** コマンドを使用します。RPF と ACL がイネーブルの場合にハードウェアの uRPF をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip cef rpf hw-enable-rpf-acl

no mls ip cef rpf hw-enable-rpf-acl

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

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

mls ip cef rpf hw-enable-rpf-acl コマンドを入力しない場合、uRPF ACL を指定すると、uRPF ACL によって許可されたパケットはハードウェアに転送され、拒否されたパケットは PISA に送信されて、uRPF チェックが行われます。このコマンドは、uRPF ACL によって拒否されたパケットの uRPF チェックを伴うハードウェア転送をイネーブルにします。ただし、この場合、uRPF ACL によって許可されたパケットは PISA に送信されて、転送されます。

uRPF は、PVLAN ホスト ポートではサポートされていません。

例

次に、RPF と ACL がイネーブルの場合にハードウェアの uRPF をイネーブルにする例を示します。

```
Router(config)# mls ip cef rpf hw-enable-rpf-acl
Router(config)#
```

次に、RPF と ACL がイネーブルの場合にハードウェアの uRPF をディセーブルにする例を示します。

```
Router(config)# no mls ip cef rpf hw-enable-rpf-acl
Router(config)#
```

関連コマンド

コマンド	説明
ip verify unicast source reachable-via {any | rx}	RPF ACL チェックをイネーブルにし、設定します。

mls ip cef rpf interface-group

RPF_VLAN テーブルでインターフェイス グループを定義するには、**mls ip cef rpf interface-group** コマンドを使用します。インターフェイス グループを削除するには、このコマンドの **no** 形式を使用します。

mls ip cef rpf interface-group *group-number interface1 interface2 interface3* [...]

no mls ip cef rpf interface-group *group-number interface1 interface2 interface3* [...]

シンタックスの説明

group-number	インターフェイス グループ番号。有効値は 1 ～ 4 です。
interface	インターフェイス番号。フォーマットの注意事項については、「使用上のガイドライン」を参照してください。
...	（任意）インターフェイス番号を追加で指定します。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

グループは設定されていません。

コマンド モード

グローバル コンフィギュレーション（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

1 つのインターフェイス グループには、3 ～ 6 個のインターフェイスがあります。インターフェイス グループは最大 4 つまで設定できます。各インターフェイス グループについて、最初の 4 つのエントリはハードウェアの RPF_VLAN テーブルに組み込まれます。

interface は *interface-typemod/port* の形式で入力します。

各インターフェイスは、スペースで区切って入力してください。*interface-type* 引数と *mod/port* 引数の間には、スペースは不要です。入力例については、「例」を参照してください。

例

次に、インターフェイス グループを定義する例を示します。

```
Router(config)# mls ip cef rpf interface-group 0 F2/1 F2/2 F2/3 F2/4 F2/5 F2/6
Router(config)#
```

mls ip cef rpf multipath

RPF モードを設定するには、**mls ip cef rpf multipath** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip cef rpf multipath {**interface-group** | **punt** | **pass**}

シンタックスの説明

interface-group	複数パス ルートから着信するパケットの RPF チェックをディセーブルにします。詳しくは、「使用上のガイドライン」を参照してください。
punt	RPF に失敗したパケットをルート プロセッサにリダイレクトして、複数パスのプレフィクスに対応します。
pass	複数パス ルートから着信するパケットの RPF チェックをディセーブルにします。

コマンドのデフォルト

punt

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

interface-group モードは pass モードと類似していますが、RPF チェックに RPF_VLAN グローバル テーブルを使用します。その他の複数パス プレフィクスからのパケットは、常に RPF チェックを通過します。

RPF_VLAN テーブルのインターフェイス グループを定義するには、**mls ip cef rpf multipath interface-group** コマンドを使用します。1 つのインターフェイス グループには、3 ～ 6 個のインターフェイスがあり、最大 4 つのインターフェイス グループを設定できます。各インターフェイス グループについて、最初の 4 つのエントリはハードウェアの RPF_VLAN テーブルに組み込まれます。4 つ以上の複数パスを持つプレフィクスの場合、2 つを除いてパスはすべてインターフェイス グループに属し、そのプレフィクスの FIB エントリはこの RPF_VLAN エントリを使用します。

例

次に、RPF に失敗したパケットをルート プロセッサにリダイレクトして、複数パスのプレフィクスに対応する例を示します。

```
Router(config)# mls ip cef rpf multipath interface-group
Router(config)#
```

関連コマンド

コマンド	説明
show mls cef ip	MLS ハードウェア レイヤ 3 スイッチング テーブルの IP エントリを表示します。

mls ip delete-threshold

設定済みの ACL しきい値を削除するには、**mls ip delete-threshold** コマンドを使用します。

mls ip delete-threshold *acl-num*

シンタックスの説明

acl-num	再帰 ACL 番号。有効値は 1 ～ 10,000 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。

コマンドのデフォルト

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

mls ip delete-threshold コマンドは、**mls ip reflexive ndr-entry tcam** コマンドをイネーブルに設定した場合にだけアクティブになります。

例

次に、ACL しきい値を削除する例を示します。

```
Router(config)# mls ip delete-threshold 223
Router(config)#
```

関連コマンド

コマンド	説明
mls ip install-threshold	設定済み ACL しきい値を組み込みます。
mls ip reflexive ndr-entry tcam	No Drop Rate（NDR）によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにします。

mls ip directed-broadcast

IP 転送ブロードキャストのハードウェア スイッチングをイネーブルにするには、**mls ip directed-broadcast** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip directed-broadcast {**exclude-router** | **include-router**}

no mls ip directed-broadcast

シンタックスの説明

exclude-router	IP 転送ブロードキャスト パケットを、ルータを除く VLAN 内のすべてのホストに、ハードウェア転送します。
include-router	IP 転送ブロードキャスト パケットを、ルータを含む VLAN 内のすべてのホストに、ハードウェア転送します。

コマンド モード

ディセーブル

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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

exclude-router および **include-router** キーワードは両方ともハードウェア スイッチングをサポートします。ただし、**exclude-router** の場合は、ハードウェアによりスイッチングされたパケットのコピーをルータに送信しません。**include-router** キーワードを入力した場合、ルータは IP 転送ブロードキャスト パケットを再転送しません。

デフォルト モードの場合、IP 転送ブロードキャスト パケットはハードウェアで転送されません。PISA によってプロセス レベルで処理されます。PISA がパケットを転送するかどうかは、**ip directed-broadcast** コマンド設定によって決まります。

ip directed-broadcast コマンドと **mls ip directed-broadcast** コマンドの間には連動関係がありません。**ip directed-broadcast** コマンドはソフトウェア転送に関係し、**mls ip directed-broadcast** コマンドはハードウェア転送に関係します。

MLS IP 転送ブロードキャストは、セカンダリ インターフェイス アドレスをサポートします。

ip directed-broadcast コマンドを同じインターフェイスに追加しないかぎり、CPU に到達したパケットは転送されません。

ポートチャネル インターフェイスには MLS IP 転送ブロードキャストを設定できますが、ポートチャネル インターフェイスの物理インターフェイスには設定できません。物理インターフェイスに MLS IP 転送ブロードキャストを設定したまま、ポートチャネル グループに物理インターフェイスを追加することはできません。まず、設定を手動で削除してから、チャネル グループに物理インターフェイスを追加する必要があります。物理インターフェイスがすでにチャネルグループに含まれている場合、CLI はこの物理インターフェイス上で **mls ip directed-broadcast** コンフィギュレーション コマンドを受け入れません。

例

次に、IP 転送ブロードキャスト パケットを、ルータを除く VLAN 内のすべてのホストにハードウェア転送する例を示します。

```
Router(config-if)# mls ip directed-broadcast exclude-router
Router(config-if)#
```

次に、IP 転送ブロードキャスト パケットを、VLAN 内のすべてのホストにハードウェア転送する例を示します。

```
Router(config-if)# mls ip directed-broadcast include-router
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls cef adjacency	ハードウェアによりスイッチングされる IP 転送ブロードキャスト情報を表示します。

mls ip inspect

他のインターフェイス経由のトラフィックを拒否する任意の ACL を使用してトラフィックを許可するには、**mls ip inspect** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip inspect *acl-name*

no mls ip inspect *acl-name*

シンタックスの説明

acl-name	ACL 名

コマンド モード

ディセーブル

コマンドのデフォルト

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

Catalyst 6500 シリーズ スイッチ上で、トラフィックを拒否するようにインターフェイスが設定されている場合、context based access control（CBAC; コンテキスト ベースのアクセス制御）が双方向のトラフィック フローを許可するのは、**ip inspect** コマンドで設定されたインターフェイスだけです。

例

次に、特定の ACL（deny_ftp_c）を使用してトラフィックを許可する例を示します。

```
Router(config)# mls ip inspect deny_ftp_c
Router(config)#
```

関連コマンド

コマンド	説明
ip inspect	検査規則のセットをインターフェイスに適用します。

mls ip install-threshold

設定済みの ACL しきい値を組み込むには、**mls ip install-threshold** コマンドを使用します。

mls ip install-threshold *acl-num*

シンタックスの説明

acl-num	再帰 ACL 番号。有効値は 1 ～ 10,000 です。

コマンド モード

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

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

mls ip install-threshold コマンドは、**mls ip reflexive ndr-entry tcam** コマンドをイネーブルに設定した場合にだけアクティブになります。

例

次に、ACL しきい値を組み込む例を示します。

```
Router(config)# mls ip install-threshold 123
Router(config)#
```

関連コマンド

コマンド	説明
mls ip delete-threshold	設定済み ACL しきい値を削除します。
mls ip reflexive ndr-entry tcam	NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにします。

mls ip multicast (global configuration mode)

MLS IP をイネーブルにして、ハードウェア スイッチングをグローバルに設定するには、**mls ip multicast** コマンドを使用します。MLS IP をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast [**capability**]

mls ip multicast [**vrf** *name*] [**connected** | **egress local** | **mfd** | **refresh-state** | **shared-tree-mfd** | **threshold** *ppsec*]

no mls ip multicast [**vrf**]

シンタックスの説明

capability	（任意）スイッチ プロセッサからルート プロセッサに出力機能情報をエクスポートします。
vrf *name*	（任意）VRF 名を指定します。
connected	（任意）直接接続されている送信元を内部ルータにブリッジングするために、インターフェイスまたはマスク エントリを組み込みます。
egress local	（任意）ローカル レイヤ 3 ルーテッド インターフェイスをマルチキャスト拡張テーブルに入力します。
mfd	（任意）完全なハードウェア スイッチングをイネーブルにします。
refresh-state	（任意）（S,G）エントリまたは Outgoing interface of a multicast {*,G} or {source, group} flow（OIF; マルチキャスト {*,G} または {S,G} フローの Outgoing Interface）がヌルの（*,G）エントリの期限切れ時間をリフレッシュします。
shared-tree-mfd	（任意）（*,G）フローのすべてのショートカットをイネーブルにします。
threshold *ppsec*	（任意）最小トラフィック レートを設定します。このレートを下回る場合、フローはハードウェアでスイッチングされずにソフトウェアでスイッチングされます。有効値は、10 ～ 10,000 秒です。

コマンド モード

デフォルト設定は次のとおりです。

- マルチキャストはディセーブルです。
- ハードウェア スイッチングは、すべての適格なマルチキャスト ルートに対して許可されます。
- **connected** はイネーブルです。
- **egress local** はディセーブルです。
- **mfd** はイネーブルです。
- **refresh-state** はイネーブルです。
- **shared-tree-mfd** はイネーブルです。

コマンドのデフォルト

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）　**mls ip multicast egress local** コマンドの入力後、システムをリセットして設定を有効にする必要があります。

mls ip multicast egress local コマンドを入力するとき、IPv6 マルチキャストがイネーブルでないことを確認してください。出力マルチキャスト レプリケーション パフォーマンス拡張機能は、IPv4 および IPv6 のオンまたはオフを個別に実行できないので、この機能をオンに切り替えるとき、IPv4 および IPv6 のマルチキャストをイネーブルにすることはできません。

次のオプションのキーワードがサポートされています。

- **threshold**
- **connected**
- **refresh-state**
- **shared-tree-mfd**
- **mfd**

オプションの **threshold** *ppsec* キーワードおよび引数は、ハードウェア キャッシュにすでに存在しているフローには影響しません。

フロー統計情報を Catalyst 6500 シリーズ スイッチが受信すると（トラフィックが RPF インターフェイスから受信されることを示します）、期限切れ時間のリフレッシュが更新されます。

例

次に、MLS IP ショートカットをイネーブルにする例を示します。

```
Router(config)# mls ip multicast
Router(config)#
```

次に、特定のマルチキャスト ルートのハードウェア スイッチングをイネーブルにする例を示します。

```
Router(config)# mls ip multicast vrf test1
Router(config)#
```

次に、スイッチ プロセッサからルート プロセッサに出力機能情報をエクスポートする例を示します。

```
Router(config)# mls ip multicast capability
Router(config)#
```

次に、ローカル レイヤ 3 ルーテッド インターフェイスをマルチキャスト拡張テーブルに入力する例を示します。

```
Router(config)# mls ip multicast egress local
Router(config)#
```

関連コマンド

コマンド	説明
mls rp ip (global configuration mode)	外部システムが PISA への IP ショートカットを確立できるようにします。
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast (interface configuration mode)

インターフェイス上で MLS IP ショートカットをイネーブルにするには、**mls ip multicast** コマンドを使用します。MLS IP ショートカットをインターフェイス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。

mls ip multicast

no mls ip multicast

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 モード

マルチキャストはディセーブルです。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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、MLS IP ショートカットをイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast bidir gm-scan-interval

Bidir ランデブー ポイントの RPF スキャン インターバルを設定するには、**mls ip multicast bidir gm-scan-interval** コマンドを使用します。Bidir RP の RPF スキャン インターバルをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls ip multicast bidir gm-scan-interval *interval*

no mls ip multicast bidir gm-scan-interval

シンタックスの説明

interval	Bidir RP の RPF スキャン インターバル。有効値は、1 ～ 1000 秒です。

コマンド モード

10 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

Bidir ランデブーポイントの RPF スキャン インターバルを設定する場合、ハードウェアのすべての Bidir ランデブーポイントの DF テーブルで、定期スキャン タイマーが RPF を更新する時間を設定します。

例

次に、Bidir ランデブーポイントの RPF スキャン インターバルを設定する例を示します。

```
Router(config)# mls ip multicast bidir gm-scan-interval 30
Router(config)#
```

関連コマンド

コマンド	説明
show mls ip multicast bidir	Bidir ハードウェアでスイッチングされるエントリを表示します。

mls ip multicast connected

直接接続されているサブネットのダウンロードをグローバルにイネーブルにするには、**mls ip multicast connected** コマンドを使用します。直接接続されているサブネットのダウンロード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。

mls ip multicast connected

no mls ip multicast connected

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 モード　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　次の場合には、直接接続されたサブネットを作成しないでください。

- FIB TCAM で利用できる空間を増やす場合
- スイッチが送信元の最初のホップ ルータである場合
- エントリが双方向、SSM、および DM モードのグループの場合

これらの場合、直接接続されたサブネットのダウンロードをイネーブルにすると、直接接続された送信元は multicast multilayer switching（MMLS; マルチキャスト マルチレイヤ スイッチング）（*,G）エントリに到達し、MMLS（*,G）エントリを使用してスイッチングされます。レジスタはルート プロセッサに送信されず（PIM-SM の場合）、また、最初のホップで（S,G）ステートは作成されません（PIM-DM の場合）。

直接接続された送信元がこれらのエントリに到達する前に、直接接続された送信元を捕捉するために、マスクを短くしてサブネット エントリを TCAM エントリに組み込みます。直接接続された送信元から PISA にトラフィックをパントできます。PISA がこのトラフィックを確認すると、PISA はこの送信元の MMLS（S,G）エントリを組み込みます。MMLS（S,G）エントリは、TCAM のサブネット エントリよりも前に組み込まれます。これで、この送信元からのパケットは（S,G）エントリを使用してスイッチングされます。

例　次に、直接接続されたサブネットのダウンロードをイネーブルにする例を示します。

```
Router(config)# mls ip multicast connected
Router(config)#
```

関連コマンド

コマンド	説明
mls ip multicast (global configuration mode)	MLS IP をイネーブルにして、ハードウェア スイッチングをグローバルに設定します。
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast consistency-check

ハードウェアによるショートカットの一貫性チェッカーのイネーブル化および設定を行うには、**mls ip multicast consistency-check** コマンドを使用します。一貫性チェッカ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。

mls ip multicast consistency-check [{**settle-time** *seconds*} | {**type scan-mroute** [**count** *count-number*] | {**settle-time** *seconds*}} | {**period** *seconds*}]

no mls ip multicast consistency-check

シンタックスの説明

settle-time *seconds*	（任意）一貫性チェッカーに対するエントリ /OIF の処理時間を指定します。有効値は、2 ～ 3600 秒です。
type scan-mroute	（任意）一貫性チェックのタイプをマルチキャスト ルート テーブルのスキャン チェックに指定します。
count *count-number*	（任意）各スキャンでチェックする最大プレフィクス数を指定します。有効値は 2 ～ 500 です。
period *seconds*	（任意）スキャン間隔を指定します。有効値は 2 ～ 3600 秒です。

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。

- 一貫性チェックはイネーブルです。
- **count** *count-number* は **20** です。
- **period** *seconds* は **2** 秒です。
- **settle-time** *seconds* は **60** 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（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

oif エントリは、マルチキャスト {*,G} または {S,G} フローの Outgoing Interface です。

一貫性チェッカーはマルチキャスト ルート テーブルをスキャンし、マルチキャスト ハードウェア エントリとマルチキャスト ルート テーブルの一貫性を保証します。不一致が検出されると、その不一致は自動的に訂正されます。

不一致エラーを表示するには、**show mls ip multicast consistency-check** コマンドを使用します。

例

次に、ハードウェアによるショートカットの一貫性チェッカーをイネーブルにする例を示します。

```
Router (config)# mls ip multicast consistency-check
Router (config)#
```

次に、ハードウェアによるショートカットの一貫性チェッカーをイネーブルにし、マルチキャスト ルート テーブルのスキャン チェックを設定する例を示します。

```
Router (config)# mls ip multicast consistency-check type scan-mroute count 20 period 35
Router (config)#
```

次に、ハードウェアによるショートカットの一貫性チェッカーをイネーブルにし、スキャン間隔を指定する例を示します。

```
Router (config)# mls ip multicast consistency-check type scan-mroute period 35
Router (config)#
```

関連コマンド

コマンド	説明
show mls ip multicast consistency-check	MLS IP 情報を表示します。

mls ip multicast flow-stat-timer

スイッチ プロセッサからルート プロセッサへのフロー統計情報メッセージのバッチ間隔を設定するには、**mls ip multicast flow-stat-timer** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip multicast flow-stat-timer *num*

no mls ip multicast flow-stat-timer

シンタックスの説明

num	スイッチ プロセッサからルート プロセッサへのフロー統計情報メッセージのバッチ間隔

コマンドのデフォルト

25 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。

例

次に、スイッチ プロセッサからルート プロセッサへのフロー統計情報メッセージのバッチ間隔を指定する例を示します。

```
Router (config)# mls ip multicast flow-stat-timer 10
Router (config)#
```

関連コマンド

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast replication-mode

レプリケーション モードのイネーブル化および指定を行うには、**mls ip multicast replication-mode** コマンドを使用します。システムを自動検出モードに戻すには、このコマンドの **no** 形式を使用します。

mls ip multicast replication-mode {**egress** | **ingress**}

no mls ip multicast replication-mode {**egress** | **ingress**}

シンタックスの説明

egress	システムをレプリケーションの出力モードに強制します。
ingress	システムをレプリケーションの入力モードに強制します。

コマンドのデフォルト

ingress

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

Supervisor Engine 32 PISA は、**egress** キーワードをサポートしていません。

（注） 出力から入力レプリケーション モードに移行中、ショートカットが削除され、再インストールされるために、トラフィックが分断される可能性があります。トラフィック転送中の分断を防ぐには、**mls ip multicast replication-mode ingress** コマンドを入力します。

no mls ip multicast replication-mode ingress コマンドを入力すると、強制入力モードだけがリセットされます。

例

次に、入力レプリケーション モードをイネーブルにする例を示します。

```
Router (config)# mls ip multicast replication-mode ingress
Router (config)#
```

関連コマンド

コマンド	説明
show mls ip multicast capability	MLS IP 情報を表示します。

mls ip multicast sso

Stateful Switch Over（SSO）パラメータを設定するには、**mls ip multicast sso** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls ip multicast sso {{**convergence-time** *time*} | {**leak** *interval*} | {**leak** *percentage*}}

シンタックスの説明

convergence-time *time*	プロトコル コンバージェンスまでの最大待機時間を指定します。有効値は、0 ～ 3600 秒です。
leak *interval*	パケット リークのインターバルを指定します。有効値は、0 ～ 3600 秒です。
leak *percentage*	プロトコル コンバージェンスを実行するよう、スイッチオーバー中にルータにリークされるマルチキャスト パケットのパーセンテージを指定します。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。

- **convergence-time** *time*：20 秒
- **leak** *interval*：60 秒
- **leak** *percentage*：10%

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、プロトコル コンバージェンスまでの最大待機時間を設定する例を示します。

```
Router (config)# mls ip multicast sso convergence-time 300
Router (config)#
```

次に、パケット リークのインターバルを設定する例を示します。

```
Router (config)# mls ip multicast sso leak 200
Router (config)#
```

次に、パケット リークのパーセンテージを設定する例を示します。

```
Router (config)# mls ip multicast sso leak 55
Router (config)#
```

関連コマンド

コマンド	説明
show mls ip multicast sso	マルチキャスト ハイ アベイラビリティ SSO に関する情報を表示します。

mls ip multicast stub

PIM sparse（疎）モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポートをイネーブルにするには、**mls ip multicast stub** コマンドを使用します。PIM sparse（疎）モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポ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。

mls ip multicast stub

no mls ip multicast stub

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

マルチキャストはディセーブルです。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

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

mls ip multicast stub コマンドでは、ルーテッド インターフェイスまたは VLAN で次のフィルタが作成されます。

- インターフェイスに接続されているすべてのアドレスからすべての IP 宛先への IP パケットを許可します。**ip address** *addr mask* [**secondary**] コマンドで設定した IP アドレス プレフィクス内にアドレスが収まる場合、アドレスはインターフェイスに接続されています。

  このフィルタでは、直接接続されている送信元からのユニキャスト パケットおよびマルチキャスト パケットが許可されます。

- すべての送信元アドレスからマルチキャスト グループ プレフィクス 224.0.0.0/24 および 224.0.1.0/24 への IP マルチキャスト パケットを許可します。

  このフィルタでは、すべての送信元アドレスから well-Known マルチキャスト アドレスへパケットを送信できます。224.0.0.0/24 は、PIM、open shortest path first（OSPF）、EIGRP、Network Time Protocol（NTP）などのプロトコルによって使用されます。224.0.1.0/24 のアドレスは、AutoRP などのプロトコルによって使用されます（224.0.1.39、224.0.1.40）。

- その他すべての IP マルチキャスト パケットを拒否します。

  この拒否フィルタは、直接接続されていない送信元からのマルチキャスト パケットを禁止し、このインターフェイスまたは VLAN で受信したパケットに適用されます。

IP マルチキャスト パケットを許可するフィルタ、およびその他すべての IP マルチキャスト パケットを拒否するフィルタは、**mls ip multicast stub** コマンドを設定したすべてのインターフェイスまたは VLAN で同じです。インターフェイスに接続されているすべてのアドレスからすべての IP 宛先への IP パケットを許可するフィルタは、インターフェイスまたは VLAN ごとに異なります。

例

次に、PIM sparse（疎）モードのスタブ ネットワークに対して、非 RPF トラフィック廃棄のサポートをイネーブルにする例を示します。

```
Router(config-if)# mls ip multicast stub
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls ip multicast	MLS IP 情報を表示します。

mls ip multicast threshold

ハードウェアによるショートカットを組み込むために、しきい値レートを設定するには、**mls ip multicast threshold** コマンドを使用します。しきい値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。

mls ip multicast threshold *ppsec*

no mls ip multicast threshold

シンタックスの説明

ppsec	しきい値（パケット/秒）。有効値は 10 ～ 10,000 パケット/秒です。

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

このコマンドは、join 要求など、存続期間の短いマルチキャスト フローに対して MLS エントリの作成を禁止する場合に使用します。

マルチキャスト トラフィックが設定されたマルチキャスト レートのしきい値を下回ると、マルチキャスト トラフィックはすべて PISA でルーティングされます。

このコマンドは組み込み済みのルートには影響しません。たとえば、ショートカットがすでに組み込まれている場合に、このコマンドを入力しても、それらのショートカットは不適格な場合でも削除されません。既存のルートにしきい値を適用するには、ルートをいったん消去して、再確立します。

例

次に、IP MLS しきい値を 10 パケット/秒に設定する例を示します。

```
Router (config)# mls ip multicast threshold 10
Router (config)#
```

関連コマンド

コマンド	説明
mls rp ip (global configuration mode)	外部システムが PISA への IP ショートカットを確立できるようにします。
show mls ip multicast	MLS IP 情報を表示します。

mls ip nat netflow-frag-l4-zero

フラグメントされたパケットに関する NetFlow 検索テーブルのレイヤ 4 情報を消去するには、**mls ip nat netflow-frag-l4-zero** コマンドを使用します。

mls ip nat netflow-frag-l4-zero

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

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

このコマンドは、PFC3BXL または PFC3B モードだけでサポートされます。

ソフトウェアに送信される最初のフラグメントを NetFlow ショートカットと照合する（通常の処理）のを回避するには、**mls ip nat netflow-frag-l4-zero** コマンドを使用します。ソフトウェアに送信される次のフラグメントは、最初のフラグメントからのレイヤ 4 ポート情報に基づいて変換されます。最初のフラグメントからのレイヤ 4 ポート情報に基づく変換は、NetFlow キーに照合用のフラグメント ビットがないために実行されます。

TCAM でプログラムされる ACL TCAM エントリ/マスクを多数必要とする大規模の機能設定がインターフェイス上にある場合、インターフェイスが network address translation（NAT; ネットワーク アドレス変換）内部インターフェイスとして設定されていると、この機能設定が ACL TCAM に適合せず、インターフェイス上のトラフィックはソフトウェアでスイッチングされることがあります。

例

次に、フラグメントされたパケットに関する NetFlow 検索テーブルのレイヤ 4 情報を消去する例を示します。

```
Router (config)# mls ip nat netflow-frag-l4-zero
Router (config)#
```

mls ip pbr

ポリシー ルーティング パケットの MLS サポートをイネーブルにするには、**mls ip pbr** コマンドを使用します。ポリシー ルーティング パケットの MLS サポ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。

mls ip pbr [**null0**]

no mls ip pbr

シンタックスの説明

null0	（任意）ルート マップのインターフェイス null0 へのハードウェア サポートをイネーブルにします。

コマンドのデフォルト

ポリシー ルーティング パケットへの MLS サポート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（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）　同じインターフェイス上で policy-based routing（PBR; ポリシー ベース ルーティング）と SLB をイネーブルにしないでください。PBR ベースのパケットが正しく転送されなくなります。

mls ip pbr コマンドを入力してハードウェア ポリシー ルーティングをイネーブルにすると、ハードウェアですべてのポリシー ルーティングが行われ、ポリシー ルーティングにインターフェイスが設定されているかどうかに関係なく、すべてのインターフェイスに適用されます。

ルートマップの **set interface null0** のハードウェア サポートをイネーブルにするためだけにルーテッド トラフィックがある場合は、**null0** キーワードを使用します。

例

次に、ポリシー ルーティング パケットの MLS サポートをイネーブルにする例を示します。

```
Router(config)# mls ip pbr
Router(config)#
```

関連コマンド

コマンド	説明
show tcam interface vlan acl	インターフェイスベースの TCAM に関する情報を表示します。

mls ip reflexive ndr-entry tcam

NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにするには、**mls ip reflexive ndr-entry tcam** コマンドを使用します。NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカッ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。

mls ip reflexive ndr-entry tcam

no mls ip reflexive ndr-entry tcam

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

mls ip reflexive ndr-entry tcam コマンドを入力すると、再帰 ACL ダイナミック エントリは NetFlow ではなく TCAM に組み込まれます。

例

次に、NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをイネーブルにする例を示します。

```
Router(config)# mls ip reflexive ndr-entry tcam
Router(config)#
```

次に、NDR によって組み込まれた再帰 TCP/UDP エントリに対して TCAM 内のショートカットをディセーブルにする例を示します。

```
Router(config)# no mls ip reflexive ndr-entry tcam
Router(config)#
```

関連コマンド

コマンド	説明
mls ip delete-threshold	設定済み ACL しきい値を削除します。
mls ip install-threshold	設定済み ACL しきい値を組み込みます。

mls ipv6 acl compress address unicast

IPv6 のアドレスの圧縮をオンにするには、**mls ipv6 acl compress address unicast** コマンドを使用します。IPv6 アドレスの圧縮をオフに切り替えるには、このコマンドの **no** 形式を使用します。

mls ipv6 acl compress address unicast

no mls ipv6 acl compress address unicast

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

注意　ネットワーク内に非圧縮アドレス タイプがある場合は、圧縮モードをイネーブルにしないでください。表 2-15 に、圧縮アドレスのタイプおよびアドレス圧縮方式の一覧を示します。

表 2-15　圧縮アドレスのタイプおよび方式

アドレス タイプ	圧縮方式
MAC アドレスに基づく EUI-64	このアドレスは、ビット ロケーション [39:24] から 16 ビットを削除することにより圧縮されます。ハードウェアがこれらのアドレスを圧縮する際、情報は損失しません。
組み込み型 IPv4 アドレス	このアドレスは、上位 16 ビットを削除することにより圧縮されます。ハードウェアがこれらのアドレスを圧縮する際、情報は損失しません。

表 2-15　圧縮アドレスのタイプおよび方式　（続き）

アドレス タイプ	圧縮方式
リンク ローカル	これらのアドレスは、ビット [95:80] のゼロを削除することにより圧縮され、組み込み型 IPv4 アドレスと同じパケット タイプを使用して識別されます。ハードウェアがこれらのアドレスを圧縮する際、情報は損失しません。
その他	上記のカテゴリに該当しない IPv6 アドレスは、その他に分類されます。IPv6 アドレスがその他に分類される場合、次のようになります。 • 圧縮モードがオンの場合、IPv6 アドレスは EUI-64 圧縮方式（ビット [39:24] の削除）と同様に圧縮され、レイヤ 4 情報を QoS TCAM を検索するのに使用されるキーの一部として使用できるが、レイヤ 3 情報は損失されます。 • グローバル圧縮モードがオフの場合、IPv6 アドレスの 128 ビット全体が使用されます。レイヤ 4 のポート情報は IPv6 検索キーのサイズ制限のため、QoS TCAM を検索するためのキーに含まれません。

例

次に、IPv6 の非圧縮アドレスの圧縮をオンにする例を示します。

```
Router(config)# mls ipv6 acl compress address unicast
Router(config)#
```

次に、IPv6 の非圧縮アドレスの圧縮をオフにする例を示します。

```
Router(config)# no mls ipv6 acl compress address unicast
Router(config)#
```

関連コマンド

コマンド	説明
show fm ipv6 traffic-filter	IPv6 情報を表示します。
show mls netflow ipv6	NetFlow ハードウェアに関する設定情報を表示します。

mls ipv6 acl source

送信元特定アドレスからのすべての IPv6 パケットを拒否するには、**mls ipv6 acl source** コマンドを使用します。送信元特定アドレスからのすべての IPv6 パケットを受け入れるには、このコマンドの **no** 形式を使用します。

mls ipv6 acl source {**loopback** | **multicast**}

no mls ipv6 acl source {**loopback** | **multicast**}

シンタックスの説明

loopback	送信元ループバック アドレスを含むすべての IPv6 パケットを拒否します。
multicast	送信元マルチキャスト アドレスを含むすべての IPv6 パケットを拒否します。

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。

例

次に、送信元ループバック アドレスを含むすべての IPv6 パケットを拒否する例を示します。

```
Router(config)# mls ipv6 acl source loopback
Router(config)#
```

次に、送信元マルチキャスト アドレスを含むすべての IPv6 パケットを拒否する例を示します。

```
Router(config)# no mls ipv6 acl source multicast
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow ipv6	NetFlow ハードウェアに関する設定情報を表示します。

mls mpls (recirculation)

MPLS 再循環をイネーブルにするには、**mls mpls** コマンドを使用します。MPLS 再循環をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls mpls {**recir-agg** | **tunnel-recir**}

no mls mpls {**recir-agg** | **tunnel-recir**}

シンタックスの説明

recir-agg	MPLS 集約ラベル パケットを再循環します（新規の集約ラベルは、影響されるだけです）。
tunnel-recir	トンネル MPLS パケットを再循環します。

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

トンネル MPLS 再循環をイネーブルにしない場合、ラベリングされる必要のある IPv4 および IPv4 トンネル パケット（MPLS ヘッダーでカプセル化されたパケット等）は、Catalyst 6500 シリーズ スイッチから転送される際に破壊されます。

IPv4、IPv6、および MPLS プロトコルの FIB TCAM 例外ステータスを表示するには、**show erm statistics** コマンドを使用します。

例

次に、集約ラベル MPLS 再循環をイネーブルにする例を示します。

```
Router(config)# mls mpls recir-agg
Router(config)#
```

次に、トンネル MPLS 再循環をイネーブルにする例を示します。

```
Router(config)# mls mpls tunnel-recir
Router(config)#
```

次に、集約ラベル MPLS 再循環をディセーブルにする例を示します。

```
Router(config)# no mls mpls recir-agg
Router(config)#
```

次に、トンネル MPLS 再循環をディセーブルにする例を示します。

```
Router(config)# no mls mpls tunnel-recir
Router(config)#
```

関連コマンド

コマンド	説明
show erm statistics	IPv4、IPv6、MPLS プロトコルの FIB TCAM 例外ステータスを表示します。

mls mpls (guaranteed bandwidth traffic engineering)

guaranteed bandwidth traffic engineering（GBTE; 保証帯域幅トラフィック エンジニアリング）のフロー パラメータをグローバルに設定するには、**mls 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。

mls mpls {{**gb-te-burst** *burst*} | {**gb-te-cir-ratio** *ratio*} | {**gb-te-dscp** *dscp-value* [**markdown**]} | {**gb-te-enable** [**global-pool**]}}

no mls mpls {{**gb-te-burst** *burst*} | {**gb-te-cir-ratio** *ratio*} | {**gb-te-dscp** *dscp-value* [**markdown**]} | {**gb-te-enable** [**global-pool**]}}

シンタックスの説明

gb-te-burst *burst*	保証帯域幅トラフィック エンジニアリングのフローのバースト期間を指定します。有効値は、100 ～ 30000 ミリ秒です。
gb-te-cir-ratio *ratio*	Committed Information Rate（CIR; 認定情報レート）のポリシングの比率を指定します。有効値は 1 ～ 100% です。
gb-te-dscp *dscp-value*	保証帯域幅トラフィック エンジニアリングのフローの DSCP マップを指定します。有効値は、0 ～ 63 です。
markdown	（任意）不適合フローをマークダウンまたは廃棄します。
gb-te-enable	保証帯域幅トラフィック エンジニアリングのフロー ポリシングをイネーブルにします。
global-pool	（任意）グローバル プールからポリシング トラフィック エンジニアリング フローに割り当てられたリソースの使用を指定します。

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。

- *burst* は 1000 ミリ秒です。
- *ratio* は、1% です。
- *dscp-value* は 40 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

ラベルなしのパケットが交換された場合に MPLS パケットの EXP 値をリセットするには、**mls qos map dscp-exp** コマンドを使用します。

トンネル MPLS 再循環をイネーブルにしない場合、ラベリングされる必要のある IPv4 および IPv4 トンネル パケット（MPLS ヘッダーでカプセル化されたパケット等）は、Catalyst 6500 シリーズ スイッチから転送される際に破壊されます。

IPv4、IPv6、および MPLS プロトコルの FIB TCAM 例外ステータスを表示するには、**show erm statistics** コマンドを使用します。

例

次に、保証帯域幅トラフィック エンジニアリング フローのバースト期間を指定する例を示します。

```
Router(config)# mls mpls gb-te-burst 2000
Router(config)#
```

次に、CIR ポリシングの比率を指定する例を示します。

```
Router(config)# mls mpls gb-te-ratio 30
Router(config)#
```

次に、保証帯域幅トラフィック エンジニアリング フローの DSCP マップを指定し、不適合なフローを廃棄する例を示します。

```
Router(config)# mls mpls gb-te-dscp 25 markdown
Router(config)#
```

次に、保証帯域幅トラフィック エンジニアリング フローのポリシングをイネーブルにする例を示します。

```
Router(config)# mls mpls gb-te-enable
Router(config)#
```

関連コマンド

コマンド	説明
show erm statistics	IPv4、IPv6、MPLS プロトコルの FIB TCAM 例外ステータスを表示します。

mls nde flow

NDE のフィルタ オプションを指定するには、**mls nde flow** コマンドを使用します。NDE フロー フィルタをクリアし、フィルタをリセットしてデフォルト設定に戻す場合は、このコマンドの **no** 形式を使用します。

mls nde flow {**include** | **exclude**} {{**dest-port** *port-num*} | {**destination** *ip-addr ip-mask*} | {**protocol** {**tcp** | **udp**}} | {**source** *ip-addr ip-mask*} | {**src-port** *port-num*}}

no mls nde flow {**include** | **exclude**}

シンタックスの説明

include	指定したフィルタと一致するフローを除くすべてのフローのインポートを許可します。
exclude	指定したフィルタと一致するすべてのフローのエクスポートを許可します。
dest-port *port-num*	フィルタする宛先ポートを指定します。有効値は 1 ～ 100 です。
destination *ip-addr ip-mask*	フィルタする宛先 IP アドレスおよびマスクを指定します。
protocol	追加または除外対象のプロトコルを指定します。
tcp	TCP を追加または除外対象にします。
udp	UDP を追加または除外対象にします。
source *ip-addr ip-mask*	フィルタする送信元 IP アドレスおよびサブネット マスクビットを指定します。
src-port *port-num*	フィルタする送信元ポートを指定します。

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。

- すべての期限切れフローはインポートされます。
- インターフェイスのエクスポートはディセーブルです（**no mls nde interface**）。

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

mls nde flow コマンドは、NDE にフィルタリングを追加します。指定された基準と一致する期限切れフローがエクスポートされます。これらの値は NVRAM に保存され、NDE をディセーブルにしてもクリアされません。このコマンドにオプションを指定しなかった場合は、ワイルドカードとして処理されます。NVRAM 内の NDE フィルタは、NDE をディセーブルにしてもクリアされません。

同時にアクティブにできるフィルタは、1 つだけです。**exclude** または **include** キーワードを入力しなかった場合は、フィルタは包含フィルタとして使用されます。

包含および排除フィルタは NVRAM に保存され、NDE をディセーブルにしても削除されません。

ip-addr/maskbits は、サブネット アドレスの簡易ロング フォーマットです。マスク ビットは、ネットワーク マスクのビット数を指定します。たとえば、172.25.2.1/22 は、22 ビット サブネット アドレスを示します。*ip-addr* は、193.22.253.1/22 のような完全ホスト アドレスです。

例

次に、宛先ポート 23 への期限切れフローだけがエクスポートされるように、インターフェイス フロー フィルタを指定する例を示します（フロー マスクは ip-flow に設定されているものと想定します）。

```
Router(config)# mls nde flow include dest-port 23
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls nde interface

NDE パケットに追加フィールドを入力するには、**mls nde interface** コマンドを使用します。追加フィールドの入力をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls nde interface

no mls nde interface

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

イネーブル

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

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

NDE パケットに次の追加フィールドを入力するように、NDE を設定できます。

- 出力インターフェイス SNMP インデックス
- 送信元自律システム番号
- 宛先自律システム番号
- ネクスト ホップ ルータの IP アドレス

フロー マスクが interface-full または interface-src-dst の場合、入力インターフェイス SNMP インデックスは必ず入力されます。

詳細については、『*Catalyst Supervisor Engine 32 PISA Cisco IOS Software Configuration Guide Release 12.2ZY*』の「Configuring NDE」の章を参照してください。

例

次に、NDE パケットに追加フィールドを入力する例を示します。

```
Router(config)# mls nde interface
Router(config)#
```

次に、追加フィールドの入力をディセーブルにする例を示します。

```
Router(config)# no mls nde interface
Router(config)#
```

関連コマンド

コマンド	説明
mls netflow	NetFlow で統計収集を可能にします。
mls netflow sampling	インターフェイス上でサンプリング済み NetFlow をイネーブルにします。

mls nde sender

MLS NDE エクスポートをイネーブルにするには、**mls nde sender** コマンドを使用します。MLS NDE エクスポ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。

mls nde sender [**version** *version*]

no mls nde sender

シンタックスの説明

version *version*	（任意）NDE を指定します。有効値は **5** および **7** 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。

- MLS NDE エクスポートはディセーブルです。
- *version* は **7** 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。

例

次に、MLS NDE エクスポートをイネーブルにする例を示します。

```
Router(config)# mls nde sender
Router(config)#
```

次に、MLS NDE エクスポートをディセーブルにする例を示します。

```
Router(config)# no mls nde sender
Router(config)#
```

関連コマンド

コマンド	説明
show mls nde	NDE ハードウェアによってスイッチングされるフローに関する情報を表示します。

mls netflow

統計情報を収集する NetFlow をイネーブルにするには、**mls netflow** コマンドを使用します。NetFlow による統計収集をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls netflow

no mls netflow

シンタックスの説明

interface	（任意）インターフェイス単位の統計情報収集を指定します。

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

NetFlow は、Catalyst 6500 シリーズ スイッチを流れるトラフィックから統計情報を収集し、その統計情報を NetFlow テーブルに保存します。プロトコルに基づいてグローバルに、またはインターフェイス単位（任意）で統計情報を収集できます。

NDE、またはハードウェア NetFlow テーブルを使用する Cisco IOS 機能（micro-flow QoS、WCCP、TCP Intercept、または再帰 ACL）を使用していない場合は、グローバル コンフィギュレーション モードで **no mls netflow** コマンドを使用して、ハードウェア NetFlow テーブルの使用およびメンテナンスを安全にディセーブルにできます。

例

次に、統計情報を収集する例を示します。

```
Router(config)# mls netflow
Router(config)#
```

次に、統計情報収集の NetFlow をディセーブルにする例を示します。

```
Router(config)# no mls netflow
Disabling MLS netflow entry creation.
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow	NetFlow ハードウェアに関する設定情報を表示します。

mls netflow maximum-flows

NetFlow テーブルの最大フロー割り当てを設定するには、**mls netflow maximum-flows** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls netflow maximum-flows [*maximum-flows*]

no mls netflow maximum-flows

シンタックスの説明

maximum-flows	（任意）フローの最大数。有効値は、**16**、**32**、**64**、**80**、**96**、および **128** です。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

128

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

フローの最大数に指定する値は、その 1000 倍の値になります。たとえば、32 を入力すると、許可されたフローの最大数は 32000 に指定されます。

例

次に、NetFlow テーブルの最大フロー割り当てを設定する例を示します。

```
Router(config)# mls netflow maximum-flows 96
Router(config)#
```

次に、デフォルト設定に戻す例を示します。

```
Router(config)# no mls netflow maximum-flows
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow table-contention	NetFlow ハードウェアの table contention level（TCL; テーブル コンテンション レベル）の設定情報を表示します。

mls netflow sampling

インターフェイス上でサンプリング済み NetFlow をイネーブルにするには、**mls netflow sampling** コマンドを使用します。サンプリング済み NetFlow をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls netflow sampling

no mls netflow sampling

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

インターフェイス 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

サンプリングをイネーブルにするには、**mls sampling** コマンドおよび **mls netflow sampling** コマンドを適切なインターフェイスで入力する必要があります。**mls netflow sampling** コマンドを入力しないと、NDE はフローをエクスポートしません。

現在のフロー マスクに応じて、サンプリング済み NetFlow をグローバルに、またはインターフェイス単位で設定できます。Interface-Full および Interface-Src-Dest フロー マスクの場合、サンプリング済み NetFlow はインターフェイス単位でイネーブル化されます。その他のすべてのフロー マスクの場合、サンプリング済み NetFlow は常にグローバルであり、すべてのインターフェイスに対して一括でイネーブルまたはディセーブルになります。

サンプリング済み NetFlow をグローバルにイネーブルにするには、**mls sampling** コマンドを入力します。

例

次に、インターフェイス上でサンプリング済み NetFlow をイネーブルにする例を示します。

```
Router(config-if)# mls netflow sampling
Router(config-if)#
```

次に、インターフェイス上でサンプリング済み NetFlow をディセーブルにする例を示します。

```
Router(config-if)# no mls netflow sampling
Router(config-if)#
```

関連コマンド

コマンド	説明
mls sampling	サンプリング済み NetFlow のイネーブル化およびサンプリング方式の指定を行います。
show mls sampling	サンプリング済み NDE ステータスに関する情報を表示します。

mls netflow usage notify

スイッチ プロセッサ上での NetFlow テーブル使用率をモニタするには、**mls netflow usage notify** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls netflow usage notify {*threshold interval*}

no mls netflow usage notify

シンタックスの説明

threshold	超過した場合に警告メッセージを表示するしきい値パーセンテージ。有効値は、20 ～ 100% です。
interval	NetFlow テーブル使用率が確認される頻度。有効値は、120 ～ 1,000,000 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

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

NetFlow テーブル使用のモニタリングがイネーブルで、NetFlow テーブル使用がしきい値パーセンテージを超えると、警告メッセージが表示されます。

NetFlow は、Catalyst 6500 シリーズ スイッチを流れるトラフィックから統計情報を収集し、その統計情報を NetFlow テーブルに保存します。プロトコルに基づいてグローバルに、またはインターフェイス単位（任意）で統計情報を収集できます。

NDE、またはハードウェア NetFlow テーブルを使用する Cisco IOS 機能（micro-flow QoS、WCCP、TCP Intercept、または再帰 ACL）を使用していない場合は、グローバル コンフィギュレーション モードで **no mls netflow** コマンドを使用して、ハードウェア NetFlow テーブルの使用およびメンテナンスを安全にディセーブルにできます。

例

次に、スイッチ プロセッサに NetFlow テーブル使用率のモニタを設定する例を示します。

```
Router(config)# mls netflow usage notify 80 300
Router(config)#
```

関連コマンド

コマンド	説明
show mls netflow usage	NetFlow ハードウェアに関する設定情報を表示します。

mls qos (global configuration mode)

QoS 機能をグローバルにイネーブルにするには、**mls qos** コマンドを使用します。QoS 機能をグローバルにディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos

no mls qos

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

QoS はグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション（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 がグローバルにイネーブルの場合は、QoS がディセーブル化されているインターフェイスを除いて、すべてのインターフェイスで QoS がイネーブルになります。QoS がグローバルにディセーブルの場合は、すべてのトラフィックが QoS パススルー モードで渡されます。

ポートキューイング モードでは、PFC QoS（マーキングおよびポリシング）はディセーブルであり、パケットの Type of Service（ToS; サービス タイプ）および CoS は PFC で変更されません。受信および送信に関するすべてのキューイングは、着信パケットの QoS タグに基づいて行われます。この QoS タグは、着信 CoS に基づきます。

802.1Q または ISL カプセル化ポート リンクでは、キューイングはパケット 802.1Q または ISL CoS に基づいて行われます。

ルータのメイン インターフェイスまたはアクセス ポートでは、キューイングは設定されたポート単位の CoS（デフォルト CoS は 0）に基づいて行われます。

このコマンドは、オフの状態のすべてのインターフェイス上で TCAM QoS をイネーブルまたはディセーブルにできます。

例

次に、QoS をグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos
Router(config)#
```

次に、Catalyst 6500 シリーズ スイッチで QoS をグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos
Router(config)#
```

関連コマンド

コマンド	説明
mls qos (interface configuration mode)	インターフェイス上の QoS 機能をイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos (interface configuration mode)

インターフェイス上で QoS 機能をイネーブルにするには、**mls qos** コマンドを使用します。QoS 機能をインターフェイス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。

mls qos

no mls qos

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

イネーブル

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

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

CLI を使用すると、OC-12 ATM OSM の WAN ポートおよびチャネライズド OSM の WAN ポートに PFC ベースの QoS を設定できますが、PFC ベースの QoS はこれらの OSM の WAN ポートではサポートされていません。

QoS をグローバルにディセーブルにすると、すべてのインターフェイスでディセーブルになります。

このコマンドは、インターフェイスの TCAM QoS（分類、マーキング、およびポリシング）をイネーブルまたはディセーブルにします。

例

次に、インターフェイス上で QoS をイネーブルにする例を示します。

```
Router(config-if)# mls qos
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos aggregate-policer

ポリシー マップで使用する名前付き集約ポリサーを定義するには、**mls qos aggregate-policer** コマンドを使用します。このポリサーは、異なったポリシー マップ クラスおよび異なったインターフェイスで共有できます。名前付き集約ポリサーを削除するには、このコマンドの **no** 形式を使用します。

mls qos aggregate-policer *name rate-bps*

mls qos aggregate-policer *name rate-bps burst-bytes maximum-burst-bytes*

mls qos aggregate-policer *name rate-bps* [{**conform-action** {**drop** [**exceed-action** *action*]}} | {**set-dscp-transmit** [*new-dscp*]} | {**set-prec-transmit** [*new-precedence*]} | {**transmit** [{**exceed-action** *action*} | {**violate-action** *action*]}}

mls qos aggregate-policer *aggregate-name rate-bps* {**pir** *peak-rate-bps* [{**conform-action** {**drop** [**exceed-action** *action*]}} | {**set-dscp-transmit** [*new-dscp*]} | {**set-prec-transmit** [*new-precedence*]} | {**transmit** [{**exceed-action** *action*}} | {**violate-action** *action*}]]}

no mls qos aggregate-policer *name*

シンタックスの説明

name	集約ポリサー名
rate-bps	最大 bps。有効値は、32000 ～ 10,000,000,000 です。
burst-bytes	バースト バイト。有効値は 1000 ～ 31,250,000 です。
maximum-burst-bytes	最大バースト バイト。有効値は 1000 ～ 31,250,000 です（入力する場合は、標準バースト バイトと同じ値に設定する必要があります）。
conform-action	（任意）レートが超えない場合に実行するアクションを指定します。
drop	（任意）パケットを廃棄します。
exceed-action *action*	（任意）QoS 値を超えた場合に実行する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。
set-dscp-transmit	DSCP 値を設定し、パケットを送信します。
new-dscp	（任意）新しい DSCP 値。有効値は 0 ～ 63 です。
set-prec-transmit	パケットの優先順位を書き換えて、パケットを送信します。
new-precedence	（任意）新しい優先順位値。有効値は 0 ～ 7 です。
violate-action *action*	（任意）QoS 値に違反した場合に実行する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。
pir peak-*rate-bps*	Peak Information Rate（PIR; 最大情報レート）ピーク レートを設定します。有効値は 32000 ～10,000,000,000 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。

- *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

action の有効値は次のとおりです。

- **drop**：パケットを廃棄します。
- **policed-dscp-transmit**：ポリシング済み DSCP マップごとに DSCP を変更して、送信します。
- **transmit**：パケットを伝送します。

Catalyst 6500 シリーズ スイッチでは、1023 までの集約規則および 1023 までのポリシング規則がサポートされます。

mls qos aggregate-policer コマンドを使用すると、集約フローおよびその集約のポリシング規則を設定できます。レートおよびバースト パラメータを入力すると、平均レートの範囲は 32 Kbps ～ 4 Gbps（それぞれ 32000、4000000000 と入力）となり、バースト サイズの範囲は 1 KB（1000 と入力）～ 512 MB（512000000 と入力）となります。既存の集約レート制限エントリを変更すると、そのエントリが使用中の場合には、NVRAM および Catalyst 6500 シリーズ スイッチのエントリが変更されます。

（注） ハードウェア粒度のため、レート値が制限されます。そのため、設定したバースト値が使用されない場合があります。

既存のマイクロフローまたは集約レート制限を変更すると、使用中の場合には NVRAM および Catalyst 6500 シリーズ スイッチのエントリが変更されます。

集約ポリサー名を入力する場合、次の命名規則に従います。

- 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（_）、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。
- 番号は使用できません。
- 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。

例

次に、QoS 集約ポリサーが最大 100,000 bps および 10,000 バイトの標準バースト サイズを許可し、これらのレートを超過しない場合には DSCP を 48 に設定し、これらのレートを超過した場合にはパケットを廃棄するよう設定する例を示します。

```
Router(config)# mls qos aggregate-policer micro-one 100000 10000 conform-action set-dscp
48 exceed action drop
Router(config)#
```

関連コマンド

コマンド	説明
set ip dscp (policy-map configuration)	ToS バイトの IP DSCP を設定してパケットにマーキングします。

mls qos bridged

レイヤ 3 の LAN インターフェイス上でブリッジド トラフィックのマイクロフロー ポリシングをイネーブルにするには、**mls qos bridged** コマンドを使用します。ブリッジド トラフィックのマイクロフロー 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。

mls qos bridged

no mls qos bridged

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

インターフェイス 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

このコマンドをサポートするのは、SVI だけです。

例

次に、VLAN インターフェイスのブリッジド トラフィックに対してマイクロフロー ポリシングをイネーブルにする例を示します。

```
Router(config-if)# mls qos bridged
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls qos	MLS QoS 情報を表示します。

mls qos channel-consistency

EtherChannel バンドリングに関する QoS ポート属性チェックをイネーブルにするには、**mls qos channel-consistency** コマンドを使用します。EtherChannel バンドリングに関する QoS ポート属性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。

mls qos channel-consistency

no mls qos channel-consistency

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

イネーブル

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

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

mls qos channel-consistency コマンドは、ポート チャネルだけでサポートされています。

例

次に、EtherChannel バンドリングに関する QoS ポート属性チェックをイネーブルにする例を示します。

```
Router(config-if)# mls qos channel-consistency
Router(config-if)#
```

次に、EtherChannel バンドリングに関する QoS ポート属性チェックをディセーブルにする例を示します。

```
Router(config-if)# no mls qos channel-consistency
Router(config-if)#
```

mls qos cos

インターフェイスのデフォルトの CoS 値を定義するには、**mls qos cos** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos cos *cos-value*

no mls qos cos *cos-value*

シンタックスの説明

cos-value	インターフェイスのデフォルト CoS 値。有効値は 0 ～ 7 です。

コマンドのデフォルト

デフォルト設定は次のとおりです。

- *cos-value* は **0** です。
- CoS の上書きは設定されていません。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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

CoS 値は、物理 LAN ポートだけで設定できます。

例

次に、デフォルト QoS CoS 値を 6 に設定する例を示します。

```
Router(config-if)# mls qos cos 6
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls qos	MLS QoS 情報を表示します。

mls qos cos-mutation

入力 CoS 変換マップをインターフェイスに付加するには、**mls qos cos-mutation** コマンドを使用します。インターフェイスから入力 CoS 変換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。

mls qos cos-mutation *cos-mutation-table-name*

no mls qos cos-mutation

シンタックスの説明

cos-mutation-table-name	入力 CoS 変換テーブル名

コマンド モード

テーブルは定義されていません。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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、入力 CoS 変換マップ（mutemap2）を付加する例を示します。

```
Router(config-if)# mls qos cos-mutation mutemap2
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos map cos-mutation	パケットの CoS を新しい CoS 値にマッピングします。
show mls qos	MLS QoS 情報を表示します。

mls qos dscp-mutation

出力 DSCP 変換マップをインターフェイスに付加するには、**mls qos dscp-mutation** コマンドを使用します。インターフェイスから出力 DSCP 変換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。

mls qos dscp-mutation *dscp-mutation-table-name*

no mls qos dscp-mutation

シンタックスの説明

dscp-mutation-table-name	出力 DSCP 変換テーブル名

コマンド モード

テーブルは定義されていません。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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、出力 DSCP 変換マップ（mutemap1）を付加する例を示します。

```
Router(config-if)# mls qos dscp-mutation mutemap1
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos map dscp-mutation	指定した DSCP 変換マップを定義します。
show mls qos	MLS QoS 情報を表示します。

mls qos exp-mutation

出力 EXP 変換マップをインターフェイスに付加するには、**mls qos exp-mutation** コマンドを使用します。インターフェイスから出力 EXP 変換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。

mls qos exp-mutation *exp-mutation-table-name*

no mls qos exp-mutation

シンタックスの説明

exp-mutation-table-name	出力 EXP 変換テーブル名

コマンドのデフォルト

テーブルは定義されていません。

コマンド モード

インターフェイス コンフィギュレーション

コマンドの履歴

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、出力 EXP 変換マップ（mutemap2）を付加する例を示します。

```
Router(config-if)# mls qos exp-mutation mutemap2
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos map dscp-mutation	指定した DSCP 変換マップを定義します。
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos loopback

ループバック ケーブルを介した VLAN の SVI フラッドからルータ ポートを削除するには、**mls qos loopback** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos loopback

no mls qos loopback

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

コマンドのデフォルト　インターフェイス コンフィギュレーション

コマンドの履歴

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　インターフェイスに **mls qos loopback** コマンドを適用すると、パケットはそのインターフェイスに対して転送されなくなります。

mls qos loopback コマンドを入力する前に、OSM インターフェイスの MAC アドレスを指定する必要があります。MAC アドレスは、PFC2 ハードウェア スイッチングに使用される LAN ルータの MAC アドレスとは異なるものを設定します。

例　次に、パケットをそのインターフェイスに対して転送しないようにする例を示します。

```
Router (config-if)# mls qos loopback
Router (config-if)#
```

mls qos map cos-dscp

信頼されたインターフェイスに入力 CoS/DSCP マップを定義するには、**mls qos map cos-dscp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map cos-dscp *values*

no mls qos map cos-dscp

シンタックスの説明

values	スペースで区切った、CoS 値に対応する 8 つの DSCP 値。有効値は 0 ～ 63 です。

コマンド モード

表 2-16 に、デフォルトの CoS/DSCP 設定を示します。

表 2-16　デフォルトの CoS/DSCP マッピング

CoS	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンドのデフォルト

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

CoS/DSCP マップは、信頼されたインターフェイス（またはフロー）に着信したパケットの CoS を、信頼タイプが trust-cos である DSCP にマッピングする場合に使用します。このマップは、8 つの CoS 値（0 ～ 7）およびこれに対応する DSCP 値のテーブルです。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

例

次に、信頼されたインターフェイスに入力 CoS/DSCP マッピングを設定する例を示します。

```
Router(config)# mls qos map cos-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map ip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
mls qos map policed-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map cos-mutation

パケットの CoS を新しい CoS 値にマッピングするには、**mls qos map cos-mutation** コマンドを使用します。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。

mls qos map cos-mutation *name mutated_cos1 mutated_cos2 mutated_cos3 mutated_cos4 mutated_cos5 mutated_cos6 mutated_cos7 mutated_cos8*

no mls qos map cos-mutation *name*

シンタックスの説明

name	CoS マップ名
mutated_cos1 … *mutated_cos8*	スペースで区切った、8 つの CoS 出力値。有効値は 0 ～ 7 です。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 モード

表 2-17 に、CoS/CoS 変換マップが設定されていない場合のデフォルトの CoS/CoS 変換マッピングを示します。

表 2-17　デフォルトの CoS/CoS マッピング

CoS 入力	0	1	2	3	4	5	6	7
CoS 出力	0	1	2	3	4	5	6	7

コマンドのデフォルト

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

次のモジュールを搭載した Catalyst 6500 シリーズ スイッチだけで、このコマンドはサポートされます。

- WS-X6704-10GE
- WS-X6724-SFP
- WS-X6748-GE-TX

CoS 変換は非 802.1Q トンネル ポートではサポートされません。

mls qos map cos-mutation コマンドを入力すると、変換 CoS 値は、シーケンス番号にマッピングされます。たとえば、**mls qos map cos-mutation 2 3 4 5 6 7 0 1** コマンドを入力すると、次のようなマップが設定されます。

CoS 入力	0	1	2	3	4	5	6	7
CoS 出力	2	3	4	5	6	7	0	1

8 つの CoS 値はスペースで区切ります。

マップをグローバル コンフィギュレーション モードで定義したあと、マップをポートに付加できます。

QoS がディセーブルにされていると、ポートは CoS 信頼モードおよび 802.1Q トンネリング モードになりません。ポートを CoS 信頼モードにし、ポートが 802.1Q トンネル ポートとして設定されれば、変更されます。

802.1Q トンネル ポートでの入力 CoS 変換をサポートしますが、ポート グループ単位ベースだけです。

入力 CoS 変換コンフィギュレーションを失敗しないようにするには、すべてのメンバー ポートが入力 CoS 変換をサポートする EtherChannel だけを作成するか、またはどのメンバーも入力 CoS 変換をサポートしない EtherChannel だけを作成します。入力 CoS 変換のサポートと非サポートが混在するような EtherChannel を作成しないでください。

EtherChannel のメンバーであるポートに入力 CoS 変換を設定する場合、入力 CoS 変換はポートチャネル インターフェイスに適用されます。

入力 CoS 変換をポートチャネル インターフェイスに設定できます。

例

次に、CoS/CoS マップを定義する例を示します。

```
Router(config)# mls qos map cos-mutation test-map 5 4 3 to 1
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map dscp-cos

出力 DSCP/CoS マップを定義するには、**mls qos map dscp-cos** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map dscp-cos *dscp-values* **to** *cos-values*

no mls qos map dscp-cos

シンタックスの説明

dscp-values	DSCP 値。有効値は、0 ～ 63 です。
to	マッピングを定義します。
cos-values	CoS 値。有効値は、0 ～ 63 です。

コマンド モード

表 2-18 に、デフォルトの DSCP/CoS マップを示します。

表 2-18　デフォルトの DSCP/CoS マップ

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
CoS	0	1	2	3	4	5	6	7

コマンドのデフォルト

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

DSCP/CoS マップは、最終 DSCP 分類を最終 CoS にマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。CoS マップは、トランク インターフェイス上の送信済みパケットの ISL ヘッダーまたは 802.1Q タグに書き込まれます。CoS マップには、64 個の DSCP 値およびこれに対応する CoS 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。スペースで区切ることにより最大 8 つの CoS 値を入力できます。

例

次に、信頼されたインターフェイスに出力 DSCP/CoS マップを設定する例を示します。

```
Router(config)# mls qos map dscp-cos 20 25 to 3
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map dscp-exp

最終 DSCP 分類を最終 EXP 値に定義するには、**mls qos map dscp-exp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map dscp-exp *dscp-values* **to** *exp-values*

no mls qos map dscp-exp

シンタックスの説明

dscp-values	DSCP 値。有効値は、0 ～ 63 です。
to	マッピングを定義します。
exp-values	EXP 値。有効値は、0 ～ 7 です。

コマンド モード

表 2-19 に、デフォルトの DSCP/EXP マップを示します。

表 2-19　デフォルトの DSCP/EXP マップ

DSCP	0-7	8-15	16-23	24-31	32-39	40-47	48-55	56-63
EXP	0	1	2	3	4	5	6	7

コマンドのデフォルト

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

DSCP/EXP マップは、最終 DSCP 分類を最終 EXP にマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。EXP マップには、64 個の DSCP 値およびこれに対応する EXP 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。スペースで区切ることにより最大 8 つの EXP 値を入力できます。

例

次に、最終 DSCP 分類を最終 EXP 値に設定する例を示します。

```
Router(config)# mls qos map dscp-exp 20 25 to 3
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map dscp-mutation

名前付き DSCP 変換マップを定義するには、**mls qos map dscp-mutation** 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。

mls qos map dscp-mutation *map-name input-dscp1* [*input-dscp2* [*input-dscp3* [*input-dscp4* [*input-dscp5* [*input-dscp6* [*input-dscp7* [*input-dscp8*]]]]]]] **to** *output-dscp*

no mls qos map dscp-mutation *map-name*

シンタックスの説明

map-name	DSCP 変換マップ名
input-dscp#	内部 DSCP 値。有効値は 0 ～ 63 です。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。
to	マッピングを定義します。
output-dscp	出力 DSCP 値。有効値は 0 ～ 63 です。

コマンドのデフォルト

output-dscp は *input-dscp* 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

名前付き DSCP 変換マップを設定する場合、次のことに注意してください。

- 変換された DSCP 値にマッピングする入力 DSCP 値を、最大 8 つ入力できます。
- コマンドを複数入力して、変換された DSCP 値にマッピングする DSCP 値を追加できます。
- 個々の変換された DSCP 値に対して、個別のコマンドを入力できます。

出力 DSCP 値として書き込まれる前に内部 DSCP 値を変換するために、15 個の出力 DSCP 変換マップを設定できます。PFC QoS が対応する任意のインターフェイスに対して、出力 DSCP 変換マップを付加できます。

PFC QoS は、内部 DSCP 値から出力 CoS 値を取得します。出力 DSCP 変換を設定した場合は、PFC QoS は変換された DSCP 値から出力 CoS 値を取得しません。

例

次に、DSCP 30 を変換された DSCP 値 8 にマッピングする例を示します。

```
Router(config)# mls qos map dscp-mutation mutemap1 30 to 8
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map exp-dscp

内部 DSCP マップに入力 EXP 値を定義するには、**mls qos map exp-dscp** コマンドを使用します。デフォルト マップに戻すには、このコマンドの **no** 形式を使用します。

mls qos map exp-dscp *dscp-values*

no mls qos map exp-dscp

シンタックスの説明

dscp-values	内部 DSCP 値を指定。有効値は、0 ～ 63 です。

コマンドのデフォルト

表 2-20 に、デフォルトの EXP/DSCP マップを示します。

表 2-20　デフォルトの EXP/DSCP マップ

EXP	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンド モード

グローバル コンフィギュレーション（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

これらのマップの DSCP とは、パケット DSCP ではなく内部 DSCP を意味します。

EXP/DSCP マップは、受信された EXP 値を内部 DSCP マップにマッピングする場合に使用します。この最終マップにより、パケットが割り当てられる出力キューおよびしきい値が決まります。EXP マップには、64 個の DSCP 値およびこれに対応する EXP 値のテーブルが含まれます。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。

例

次に、受信された EXP を内部 DSCP 値に設定する例を示します。

```
Router(config)# mls qos map exp-dscp 20 25 30 31 32 32 33 34
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map exp-mutation	パケットの EXP を新しい EXP 値にマッピングします。
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos map exp-mutation

パケットの EXP を新しい EXP 値にマッピングするには、**mls qos map exp-mutation** コマンドを使用します。デフォルト マップに戻すには、このコマンドの **no** 形式を使用します。

mls qos map exp-mutation *map-name mutated-exp1 mutated-exp2 mutated-exp3 mutated-exp4 mutated-exp5 mutated-exp6 mutated-exp7 mutated-exp8*

no mls qos map exp-mutation *map-name*

シンタックスの説明

map-name	EXP 変換マップ名
mutated-exp#	スペースで区切った、8 つの EXP 値。有効値は 0 ～ 7 です。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

表 2-21 に、EXP/EXP 変換マップが設定されていない場合のデフォルトの EXP/EXP 変換マッピングを示します。

表 2-21　デフォルトの EXP/EXP マップ

EXP 入力	0	1	2	3	4	5	6	7
EXP 出力	0	1	2	3	4	5	6	7

コマンド モード

グローバル コンフィギュレーション（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

mls qos map exp-mutation コマンドを入力すると、変換された EXP 値は一連の EXP シーケンス番号にマッピングされます。たとえば、**mls qos map exp-mutation 2 3 4 5 6 7 0 1** コマンドを入力すると、次のようなマップが設定されます。

EXP 入力	0	1	2	3	4	5	6	7
EXP 出力	2	3	4	5	6	7	0	1

8 つの EXP 値はスペースで区切ります。

マップをグローバル コンフィギュレーション モードで定義したあと、マップをポートに付加できます。

入力 EXP 値として書き込まれる前に内部 EXP 値を変換するために、15 個の入力 EXP 変換マップを設定できます。PFC QoS が対応する任意のインターフェイスに対して、入力 EXP 変換マップを付加できます。

PFC QoS は、内部 DSCP 値から出力 EXP 値を取得します。入力 EXP 変換を設定した場合は、PFC QoS は変換された EXP 値から入力 EXP 値を取得しません。

例

次に、パケットの EXP を新しい EXP 値にマッピングする例を示します。

```
Router(config)# mls qos map exp-mutation mutemap1 1 2 3 4 5 6 7 0
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map exp-dscp	内部 DSCP マップに入力 EXP 値を定義します。
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos map ip-prec-dscp

信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義するには、**mls qos map ip-prec-dscp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map ip-prec-dscp *dscp-values*

no mls qos map ip-prec-dscp

シンタックスの説明

dscp-values	IP precedence 値 0 ～ 7 に対応する DSCP 値。有効値は 0 ～ 63 です。

コマンドのデフォルト

表 2-22 に、デフォルトの IP precedence/DSCP 設定を示します。

表 2-22　デフォルトの IP precedence/DSCP マップ

IP precedence	0	1	2	3	4	5	6	7
DSCP	0	8	16	24	32	40	48	56

コマンドのデフォルト

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

このコマンドは、信頼されたインターフェイス（またはフロー）に着信した IP パケットの IP precedence を、信頼タイプが trust-ipprec である DSCP にマッピングする場合に使用します。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。

このマップは、8 つの優先順位値（0 ～ 7）およびこれに対応する DSCP 値のテーブルです。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。IP precedence 値は次のとおりです。

- network **7**
- internet **6**
- critical **5**
- flash-override **4**
- flash **3**
- immediate **2**
- priority **1**
- routine **0**

例

次に、信頼されたインターフェイスに入力 IP precedence/DSCP マッピングを設定する例を示します。

```
Router(config)# mls qos map ip-prec-dscp 20 30 1 43 63 12 13 8
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map policed-dscp	ポリシング済み DSCP 値とマーキング済み DSCP 値のマップを設定します。
show mls qos maps	QoS マップ設定およびランタイム バージョンに関する情報を表示します。

mls qos map policed-dscp

DSCP マークダウン マップを設定するには、**mls qos map policed-dscp** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls qos map policed-dscp {**normal-burst** | **max-burst**} *dscp1* [*dscp2* [*dscp3* [*dscp4* [*dscp5* [*dscp6* [*dscp7* [*dscp8*]]]]]]] **to** *policed-dscp*

no mls qos map policed-dscp

シンタックスの説明

normal-burst	**exceed-action policed-dscp-transmit** キーワードによって使用されるマークダウン マップを設定します。
max-burst	**violate-action policed-dscp-transmit** キーワードによって使用されるマークダウン マップを設定します。
dscp1	DSCP 値。有効値は、0 ～ 63 です。
dscp2 ～ *dscp8*	（任意）DSCP 値。有効値は、0 ～ 63 です。
to	マッピングを定義します。
policed-dscp	ポリシング済み DSCP 値を指定します。有効値は、0 ～ 63 です。

コマンドのデフォルト

マーキング済みの値は設定されていません。

コマンド モード

グローバル コンフィギュレーション（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

DSCP/ポリシング済み DSCP マップにより、不適合なフローに適用されるマーキング済み DSCP 値が決定します。Catalyst 6500 シリーズ スイッチには 1 つのマップがあります。

スペースで区切ることにより最大 8 つの DSCP 値を入力できます。

スペースで区切ることにより最大 8 つのポリシング済み DSCP 値を入力できます。

（注） シーケンス外パケットを避けるため、DSCP/ポリシング済み DSCP マップを設定して、マーキング済みパケットが適合トラフィックと同じキューに留まるようにします。

例

次に、複数の DSCP を単一のポリシング済み DSCP 値にマッピングする例を示します。

```
Router(config)# mls qos map policed-dscp normal-burst 20 25 43 to 4
Router(config)#
```

関連コマンド

コマンド	説明
mls qos map cos-dscp	信頼されたインターフェイスに入力 CoS/DSCP マップを定義します。
mls qos map dscp-cos	出力 DSCP/CoS マップを定義します。
mls qos map ip-prec-dscp	信頼されたインターフェイスに入力 IP precedence/DSCP マップを定義します。
show mls qos	MLS QoS 情報を表示します。

mls qos marking ignore port-trust

インターフェイスが信頼されていてもパケットをマークするには、**mls qos marking ignore port-trust** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos marking ignore port-trust

no mls qos marking ignore port-trust

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

ポート信頼はイネーブルです。

コマンドのデフォルト

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

インターフェイスが信頼されていてもパケットをマークするには、**mls qos marking ignore port-trust** コマンドを使用します。

例

次に、インターフェイスが信頼されていてもパケットをマークする例を示します。

```
Router(config)# mls qos marking ignore port-trust
Router(config)#
```

次に、ポート信頼をイネーブルにする例を示します。

```
Router(config)# no mls qos marking ignore port-trust
Router(config)#
```

関連コマンド

mls qos trust

mls qos marking statistics

ポリサー トラフィック クラス ID の設定済みアクションへの割り当てをディセーブルにするには、**mls qos marking statistics** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos marking statistics

no mls qos marking statistics

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

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

ポリシー マップ統計情報を表示するには、**show policy-map interface** コマンドを使用します。

例

次に、ポリサー トラフィック クラス ID の設定済みアクションへの割り当てをディセーブルにする例を示します。

```
Router(config)# mls qos marking statistics
Router(config)#
```

次に、ポリサー トラフィック クラス ID の設定済みアクションへの割り当てを許可する例を示します。

```
Router(config)# no mls qos marking statistics
Router(config)#
```

関連コマンド

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

mls qos mpls trust exp

MPLS パケットだけの信頼状態を設定するには、**mls qos mpls trust exp** コマンドを使用します。MPLS パケットの信頼状態を信頼不可に設定するには、このコマンドの **no** 形式を使用します。

mls qos mpls trust exp

no qos mpls trust exp

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

信頼状態がイネーブルである場合、デフォルトは次のとおりです。

- 信頼不可：パケットは 0 に、またはポリシーによってマークされます。
- trust-cos

信頼状態がディセーブルである場合、デフォルトは次のとおりです。

- trust-exp：ポート / ポリシー信頼状態は無視されます。
- パケットはポリシーによってマークされます。

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

CoS および出力キューイングのため（たとえば、ポートまたはポリシーの信頼を適用）、MPLS パケットを別のレイヤ 2 パケットとして扱うには、**mls qos mpls trust exp** コマンドを入力できます。すべて信頼される場合（CoS/IP/DSCP を信頼）は、trust-cos として扱われます。

例

次に、MPLS パケットの信頼状態を trust-cos に設定する例を示します。

```
Router(config-if)# mls qos mpls trust exp
Router(config-if)#
```

次に、MPLS パケットの信頼状態を信頼不可に設定する例を示します。

```
Router(config-if)# no mls qos mpls trust exp
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls qos mpls	ポリシー マップの MPLS QoS クラスのインターフェイス概要を表示します。

mls qos police redirected

ACL リダイレクト パケットのポリシングをオンにするには、**mls qos police redirected** コマンドを使用します。ACL リダイレクト パケットのポリシングをオフに切り替えるには、このコマンドの **no** 形式を使用します。

mls qos police redirected

no mls qos police redirected

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

イネーブル

コマンドのデフォルト

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 リダイレクト パケットを必要としない代わりに）NDE の精度を必要とする場合、**no mls qos police redirected** コマンドを使用します。

例

次に、ACL リダイレクト パケットのポリシングをオンにする例を示します。

```
Router(config)# mls qos police redirected
Router(config)#
```

次に、ACL リダイレクト パケットのポリシングをオフにする例を示します。

```
Router(config)# no mls qos police redirected
Router(config)#
```

関連コマンド

コマンド	説明
show platform earl-mode	プラットフォーム情報を表示します。

mls qos protocol

ルーティング プロトコル パケットのポリシングを定義するには、**mls qos protocol** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos protocol *protocol-name* {**pass-through** | {**police** *rate burst*} | {**precedence** *value* [**police** *rate burst*]}}

no mls qos protocol

シンタックスの説明

protocol-name	プロトコル名。有効値は、**arp**、**bgp**、**eigrp**、**igrp**、**isis**、**ldp**、**nd**、**ospf**、および **rip** です。
pass-through	パススルー モードを指定します。
police *rate*	ポリシングする最大のビット/秒（bps）を指定します。有効値は、32,000 ～ 10,000,000,000 bps です。
burst	標準バースト バイト。有効値は 1000 ～ 31,250,000 バイトです。
precedence *value*	プロトコル パケットの書き換え後の IP precedence 値を指定します。有効値は、0 ～ 7 です。

コマンド モード

デフォルト設定は次のとおりです。

- *burst* は、1000 bps です。
- QoS がイネーブルの場合、DSCP は 0 に書き換えられます。
- QoS がディセーブルの場合、ポートはパススルー モード（マーキングまたはポリシングなし）になります。

コマンドのデフォルト

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

precedence *value* キーワードおよび引数を **police** *rate burst* キーワードおよび引数なしで入力すると、信頼できないポートからのパケットだけがマーキングされます。

police *rate*、**pass-through**、または **precedence** *value* キーワードおよび引数を入力すると、プロトコル パケットがインターフェイス単位のポリシー マップを回避するようにできます。

mls qos protocol コマンドにより、次のようにルーティング プロトコル パケット ポリシングを定義できます。

- **pass-through** モードを指定すると、DSCP 値は変更せず、ポリシングされません。
- **police** *rate* を設定すると、DSCP 値は変更せず、ポリシングされます。
- **precedence** *value* を指定すると、信頼できないポートからのパケットの DSCP 値は変更し、DSCP/CoS マップに基づく CoS 値は変更し、トラフィックはポリシングされません。

- **precedence** *value* および **police** *rate* を指定すると、DSCP 値は変更し、DSCP/CoS マップに基づく CoS 値は変更し、DSCP 値はポリシングされます。この場合、DSCP 値の変更は、ポートの信頼状態に基づきます。DSCP 値が変更されるのは、信頼できないポートからのパケットに対してだけです。
- **precedence** *value* を入力しない場合、DSCP 値は MLS QoS がイネーブルであるかどうかに基づきます。詳細は、次のとおりです。
  - MLS QoS がイネーブルでポートが信頼できない場合、内部 DSCP 値は 0 に上書きされます。
  - MLS QoS がイネーブルでポートが信頼できる場合、着信 DSCP 値は維持されます。

パススルー モードを選択した場合、プロトコル パケットが完全にポリシングを避けるようにできます。ポリス モードが選択された場合、指定された CIR がすべての指定プロトコルのパケット（Catalyst 6500 シリーズ スイッチに着信または発信の両方）をポリシングするのに使用されるレートになります。

ARP ブロードキャストからシステムを保護するには、**mls qos protocol arp police** *bps* コマンドを入力します。

例

次に、ルーティング プロトコル パケットのポリシングを定義する例を示します。

```
Router(config)# mls qos protocol arp police 43000
Router(config)#
```

次に、ポリシングを完全に避けるようにする例を示します。

```
Router(config)# mls qos protocol arp pass-through 43000
Router(config)#
```

次に、プロトコル パケットの書き換え後の IP precedence 値を定義する例を示します。

```
Router(config)# mls qos protocol bgp precedence 4
Router(config)#
```

次に、プロトコル パケットの書き換え後の IP-precedence 値を定義し、DSCP 値をポリシングする例を示します。

```
Router(config)# mls qos protocol bgp precedence 4 police 32000
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos protocol	プロトコル パススルー情報を表示します。

mls qos queueing-only

ポートキューイング モードをイネーブルにするには、**mls qos queueing-only** コマンドを使用します。ポートキューイング モードをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos queueing-only

no mls qos queueing-only

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

QoS はグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション（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

ポートキューイング モードでは、PFC QoS （マーキングおよびポリシング）はディセーブルであり、パケットの ToS および CoS は PFC で変更されません。受信および送信に関するすべてのキューイングは、着信パケットの QoS タグに基づいて行われます。この QoS タグは、着信 CoS に基づきます。

802.1Q または ISL カプセル化ポート リンクでは、キューイングはパケット 802.1Q または ISL CoS に基づいて行われます。

ルータのメイン インターフェイスまたはアクセス ポートでは、キューイングは設定されたポート単位の CoS（デフォルト CoS は 0）に基づいて行われます。

例

次に、ポートキューイング モードをグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos queueing-only
Router(config)#
```

次に、ポートキューイング モードをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos queueing-only
Router(config)#
```

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos queue-mode mode-dscp

インターフェイスでキューイング モードを DSCP に設定するには、**mls qos queue-mode mode-dscp** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos queue-mode mode-dscp

no mls qos queue-mode mode-dscp

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

CoS モード

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、10 ギガビット イーサネット ポートだけでサポートされます。

有効なレイヤ 3 DSCP を運ぶトラフィックを受信する場合にだけ DSCP を信頼するようにポートを設定する必要があります。

DSCP ベースの入力キューおよびしきい値を WS-X6708-10GE ポートでイネーブルにして、輻輳を回避できます。

信頼された DSCP ポートからのトラフィックの場合、PFC QoS は、受信した DSCP 値を初期内部 DSCP 値として使用します。PFC QoS は、受信 DSCP を信頼するように設定された入力ポートのトラフィックをマークしません。

例

次の例は、インターフェイスでキューイング モードを DSCP に設定する方法を示しています。

```
Router(config-if)# mls qos queue-mode mode-dscp
Router(config-if)#
```

関連コマンド

コマンド	説明
priority-queue queue-limit	使用可能バッファ スペースをキューに割り当てます。
show mls qos	MLS QoS 情報を表示します。

mls qos rewrite ip dscp

ToS から DSCP への書き換えをイネーブルにするには、**mls qos rewrite ip dscp** コマンドを使用します。ToS から DSCP への書き換えをディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos rewrite ip dscp

no mls qos rewrite ip dscp

シンタックスの説明

このコマンドには、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

QoS はグローバルにディセーブルです。

コマンド モード

グローバル コンフィギュレーション（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

ToS から DSCP への書き換えをディセーブルにして、QoS をグローバルにイネーブルした場合、次のようになります。

- 最終 ToS から DSCP への書き換えがディセーブルになり、ToS から DSCP へのパケットはそのまま保持されます。
- ポリシングおよびマーキングは、QoS 設定に従って動作します。
- キューイングにはマーキングされた CoS が使用されます。
- QoS ディセーブル モードでは、ToS および CoS はそのまま保持されます。

no mls qos rewrite ip dscp コマンドは、MPLS との互換性がありません。デフォルトの **mls qos rewrite ip dscp** コマンドは、PFC3BXL または PFC3B が賦課するラベルの正しい EXP 値を割り当てるように、イネーブルのままにする必要があります。

例

次に、ToS から DSCP への書き換えをディセーブルにする例を示します。

```
Router(config)# mls qos rewrite ip dscp
Router(config)#
```

次に、ポートキューイング モードをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos rewrite ip dscp
Router(config)#
```

関連コマンド

コマンド	説明
mls qos (global configuration mode)	QoS 機能をグローバルにイネーブルにします。
show mls qos	MLS QoS 情報を表示します。

mls qos statistics-export (global configuration mode)

QoS 統計データのエクスポートをグローバルにイネーブルにするには、**mls qos statistics-export** コマンドを使用します。QoS 統計データのエクスポート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。

mls qos statistics-export

no mls qos statistics-export

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

コマンドのデフォルト

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

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、データ エクスポートをグローバルにイネーブルにする必要があります。

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

QoS 統計データのエクスポートを正常に実行するには、エクスポートの宛先ホスト名または IP アドレス、および UDP ポート番号を設定する必要があります。

例

次に、データ エクスポートをグローバルにイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export
Router(config)#
```

次に、データ エクスポートをグローバルにディセーブルにする例を示します。

```
Router(config)# no mls qos statistics-export
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export (interface configuration mode)

ポート単位の QoS 統計データのエクスポートをイネーブルにするには、**mls qos statistics-export** コマンドを使用します。ポート単位の QoS 統計データのエクスポ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。

mls qos statistics-export

no mls qos statistics-export

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 モード

ディセーブル

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、ポートで、グローバルにデータ エクスポートをイネーブルにする必要があります。

QoS 統計データのエクスポートを正常に実行するには、エクスポートの宛先ホスト名または IP アドレス、および UDP ポート番号を設定する必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。デリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。

ポートの統計情報はエクスポートされますが、ポートの QoS 統計情報はエクスポートされません。データ エクスポートがイネーブルであるポートでは、次の情報がエクスポートされます。

- タイプ（1 はポート タイプを意味します）
- モジュール / ポート
- 着信パケット数（ハードウェアの累積カウンタ値）
- 着信バイト数（ハードウェアの累積カウンタ値）
- 発信パケット数（ハードウェアの累積カウンタ値）
- 発信バイト数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 Coordinated Universal Time（UTC; 協定世界時）を起点とする秒数）

たとえば、FastEthernet4/5 で QoS 統計データのエクスポートがイネーブルの場合、エクスポートされたレコードは次のようになります（この例では、デリミタは |（パイプ））。

```
|1|4/5|123|80|12500|6800|982361894|
```

例

次に、QoS 統計データ エクスポートをイネーブルにする例を示します。

```
Router(config-if)# mls qos statistics-export
Router(config-if)#
```

次に、QoS 統計データ エクスポートをディセーブルにする例を示します。

```
Router(config-if)# no mls qos statistics-export
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export aggregate-policer

名前付き集約ポリサー上で QoS 統計データのエクスポートをイネーブルにするには、**mls qos statistics-export aggregate-policer** コマンドを使用します。名前付き集約ポリサー上で QoS 統計データのエクスポ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。

mls qos statistics-export aggregate-policer *policer-name*

no mls qos statistics-export aggregate-policer *policer-name*

シンタックスの説明

policer-name	ポリサー名

コマンド モード

共有集約ポリサーの場合はすべてディセーブル

コマンドのデフォルト

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 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、共有集約ポリサーで、グローバルにデータ エクスポートをイネーブルにする必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。デリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。

データ エクスポートがイネーブルである共有集約ポリサーまたは名前付きポリサーごとに、統計データがポリサー単位、および EARL 単位でエクスポートされます。データ エクスポートがイネーブルである共有集約ポリサーまたは名前付きポリサーでは、次の情報がエクスポートされます。

- タイプ（3 は集約ポリサーのエクスポート タイプを意味します）
- 集約名
- 方向（着信または発信）
- EARL 識別情報
- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

共有集約ポリサーがポリシーの両方の方向に付加されている場合、2 つのレコードがエクスポートされます（各方向に 1 つずつ）。各レコードには、受け入れパケット、拒否標準レート パケット、および拒否超過レート パケットに関する同じカウンタ値が格納されます。

たとえばエクスポート レコードは次のようになります（この例では、デリミタは |（パイプ））。

```
|3|agg_1|in|1|45543|2345|982361894|
|3|agg_1|in|3|45543|2345|982361894|
```

上記の例は、以下の情報を示しています。

- 共有集約ポリサー「aggr_1」上で QoS 統計データのエクスポートがイネーブル
- スロット 1 に装着されたスーパーバイザ エンジンに EARL が搭載
- スロット 3 に EARL が搭載

例

次に、共有集約ポリサー単位、または名前付きポリサー単位でデータ エクスポートをイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export aggregate-policer aggr1M
Router(config)#
```

関連コマンド

コマンド	説明
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export class-map

クラス マップの QoS 統計データ エクスポートをイネーブルにするには、**mls qos statistics-export class-map** コマンドを使用します。QoS 統計データのエクスポートをクラス マップ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。

mls qos statistics-export class-map *classmap-name*

no mls qos statistics-export class-map *classmap-name*

シンタックスの説明

classmap-name	クラス マップ名

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

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、クラス マップで、グローバルにデータ エクスポートをイネーブルにする必要があります。

QoS 統計データは、デリミタ区切りフィールドを使用してエクスポートされます。デリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。

データ エクスポートがイネーブルであるクラス マップごとに、統計データがポリサー単位、およびインターフェイス単位でエクスポートされます。インターフェイスが物理インターフェイスの場合、次の情報がエクスポートされます。

- タイプ（4 はクラス マップ物理エクスポートを意味します）
- クラスマップ名
- 方向（着信または発信）
- モジュール/ポート
- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

インターフェイスが Catalyst 6500 シリーズ スイッチ VLAN である場合は、次の情報がエクスポートされます。

- タイプ（5 はクラス マップ VLAN エクスポートを意味します）
- クラスマップ名

- 方向（着信または発信）
- EARL 識別情報（EARL が搭載されたスロット番号）
- VLAN 番号
- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

インターフェイスが Catalyst 6500 シリーズ スイッチ ポート チャネルである場合は、次の情報がエクスポートされます。

- タイプ（6 はクラス マップ ポート チャネル エクスポートを意味します）
- クラスマップ名
- 方向（着信または発信）
- EARL 識別情報（EARL が搭載されたスロット番号）
- ポート チャネル番号
- 受け入れパケット数（ハードウェアの累積カウンタ値）
- 拒否標準レート パケット数（ハードウェアの累積カウンタ値）
- 拒否超過レート パケット数（ハードウェアの累積カウンタ値）
- タイム スタンプ（1970 年 1 月 1 日 UTC を起点とする秒数）

たとえば、次のように設定されているとします。

- クラス マップ「class_1」上で QoS 統計データ エクスポートがイネーブル
- スロット 1 に装着されたスーパーバイザ エンジンに EARL が搭載
- スロット 3 に EARL が搭載
- Catalyst 6500 シリーズ スイッチは、「policy_1」というポリシー マップ内に存在
- policy_1 は、次のインターフェイスの入力方向に付加
  - FastEthernet4/5
  - VLAN 100
  - ポート チャネル 24

  エクスポートされたレコードは、次のようになります（この例では、デリミタは|（パイプ））。

```
|4|class_1|in|4/5|45543|2345|2345|982361894|
|5|class_1|in|1|100|44000|3554|36678|982361894|
|5|class_1|in|3|100|30234|1575|1575|982361894|
```

例

次に、クラス マップの QoS 統計データ エクスポートをイネーブルにする例を示します。

```
Router(config)# mls qos statistics-export class-map class3
Router(config)#
```

関連コマンド

コマンド	説明
mls qos statistics-export delimiter	QoS 統計データのエクスポート フィールドのデリミタを設定します。
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export delimiter

QoS 統計データ エクスポート フィールドのデリミタを設定するには、**mls qos statistics-export delimiter** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export delimiter

no mls qos statistics-export delimiter

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

デフォルトのデリミタはパイプ記号（|）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 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

Catalyst 6500 シリーズ スイッチにデータ エクスポートを設定するには、データ エクスポートをグローバルにイネーブルにする必要があります。

例

次に、QoS 統計データ エクスポート フィールドのデリミタ（カンマ）を設定し、設定を確認する例を示します。

```
Router(config)# mls qos statistics-export delimiter ,
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export destination

QoS 統計データ エクスポートの宛先ホストおよび UDP ポート番号を設定するには、**mls qos statistics-export destination** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export destination {*host-name* | *host-ip-address*} {{**port** *port-number*} | **syslog**} [**facility** *facility-name*] [**severity** *severity-value*]

シンタックスの説明

host-name	ホスト名
host-ip-address	ホストの IP アドレス
port *port-number*	UDP ポート番号を指定します。
syslog	Syslog ポートを指定します。
facility *facility-name*	（任意）エクスポートするファシリティ タイプを指定します。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。
severity *severity-value*	（任意）エクスポートする重大度を指定します。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

syslog を指定しないかぎり、デフォルトでは何も設定されません。**syslog** を指定した場合、デフォルトは次のとおりです。

- *port* は **514** です。
- *facility* は **local6** です。
- *severity* は **debug** 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 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

有効な *facility* 値は次のとおりです。

- **authorization**：セキュリティ / 認証メッセージ
- **cron**：クロック デーモン
- **daemon**：システム デーモン
- **kernel**：カーネル メッセージ
- **local0**：ローカル使用 0
- **local1**：ローカル使用 1
- **local2**：ローカル使用 2

- **local3**：ローカル使用 3
- **local4**：ローカル使用 4
- **local5**：ローカル使用 5
- **local6**：ローカル使用 6
- **local7**：ローカル使用 7
- **lpr**：ライン プリンタ サブシステム
- **mail**：メール システム
- **news**：ネットワーク ニュース サブシステム
- **syslog**：syslogd により内部で生成されるメッセージ
- **user**：ユーザレベル メッセージ
- **uucp**：UUCP サブシステム

有効な *severity* レベルは次のとおりです。

- **alert**：ただちに対処が必要
- **critical**：クリティカルな状況
- **debug**：デバッグレベル メッセージ
- **emergency**：システムが使用不可
- **error**：エラー
- **informational**：情報提供
- **notice**：正常だが特異な状況
- **warning**：警告

例

次に、宛先ホスト アドレス、および UDP ポート番号として Syslog を指定する例を示します。

```
Router(config)# mls qos statistics-export destination 172.20.52.3 syslog
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos statistics-export interval

ポートまたは集約ポリサー QoS 統計データの読み込み頻度およびエクスポート頻度を指定するには、**mls qos statistics-export interval** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos statistics-export interval *interval*

no mls qos statistics-export interval

シンタックスの説明

interval	エクスポート時間。有効値は 30 ～ 65,535 秒です。

コマンドのデフォルト

300 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

QoS 統計データのエクスポートは、OSM インターフェイスではサポートされていません。

interval は、設定内のアクティビティによるカウンタ ラップアラウンドを防止できるように、十分短い値を設定する必要があります。

注意　QoS 統計をエクスポートすると、Catalyst 6500 シリーズ スイッチでトラフィックが増加するので、インターバルを短縮する場合は注意してください。

例

次に、QoS 統計データ エクスポートのインターバルを設定する例を示します。

```
Router(config)# mls qos statistics-export interval 250
Router(config)#
```

関連コマンド

コマンド	説明
show mls qos statistics-export info	MLS 統計データ エクスポート ステータスおよび設定に関する情報を表示します。

mls qos trust

インターフェイスの信頼状態を設定するには、**mls qos trust** コマンドを使用します。インターフェイスを信頼しない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。

mls qos trust [**cos** | **dscp** | **ip-precedence**]

no mls qos trust

シンタックスの説明

cos	（任意）着信フレームの CoS ビットを信頼し、CoS ビットから内部 DSCP 値を取得することを指定します。
dscp	（任意）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。
ip-precedence	（任意）着信パケットの ToS ビットに IP precedence 値が含まれていて、IP precedence ビットから内部 DSCP 値を取得することを指定します。

コマンドのデフォルト

OSM 上の LAN インターフェイスおよび WAN インターフェイスのデフォルトは、次のとおりです。

- グローバル QoS がイネーブルの場合、ポートは信頼できない状態です。
- グローバル QoS がディセーブルの場合、デフォルトは **dscp** です。
- 引数を入力しない場合は、**trust dscp** が使用されます。

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

mls qos trust コマンドを使用して、インターフェイスの信頼状態を設定できます。たとえば、特定のインターフェイスに着信するパケットの CoS、ToS、および DSCP の分類が正しいものであると信頼するかどうかを設定できます。

cos キーワードは、**pos** または **atm** インターフェイス タイプではサポートされません。

FlexWAN モジュールに信頼状態を設定できません。

ギガビット イーサネット ポートを除く 1q4t LAN ポートには、信頼状態を設定できません。

4 ポートギガビット イーサネット WAN モジュールに **mls qos trust cos** コマンドを入力した場合、入力キュー廃棄しきい値は実装されません。

レイヤ 2 WAN インターフェイスの信頼状態を設定するには、**set qos-group** コマンドを使用します。

例

次に、インターフェイスの信頼状態を IP precedence に設定する例を示します。

```
Router(config-if)# mls qos trust ip-precedence
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos bridged	レイヤ 3 LAN インターフェイスのブリッジド トラフィックにマイクロフロー ポリシングをイネーブルにします。
mls qos cos	インターフェイスのデフォルト CoS 値を定義します。
mls qos vlan-based	VLAN のデフォルト CoS 値を定義します。
show queueing interface	キューイング情報を表示します。

mls qos trust extend

電話の信頼モードを設定するには、**mls qos trust extend** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

mls qos trust extend [**cos** *value*]

no mls qos trust extend

シンタックスの説明

cos *value*	（任意）PC からのパケットに設定するために使用される CoS 値を指定します。有効値は 0 ～ 7 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。

- モードは untrusted です。
- **cos** *value* 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

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、WAN モジュールではサポートされません。

電話が信頼モードに設定されている場合、PC から着信したすべてのパケットはそのまま電話を経由して Catalyst 6500 シリーズ スイッチに直接送信されます。電話が非信頼モードに設定されている場合、PC から着信したすべてのトラフィックは、所定の CoS 値に設定されてから、Catalyst 6500 シリーズ スイッチに送信されます。

mls qos trust extend コマンドを入力するたびに、モードが変わります。たとえば、モードが信頼に設定されている場合にコマンドを入力すると、モードは非信頼に変わります。現在設定されている信頼モードを表示するには、**show queueing interface** コマンドを入力します。

例

次に、スイッチ ポートに接続された電話を信頼モードで設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend
Router(config-if)#
```

次に、モードを非信頼に変更して、CoS 値を 3 に設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# mls qos trust extend cos 3
Router(config-if)#
```

次に、設定をデフォルト モードに設定する例を示します。

```
Router(config-if)# interface fastethernet5/1
Router(config-if)# no mls qos trust extend
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。

mls qos vlan-based

レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにするには、**mls qos vlan-based** コマンドを使用します。レイヤ 2 インターフェイスの VLAN 単位の QoS をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls qos vlan-based

no mls qos vlan-based

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

インターフェイス 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

このコマンドは、スイッチポートおよびポートチャネル インターフェイスだけでサポートされます。

VLAN ベース モードでは、レイヤ 2 インターフェイスに対応付けられたポリシー マップは無視され、QoS は対応する VLAN インターフェイスに対応付けられたポリシー マップによって実行されます。

VLAN 単位の QoS は、レイヤ 2 インターフェイス上だけで設定できます。

（注）　レイヤ 3 インターフェイスは常にインターフェイスベース モードです。レイヤ 3 VLAN インターフェイスは常に VLAN ベース モードです。

例

次に、レイヤ 2 インターフェイスの VLAN 単位の QoS をイネーブルにする例を示します。

```
Router(config-if)# mls qos vlan-based
Router(config-if)#
```

関連コマンド

コマンド	説明
mls qos bridged	レイヤ 3 LAN インターフェイスのブリッジド トラフィックにマイクロフロー ポリシングをイネーブルにします。
mls qos cos	インターフェイスのデフォルト CoS 値を定義します。
show queueing interface	キューイング情報を表示します。

mls rate-limit all

ユニキャスト パケットとマルチキャスト パケットに共通のレート リミッタのイネーブル化および設定を行うには、**mls rate-limit all** コマンドを使用します。レート リミッ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。

mls rate-limit all {**mtu-failure** | **ttl-failure**} *pps* [*packets-in-burst*]

no mls rate-limit all {**mtu-failure** | **ttl-failure**}

シンタックスの説明

all	ユニキャストおよびマルチキャスト パケットのレート制限を指定します。
mtu-failure	MTU 障害パケットに対するレート リミッタのイネーブル化および設定を行います。
ttl-failure	TTL 障害パケットに対するレート リミッタのイネーブル化および設定を行います。
pps	パケット/秒。有効値は 10 ～ 1,000,000 パケット/秒です。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 です。

コマンドのデフォルト

デフォルトでは、レイヤ 2 レート リミッタはオフです。レート リミッタのイネーブル化および設定を行う場合、*packets-in-burst* は、デフォルトで **10** になります。

コマンド モード

グローバル コンフィギュレーション（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

レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、設定したレートを超えるトラフィックを廃棄することにより、ソフトウェアの制御パスが輻輳しないようにします。

例

次に、ユニキャストおよびマルチキャスト パケットに対する TTL 障害リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit all ttl-failure 15
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit layer2

レイヤ 2 の制御パケットのイネーブル化およびレート制限を行うには、**mls rate-limit layer2** コマンドを使用します。ハードウェアでレート リミッ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。

mls rate-limit layer2 {**pdu | l2pt** | **port-security**} *pps* [*packets-in-burst*]

no mls rate-limit layer2 [**pdu | l2pt** | **port-security**]

シンタックスの説明

pdu *pps*	BPDU、CDP、PDU、および VTP PDU のレイヤ 2 制御パケットのレート制限を指定します。有効値は、10 ～ 1,000,000 パケット/秒です。
l2pt *pps*	レイヤ 2 プロトコル トンネリングのマルチキャスト MAC アドレスを使用して、レイヤ 2 制御パケットのレート制限を指定します。有効値は、10 ～ 1,000,000 パケット/秒です。
port-security *pps*	ポート セキュリティ トラフィックのレート制限を指定します。有効値は 10 ～ 1,000,000 パケット/秒です。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 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。

- デフォルトでは、レイヤ 2 レート リミッタはオフです。
- レート リミッタのイネーブル化および設定を行う場合、*packets-in-burst* のデフォルト設定は **10** であり、*pps* 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

グローバル スイッチング モードが truncated モードに設定されている場合は、レイヤ 2 レート リミッタを設定できません。

port-security *pps* キーワードおよび引数については、次の注意事項に従ってください。

- PFC2 ではポートセキュリティ レート リミッタがサポートされません。
- truncated スイッチング モードでは、ポートセキュリティ レート リミッタがサポートされません。
- 値を下げると、CPU はより効果的に保護されます。

レート リミッタは、次のようにパケットを制限します。

- フレームは、宛先 MAC アドレスによってレイヤ 2 制御フレームとして分類されます。宛先 MAC アドレスは、次のように使用されます。
  - IEEE BPDU には、0180.C200.0000
  - CDP には、0100.0CCC.CCCC

  - PVST/SSTP BPDU には、0100.0CCC.CCCD
- ソフトウェアは、フレームに Local Target Logic（LTL）インデックスを割り当てます。
- LTL インデックスは、すべての関連付けられたフレームの集約レート制限のために転送エンジンへ送られます。

レイヤ 2 制御パケットは、次のとおりです。

- GARP VLAN Registration Protocol（GVRP）
- BPDU
- CDP/DTP/PAgP/UDLD/LACP/VTP PDU
- PVST/SSTP PDU

トラフィック レートが設定した *レート*を超えると、超過したパケットはハードウェアで廃棄されます。

pdu および **l2pt** のレート リミッタは、特定のハードウェアのレート リミッタ番号（9 ～ 12 など）だけを使用します。使用可能なレート リミッタ番号を表示するには、**show mls rate-limit usage** コマンドを入力します。使用可能な番号に対しては、出力フィールドに [Free] と表示されます。他の機能でレート リミッタ機能が 4 つとも使用されている場合、レイヤ 2 制御パケットのレート制限を行うには他の機能をオフにする必要があるというシステム メッセージが表示されます。

MAC 移動が発生して 1 つのパケットが 2 つのポートで認識された場合、そのパケットはソフトウェアにリダイレクトされます。いずれかのポートで違反モードが制限または保護に設定されている場合、パケットはソフトウェアで廃棄されます。このようなパケットがソフトウェアにリダイレクトされる量を抑制するには、ポートセキュリティ レート リミッタを使用できます。これにより、高トラフィック レートからソフトウェアを保護できます。

例

次に、レイヤ 2 プロトコル トンネリング パケットのレート リミッタ機能のイネーブル化および設定を行う例を示します。

```
Router(config)# mls rate-limit layer2 l2pt 3000
Router(config)#
```

次に、ポートセキュリティ レート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit layer2 port-security 500
Router(config)# end
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit multicast ipv4

IPv4 マルチキャスト パケットのレート リミッタのイネーブル化および設定を行うには、**mls rate-limit multicast ipv4** コマンドを使用します。レート リミッ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。

mls rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **partial** | **non-rpf**} *pps* [*packets-in-burst*]

no mls rate-limit multicast ipv4 {**connected** | **fib-miss** | **igmp** | **ip-option** | **partial** | **non-rpf**}

シンタックスの説明

connected	直接接続された送信元からのマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
fib-miss	FIB 不一致マルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
igmp	IGMP パケットに対するレート リミッタのイネーブル化および設定を行います。
ip-option	IP オプションを持つマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
partial	パーシャル SC 状態時のマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
non-rpf	RPF チェックに失敗したマルチキャスト パケットに対するレート リミッタのイネーブル化および設定を行います。
pps	パケット / 秒。有効値は 10 ～ 1,000,000 パケット / 秒です。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 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。

- *packets-in-burst* を設定しないと、マルチキャストの場合はデフォルトの **100** が適用されます。
- **fib-miss**：イネーブル（**100,000** *pps*）で、*packet-in-burst* は **100** に設定されています。
- **ip-option**：ディセーブル
- **partial**：イネーブル（**100,000** *pps*）で、*packet-in-burst* は **100** に設定されています。

コマンド モード

グローバル コンフィギュレーション（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

グローバル スイッチング モードが truncated モードに設定されている場合は、IPv4 レート リミッタを設定できません。

レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

ip-option キーワードは、PFC3BXL または PFC3B モードだけでサポートされます。

例

次に、RPF チェックに失敗したマルチキャスト パケットに対するレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
Router(config)#
```

次に、パーシャル SC 状態時のマルチキャスト パケットに対するレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 partial 250
Router(config)#
```

次に、FIB 不一致マルチキャスト パケットに対するレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 15
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit multicast ipv6

IPv6 マルチキャスト レート リミッタを設定するには、**mls rate-limit multicast ipv6** コマンドを使用します。レート リミッ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。

mls rate-limit multicast ipv6 {**connected** *pps* [*packets-in-burst*]} | {*rate-limiter-name* {**share** {**auto** | *target-rate-limiter*}}}

no mls rate-limit multicast ipv6 {**connected** | *rate-limiter-type*}

シンタックスの説明

connected *pps*	直接接続された送信元からの IPv6 マルチキャスト パケットのレート リミッタをイネーブル化および設定します。有効値は、10 ～ 1,000,000 パケット/秒です。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 です。
rate-limiter-name	レート リミッタ名。有効値は、**default-drop**、**route-cntl**、**secondary-drop**、**sg**、**starg-bridge**、および **starg-m-bridge** です。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。
share	IPv6 レート リミッタの共有ポリシーを指定します。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。
auto	共有ポリシーを自動的に決定します。
target-rate-limiter	このグループ用にハードウェアでプログラムされた最初のレート リミッタ名です。有効値は、**default-drop**、**route-cntl**、**secondary-drop**、**sg**、**starg-bridge**、および **starg-m-bridge** です。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

*バースト値*を設定しないと、マルチキャストの場合はデフォルトの **100** が適用されます。

コマンド モード

グローバル コンフィギュレーション（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

rate-limiter-name 引数は、現在プログラムされていないレート リミッタである必要があります。

target-rate-limiter 引数は、ハードウェアでプログラムされているレート リミッタで、そのグループ用にプログラムされた最初のレート リミッタである必要があります。

表 2-23 に、IPv6 レート リミッタおよび各レート リミッタの対象トラフィック クラスを示します。

表 2-23　IPv6 レート リミッタ

レート リミッタ ID	レート制限されるトラフィック クラス
Connected	直接接続された送信元トラフィック
Default-drop	* (*, G/m)SSM * (*, G/m)SSM 非 rpf
Route-control	* (*, FF02::X/128)
Secondary-drop	* (*, G/128) SPT しきい値は無限
SG	* (S, G)RP-RPF ポスト スイッチオーバー * (*, FFx2/16)
Starg-bridge	* (*, G/128) SM (*, G) が存在する場合の * SM 非 rpf トラフィック
Starg-M-bridge	* (*, G/m) SM * (*, FF/8) * (*, G) が存在しない場合の SM 非 rpf トラフィック

次の方式のいずれかを使用して、IPv6 マルチキャスト トラフィックのレート リミッタを設定できます。

- トラフィック クラス用のレート リミッタの直接アソシエーション：レートを選択して、レート リミッタとレートを関連付けます。次に、1000 pps および 20 パケット/バーストのレートを選択し、**default-drop** レート リミッタとレートを関連付ける例を示します。

  ```
  Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
  ```

- レート リミッタと事前設定された他のレート リミッタとのスタティックな共有：隣接ベースの使用可能なレート リミッタが十分にない場合は、すでに設定済みのレート リミッタ（ターゲット レート リミッタ）と、レート リミッタを共有できます。次に、**route-cntl** レート リミッタを **default-drop** ターゲット レート リミッタと共有する例を示します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
  ```

  ターゲット レート リミッタが設定されていない場合は、ターゲット レート リミッタを他のレート リミッタと共有できるように設定する必要があるというメッセージが表示されます。

- レート リミッタのダイナミックな共有：共有するレート リミッタがいずれか不明な場合、**share auto** キーワードを使用してダイナミックな共有をイネーブルにします。ダイナミックな共有をイネーブルにすると、システムは事前設定されたレート リミッタを選択し、所定のレート リミッタとこの事前設定されたレート リミッタを共有します。次に、**route-cntrl** レート リミッタ用にダイナミックな共有を選択する例を示します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
  ```

例

次に、直接接続された送信元からの IPv6 マルチキャスト パケットにレート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
Router(config)#
```

次に、トラフィック クラスのレート リミッタの直接アソシエーションを設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

```
Router(config)#
```

次に、任意のレート リミッタと他の事前設定されたレート リミッタとのスタティックな共有を設定する例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
Router(config)#
```

次に、**route-cntrl** レート リミッタ用にダイナミックな共有をイネーブルにする例を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast acl

ACL ブリッジド レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast acl** コマンドを使用します。レート リミッ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。

mls rate-limit unicast acl {**input** | **output** | **vacl-log**} {*pps* [*packets-in-burst*]}

no mls rate-limit unicast acl {**input** | **output** | **vacl-log**}

シンタックスの説明

input	入力 ACL ブリッジド ユニキャスト パケットに対するレート リミッタ機能を指定します。
output	出力 ACL ブリッジド ユニキャスト パケットに対するレート リミッタ機能を指定します。
vacl-log	VACL ログに対するレート リミッタ機能を指定します。
pps	パケット / 秒。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。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 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。

- **input**：ディセーブル
- **output**：ディセーブル
- **vacl-log**：イネーブル（**2000** *pps*）で、*packet-in-burst* は **1** に設定されています。
- *packets-in-burst* を設定しないと、ユニキャストの場合は **10** が適用されます。

コマンド モード

グローバル コンフィギュレーション（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

レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

pps を設定する場合、有効値は次のとおりです。

- ACL 入力および出力の場合：10 ～ 1,000,000 *pps*
- VACL ログの場合：10 ～ 5000 *pps*

vacl-log *packets-in-burst* キーワードおよび引数を変更することはできず、デフォルトで **1** に設定されます。

同じハードウェア レジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1：
  - 出力 ACL ブリッジド パケット
  - 入力 ACL ブリッジド パケット
- グループ 2：
  - RPF 障害
  - ACL 廃棄に対する ICMP 到達不能
  - ルートなしに対する ICMP 到達不能
  - IP エラー

各グループのすべてのコンポーネントは、同じハードウェア レジスタを使用または共有します。たとえば、ACL ブリッジド入力および出力パケットはレジスタ A を使用します。一方、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたときに、グループ内のコンポーネントはすべて同じハードウェア レジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、サービス内部モードをイネーブルにしておく必要があります。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が **0**（ゼロ）に設定されている場合
- 入力および出力 ACL ブリッジド パケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジド パケットを 100 pps に設定したあとに、出力 ACL ブリッジド パケットを 200 pps に設定すると、入力 ACL ブリッジド パケットの値は 200 pps に上書きされ、入力および出力 ACL ブリッジド パケットは両方とも 200 pps になります。

例

次に、ユニキャスト パケットに対する入力 ACL ブリッジド パケット リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast acl ingress 100
Router(config)#
```

次に、ユニキャスト パケットに対する入力 ACL ブリッジド パケット リミッタ機能をディセーブルにする例を示します。

```
Router(config)# no mls rate-limit unicast acl ingress
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast cef

CEF レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast cef** コマンドを使用します。レート リミッ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。

mls rate-limit unicast cef {**receive** | **glean**} *pps* [*packets-in-burst*]

no mls rate-limit unicast cef {**receive** | **glean**}

シンタックスの説明

receive	受信パケットに対するレート リミッタのイネーブル化と設定を行います。
glean	ARP 解決パケットに対するレート リミッタのイネーブル化と設定を行います。
pps	パケット/秒。有効値は 10 ～ 1,000,000 パケット/秒です。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 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。

- **receive**：ディセーブル
- **glean**：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

CEF レート リミッタ機能をイネーブルにする場合、次の状況が発生します（これらの状況が望ましくない場合は、CEF レート リミッタをディセーブルにしてください）。

- パケットが glean/receive 隣接関係にヒットする場合、パケットはソフトウェアに送信されず、廃棄される可能性があります（入力 VLAN に出力 ACL があり、一致したエントリの結果が deny（拒否）である場合）。
- 一致した ACL エントリの結果が bridge（ブリッジ）である場合、パケットは glean/receive レート制限ではなく、出力 ACL ブリッジ レート制限（オンの場合）の制約を受けます。
- glean/receive 隣接レート制限は、出力 ACL 検索の結果が permit（許可）、または入力 VLAN に出力 ACL がない場合にだけ適用されます。

例

次に、ユニキャスト パケットに対する CEF の glean リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast cef glean 5000
Router(config)#
```

次に、ユニキャスト パケットに対する CEF の glean リミッタ機能をディセーブルにする例を示します。

```
Router(config)# no mls rate-limit unicast cef glean
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast ip

ユニキャスト パケットのレート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast ip** コマンドを使用します。レート リミッ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。

mls rate-limit unicast ip {**errors** | **features** | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

mls rate-limit unicast ip icmp {**redirect** | **unreachable** {**acl-drop** *pps*} | **no-route** *pps*} [*packets-in-burst*]

no mls rate-limit unicast ip {**errors** | **features** | {**icmp** {**redirect** | **unreachable** {**acl-drop** | **no-route**}}} | **options** | **rpf-failure**} *pps* [*packets-in-burst*]

シンタックスの説明

errors	IP チェックサム エラーおよび IP 長エラーのユニキャスト パケットのレート制限を指定します。
features	レイヤ 3 のソフトウェア セキュリティ機能（認証プロキシ、IPSec、および検査など）を使用したユニキャスト パケットのレート制限を指定します。
options	オプションを持つユニキャスト IPv4 パケットのレート制限を指定します。
rpf-failure	RPF 障害のユニキャスト パケットのレート制限を指定します。
pps	パケット/秒。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。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 です。
icmp redirect	ICMP リダイレクトを必要とするユニキャスト パケットのレート制限を指定します。
icmp unreachable acl-drop *pps*	ACL 廃棄パケットに対する ICMP 到達不能のレート リミッタのイネーブル化および設定を行います。
icmp unreachable no-route *pps*	FIB 不一致パケットに対する ICMP 到達不能のレート リミッタのイネーブル化および設定を行います。

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。

- *packets-in-burst* を設定しないと、ユニキャストのバーストとしてデフォルトの **10** が設定されます。
- **errors**：イネーブル（**100** *pps*）で、*packets-in-burst* は **10** に設定されています。
- **rpf-failure**：イネーブル（**100** *pps*）で、*packets-in-burst* は **10** に設定されています。
- **icmp unreachable acl-drop**：イネーブル（**100** *pps*）で、*packets-in-burst* は **10** に設定されています。
- **icmp unreachable no-route**：イネーブル（**100** *pps*）で、*packets-in-burst* は **10** に設定されています。
- **icmp redirect**：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

拒否されたパケットに対して OAL サポートを提供するには、**mls rate-limit unicast ip icmp unreachable acl-drop 0** コマンドを入力します。

OAL キャプチャと VACL キャプチャは、互換性がありません。スイッチに両方の機能を設定しないでください。OAL を設定した場合は、SPAN を使用してトラフィックをキャプチャします。

レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

（注） ICMP レート リミッタを設定して ICMP リダイレクトが発生する場合、既存のデータ トラフィックが廃棄されますが、同じインターフェイス上の残りのトラフィックは転送されます。

pps を設定する場合、有効値は **0** および 10 ～ 1,000,000 です。*pps* をグローバルに **0** に設定すると、ルート プロセッサへのパケットのリダイレクトがディセーブルになります。**0** の値は、次のレート リミッタでサポートされます。

- icmp unreachable acl-drop
- icmp unreachable no-route
- icmp redirect
- ip rpf failure

同じハードウェア レジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1：
  - 出力 ACL ブリッジド パケット
  - 入力 ACL ブリッジド パケット
- グループ 2：
  - RPF 障害
  - ACL 廃棄に対する ICMP 到達不能
  - ルートなしに対する ICMP 到達不能
  - IP エラー

各グループのすべてのコンポーネントは、同じハードウェア レジスタを使用または共有します。たとえば、ACL ブリッジド入力および出力パケットはレジスタ A を使用します。一方、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたときに、グループ内のコンポーネントはすべて同じハードウェア レジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、サービス内部モードをイネーブルにしておく必要があります。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が **0**（ゼロ）に設定されている場合

- 入力および出力 ACL ブリッジド パケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジド パケットを 100 pps に設定したあとに、出力 ACL ブリッジド パケットを 200 pps に設定すると、入力 ACL ブリッジド パケットの値は 200 pps に上書きされ、入力および出力 ACL ブリッジド パケットは両方とも 200 pps になります。

例

次に、ユニキャスト パケットに対する ICMP リダイレクトのリミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast ip icmp redirect 250
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast l3-features

ユニキャスト パケットのレイヤ 3 セキュリティ レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit unicast l3-features** コマンドを使用します。レート リミッ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。

mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

no mls rate-limit unicast l3-features *pps* [*packets-in-burst*]

シンタックスの説明

pps	パケット/秒。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。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 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。

- イネーブル （**2000** *pps*）で、*packet-in-burst* は **1** に設定されています。
- *packets-in-burst* を設定しないと、ユニキャストの場合は **10** が適用されます。

コマンド モード

グローバル コンフィギュレーション（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、ユニキャスト パケットにレイヤ 3 セキュリティ レート リミッタを設定する例を示します。

```
Router(config)# mls rate-limit unicast l3-features 5000
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rate-limit unicast vacl-log

VACL ログ レート リミッタ機能のイネーブル化および設定を行うには、**mls rate-limit** unicast vacl-log コマンドを使用します。レート リミッ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。

mls rate-limit unicast vacl-log {*pps* [*packets-in-burst*]}

no mls rate-limit unicast vacl-log

シンタックスの説明

pps	パケット/秒。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。
packets-in-burst	（任意）バースト状態のパケット。有効値は 1 ～ 255 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。

- イネーブル （**2000** *pps*）で、*packet-in-burst* は **1** に設定されています。
- *packets-in-burst* を設定しないと、ユニキャストの場合は **10** が適用されます。

コマンド モード

グローバル コンフィギュレーション（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

レート リミッタ機能は、ハードウェアのデータ パスからソフトウェアのデータ パスにパントされたパケットをレート制限できます。レート リミッタ機能は、ソフトウェアの制御パスが輻輳しないようにし、設定したレートを超えるトラフィックを廃棄します。

pps を設定する場合、有効値は次のとおりです。

- ACL 入力および出力の場合：10 ～ 1,000,000 *pps*
- VACL ログの場合：10 ～ 5000 *pps*

pps をグローバルに **0** に設定すると、ルート プロセッサへのパケットのリダイレクトがディセーブルになります。

vacl-log *packets-in-burst* キーワードおよび引数を変更することはできず、デフォルトで **1** に設定されます。

同じハードウェア レジスタが共有される場合もあります。これは次の 2 つのグループに分けられます。

- グループ 1：
  - 出力 ACL ブリッジド パケット
  - 入力 ACL ブリッジド パケット
- グループ 2：
  - RPF 障害

- ACL 廃棄に対する ICMP 到達不能
- ルートなしに対する ICMP 到達不能
- IP エラー

各グループのすべてのコンポーネントは、同じハードウェア レジスタを使用または共有します。たとえば、ACL ブリッジド入力および出力パケットはレジスタ A を使用します。一方、ICMP 到達不能、ルートなし、および RPF 障害はレジスタ B を使用します。

ほとんどの場合、グループのコンポーネントを変更すると、最初のコンポーネントが変更されたときに、グループ内のコンポーネントはすべて同じハードウェア レジスタを使用するように上書きされます。上書きが行われるたびに、警告メッセージが出力されますが、サービス内部モードをイネーブルにしておく必要があります。次の場合には、上書きは行われません。

- 特別な場合で、*pps* の値が **0**（ゼロ）に設定されている場合。
- 入力および出力 ACL ブリッジド パケットがディセーブルの場合、これらを再度イネーブルにするまで上書きは行われません。一方がディセーブルの場合、もう一方はイネーブルであるかぎり影響を受けません。たとえば、入力 ACL ブリッジド パケットを 100 pps に設定したあとに、出力 ACL ブリッジド パケットを 200 pps に設定すると、入力 ACL ブリッジド パケットの値は 200 pps に上書きされ、入力および出力 ACL ブリッジド パケットは両方とも 200 pps になります。

例

次に、ユニキャスト パケットに対する VACL ログ パケット リミッタ機能を設定する例を示します。

```
Router(config)# mls rate-limit unicast vacl-log 100
Router(config)#
```

次に、レート リミッタをディセーブルにする例を示します。

```
Router(config)# no mls rate-limit unicast vacl-log 100
Router(config)#
```

関連コマンド

コマンド	説明
show mls rate-limit	MLS レート リミッタに関する情報を表示します。

mls rp ip (global configuration mode)

外部システムが PISA への IP ショートカットを確立できるようにするには、**mls rp ip** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp ip [**input-acl** | **route-map**]

no mls rp ip

シンタックスの説明

input-acl	（任意）IP 入力アクセス リストをイネーブルにします。
route-map	（任意）IP ルート マップをイネーブルにします。

コマンドのデフォルト

ショートカットは設定されていません。

コマンド モード

グローバル コンフィギュレーション（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、外部システムが IP 入力アクセス リストを使用して IP ショートカットを確立できるようにする例を示します。

```
Router(config)# mls rp ip input-acl
Router(config)#
```

関連コマンド

コマンド	説明
mls ip	インターフェイス上で内部ルータの MLS IP をイネーブルにします。
show mls ip multicast	MLS IP 情報を表示します。

mls rp ip (interface configuration mode)

外部システムが指定のインターフェイス上で MLS IP をイネーブルにできるようにするには、**mls rp ip** コマンドを使用します。MLS IP をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls rp ip

no mls rp ip

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

インターフェイス 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。

例

次に、外部システムがインターフェイス上で MLS IP をイネーブルにできるようにする例を示します。

```
Router(config-if)# mls rp ip
Router(config-if)
```

関連コマンド

コマンド	説明
mls rp ip (global configuration mode)	外部システムが PISA への IP ショートカットを確立できるようにします。
show mls ip multicast	MLS IP 情報を表示します。

mls rp ipx (global configuration mode)

外部システムが PISA への MLS IPX をイネーブルにできるようにするには、**mls rp ipx** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp ipx [**input-acl**]

no mls rp ipx

シンタックスの説明

input-acl	（任意）MLS IPX をイネーブルにして、ACL を上書きします。

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

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、外部システムが PISA への MLS IPX をイネーブルにして、ACL を上書きできるようにする例を示します。

```
Router(config)# mls rp ipx input-acl
Router(config)#
```

関連コマンド

コマンド	説明
mls rp ipx (interface configuration mode)	外部システムがインターフェイスで MLS IPX をイネーブルにすることができるようにします。
show mls rp ipx	IPX MLS ルータにおけるすべての IPX MLS インターフェイスの詳細を表示します。

mls rp ipx (interface configuration mode)

外部システムがインターフェイス上で MLS IPX をイネーブルにできるようにするには、**mls rp ipx** コマンドを使用します。MLS IPX をインターフェイス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。

mls rp ipx

no mls rp ipx

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

インターフェイス 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。

例

次に、外部システムがインターフェイス上で MLS IPX をイネーブルにできるようにする例を示します。

```
Router(config-if)# mls rp ipx
Router(config-if)#
```

関連コマンド

コマンド	説明
mls rp ipx (global configuration mode)	外部システムが PISA で MLS IPX をイネーブルにできるようにします。
show mls rp ipx	IPX MLS ルータにおけるすべての IPX MLS インターフェイスの詳細を表示します。

mls rp management-interface

インターフェイスを管理インターフェイスとしてイネーブルにするには、**mls rp management-interface** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp management-interface

no mls rp management-interface

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

インターフェイス 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。

例

次に、インターフェイスを管理インターフェイスとしてイネーブルにする例を示します。

```
Router(config-if)# mls rp management-interface
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls rp	MLS 詳細を表示します。

mls rp nde-address

NDE アドレスを指定するには、**mls rp nde-address** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp nde-address *ip-address*

no mls rp nde-address *ip-address*

シンタックスの説明

ip-address	NDE IP アドレス

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

IP サブネット アドレスを指定するには、次の構文を使用します。

- *ip-subnet-addr* : サブネット アドレスのショート フォーマット。IP アドレス YY.YY.YY.00 の末尾の 10 進数 00 は、IP サブネット アドレスの境界を指定します。たとえば、172.22.36.00 は 24 ビット サブネット アドレス（サブネット マスク 172.22.36.00/255.255.255.0）を示し、173.24.00.00 は 16 ビット サブネット アドレス（サブネット マスク 173.24.00.00/255.255.0.0）を示します。ただし、このフォーマットで識別できるのは、8、16、または 24 ビットのサブネット アドレスだけです。
- *ip-addr/subnet-mask* : サブネット アドレスのロング フォーマット。たとえば、172.22.252.00/255.255.252.00 は、22 ビット サブネット アドレスを示します。このフォーマットは、任意のビット数のサブネット アドレスを指定できます。より柔軟に指定するには、*ip-addr* に 172.22.253.1/255.255.252.00 のような完全ホスト アドレスを指定します。
- *ip-addr/maskbits* : サブネット アドレスの簡易ロング フォーマット。マスク ビットは、ネットワーク マスクのビット数を指定します。たとえば、172.22.252.00/22 は、22 ビット サブネット アドレスを示します。*ip-addr* は、193.22.253.1/22 のような完全ホスト アドレスです。このアドレスのサブネット アドレスは、*ip-subnet-addr* と同じです。

例

次に、NDE アドレスを 170.25.2.1 に設定する例を示します。

```
Router(config)# mls rp nde-address 170.25.2.1
Router(config)#
```

関連コマンド

コマンド	説明
show mls rp	MLS 詳細を表示します。

mls rp vlan-id

インターフェイスに VLAN ID を割り当てるには、**mls rp vlan-id** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp vlan-id {*vlan-id*}

no mls rp vlan-id

シンタックスの説明

vlan-id	VLAN ID 番号。有効値は 1 ～ 4094 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

インターフェイス 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。

例

次に、インターフェイスに VLAN ID を割り当てる例を示します。

```
Router(config-if)# mls rp vlan-id 4
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls rp	MLS 詳細を表示します。

mls rp vtp-domain

インターフェイスを VTP ドメインにリンクするには、**mls rp vtp-domain** コマンドを使用します。以前のエントリを削除する場合は、このコマンドの **no** 形式を使用します。

mls rp vtp-domain *name*

no mls rp vtp-domain *name*

シンタックスの説明

name	VLAN ドメイン名

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

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、インターフェイスを VTP ドメインにリンクする例を示します。

```
Router(config-if)# mls rp vtp-domain EverQuest
Router(config-if)#
```

関連コマンド

コマンド	説明
show mls rp	MLS 詳細を表示します。
vtp	グローバル VTP ステートを設定します。

mls sampling

サンプリング済み NetFlow のイネーブル化およびサンプリング方式の指定を行うには、**mls sampling** コマンドを使用します。サンプリング済み NetFlow をディセーブルにするには、このコマンドの **no** 形式を使用します。

mls sampling {{**time-based** *rate*} | {**packet-based** *rate* [*interval*]}}

no mls sampling

シンタックスの説明

time-based *rate*	時間ベースのサンプリング レートを指定します。有効値は **64**、**128**、**256**、**512**、**1024**、**2046**、**4096**、および **8192** です。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。
packet-based *rate*	パケットベースのサンプリング レートを指定します。有効値は **64**、**128**、**256**、**512**、**1024**、**2046**、**4096**、および **8192** です。
interval	（任意）サンプリング インターバル。有効値は 8000 ～ 16,000 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

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

PFC3 でサンプリングをイネーブルにするには、**mls sampling** コマンドおよび **mls netflow sampling** コマンドを適切なインターフェイスで入力する必要があります。**mls netflow sampling** コマンドを入力しないと、NDE はフローをエクスポートしません。

サンプリング済み NetFlow がサポートされるのは、レイヤ 3 インターフェイスだけです。

NDE がディセーブルの場合も、サンプリング済み NetFlow をイネーブルにできますが、フローはエクスポートされません。

パケットベース サンプリングの場合、パケット数が n のフローは n/m 回サンプリングされます（m はサンプリング レート）。

時間ベース サンプリングは、各サンプリング レートに事前設定されたインターバルに基づいて実行されます。表 2-24 に、各レートおよび期間におけるサンプル インターバルを示します。

表 2-24　時間ベース サンプリングのインターバル

サンプリング レート	サンプリング時間（ミリ秒）	エクスポート インターバル（ミリ秒）
1/64	128	8192
1/128	64	8192
1/256	32	8192

表 2-24　時間ベース サンプリングのインターバル （続き）

サンプリング レート	サンプリング時間（ミリ秒）	エクスポート インターバル（ミリ秒）
1/512	16	8192
1/1024	8	8192
1/2048	4	8192
1/4096	4	16384
1/8192	4	32768

例

次に、時間ベース NetFlow サンプリングをイネーブルにして、サンプリング レートを設定する例を示します。

```
Router(config)# mls sampling time-based 1024
Router(config)#
```

次に、パケットベース NetFlow サンプリングをイネーブルにして、サンプリング レートおよびインターバルを設定する例を示します。

```
Router(config)# mls sampling packet-based 1024 8192
Router(config)#
```

関連コマンド

コマンド	説明
mls netflow sampling	インターフェイス上でサンプリング済み NetFlow をイネーブルにします。
show mls sampling	サンプリング済み NDE ステータスに関する情報を表示します。

mls switching

ハードウェア スイッチングをイネーブルにするには、**mls switching** コマンドを使用します。ハードウェア スイッチ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。

mls switching

no mls switching

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

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、ハードウェア スイッチングをイネーブルにする例を示します。

```
Router(config)# mls switching
Router(config)#
```

次に、ハードウェア スイッチングをディセーブルにする例を示します。

```
Router(config)# no mls switching
Router(config)#
```

関連コマンド

コマンド	説明
mls switching unicast	ユニキャスト トラフィックのハードウェア スイッチングをインターフェイスでイネーブルにします。

mls switching unicast

インターフェイスに対するユニキャスト トラフィックのハードウェア スイッチングをイネーブルにするには、**mls switching unicast** コマンドを使用します。インターフェイスに対するユニキャスト トラフィックのハードウェア スイッチ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。

mls switching unicast

no mls switching unicast

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

インターフェイス 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。

例

次に、インターフェイスのハードウェア スイッチングをイネーブルにする例を示します。

```
Router(config-if)# mls switching unicast
Router(config-if)#
```

次に、インターフェイスのハードウェア スイッチングをディセーブルにする例を示します。

```
Router(config-if)# no mls switching unicast
Router(config-if)#
```

関連コマンド

コマンド	説明
mls switching	ハードウェア スイッチングをイネーブルにします。

mls verify

ハードウェア パケット解析エラー チェックをイネーブルにするには、**mls verify** コマンドを使用します。ハードウェアでレイヤ 3 エラー 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。

mls verify {**ip** | **ipx**} {**checksum** | {**length** {**consistent** | **minimum**}} | **same-address** | **syslog**}

no mls verify {**ip** | **ipx**} {**checksum** | {**length** {**consistent** | **minimum**}} **same-address** | **syslog**}

シンタックスの説明

ip	IP チェックサム エラーを指定します。
ipx	IPX チェックサム エラーを指定します。
checksum	チェックサムのエラー チェックを指定します。
length consistent	物理フレーム長と比較してヘッダーの長さをチェックします。
length minimum	最小パケット長をチェックします。
same-address	送信元 IP アドレスと宛先 IP アドレスが同一であるパケットをチェックします。
syslog	Syslog パケット解析エラー トラップを指定します。

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。

- **checksum**
- **same-address** はディセーブルです。
- **syslog** 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（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

短すぎる IP パケットとは、IP ヘッダーの長さの IP パケット、または IP の全長フィールドが 20 バイト未満のパケットのことです。

mls verify ip length minimum コマンドを入力すると、IP プロトコル フィールドが次のうちいずれかのタイプと同じである場合に限り、有効な IPv4 パケットがハードウェアでスイッチングされます。

- ICMP（1）
- IGMP（2）
- IP（4）
- TCP（6）

- UDP（17）
- IPv6（41）
- generic routing encapsulation（GRE; 総称ルーティングカプセル化）（47）
- SIPP-ESP（50）

no mls verify ip length minimum コマンドを入力すると、短すぎるパケットはハードウェアでスイッチングされます。IP プロトコルが 6（TCP）の短すぎるパケットはソフトウェアに送信されます。

送信元と宛先の IP アドレスが同じであるパケットがハードウェアでスイッチングされることを防ぐには、**mls verify ip same-address** コマンドを使用します。

例

次に、ハードウェアでのレイヤ 3 エラー チェックをイネーブルにする例を示します。

```
Router(config)# mls verify ip checksum
Router(config)#
```

次に、ハードウェアでのレイヤ 3 エラー チェックをディセーブルにする例を示します。

```
Router(config)# no mls verify ip checksum
Router(config)#
```

次に、送信元と宛先の IP アドレスが同じであるパケットがハードウェアでスイッチングされることを防止する例を示します。

```
Router(config)# mls verify ip same-address
Router(config)#
```

mobility

ワイヤレス multipoint generic routing encapsulation（mGRE; マルチポイント総称ルーティングカプセル化）トンネルを設定するには、**mobility** 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。

mobility {**network-id** *id*} | {**tcp adjust-mss**}

mobility [**trust** | **broadcast**]

シンタックスの説明

network-id *id*	mGRE トンネル用のワイヤレス ネットワーク ID を指定します。有効値は、1 ～ 4095 です。
tcp adjust-mss	アクセス ポイント上の TCP SYN および TCP ACK の maximum segment size（MSS; 最大セグメント サイズ）値を自動調整します。
trust	（任意）信頼されるネットワークを指定します。
broadcast	（任意）mGRE トンネルが nonbroadcast multiaccess（NBMA; 非ブロードキャスト マルチアクセス）から broadcast multiaccess（BMA; ブロードキャスト マルチアクセス）へ変換するよう指定します。

コマンドのデフォルト

信頼されないネットワーク

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、WLSM が搭載された Catalyst 6500 シリーズ スイッチだけでサポートされます。

tcp adjust-mss キーワードは、mGRE トンネル インターフェイス上だけでサポートされます。

TCC MSS を小さい値に変更する場合、**ip tcp adjust-mss** *value* コマンドを入力できます。

信頼されるネットワークは、DHCP またはスタティックな IP アドレスを使用できます。信頼されないネットワークは、DHCP クライアントだけをサポートします。

例

次に、mGRE トンネルのネットワーク識別番号を指定する例を示します。

```
Router (config-if)# mobility network-id 200
Router (config-if)#
```

次に、信頼されるネットワークを指定する例を示します。

```
Router (config-if)# mobility trust
Router (config-if)#
```

次に、mGRE トンネルが NBMA から BMA へと変換するよう指定する例を示します。

```
Router (config-if)# mobility broadcast
Router (config-if)#
```

次に、アクセス ポイント上の TCP SYN および TCP ACK の MSS 値を自動調整する例を示します。

```
Router (config-if)# mobility tcp adjust-mss
Router (config-if)#
```

関連コマンド

コマンド	説明
ip tcp adjust-mss	ルータを通過する TCP SYN パケットの MSS 値を調整します。
show mobility	レイヤ 3 モビリティおよびワイヤレス ネットワークに関する情報を表示します。

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** | **rpr-plus** | **sso**}

シンタックスの説明

rpr	RPR モードを指定します。
rpr-plus	RPR+ モードを指定します。
sso	SSO モードを指定します。

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。

- システムが冗長モードに設定されておらず、アクティブおよびスタンバイ スーパーバイザ エンジンに同じイメージがある場合は SSO モードになります。
- 異なるバージョンがインストールされている場合は RPR モードになります。
- 冗長機能がイネーブルの場合、デフォルトは設定されたモードになります。

コマンド モード

冗長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

rpr-plus キーワードは、Supervisor Engine 32 PISA ではサポートされていません。

Non-Stop Forwarding（NSF）/SSO 冗長モードは IPv4 をサポートします。NSF/SSO 冗長モードは、IPv6、IPX、および MPLS をサポートしません。

冗長スーパーバイザ エンジンが搭載された Catalyst 6500 シリーズ スイッチで MPLS を設定する場合は、Catalyst 6500 シリーズ スイッチを RPR モードで設定する必要があります。スイッチは、SSO のデフォルト モードで稼動しないでください。

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** コマンドを入力します。冗長コンフィギュレーション モードで、**mode** コマンドを入力できます。

スタンバイ 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、現在のモードで処理を開始します。

例

次に、冗長モードを SSO に設定する例を示します。

```
Router(config)# redundancy
Router(config-red)# mode sso
Router(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 エンジンへのスイッチオーバーを強制します。
route-converge-interval	古い FIB エントリの消去を開始する間隔を設定します。
show redundancy	Redundancy Facility（RF）情報を表示します。
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。

mode dot1q-in-dot1q access-gateway

ギガビット イーサネット WAN インターフェイスをイネーブルにして、QinQ VLAN 変換に関してゲートウェイとして動作させるには、**mode dot1q-in-dot1q access-gateway** コマンドを使用します。QinQ VLAN 変換をインターフェイス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。

mode dot1q-in-dot1q access-gateway

no mode dot1q-in-dot1q access-gateway

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　インターフェイス 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　このコマンドは、OSM-2+4GE-WAN+ OSM モジュールが搭載された Catalyst 6500 シリーズ スイッチのギガビット イーサネット WAN インターフェイスだけでサポートされます。

802.1Q は、パケットに 2 つの VLAN タグでタグ付けするトランキング オプションを提供して、複数の VLAN が中間ネットワークで同時にトランキングできるようにします。二重タグ付きトンネルのこの使用方法もまた、QinQ トンネリングといいます。

mode dot1q-in-dot1q access-gateway コマンドは、2 つの VLAN タグでパケットにタグ付けすることにより QinQ トンネリングを拡張し、中間ネットワークで複数の VLAN を同時にトランキングできるようにします。二重タグ付きトンネルでは次の機能が実行されます。

- 2 つの 802.1Q VLAN タグでタグ付けされたパケットを、VLAN タグの組み合わせに基づく宛先サービスにスイッチングします。
- VLAN タグに基づくトラフィック シェーピングをサポートします。
- 802.1P prioritization bit（P bit; 優先順位ビット）を内部（カスタマー）VLAN タグから外部（サービス プロバイダー）VLAN タグにコピーします。

複数の GE-WAN インターフェイスを 1 つの仮想ポートチャネル インターフェイスに統合して、QinQ リンク バンドルを有効にすることもできます。インターフェイスの統合は設定を簡略化するだけではなく、GE-WAN OSM がバンドルのメンバーである物理インターフェイス間の PE VLAN をロード バランシングできるようになります。また、リンク バンドルのインターフェイス メンバーの 1 つがダウンした場合、PE VLAN は自動的に他のバンドル メンバーへと再割り当てされます。

（注）　**mode dot1q-in-dot1q access-gateway** コマンドを使用する前に、インターフェイス上で設定されたすべての IP アドレスを削除する必要があります。

mode dot1q-in-dot1q access-gateway コマンドを設定したあと、各サブインターフェイス上で使用される VLAN マッピングを設定するには、**bridge-domain**（サブインターフェイス コンフィギュレーション）コマンドを使用します。

注意　インターフェイス上で **mode dot1q-in-dot1q access-gateway** コマンドを使用することにより、インターフェイスで設定された可能性のあるすべてのサブインターフェイスは自動的に削除されます。また、インターフェイスおよびそのサブインターフェイス上で事前に使用された可能性のあるすべての内部 VLAN が解放され、QinQ 変換で再利用できるようになります。このコマンドの **no** 形式を使用すると、すべてのサブインターフェイスが削除され、そのインターフェイスおよびサブインターフェイスによって現在使用されているすべての VLAN が解放されます。**mode dot1q-in-dot1q access-gateway** コマンドを入力する前に、インターフェイスのコンフィギュレーションを保存しておくことを推奨します。

（注）　ポートチャネル インターフェイス カウンタは（**show counters interface port-channel** コマンドおよび **show interface port-channel counters** コマンドにより表示される）、QinQ リンク バンドルに GE-WAN インターフェイスを使用するチャネル グループではサポートされません。ただし、**show interface port-channel** {*number* | *number.subif*} コマンド（**counters** キーワードなし）は、サポートされます。

ヒント　**mls qos trust** コマンドは、**mode dot1q-in-dot1q access-gateway** コマンドで設定された GE-WAN インターフェイスまたはポートチャネル グループには影響しません。これらのインターフェイスおよびポートチャネルは常に、この設定における VLAN CoS ビットを信頼します。

例

次に、**mode dot1q-in-dot1q access-gateway** コマンドの一般的な設定例を示します。

```
Router# configure terminal
Router(config)# interface GE-WAN 4/1
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、IP アドレスの設定を最初に削除せずに **mode dot1q-in-dot1q access-gateway** コマンドを設定しようとした場合に表示されるシステム メッセージの例を示します。

```
Router# configure terminal
Router(config)# interface GE-WAN 3/0
Router(config-if)# mode dot1q-in-dot1q access-gateway

% interface GE-WAN3/0 has IP address 192.168.100.101
configured. Please remove the IP address before configuring
'mode dot1q-in-dot1q access-gateway' on this interface.

Router(config-if)# no ip address 192.168.100.101 255.255.255
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、**mode dot1q-in-dot1q access-gateway** コマンドの **no** 形式を使用してインターフェイス上の QinQ マッピングをディセーブルにする例を示します。さらに、このコマンドはインターフェイス上のすべてのサブインターフェイス、およびサブインターフェイス QinQ マッピング（**bridge-domain**（サブインターフェイス コンフィギュレーション）コマンドで設定される）とサービス ポリシーのすべてを自動的に削除します。

```
Router# configure terminal
```

```
Router(config)# interface GE-WAN 3/0
Router(config-if)# no mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、2 つの GE-WAN インターフェイスで作成され割り当てられた仮想ポートチャネル インターフェイスの例を示します。**mode dot1q-in-dot1q access-gateway** コマンドはポートチャネル インターフェイス上でイネーブルとなり、ポートチャネル インターフェイスが QinQ リンク バンドルとして動作できるようになります。

```
Router(config)# interface port-channel 20
Router(config-if)# interface GE-WAN 3/0
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface GE-WAN 3/1
Router(config-if)# port-channel 20 mode on
Router(config-if)# interface port-channel 20
Router(config-if)# no ip address
Router(config-if)# mode dot1q-in-dot1q access-gateway
Router(config-if)#
```

次に、1 つまたは複数の無効なインターフェイスを含むポートチャネル インターフェイス上で QinQ 変換をイネーブルにしようとした場合に表示されるエラー メッセージの例を示します。

```
Router# configure terminal
Router(config)# interface port-channel 30
7600-2(config-if)# mode dot1q-in-dot1q access-gateway

% 'mode dot1q-in-dot1q access-gateway' is not supported on Port-channel30
% Port-channel30 contains 2 Layer 2 Gigabit Ethernet interface(s)

Router(config-if)#
```

関連コマンド

コマンド	説明
bridge-domain（サブインターフェイス コンフィギュレーション）	PVC を指定された *vlan-id* にバインドします。
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。
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。
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。
set cos cos-inner (policy-map configuration)	QinQ 変換された送信パケットのトランク VLAN タグの 802.1Q 優先順位ビットを、内部カスタマー エッジの VLAN タグからのプライオリティ値で設定します。

monitor event-trace (EXEC)

指定された Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレース機能を制御するには、**monitor event-trace** コマンドを使用します。

monitor event-trace all-traces {{**continuous** [**cancel**]} | {**dump** [**merged**] [**pretty**]}}

monitor event-trace l3 {**clear** | {**continuous** [**cancel**]} | **disable** | {**dump** [**pretty**]} | **enable** | {**interface** *type mod/port*} | **one-shot**}

monitor event-trace spa {**clear** | {**continuous** [**cancel**]} | **disable** | {**dump** [**pretty**]} | **enable** | **one-shot**}

monitor event-trace subsys {**clear** | {**continuous** [**cancel**]} | **disable** | {**dump** [**pretty**]} | **enable** | **one-shot**}

シンタックスの説明

all-traces	設定された統合イベント トレースを表示します。
continuous	最新のイベント トレース エントリを連続的に表示します。
cancel	（任意）最新のトレース エントリの連続表示をキャンセルします。
dump	**monitor event-trace (global configuration)** コマンドにより設定されたファイルにイベント トレース結果を書き込みます。
merged	（任意）時間でソートされたすべてのイベント トレースのエントリをダンプします。
pretty	（任意）イベント トレース メッセージを ASCII 形式で保存します。
l3	レイヤ 3 トレースに関する情報を表示します。
clear	トレースをクリアします。
disable	指定されたコンポーネントのイベント トレーシングをオフにします。
enable	指定されたコンポーネントのイベント トレーシングをオンにします。
interface *type mod/port*	記録されるインターフェイスを指定します。
one-shot	メモリからすべての既存トレース情報をクリアし、イベント トレーシングを再開し、トレースが **monitor event-trace (global configuration)** コマンドで指定されたサイズに到達するとトレースをディセーブルにします。
spa	SPA トレースに関する情報を表示します。
subsys	サブシステムの初期トレースに関する情報を表示します。

コマンドのデフォルト

トレース情報は、バイナリ形式で保存されます。

コマンド モード

特権 EXEC (#)

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

収集されるイベント トレース データの種類、収集時期、および方法を制御するには、**monitor event-trace**（EXEC）コマンドを使用します。このコマンドは、**monitor event-trace (global configuration)** コマンドによりネットワーキング デバイス上でイベント トレース機能を設定してから使用してください。

トレース メッセージは、バイナリ形式で保存されます。

（注）　トレースから収集されるデータ量は、トレース インスタンスごとの **monitor event-trace (global configuration)** コマンドで設定されたトレース メッセージ サイズに応じて異なります。

Cisco IOS ソフトウェアにより、サブシステム コンポーネントはブート時のイベント トレーシングのサポートがイネーブルかディセーブルかを定義できるようになります。イベント トレーシングをイネーブルまたはディセーブルにするには、2 つの方法があります。**monitor event-trace**（EXEC）コマンド、または **monitor event-trace (global configuration)** コマンドの使用です。イベント トレーシングを再度イネーブルにするには、このコマンドのいずれかから **enable** を入力します。

サブシステムがイベント トレーシングをイネーブルまたはディセーブルにしたかどうかを判別するには、**monitor event-trace?** コマンドを使用して、イベント トレーシングをサポートするソフトウェア コンポーネントのリストを取得します。サブシステムのデフォルトでイベント トレーシングがイネーブルかどうかを判別するには、**show monitor event-trace** コマンドを使用してトレース メッセージを表示します。

トレース メッセージは、**show monitor event-trace** コマンドを使用して表示します。

単一イベントのトレース メッセージ情報を保存するには、**monitor event-trace** *component* **dump** コマンドを使用します。デフォルトでは、トレース情報はバイナリ形式で保存されます。トレース メッセージを ASCII 形式で保存するには（おそらくは追加のアプリケーション処理用に）、**monitor event-trace** *component* **dump pretty** コマンドを使用します。

ネットワーキング デバイス上で現在イネーブルなすべてのイベントのトレース メッセージをファイルに書き込むには、**monitor event-trace dump-file**（グローバル コンフィギュレーション）コマンドを入力します。

トレース情報を保存するファイルを設定するには、**monitor event-trace (global configuration)** コマンドを使用します。

例

次に、イベント トレーシングを停止して、現在のメモリをクリアし、SPA コンポーネント用にトレース機能を再度イネーブルにする例を示します。次の例では、トレーシング機能がネットワーキング デバイス上で設定され、イネーブルにされていると仮定します。

```
Router# monitor event-trace spa disable
Router# monitor event-trace spa clear
Router# monitor event-trace spa enable
```

次に、**one-shot** キーワードを使用して、それほど多くのコマンドを入力せずに前出の例と同じ機能を実現する例を示します。トレース メッセージ ファイルのサイズが超過すると、トレースは終了します。

```
Router# monitor event-trace spa one-shot
Router#
```

次に、あるイベントのトレース メッセージをバイナリ形式で書き込む例を示します。interprocessor communication（IPC; プロセッサ間通信）コンポーネント用のトレース メッセージは、次のようにファイルに書き込まれます。

```
Router# monitor event-trace ipc dump
Router#
```

次に、あるイベントのトレース メッセージを ASCII 形式で書き込む例を示します。この例では、MBUS コンポーネント用のトレース メッセージがファイルに書き込まれます。

```
Router# monitor event-trace mbus dump pretty
Router#
```

関連コマンド

コマンド	説明
monitor event-trace (global configuration)	指定 Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレーシングを設定します。
show monitor event-trace	CiscoIOS ソフトウェア サブシステム コンポーネントのイベント トレース メッセージを表示します。

monitor event-trace (global configuration)

指定した Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレース機能を設定するには、**monitor event-trace**（グローバル）コマンドを使用します。デフォルト設定を変更してイベント トレーシングをイネーブルまたはディセーブルにするには、このコマンドの「使用上のガイドライン」を参照してください。

monitor event-trace all-traces dump-file *filename*

monitor event-trace l3 {**disable** | **dump-file** *filename* | **enable** | **size** *number* | {**stacktrace** [*depth*]}}

monitor event-trace sequence-number

monitor event-trace spa {**disable** | **dump-file** *filename* | **enable** | **size** *number* | {**stacktrace** [*depth*]}}

monitor event-trace stacktrace

monitor event-trace subsys {**disable** | **dump-file** *filename* | **enable** | **size** *number* | {**stacktrace** [*depth*]}}

monitor event-trace timestamps [{**datetime** [**localtime**] [**msec**] [**show-timezone**]} | **uptime**]

シンタックスの説明

dump-file *filename*	統合トレースを含むダンプ ファイルを保存する URL を指定します。
l3	レイヤ 3 トレースに関する情報を表示します。
disable	イベント トレーシングをオフにします。
enable	イベント トレーシングをオンにします。
size *number*	トレースの単一インスタンス用にメモリに書き込めるメッセージ数を設定します。有効値は、1 ～ 65,536 メッセージです。
stacktrace	イベント トレース エントリとともに保存されるスタック トレースを表示します。
depth	（任意）トレースポイントでのトレース コール スタック。有効値は、1 ～ 16 です。
sequence-number	イベント トレース エントリをシーケンス番号とともに表示します。
spa	SPA トレースに関する情報を表示します。
subsys	サブシステムの初期トレースに関する情報を表示します。
timestamps	イベント トレース タイム スタンプの形式に関する情報を表示します。
datetime	（任意）イベント トレース タイム スタンプの形式に関する情報を表示します。
localtime	（任意）イベント トレース タイム スタンプの形式に関する情報を表示し、日時を含めます。
msec	（任意）タイム スタンプにミリ秒を含めます。
show-timezone	（任意）イベント トレース タイム スタンプの形式に関する情報を表示し、タイム ゾーン情報を含めます。
uptime	（任意）システム アップタイムに関するタイプ スタンプ情報を表示します。

コマンドのデフォルト　ソフトウェア コンポーネントに応じてイネーブルまた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（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） イベント トレーシングは、ソフトウェア診断ツールとしての使用を目的としているため TAC 代理店の指導の下だけで設定する必要があります。イベント トレース機能のサブシステムのサポートを提供しない Cisco IOS ソフトウェア イメージでは、**monitor event-trace (global configuration)** コマンドは使用できません。

Cisco IOS ソフトウェアにより、サブシステム コンポーネントはデフォルトのイベント トレーシングのサポートがイネーブルかディセーブルかを定義できるようになります。イベント トレーシングのコマンド インターフェイスにより、ユーザはデフォルトの 2 つの方法を変更できます。**monitor event-trace (EXEC)** コマンドまたは **monitor event-trace (global configuration)** コマンドの使用です。

さらに、デフォルト設定はコンフィギュレーション ファイルに表示されません。サブシステム ソフトウェアがデフォルトでイベント トレーシングをイネーブルにする場合、**monitor event-trace** *component* **enable** コマンドはネットワーキング デバイスのコンフィギュレーション ファイルに表示されません。ただし、サブシステムによりデフォルトでイネーブルになったイベント トレーシングをディセーブルにすると、コンフィギュレーション ファイル内に 1 行作成されます。

（注） トレースから収集されるデータ量は、トレース インスタンスごとの **monitor event-trace (global configuration)** コマンドで設定されたトレース メッセージ サイズに応じて異なります。

メモリ内のイベント トレース メッセージ数がサイズを超過した場合、新規メッセージはファイル内の古いメッセージを上書きします。

filename 長の最大数（パスおよびファイル名）は 100 文字で、パスはネットワーキング デバイス上のフラッシュ メモリ、または TFTP サーバか FTP サーバにすることができます。

サブシステムがイベント トレーシングをイネーブルまたはディセーブルにしたかどうかを判別するには、**monitor event-trace?** コマンドを使用して、イベント トレーシングをサポートするソフトウェア コンポーネントのリストを取得します。

サブシステムのデフォルトでイベント トレーシングがイネーブルかどうかを判別するには、**show monitor event-trace** コマンドを使用してトレース メッセージを表示します。

トレースポイントのトレース コール スタックを指定するには、まずトレース バッファをクリアする必要があります。

例

次に、イベント トレーシングを停止して、現在のメモリをクリアし、SPA コンポーネント用にトレース機能を再度イネーブルにする例を示します。次の例では、トレーシング機能がネットワーキング デバイス上で設定され、イネーブルにされていると仮定します。

```
Router(config)# monitor event-trace spa disable
Router(config)# monitor event-trace spa clear
Router(config)# monitor event-trace spa enable
```

関連コマンド

コマンド	説明
monitor event-trace (EXEC)	指定 Cisco IOS ソフトウェア サブシステム コンポーネントのイベント トレース機能を制御します。
show monitor event-trace	CiscoIOS ソフトウェア サブシステム コンポーネントのイベント トレース メッセージを表示します。

monitor permit-list

宛先ポート許可リストを設定し、既存の宛先ポート許可リストに追加するには、**monitor permit-list** コマンドを使用します。既存の宛先ポート許可リストから削除またはクリアするには、このコマンドの **no** 形式を使用します。

monitor permit-list

monitor permit-list destination {**interface** *type*} {*slot*/*port*[**-***port*] [**,** *type slot*/*port* **-** *port*]

no monitor permit-list

no monitor permit-list destination {**interface** *type*} {*slot*/*port*[**-***port*] [**,** *type slot*/*port* **-** *port*]

シンタックスの説明

destination	宛先ポートを指定します。
interface *type*	インターフェイス タイプを指定します。有効値は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** です。
slot/*port*	スロット番号およびポート番号
-port	（任意）ポート範囲
,	（任意）その他のインターフェイス タイプおよびポート範囲

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

ポートが宛先として予想外に設定されるのを回避するために、宛先として使用できるポートの許可リストを作成できます。宛先ポート許可リストを設定した場合、宛先として設定できるのは許可リスト内のポートだけです。

例

次に、ギガビット イーサネット ポート 5/1 ～ 5/4 および 6/1 を含む宛先ポート許可リストを設定する例を示します。

```
Router# configure terminal
Router(config)# monitor permit-list
Router(config)# monitor permit-list destination interface gigabitethernet 5/1-4,
gigabitethernet 6/1
```

関連コマンド

コマンド	説明
show monitor permit-list	許可リストの状態、および設定されているインターフェイスを表示します。

monitor session

新規 Encapsulated remote SPAN（ERSPAN）、SPAN または remote SPAN（RSPAN）セッションの開始、既存セッションに対するインターフェイスまたは VLAN の追加や削除、特定の VLAN への ERSPAN、SPAN、または RSPAN トラフィックのフィルタリング、またはセッションの削除を行うには、**monitor session** コマンドを使用します。セッションから送信元または宛先インターフェイスを 1 つまたは複数削除したり、セッションから送信元 VLAN を削除したり、セッションを削除するには、このコマンドの **no** 形式を使用します。

monitor session *session* **source** {{**interface** *type*} | {{**vlan** *vlan-id*} [**rx** | **tx** | **both**]} | {**remote vlan** *rspan-vlan-id*}}

monitor session *session* **destination** {{**interface** *type*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*} | {**analysis-module** *slot-number*} | {**data-port** *port-number*}}

monitor session *session-number* **filter vlan** *vlan-range*

monitor session servicemodule *mod-list*

monitor session *session-number* **type** {**erspan-source | erspan-destination**}

no monitor session {{**range** *session-range*} | **local** | **remote** | **all** | *session*}

no monitor session *session* **source** {{**interface** *type*} | {{**vlan** *vlan-id*} [**rx** | **tx** | **both**]} | {**remote vlan** *rspan-vlan-id*}}

no monitor session *session* **destination** {{**interface** *type*} | {**vlan** *vlan-id*} | {**remote vlan** *vlan-id*} | {**analysis-module** *slot-number*} | {**data-port** *port-number*}}

シンタックスの説明

session	SPAN セッション番号。有効値は 1 ～ 66 です。
source	SPAN の始点を指定します。
interface *type*	インターフェイス タイプを指定します。フォーマットの詳細については、「使用上のガイドライン」を参照してください。
vlan *vlan-id*	VLAN ID を指定します。有効値は 1 ～ 4094 です。
rx	（任意）受信トラフィックだけをモニタするように指定します。
tx	（任意）送信トラフィックだけをモニタするように指定します。
both	（任意）受信トラフィックおよび送信トラフィックをモニタするように指定します。
remote vlan *rspan-vlan-id*	宛先 VLAN として RSPAN VLAN を指定します。
destination	SPAN 宛先インターフェイスを指定します。
analysis-module *slot-number*	ネットワーク解析モジュール番号を指定します。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。
data-port *port-number*	データポート番号を指定します。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。
filter vlan *vlan-range*	SPAN 送信元トラフィックを特定の VLAN に限定します。
servicemodule	サービス モジュールを指定します。
mod-list	（任意）サービス モジュール番号のリスト

type erspan-source	ERSPAN 送信元セッション コンフィギュレーション モードを開始します。詳細については、**monitor session type** コマンドを参照してください。
type erspan-destination	ERSPAN 宛先セッション コンフィギュレーション モードを開始します。詳細については、**monitor session type** コマンドを参照してください。
range *session-range*	セッション範囲を指定します。
local	ローカル セッションを指定します。
remote	リモート セッションを指定します。
all	すべてのセッションを指定します。

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。

- **both**
- **servicemodule** : すべてのサービス モジュールが、SPAN サービスモジュール セッションの使用を許可されます。

コマンドのデフォルト　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）　SPAN タイプ宛先ポートに関連付ける SPAN タイプ送信元ポートを設定するときは注意してください。高トラフィック インターフェイスでは SPAN を設定しません。高トラフィック インターフェイスで SPAN を設定すると、レプリケーション エンジンおよびインターフェイスを飽和させることがあります。SPAN タイプ宛先ポートに関連付ける SPAN タイプ送信元ポートを設定するには、**monitor session** *session* **source** {{**interface** *type*} | {{**vlan** *vlan-id*} [**rx** | **tx** | **both**]} | {**remote vlan** *rspan-vlan-id*}} コマンドを入力します。

モニタ セッションを設定するには、フォーマットに関する次の注意事項に従ってください。

- *interface* および *single-interface* のフォーマットは、*type slot*/*port* です。*type* の有効値は **ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** です。
- *interface-list* は、カンマで区切られたインターフェイス リストです。次の例のように、各カンマの前後にスペースを挿入します。

  single-interface , *single-interface* , *single-interface ...*
- *interface-range* は、ダッシュで区切られたインターフェイスの範囲です。各ダッシュの前後にスペースを挿入します。複数の範囲を入力するには、次の例のように各範囲をカンマで区切ります。

  type slot/*first-port - last-port*
- *mixed-interface-list* は、インターフェイス リストを組み合わせたものです。次の例のように、各ダッシュおよびカンマの前後にスペースを挿入します。

  single-interface, interface-range , ...（任意の順番）
- *single-vlan* は、単一 VLAN の ID 番号です。有効値は 1 ～ 4094 です。
- *vlan-list* は、カンマで区切られた VLAN ID リストです。次に例を示します。

  single-vlan , *single-vlan* , *single-vlan ...*
- *vlan-range* は、ダッシュで区切られた VLAN ID の範囲です。次に例を示します。

  first-vlan-ID - last-vlan-ID
- *mixed-vlan-list* は、VLAN ID リストを組み合わせたものです。各ダッシュの前後にスペースを挿入します。複数の範囲を入力するには、次の例のように各 VLAN ID をカンマで区切ります。

  single-vlan , *vlan-range* , ...（任意の順番）

analysis-module *slot-number* および **data-port** *port-number* キーワードおよび引数は、ネットワーク解析モジュールだけでサポートされています。

port-channel *number* の有効値は、1 ～ 256 の範囲の最大 64 個の値です。

SPAN セッション間で宛先インターフェイスを共有することはできません。たとえば、1 つの宛先インターフェイスは 1 つの SPAN セッションにだけ属することができ、別の SPAN セッションの宛先インターフェイスとして設定することはできません。

ローカル SPAN、RSPAN、および ERSPAN セッションの制限は次のとおりです。

総セッション	ローカル SPAN、RSPAN 送信元、または ERSPAN 送信元のセッション	RSPAN 宛先セッション	ERSPAN 宛先セッション
66	2（入力、出力、または両方）	64	23

ローカル SPAN、RSPAN、および ERSPAN の送信元および宛先の制限は次のとおりです。

	各ローカル SPAN セッション内	各 RSPAN 送信元セッション内	各 ERSPAN 送信元セッション内	各 RSPAN 宛先セッション内	各 ERSPAN 宛先セッション内
出力または入力 / 出力送信元				—	—
	128	128	128		
入力送信元				—	—
	128	128	128		
RSPAN および ERSPAN 宛先セッション送信元	—	—	—	RSPAN VLAN × 1	IP アドレス × 1
セッション単位の宛先	64	RSPAN VLAN × 1	IP アドレス × 1	64	64

特定の SPAN セッションは VLAN または各インターフェイスをモニタできます。特定のインターフェイスと特定の VLAN 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、エラーとなります。送信元 VLAN で SPAN セッションを設定し、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、エラーになります。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。

モニタされたトランク 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た場合、これらは、**interface** オプションのリスト上に表示されます。VLAN インターフェイスはサポートされません。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。

show monitor コマンドにより、SPAN サービスモジュール セッションが表示されます（割り当てられている場合だけ）。また、許可モジュールのリストおよびサービスモジュール セッションを使用できるアクティブ モジュールのリストも表示されます。

show running-config コマンドを入力すると、**monitor session servicemodule** コマンドの **no** 形式だけが表示されます。

モジュールでサービスモジュール セッションの使用が許可されない場合、サービスモジュール セッションの割り当ては自動的に解除されます。少なくとも 1 つのモジュールでサービスモジュール セッションの使用が許可され、少なくとも 1 つのモジュールがオンラインである場合、サービスモジュール セッションは自動的に割り当てられます。

サービス モジュールではないモジュールのリストによるサービスモジュール セッションの使用を許可する場合も許可しない場合でも、サービスモジュール セッションの割り当てまたは割り当ての解除には影響しません。モジュールのリストだけが、設定に保存されます。

no monitor session servicemodule コマンドにより SPAN サービスモジュール セッションをディセーブルにした場合、モジュールのリストによるサービスモジュール セッションの使用を許可するか許可しないかは、サービスモジュール セッションの割り当てまたは割り当て解除に影響しません。モジュールのリストだけが、設定に保存されます。

monitor session servicemodule コマンドは、スロットにモジュールが物理的に挿入されていない場合でも受け入れられます。

例

次に、セッションに複数の送信元を設定する方法を示します。

```
Router(config)# monitor session 2 source interface fastethernet 5/15 , 7/3 rx
Router(config)# monitor session 2 source interface gigabitethernet 1/2 tx
Router(config)# monitor session 2 source interface port-channel 102
Router(config)# monitor session 2 source filter vlan 2 - 3
Router(config)# monitor session 2 destination remote vlan 901
```

次に、最終スイッチに RSPAN 宛先を設定する例を示します（RSPAN 宛先セッション）。

```
Router(config)# monitor session 8 source remote vlan 901
Router(config)# monitor session 8 destination interface fastethernet 1/2 , 2/3
```

次に、セッション 1 および 2 の設定を削除する例を示します。

```
Router(config)# no monitor session 1 - 2
Router(config)#
```

次に、すべてのセッションの設定を削除する例を示します。

```
Router(config)# no monitor session all
Router(config)#
```

次に、すべてのリモート セッションの設定を削除する例を示します。

```
Router(config)# no monitor session remote
Router(config)#
```

次に、モジュールのリストによる SPAN サービスモジュール セッションの使用を許可する例を示します。

```
Router(config)# monitor session servicemodule module 1-2
Router(config)#
```

次に、モジュールのリストによる SPAN サービスモジュール セッションの使用を許可しない例を示します。

```
Router(config)# no monitor session servicemodule module 1-2
Router(config)#
```

関連コマンド

コマンド	説明
remote-span	VLAN を RSPAN VLAN として設定します。
show monitor session	ERSPAN、SPAN、RSPAN のセッションに関する情報を表示します。

monitor session type

ERSPAN 送信元セッション番号を作成するか、またはセッションに対して ERSPAN セッション コンフィギュレーション モードを開始するには、**monitor session type** コマンドを使用します。ERSPAN 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 *erspan-session-number* **type** {**erspan-destination** | **erspan-source**}

no monitor session *erspan-session-number* **type** {**erspan-destination** | **erspan-source**}

シンタックスの説明

erspan-session-number	SPAN セッション番号。有効値は 1 ～ 66 です。
type erspan-destination	ERSPAN 宛先セッション コンフィギュレーション モードを指定します。
type erspan-source	ERSPAN 送信元セッション コンフィギュレーション モードを指定します。

コマンド モード

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

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

ERSPAN は、ハードウェア リビジョン 3.2 以上でサポートされています。ハードウェア リビジョンを表示するには、**show module version | include WS-SUP720-BASE** コマンドを入力します。

ERSPAN トラフィックは、GRE カプセル化された SPAN トラフィックで、ERSPAN 宛先セッションによってだけ処理されます。

スイッチ上のすべての ERSPAN 送信元セッションは、同じ送信元 IP アドレスを使用する必要があります。ERSPAN 送信元セッションに IP アドレスを設定するには、**origin ip address** コマンドを入力します。

スイッチ上のすべての ERSPAN 宛先セッションは、同じ IP アドレスを使用する必要があります。ERSPAN 宛先セッションに IP アドレスを設定するには、**ip address** コマンドを入力します。ERSPAN 宛先 IP アドレスが Supervisor Engine 32 PISA ではない場合（ネットワーク スニファの場合など）、トラフィックは GRE および RSPAN ヘッダー/カプセル化とともにそのまま着信します。

ERSPAN 送信元セッションの宛先 IP アドレスが（宛先スイッチ上のインターフェイスで設定される必要がある）、ERSPAN 宛先セッションが宛先ポートに送信するトラフィックの送信元です。**ip address** コマンドを使用して、送信元および宛先セッションの両方で同じアドレスを設定します。

ERSPAN ID により、同じ宛先 IP アドレスに着信する ERSPAN トラフィックと異なる ERSPAN 送信元セッションとが区別されます。

ローカル ERSPAN セッションの制限は次のとおりです。

- 総セッション：66
- 送信元セッション：2（入力、出力、または両方）
- 宛先セッション：23

monitor session type コマンドにより、新しい ERSPAN セッションが作成されるか、または ERSPAN セッション コンフィギュレーション モードが開始されます。ERSPAN は別々の送信元および宛先セッションを使用します。送信元セッションと宛先セッションは、異なるスイッチに設定します。
ERSPAN セッション コンフィギュレーション モードのプロンプトは、次のとおりです。

- Router(config-mon-erspan-src)：ERSPAN 送信元セッション コンフィギュレーション モードを示します。
- Router(config-mon-erspan-src-dst)：ERSPAN 送信元セッション宛先コンフィギュレーション モードを示します。
- Router(config-mon-erspan-dst)：ERSPAN 宛先セッション コンフィギュレーション モードを示します。
- Router(config-mon-erspan-dst-src)：ERSPAN 宛先セッション送信元コンフィギュレーション モードを示します。

表 2-25 に、ERSPAN 宛先セッション コンフィギュレーション モードの構文を示します。

表 2-25　ERSPAN 宛先セッション コンフィギュレーション モードの構文

構文	説明
グローバル コンフィギュレーション モード	
monitor session *erspan-destination-session-number* **type erspan-destination**	ERSPAN 宛先セッション コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 `Router(config-mon-erspan-dst)#`
宛先セッション コンフィギュレーション モード	
description *session-description*	（任意）ERSPAN 宛先セッションを説明します。
shutdown	（任意）（デフォルト）ERSPAN 宛先セッションを終了します。
no shutdown	ERSPAN 宛先セッションを始動します。
destination {*single-interface* | *interface-list* | *interface-range* | *mixed-interface-list*}	ERSPAN 宛先セッション数を宛先ポートに関連付けます。
source	ERSPAN 宛先セッション送信元コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 `Router(config-mon-erspan-dst-src)#`
宛先セッション送信元コンフィギュレーション モード	
ip address *ip-address* [**force**]	ERSPAN フローの宛先 IP アドレスを設定します。これは、宛先スイッチ上のインターフェイスでも設定される必要があり、ERSPAN 宛先セッション コンフィギュレーションで入力されます。
erspan-id *erspan-flow-id*	ERSPAN トラフィックを識別するために、宛先および宛先セッションで使用される ID 番号を設定します。
vrf vrf-name	（任意）ERSPAN トラフィックのパケットの VRF 名を設定します。

表 2-26 に、ERSPAN 送信元セッション コンフィギュレーション モードの構文を示します。

表 2-26　ERSPAN 送信元セッション コンフィギュレーション モードの構文

構文	説明
グローバル コンフィギュレーション モード	
monitor session *erspan-source-session-number* **type erspan-source**	ERSPAN 送信元セッション コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 `Router(config-mon-erspan-src)#`
送信元セッション コンフィギュレーション モード	
description *session-description*	（任意）ERSPAN 送信元セッションを説明します。
shutdown	（任意）（デフォルト）ERSPAN 送信元セッションを終了します。
no shutdown	ERSPAN 送信元セッションを始動します。
source {{*single-interface* | *interface-list* | *interface-range* | *mixed-interface-list* | *single-vlan* | *vlan-list* | *vlan-range* | *mixed-vlan-list*} [**rx** | **tx** | **both**]}	ERSPAN 送信元セッション番号を送信元ポートまたは VLAN に関連付け、モニタされるトラフィック方向を選択します。
filter {*single-vlan* | *vlan-list* | *vlan-range* | *mixed-vlan-list*}	（任意）ERSPAN 送信元がトランク ポートである場合に、送信元 VLAN フィルタリングを設定します。
destination	ERSPAN 送信元セッション宛先コンフィギュレーション モードを開始して、プロンプトを次のように変更します。 `Router(config-mon-erspan-src-dst)#`
送信元セッション宛先コンフィギュレーション モード	
ip address *ip-address*	ERSPAN フローの宛先 IP アドレスを設定します。これは、宛先スイッチ上のインターフェイスでも設定される必要があり、ERSPAN 宛先セッション コンフィギュレーションで入力されます。
erspan-id *erspan-flow-id*	ERSPAN トラフィックを識別するために、送信元および宛先セッションで使用される ID 番号を設定します。
origin ip address *ip-address*	ERSPAN トラフィックの送信元として使用される IP アドレスを設定します。
ip {{**ttl** *ttl-value*} | {**prec** *ipp-value*} | {**dscp** *dscp-value*}}	（任意）次の ERSPAN トラフィックのパケット値を設定します。 • **ttl** *ttl-value*：IP 存続可能時間（TTL）値 • **prec** *ipp-value* *：* IP precedence 値 • **dscp** *dscp-value* *：* IP precedence 値
vrf *vrf-name*	（任意）ERSPAN トラフィックのパケットの VRF 名を設定します。

モニタ セッションを設定する場合は、次の構文の注意事項に従ってください。

- *erspan-destination-span-session-number* の範囲は、1 ～ 66 です。
- *single-interface* は、**interface** *type slot*/*port* です。*type* は、**ethernet**、**fastethernet**、**gigabitethernet**、または **tengigabitethernet** です。

- *interface-list* の形式は、*single-interface* , *single-interface* , *single-interface* です。

（注）　リストでは、カンマの前後でスペースを入力してください。リストでは、ダッシュの前後でスペースを入力してください。

- *interface-range* の形式は、**interface** *type slot*/*first-port* - *last-port* です。
- *mixed-interface-list* の形式は、順不同で *single-interface* , *interface-range* です。
- *erspan-flow-id* の範囲は、1 ～ 1023 です。

モニタ セッションをクリアする場合は、次の構文の注意事項に従ってください。

- **no monitor session** *session-number* コマンドを他のパラメータなしで入力すると、セッションの *session-number* をクリアします。
- *session-range* の形式は、*first-session-number-last-session-number* です。

（注）　**no monitor session range** コマンドを入力する場合は、ダッシュの前後にスペースを入力しないでください。複数の範囲を入力する場合は、カンマの前後にスペースを入力しないでください。

例

次に、ERSPAN 送信元セッション番号を設定し、セッションに対して ERSPAN 送信元セッション 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)# monitor session 55 type erspan-source
Router(config-mon-erspan-src)#
```

次に、ERSPAN 宛先セッション番号を設定し、セッションに対して ERSPAN 宛先セッション 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)# monitor session 55 type erspan-destination
Router(config-mon-erspan-dst)#
```

次に、ERSPAN 宛先セッション番号を宛先ポートに関連付ける例を示します。

```
Router(config-mon-erspan-dst) destination interface fastethernet 1/2 , 2/3
```

次に、ERSPAN 宛先セッション送信元設定を開始する例を示します。

```
Router(config-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

次に、ERSPAN 宛先セッション送信元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-mon-erspan-dst)# source
Router(config-mon-erspan-dst-src)#
```

次に、セッションに複数の送信元を設定する方法を示します。

```
Router(config-mon-erspan-src)# source interface fastethernet 5/15 , 7/3 rx
Router(config-mon-erspan-src)# source interface gigabitethernet 1/2 tx
Router(config-mon-erspan-src)# source interface port-channel 102
Router(config-mon-erspan-src)# source filter vlan 2 - 3
Router(config-mon-erspan-src)#
```

次に、ERSPAN 送信元セッション宛先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-mon-erspan-src)# destination
Router(config-mon-erspan-src-dst)#
```

次に、送信元および宛先セッションで使用される ID 番号を設定して、ERSPAN トラフィックを識別する例を示します。

```
Router(config-mon-erspan-src-dst)# erspan-id 1005
Router(config-mon-erspan-src-dst)#
```

関連コマンド

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

mpls l2transport route

MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにするには、**mpls l2transport route** コマンドを使用します。MPLS 上のルーティングをディセーブルにするには、このコマンドの **no** 形式を使用します。

mpls l2transport route *destination vc-id*

no mpls l2transport route *destination vc-id*

シンタックスの説明

destination	仮想回線の宛先となるルータの IP アドレス
vc-id	ルータへの仮想回線識別子

コマンド モード

このコマンドにはデフォルト設定がありません。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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

mpls l2transport route コマンドは、VLAN パケットをルーティングするのに使用される仮想回線をイネーブルにします。使用される仮想回線のタイプは次のとおりです。

- VC タイプ 4：VLAN 内のすべてのトラフィックが MPLS ネットワークで 1 つの VC を使用するようにします。
- VC タイプ 5：ポート上のすべてのトラフィックが MPLS ネットワークで 1 つの VC を共有するようにします。

VC 設定時は、VC タイプ 5 がアドバタイズされます。ピアが VC タイプ 4 をアドバタイズする場合、VC タイプがタイプ 4 に変更され、VC が再開します。変更はタイプ 5 からタイプ 4 だけが有効で、タイプ 4 からタイプ 5 には変更できません。

レイヤ 2 の MPLS VLAN 仮想回線は、MPLS クラウドを介して、2 つの PE ルータの VLAN インターフェイスを接続します。

MPLS クラウドを介して他の PE ルータの VLAN インターフェイスにレイヤ 2 の VLAN パケットをルーティングするには、各 PE ルータの VLAN インターフェイス上で **mpls l2transport route** コマンドを使用します。宛先パラメータには、他の PE ルータの IP アドレスを指定します。コマンドを発行しているルータの IP アドレスは指定しないでください。

仮想回線 ID は任意の値を選択できます。ただし、仮想回線 ID は仮想回線に対して一意でなければなりません。大規模ネットワークでは、同じ仮想回線 ID を 2 回割り当てることがないように、割り当てを管理する必要があります。

ルーテッド仮想回線はメイン インターフェイスではサポートされますが、サブインターフェイスではサポートされません。

仮想回線 ID は、仮想回線ごとに一意でなければなりません。

例

次に、MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにする例を示します。

```
Router(config-if)# mpls l2transport route 192.16.0.1
Router(config-if)#
```

関連コマンド

コマンド	説明
show mpls l2transport vc	ルータの仮想回線の状態を表示します。

mpls load-balance per-label

タグ間のトラフィックのロードバランスをイネーブルにするには、**mpls load-balance per-label** 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。

mpls load-balance per-label

no mpls load-balance per-label

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 モード

ディセーブル

コマンドのデフォルト

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

タグ間のトラフィックのロードバランスをイネーブルにする場合、トラフィックは MPLS インターフェイス間の着信ラベル（プレフィクスごと）に基づいて分散されます。各 MPLS インターフェイスは、同数の着信ラベルをサポートします。

show mpls ttfib コマンドを使用すれば、ロードバランサに含まれる着信ラベル（アスタリスク * で表示される）を表示できます。

例

次に、タグ間のトラフィックのロードバランスをイネーブルにする例を示します。

```
Router(config)# mpls load-balance per-label
Router(config)#
```

次に、タグ間のトラフィックのロードバランスをディセーブルにする例を示します。

```
Router(config)# no mpls load-balance per-label
Router(config)#
```

関連コマンド

コマンド	説明
show mpls ttfib	MPLS Toaster Tag FIB（TTFIB）テーブルに関する情報を表示します。

mpls ttl-dec

標準 MPLS タギングを指定するには、**mpls ttl-dec** 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。

mpls ttl-dec

no mpls ttl-dec

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 モード

最適化された MPLS タギング（**no mpls ttl-dec**）

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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

MPLS ラベルがパケット ヘッダーに付加される前に、元のパケットの IP ToS および TTL 値が書き換えられるように、MPLS タギングが最適化されました。この変更により、特定のトラフィック タイプに関して少しパフォーマンスが落ちる場合があります。パケットの元の ToS/TTL 値が重要でない場合は、**mpls ttl-dec** コマンドで標準 MPLS タギングを指定してください。

例

次に、Catalyst 6500 シリーズ スイッチが標準の MPLS タギング動作を使用するよう設定する例を示します。

```
Router(config)# mpls ttl-dec
Router(config)#
```

次に、Catalyst 6500 シリーズ スイッチが最適化 MPLS タギング動作を使用するよう設定する例を示します。

```
Router(config)# no mpls ttl-dec
Router(config)#
```

関連コマンド

コマンド	説明
mpls l2transport route	MPLS 上のレイヤ 2 パケットのルーティングをイネーブルにします。

mtu

最大パケット サイズまたは MTU サイズを調整するには、**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

シンタックスの説明

bytes	バイト サイズ。有効値は、SVI ポートでは 64 ～ 9216、GE-WAN+ ポートでは 1500 ～ 9170、その他のすべてのポートでは 1500 ～ 9216 です。

コマンド モード

表 2-27 に、ジャンボ フレームがディセーブルの場合のデフォルトの MTU 値を示します。

表 2-27　デフォルトの MTU 値

メディア タイプ	デフォルトの MTU（バイト）
イーサネット	1500
シリアル	1500
トークンリング	4464
ATM	4470
FDDI	4470
HSSI（HSA）	4470

ジャンボ フレームがイネーブルの場合、デフォルトは、SVI ポートでは 64、その他のすべてのポートでは 9216 です。デフォルトでは、ジャンボ フレームがディセーブルです。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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

スイッチ ポートの場合、グローバルに使用できるのは、デフォルト値よりも大きい MTU が 1 つだけです。レイヤ 3 ポート（ルータ ポートや VLAN を含む）の場合、インターフェイスごとにデフォルト以外の MTU 値を設定できます。

ジャンボ フレームをサポートしていない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。

mtu コマンドで MTU 値を設定すると、プロトコル固有バージョンのコマンドの値に影響が及ぶことがあります（**ip mtu** コマンドなど）。**ip mtu** コマンドで指定された値が **mtu** コマンドで指定された値と同じである場合に、**mtu** コマンドの値を変更すると、**ip mtu** 値は新しい **mtu** コマンドの値と一致するように自動的に調整されます。ただし、**ip mtu** コマンドの値を変更しても、**mtu** コマンドの値には影響しません。

例

次に、1800 バイトの MTU を指定する例を示します。

```
Router(config)# interface fastethernet 5/1
Router(config-if)#  mtu 1800
```

関連コマンド

コマンド	説明
ip mtu	インターフェイスで送信される IP パケットの MTU サイズを設定します。

name (MST configuration submode)

MST リージョン名を設定するには、**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*

シンタックスの説明

name	MST リージョンに付ける名前を指定します。最大 32 文字の任意のストリングです。

コマンド モード

空のストリング

コマンドのデフォルト

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

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複数の Catalyst 6500 シリーズ スイッチは、リージョン名が異なっている場合は異なった MST リージョンにあると見なされます。

注意　**name** コマンドで MST リージョン名を設定する場合には注意してください。設定を間違えると、Catalyst 6500 シリーズ スイッチが別のリージョンに配置されます。コンフィギュレーション名は大文字と小文字の区別があります。

例

次に、リージョンに名前を付ける例を示します。

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

関連コマンド

コマンド	説明
instance	1 つまたは一連の VLAN を MST インスタンスにマッピングします。
revision	MST コンフィギュレーションのリビジョン番号を設定します。
show	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。
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。

neighbor

ピアごとにトンネル シグナリングおよびカプセル化メカニズムのタイプを指定するには、**neighbor** コマンドを使用します。スプリット ホライズ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。

neighbor *remote-router-id* {**encapsulation** *encapsulation-type*} | {**pw-class** *pw-name*} [**no-split-horizon**]

no neighbor *remote-router-id*

シンタックスの説明

remote-router-id	リモート ピアリング ルータの ID
encapsulation *encapsulation*	トンネル カプセル化タイプを指定します。有効値は **l2tpv3** および **mpls** です。
pw-class *pw-name*	エミュレート VC の設定に使用する擬似配線プロパティを指定します。
no-split-horizon	（任意）データ パスにおいてレイヤ 2 スプリット ホライズンをディセーブルにします。

コマンド モード

スプリット ホライズンはイネーブルです。

コマンドのデフォルト

レイヤ 2 VFI 手動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。

ループを避けるには、完全にメッシュ化されている Virtual PVLAN service（VPLS）ネットワークでスプリット ホライズンをディセーブルにしないでください。

例

次に、トンネル カプセル化タイプの指定する例を示します。

```
Router(config-vfi)# neighbor 333 encapsulation mpls
Router(config-vfi)#
```

次に、レイヤ 2 スプリット ホライズンをデータ パスでディセーブルにする例を示します。

```
Router(config-vfi)# neighbor 333 no-split-horizon
Router(config-vfi)#
```

net

ルーティング プロセスに IS-IS network entity title（NET）を設定するには、**net** コマンドを使用します。NET を削除するには、このコマンドの **no** 形式を使用します。

net *net1* {**alt** *net2*}

no net *net*

シンタックスの説明

net1	プライマリ スロットに搭載された PISA 上の IS-IS ルーティング プロセスの NET network service access point（NSAP; ネットワーク サービス アクセス ポイント）名またはアドレス。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。
alt *net2*	代替スロットに搭載された PISA 上の IS-IS ルーティング プロセスの NET 名またはアドレスを指定します。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。
net	削除する NET NSAP 名またはアドレス

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。

- NET は設定されていません。
- IS-IS プロセス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（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

NET は、最終バイトが常に n セレクタであって常にゼロである NSAP です。NET のバイト数は 8 ～ 20 です。

ほとんどの場合、NET を 1 つだけ設定する必要があります。

net を入力する場合、次の点に注意してください。

- 3 スロット シャーシでは、スロット 1 がプライマリ スロットでスロット 2 が代替スロットです。
- 6 スロット シャーシでは、スロット 5 がプライマリ スロットでスロット 6 が代替スロットです。
- 9 スロット シャーシでは、スロット 5 がプライマリ スロットでスロット 6 が代替スロットです。
- 13 スロット シャーシでは、スロット 7 がプライマリ スロットでスロット 8 が代替スロットです。

IS-IS を使用して IP ルーティングだけを実行している（Connection-Less Network Service（CLNS）がイネーブルでない）場合、ルータ ID およびエリア ID を定義するように NET を設定する必要があります。

ルータごとに複数の NET（最大 3 つの NET）を設定できます。まれに、2 つまたは 3 つの NET を設定できることがあります。このような場合、このルータが属するエリアは、1 つのエリアに対して 3 つのエリア アドレスを持ちます。

複数の NET があると、複数のエリアを結合したり、1 つのエリアを複数のエリアに分割するネットワーク再設定時に、一時的に便利です。複数のエリア アドレスがある場合は、必要に応じてエリアごとに番号を付け直すことができます。

例

次に、ルータのシステム ID を 0000.0c11.1110、エリア ID を 47.0004.004d.0001 に設定する例を示します。

```
router isis Pieinthesky
 net 47.0004.004d.0001.0001.0c11.1111.00
```

次に、3 つのエリアが設定された IS-IS ルーティング プロセスを示します。エリアごとに一意の ID がありますが、システム ID はすべてのエリアで同じです。

```
clns routing

...

interface Tunnel529
 ip address 10.0.0.5 255.255.255.0
 ip router isis BB
 clns router isis BB

interface Ethernet1
 ip address 10.1.1.5 255.255.255.0
 ip router isis A3253-01
 clns router isis A3253-01
!
interface Ethernet2
 ip address 10.2.2.5 255.255.255.0
 ip router isis A3253-02
 clns router isis A3253-02

...

router isis BB                          ! Defaults to "is-type level-1-2"
 net 49.2222.0000.0000.0005.00
!
router isis A3253-01
 net 49.0553.0001.0000.0000.0005.00
 is-type level-1
!
router isis A3253-02
 net 49.0553.0002.0000.0000.0005.00
 is-type level-1
```

関連コマンド

コマンド	説明
is-type	IS-IS ルーティング プロセスのインスタンスのルーティング レベルを設定します。
router isis	IS-IS ルーティング プロトコルをイネーブルにして、IS-IS プロセスを指定します。

nsf

Cisco NSF をイネーブルにし、設定するには、**nsf** コマンドを使用します。NSF 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。

nsf [**enforce global**]

nsf [{**cisco** | **ietf**} | {**interface** {**wait** *seconds*}} | {**interval** *minutes*} | {**t3** [**adjacency** | {**manual** *seconds*}}]

no nsf

シンタックスの説明

enforce global	（任意）NSF 非対応ネイバが検出された場合、OSPF NSF の再開をキャンセルします。
cisco	（任意）アクティブな RP のフェールオーバーの場合に、シスコ独自の IS-IS NSF チェックポイント方式を指定します。
ietf	（任意）アクティブな RP のフェールオーバーの場合に、IETF IS-IS NSF プロトコル変更方式を指定します。
interface wait *seconds*	（任意）フェールオーバーのあと Cisco NSF プロセスを実行するまで、インターフェイスが動作するのを待機する時間を指定します。有効値は、1 ～ 60 秒です。
interval *minutes*	（任意）ルート プロセッサが安定したあと、再開するまで待機する時間を指定します。有効値は、0 ～ 1440 分です。
t3 adjacency	（任意）Label Switched Path（LSP; ラベル スイッチド パス）データベースが同期化するのを IETF NSF が待機する時間が、スイッチオーバーの前に、指定された RP のネイバにアドバタイズされる隣接の保持時間により決定されるよう指定します。
t3 manual *seconds*	（任意）NSF データベースの同期化のあと、再開ノードを中継として見なさないようその他のノードに知らせるまでの待機時間を指定します。有効値は、5 ～ 3600 秒です。

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。

- NSF はディセーブルです。
- **enforce global**：イネーブル
- **interval** *minutes*：5 分
- **interface wait** *seconds*：10 秒
- **t3 manual** *seconds*：30 秒

コマンド モード

ルータ コンフィギュレーション IS-IS

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

nsf t3 マニュアル コマンドを使用して、シスコ独自の IS-IS NSF が設定されているかまたは Internet Engineering Task Force（IETF）IS-IS NSF がイネーブルの場合、**nsf interface wait** コマンドを使用できます。インターフェイスが動作するまで時間がかかる場合、このコマンドを使用できます。

（注） Cisco NSF は、Catalyst 6500 シリーズ スイッチが再開時に Cisco NSF の実行が予想される場合だけ必要です。Catalyst 6500 シリーズ スイッチが、Cisco NSF の再開だけを実行するネイバと協力すると予想される場合、スイッチはデフォルト（Cisco NSF をサポートするバージョンのコードを実行）で NSF 対応である必要があります。

nsf コマンドは、**router** コマンドのサブセットで、指定されたプロセスの対象となるすべてのインターフェイスに影響します。Cisco NSF は、BGP、OSPF、IS-IS、および EIGRP プロトコルをサポートします。NSF 処理をイネーブルにするコンフィギュレーション コマンドは、次のとおりです。

- **nsf** under the **router ospf** コマンド
- **nsf ietf** under the **router isis** コマンド
- **bgp graceful-restart** under the **router bgp** コマンド

これらのコマンドは、ルータの実行コンフィギュレーションの一部として発行される必要があります。再開時にこれらのコマンドは、NSF 処理を作動させるよう復元されます。

[{**cisco** | **ietf**} | {**interface** {**wait** *seconds*}} | {**interval** *minutes*} | {**t3** [**adjacency** | {**manual** *seconds*}}] キーワードおよび引数は、IS-IS だけに適応されます。

{**enforce global**} キーワードは、OSPF だけに適応されます。

BGP NSF に関するガイドライン

NSF の BGP サポートでは、ネイバ ネットワークのデバイスが NSF 対応デバイスである必要があります。つまり、これらのデバイスにはグレースフル リスタート機能があり、セッション確立中に OPEN メッセージでこの機能をアドバタイズする必要があります。NSF 対応ルータが、特定の BGP ネイバでグレースフル リスタート機能がイネーブルでないことを検出した場合、このネイバを使用した NSF 対応セッションは確立されません。他のすべてのネイバに、グレースフル リスタート機能が備わっている場合は、この NSF 対応ネットワーキング デバイスを使用して NSF 対応セッションを引き続き維持します。グレースフル リスタート機能をイネーブルにするには、**bgp graceful-restart** ルータ コンフィギュレーション コマンドを入力します。詳細については、『*Cisco IOS Release 12.2 Command Reference*』を参照してください。

EIRGP NSF に関するガイドライン

ルータは NSF 対応のルータである可能性がありますが、コールド スタートから動作するため、NSF 再開のネイバの援助には参加しない場合があります。

IS-IS NSF に関するガイドライン

ネットワーキング デバイス上で IETF は設定されていても、ネイバ ルータが IETF と互換性がない場合、NSF はスイッチオーバーのあとで打ち切られます。

IS-IS NSF を設定する場合、次の 2 つのキーワードを使用します。

- **ietf** : Internet Engineering Task Force IS-IS。スーパーバイザ エンジンのスイッチオーバー後に、NSF 対応のルータが隣接する NSF 対応デバイスに IS-IS NSF 再開要求を送信します。

- **cisco** : Cisco IS-IS。すべての隣接情報および LSP 情報が、スタンバイ スーパーバイザ エンジンに対して保存（チェックポイント）されます。スイッチオーバー後、新しいアクティブ スーパーバイザ エンジンは、迅速にそのルーティング テーブルを再確立するために、チェックポイントされたデータを使用してその隣接を維持します。

OSPF NSF に関するガイドライン

OSPF NSF では、すべてのネイバ ネットワーキング デバイスが NSF 対応デバイスである必要があります。NSF 対応ルータが、特定のネットワーク セグメントに非 NSF アウェアのネイバが存在することを検出すると、このセグメントに対する NSF 機能はディセーブルになります。完全に NSF 可能または NSF 対応のルータだけで構成されているその他のネットワーク セグメントは、引き続き NSF 機能を提供します。

OSPF NSF は、IPv4 トラフィックに対してだけ NSF/SSO をサポートします。OSPFv3 は、NSF/SSO ではサポートされません。OSPFv2 だけが、NSF/SSO でサポートされます。

例

次に、すべての OSPF プロセス インターフェイスに関して NSF をイネーブルにする例を示します。

```
Router(config)# router ospf 109
Router(config-router)# nsf
Router(config-router)#
```

次に、すべての OSPF プロセス インターフェイスに関して NSF をディセーブルにする例を示します。

```
Router(config)# router ospf 109
Router(config-router)# no nsf
Router(config-router)#
```

関連コマンド

コマンド	説明
router	ルーティング プロセスをイネーブルにします。

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。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

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

no pagp learn-method

シンタックスの説明

aggregation-port	ポート チャネルでのアドレス学習を指定します。
physical-port	バンドル内の物理ポート上のアドレス学習を指定します。

コマンドのデフォルト

aggregation-port 方式

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、バンドル内の物理ポートのアドレス学習方式を設定する例を示します。

```
Router(config-if)# pagp learn-method physical-port
Router(config-if)#
```

次に、バンドル内のポートチャネルのアドレス学習方式を設定する例を示します。

```
Router(config-if)# pagp learn-method
Router(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 モードのポートを選択するには、**pagp port-priority** コマンドを使用します。デフォルト設定に戻すには、このコマンドの **no** 形式を使用します。

pagp port-priority *priority*

no pagp port-priority

シンタックスの説明

priority	プライオリティ番号。有効値は 1 ～ 255 です。

コマンドのデフォルト

priority は **128** です。

コマンドのデフォルト

インターフェイス コンフィギュレーション

コマンドの履歴

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

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

次に、ポート プライオリティを設定する例を示します。

```
Router(config-if)# pagp port-priority 45
Router(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。