CHAPTER 6

ライン インターフェイスの設定

この章では、物理ライン インターフェイス（ポート）の接続方法、およびこれらのインターフェイスをトンネリング、VLAN 変換、TOS マーキング、トラフィック規則用に設定する方法について説明します。

ライン インターフェイス

ライン インターフェイス（サブスクライバおよびネットワーク）は、SCE プラットフォームをネットワークに接続するために使用されます。ネットワーク トポロジの詳細については、『*Cisco SCE 2000/SCE 1000 Installation and Configuration Guides*』の「*Topology*」の章を参照してください。

SCE 1000 2xGBE および SCE 2000 4xGBE には、ギガビット イーサネット ライン インターフェイスが装備されています。これらのインターフェイスには、**auto-negotiate** を設定する必要があります。

SCE 2000 4/8x FE には、ファスト イーサネット ライン インターフェイスが装備されています。これらのインターフェイスには、**speed** および **duplex** を設定する必要があります。

フロー制御および帯域幅に関する考慮事項

（注） 設計上、SCE プラットフォームはイーサネットのフロー制御を対処し、アクティブ化しません。そのため、SCE プラットフォームのキューのオーバーフローによりフロー制御が SCE プラットフォームを実際に停滞させるような状況が起こり、Rx インターフェイス上でトラフィックがドロップされる可能性があります。このような状況が 5 秒以上続くと、SCE プラットフォームの内部健全性チェックが行われ、回復のために SCE プラットフォームがリロードされる場合もあります。

（注） SCE プラットフォーム シェイパを低い値（約数十 Mbps または 数百 Mbps）で使用すると（「全インターフェイス帯域幅の設定」）、システムの輻輳が発生し、サービス ロスが起こる可能性があります。これは、既知のシステム制限です。

ギガビット イーサネット ライン インターフェイスの設定方法

（注） SCE プラットフォームでサポートされる最大パケット サイズは、1600 バイトです。

ステップ 1　SCE# プロンプトに `configure` を入力して、**Enter** キーを押します。

グローバル コンフィギュレーション モードを開始します。

ステップ 2　SCE(config if)# プロンプトに、`interface GigabitEthernet 0/` *portnumber* を入力して、**Enter** キーを押します。*portnumber* は、選択したポート（1 ～ 4）の番号です。

選択した GBE インターフェイスのインターフェイス設定モードを開始します。

ステップ 3　SCE（config if）# プロンプトで、`auto-negotiate` と入力し、**Enter** キーを押します。

自動ネゴシエーションをイネーブルにします。

ステップ 4　SCE（config if）# プロンプトで、`exit` と入力し、**Enter** キーを押します。

グローバル コンフィギュレーション モードを終了します。そこから別のギガビット イーサネット インターフェイスにアクセスできます。

ステップ 5　残りのギガビット イーサネット インターフェイスに対して、ステップ 2 と 3 を繰り返します。

自動ネゴシエーションは、ギガビット イーサネット インターフェイスごとに別々に明示的にイネーブルにする必要があります。

ファスト イーサネット ライン インターフェイスの設定方法

FE リンクの両側（SCE 2000 4/8xFE およびリモート デバイスの両方）の設定は同じである必要があります。次の 2 つの設定オプションのいずれかを使用します。

- Autonegotiation = ON
- Autonegotiation = ON、speed = 100

ステップ 1　SCE# プロンプトに `configure` を入力して、**Enter** キーを押します。

グローバル コンフィギュレーション モードを開始します。

ステップ 2　SCE(config if)# プロンプトに、`interface FastEthernet 0/` *portnumber* を入力して、**Enter** キーを押します。*portnumber* は、選択したポート（1 ～ 4）の番号です。

選択した FE インターフェイスのインターフェイス設定モードを開始します。

ステップ 3　SCE(config if)# プロンプトに、`duplex` ***auto|full|half*** を入力して、**Enter** キーを押します。

選択した FE インターフェイスのデュプレックス モードを開始します。

ステップ 4　SCE(config if)# プロンプトに、`speed` ***auto|full|half*** を入力して、**Enter** キーを押します。

選択した FE インターフェイスの速度を設定します。

ステップ 5　SCE（config if）# プロンプトで、`exit` と入力し、**Enter** キーを押します。

グローバル コンフィギュレーション モードを終了します。そこから別のファスト イーサネット インターフェイスにアクセスできます。

ステップ 6　残りのファスト イーサネット インターフェイスに対して、ステップ 2 から 5 を繰り返します。

速度とデュプレックス モードは、ファスト イーサネット インターフェイスごとに別々に明示的にイネーブルにする必要があります。

トンネリング プロトコルの設定方法

トンネリング プロトコルについて

トンネリング テクノロジーは、さまざまなネットワーキング問題を解決するために、各種のテレコミュニケーション セグメントで使用されています。SCE プラットフォームは、多様なトンネリング プロトコルを複数の方法で認識して処理するように設計されています。SCE プラットフォームでは、トンネリング プロトコルを無視する（ヘッダーを「スキップする」）か、トンネリング情報をサブスクライバ情報として扱う（「分類する」）かのいずれかを実行できます。トンネリング情報による分類の特別な場合として、プライベート IP をサポートする MPLS/VPN があります。

次の表に、各種トンネリング プロトコルに対するサポートを示します（各プロトコルのデフォルト動作は太字で表示）。

表 6-1　トンネリング プロトコルの概要

プロトコル	サポートされる処理	モード名
L2TP	トンネルを無視する	IP-tunnel L2TP skip
	トンネルを無視しない — 外部 IP により分類する	No IP-Tunnel
VLAN	トンネルを無視する	VLAN symmetric skip
	トンネルを無視する — 非対称	VLAN a-symmetric skip
	VPN 分類で使用される VLAN タグ	VLAN symmetric classify
MPLS	トンネルを無視する（ラベルなしで挿入する）	MPLS Traffic-engineering skip
	トンネルを無視する（ラベル付きで挿入する）	MPLS VPN skip
	VPN 分類で使用される MPLS ラベル	MPLS VPN auto-learn

トンネリング情報が無視される場合、サブスクライバは、トンネル内部で伝送される IP パケットのサブスクライバ IP により識別されます。

L2TP

L2TP は IP ベースのトンネリング プロトコルであるため、システムに L2TP で使用される UDP ポートを与えて、L2TP フローを認識するように特別に設定する必要があります。SCE プラットフォームは、外部 IP ヘッダー、UDP ヘッダー、および L2TP ヘッダーをスキップして、実際のサブスクライバ トラフィックである内部 IP に到達できます。L2TP が設定されていない場合、システムは外部 IP ヘッダーをサブスクライバ トラフィックとして扱うため、トンネル内のすべてのトラフィックが単一フローとして認識されます。

VLAN

パケットごとに 1 つの VLAN タグがサポートされます（QinQ はサポートされない）。

VLAN タグによるサブスクライバ分類は、対称 VLAN 環境（すなわち、アップストリームおよびダウンストリームのフロー タグが同一）でのみサポートされます。

MPLS

プライベート IP をサポートする MPLS/VPN ベースのサブスクライバは、トンネリング情報による分類の特別な場合です。

MPLS ラベルは、パケットごとに最大 15 ラベルまでサポートされます。

MPLS/VPN ベースのサブスクライバについての詳細は、「MPLS/VPN のサポート」（p.14-1）を参照してください。

VPN

VPN は名前付きのエンティティで、サブスクライバの導入と同様に導入され、VPN マッピングを含みます。

VPN には、複数の MPLS マッピングまたは単一の VLAN マッピングを含めることができます。VPN ベースのサブスクライバには、IP@VpnName という形式のマッピングのセットが含まれます。この場合、IP は単一の IP アドレスまたはアドレス範囲です。

VPN エンティティは、SM によってのみ設定できます。SCE プラットフォームの CLI は、VPN 関連情報を表示するのに使用できますが、VPN の設定には使用できません。

プライベート IP アドレス

プライベート IP アドレスは、フローの IP アドレスが属する高いレベルのエンティティ（VLAN または VPN）に関する情報を提供するため、次のモードでのみサポートされます。

- MPLS VPN auto-learn
- VLAN symmetric classify

容量

システムのサポート容量は、次のとおりです。

- 2015 VPN
- VPN 上で 80,000 IP マッピング

VPN モードの制限

相互に排他的なシステム モード

システムで VPN モードを実行している場合、次のモードはサポートされません。

- TCP バイパスの確立
- DDoS
- Value Added Services（VAS）モード

MPLS ラベル数

- 固有の VPN サイトは、BGP ラベルだけに基づいて選択される必要があります。BGP ラベルは、最も内側のラベルでなければなりません。
- MPLS/VPN ソリューションでは、各種のラベルの組み合わせがサポートされます。
- MPLS-TE または MPLS-FRR などの他の MPLS 関連機能がイネーブルに設定されている VPN は、サポートされません。

サブスクライバ関連の制限

- SM は、プッシュ モードで動作するように設定する必要があります。
- VPN ベースのサブスクライバを使用している場合、サブスクライバのエージングは導入できません。

トポロジ関連の制限

- VPN　　の識別では、各種メカニズムに対するトラフィックの双方向性を信頼するため、トラフィックが単方向となる非対称のルーティング トポロジはサポートされません。

TCP 関連の要件

- アップストリーム TCP フロー数 **—** 各時間範囲で、各 PE-PE ルート上のサブスクライバ側から十分な TCP フローがオープンされる必要があります。サブスクライバ側からの TCP フロー数が多いほど、メカニズムの精度は高くなります。

VPN 設定の要件

- 次の両方の条件に適合する場合、2 つの VPN サイトを単一の VPN として集約する必要があります。
  - 両方とも、同じ SCE プラットフォームに接続している。
  - 両方とも､同じアップストリーム ラベルおよび P ルータを使用して共通のリモート サイトと通信する。
- MPLS ベースの VPN では（MPLS auto-learn モード）、サブスクライバは複数の VPN にまたがる IP マッピングを持ちません。
- VLAN ベースの VPN（VLAN 対称分類モード）では、サブスクライバは複数の VPN にまたがる IP マッピングを持ちますが、IP マッピングが VPN の全範囲（0.0.0.0/0）である場合に限ります（このオプションは、レガシー マルチ VLAN サブスクライバをサポートする下位互換性に対して提供されます）。

トンネリング モードの選択方法

トンネリングを設定するには、次のコマンドを使用します。

- ip tunnel
- vlan
- mpls
- L2TP identify-by

IP トンネルの設定方法

デフォルトでは、IP トンネルの認識がディセーブルにされています。L2TP トンネルの認識を設定し、内部 IP パケットにスキップするには、このコマンドを使用します。

IP トンネル モードは、VPN ベースの分類の使用と排他的な関係にあります。

ステップ 1　SCE(config if)# プロンプトに、`ip tunnel L2TP skip` を入力して、Enter キーを押します。

IP トンネル モードのイネーブル化

- IP トンネルをディセーブルにするには、次のコマンドを使用します。
  no ip tunnel

VLAN 環境の設定方法

VLAN 環境を設定するには、このコマンドを使用します。

- オプション（p.6-7）
- VLAN 環境の設定例（p.6-7）

オプション

3 つのオプションがあります。

- **symmetric classify**
- **symmetric skip**（デフォルト）
- **a-symmetric skip**

対称環境とは、アップストリーム方向およびダウンストリーム方向でのトランザクションの伝送に使用される VLAN タグが同じである環境を意味します。

分類するモードを設定することは、VPN とフローの分類に VLAN タグが使用されることを意味します。VLAN 分類は、その他のトンネルベースの分類または IP トンネルの使用と排他的な関係にあります。

非対称環境とは、同一フローのアップストリーム方向およびダウンストリーム方向での VLAN タグが異なる可能性がある環境です。

SCE プラットフォームは、デフォルトで対称環境で動作するよう設定されています。SCE プラットフォームが、非対称環境で適切に動作して、各フローのアップストリームとダウンストリームで VLAN タグが異なる可能性があることを考慮に入れるように設定するには、特定のコマンドを使用する必要があります。

（注）　a-symmetric skip 値を使用すると、パフォーマンス ペナルティが生じます。

ステップ 1　SCE(config if)# プロンプトで、`vlan {symmetric classify | symmetric skip |a-symmetric skip}` と入力し、**Enter** キーを押します。

目的の VLAN モードを指定します。

VLAN 環境の設定例

次に、VLAN ベースの分類を選択する例を示します。

```
SCE(config if)#vlan symmetric classify
```

MPLS 環境の設定方法

MPLS 環境を設定するには、このコマンドを使用します。

- オプション（p.6-8）
- MPLS 環境の設定例（p.6-8）

オプション

次のオプションを使用できます。

- **traffic-engineering skip**（デフォルト）— すべての IP アドレスが一意であり、ルーティングで MPLS ラベルが必須でない場合に使用します。
- **VPN skip** — すべての IP アドレスは一意ですが、ルーティングで MPLS ラベルが必須である場合に使用します。
- **VPN auto-learn** — プライベート IP アドレスと VPN ベースのサブスクライバのいずれかまたは両方が存在するため、自動学習が必要である MPLS/VPN 環境で使用します。

  このオプションを設定する場合、**ip-tunnel** と **VLAN** の両方をデフォルト値に設定する必要があります。

トラフィックでラベルが必要な場合は、*VPN* キーワードを使用します。それ以外の場合は、*traffic-engineering*（デフォルト）を使用します。

VPN 値を使用すると、パフォーマンス ペナルティが生じます。

MPLS/VPN 環境では、*MPLS VPN auto-learn* オプションが必要です。

ステップ 1　SCE（config if）# プロンプトで、**mpls {traffic-engineering skip|vpn skip|vpn auto-learn}** と入力し、**Enter** キーを押します。

目的の MPLS モードを指定します。

MPLS 環境の設定例

次に、MPLS/VPN トンネル環境を選択する例を示します。

```
SCE(config if)#mpls vpn auto-learn
```

- VPN モードの変更（p.6-8）
- デフォルトの VLAN または MPLS 環境の復元方法（p.6-8）

VPN モードの変更

VPN は、VLAN 対称分類モードまたは MPLS VPN 自動学習モードでのみ存在できますが、これらの 2 つのモードを同時にイネーブルにすることはできません。これらの VPN 関連モードをいずれか一方からもう一方に変更する場合は、次の注意事項に留意してください。

- トンネリング モードを変更するには、すべての VPN ベースのサブスクライバをクリアする必要があります。SM との接続がダウンしている場合には、`no subscriber all with-tunnel-mappings` CLI コマンドを使用します（「VPN ベースのサブスクライバについて」[p.9-13] を参照）。
- また、すべての VPN マッピングも削除する必要があります。これは、SM CLU 経由でのみ実行できます（SM との接続がアップである必要があることを意味します）（「VPN マッピングの管理方法」[p.14-27] を参照）。

デフォルトの VLAN または MPLS 環境の復元方法

デフォルトの VLAN または MPLS 設定を戻すには、次のコマンドを使用します。

明示的にデフォルト環境に戻すことは、VLAN または MPLS コマンドを実行すると自動的に行われるため、通常は必要ありません。このように自動的にデフォルトの状態にリセットされる場合は、次のメッセージと同様な警告メッセージが表示されます。

警告：以前設定された IP トンネル サポートまたはトンネリング分類モードがディセーブルになります。

ステップ 1　SCE(config if)# プロンプトで、`default {mpls | vlan}` と入力し、**Enter** キーを押します。

L2TP 環境の設定方法

LNS と LAC が L2TP トンネル用に使用するポート番号を設定するには、このコマンドを使用します。

- L2TP 環境の外部フラグメンテーション（p.6-9）
- オプション（p.6-9）

L2TP 環境の外部フラグメンテーション

外部フラグメンテーションが L2TP 環境に存在する場合は、LNS IP アドレスまたは LAC IP アドレスのいずれかに送信されるすべての IP トラフィックをバイパスする *quick-forwarding-ignore* トラフィック規則を設定する必要があります（「トラフィック規則とカウンタの設定方法」[p.6-14] を参照）。これにより、L2TP ポート表示を含まないすべてのパケット（つまり、2 番め以降のフラグメント）をトラフィック プロセッサで処理する必要がなくなります。

さらに、L2TP トンネリングされたフラグメントがリオーダーされないように、すべての L2TP トラフィックに *quick-forwarding* トラフィック規則を定義してください。これは、トンネルの内部 IP により使用される IP 範囲（LNS により割り当てられる）に基づいて実行される場合、または単に SCE プラットフォームをパススルーするすべてのトラフィックに対して実行される場合があります。

フロー リダイレクションおよびフロー ブロッキングは、高速転送されるトラフィック上では実行できません。

オプション

次のオプションを使用できます。

- **portnumber —** LNS と LAC が L2TP トンネル用に使用するポート番号。
  デフォルト ポート番号 = 1701

ステップ 1　SCE(config if)# プロンプトに、`L2TP identify-by port-number` *portnumber* を入力して、**Enter** キーを押します。

特権 EXEC モードをイネーブルにします。

トンネリング設定の表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 MPLS|VLAN|L2TP|IP-tunnel` を入力して、**Enter** キーを押します。

指定したトンネル オプションの現在の設定を表示します。

ログインされた VPN の表示方法

オプション

次のオプションを使用できます。

- **vpn-name** — 詳細を表示する現在ログインされている VPN の名前
- **all-names** — このキーワードは、システム内で現在ログインされているすべての VPN 名を表示するのに使用します。

ステップ 1　SCE> プロンプトに、`show interface linecard 0 VPN {name` *vpn-name* `| all-names}` を入力して、**Enter** キーを押します。

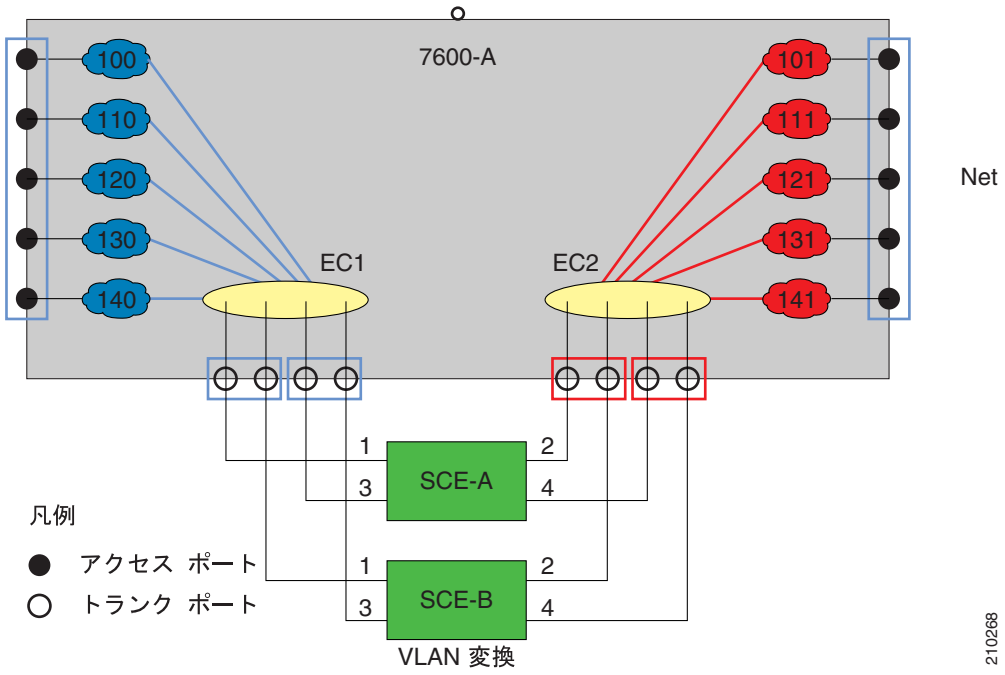
VLAN 変換の設定方法

VLAN 変換について

一部のトポロジでは、SCE プラットフォームで VLAN タグ間の変換が可能である必要があります。

次の図に、ディスパッチャとして動作するルータが、2 つの SCE 2000 プラットフォーム間でトラフィック転送およびロード バランシングを実行するシステムの例を示します。

図 6-1　VLAN 変換



この例では、トラフィックはアクセス ポートを経由してルータに入り、トランクとして設定されている EtherChannel に転送されて、SCE プラットフォームに入ります。

この図で示されるように、サブスクライバ側の VLAN タグは、ネットワーク側の VLAN タグと異なっている必要があります。そうでない場合、ルータはトラフィックを単に反対側のポートに転送することになります。SCE プラットフォームが、プリセットされた設定に従って VLAN タグを置き換えることにより、この機能を非常に単純にサポートすることができます。

VLAN 変換機能および制限事項

機能

- インクリメントまたはディクリメント定数の設定
- 定数の設定は、ラインカードに対してグローバルです。
- 設定された動作（インクリメントまたはディクリメントのいずれか）は、ネットワーク側に適用されます。
- サブスクライバ側では、自動的にその逆の動作が実行されます。すなわち、ネットワーク側で VLAN が X ずつインクリメントされる場合、サブスクライバ側では X ずつディクリメントされます。
- VLAN タグが付けられたパケットは、送信前に変更（インクリメントまたはディクリメント）されます。
- タグ付けされていないパケットは、変更されません。
- この機能により、非 VLAN トラフィックによるシームレスな処理が可能になります。

制限

- LIC バイパスはサポートされません — 変換は送信時に行われます。そのため、送信が行われない LIC バイパスでは変換も行われません。

  これは、VLAN 変換機能を使用するインストレーションは通常、障害時またはアップグレードのカットオフ（冗長 SCE プラットフォームを使用）を信頼する必要があることを意味します。
- STP ハザード — VLAN 変換は Spanning Tree Protocol（STP; スパニングツリー プロトコル）により干渉される場合があります。ソリューションを使用する場合は、このことを考慮に入れる必要があります。
- 設定可能な最大オフセットは、2047 です。ラップアラウンドに対する保護はありません。

VLAN 変換定数の設定方法

VLAN 変換定数を定義するには、このコマンドを使用します。システム内のすべての SCE プラットフォームで同じ VLAN 変換定数が設定されていることを確認します。

- オプション（p.6-12）
- VLAN 変換定数の設定：例（p.6-13）

オプション

次のオプションを使用できます。

- **increment | decrement** — VLAN を指定された *value* でインクリメントまたはディクリメントするかどうかを示すキーワード
- **value** — VLAN がインクリメントまたはディクリメントされる整数値

  設定された変換は、ネットワーク ポート側に適用されます。サブスクライバ側では、その逆の動作が実行されます。

  たとえば、「インクリメント 5」が定義された場合、ネットワーク ポートでは VLAN が 5 ずつインクリメントされ、サブスクライバ ポートでは 5 ずつディクリメントされます。

  この場合 VLAN タグは、ネットワーク側では 105、205、305 となり、サブスクライバ側では 100、200、300 となります。

  デフォルト＝ 0

  最大 = 2047（VLAN 値のラップアラウンドに対する保護がないことに注意してください）

ステップ 1　SCE(config if)# プロンプトに、`vlan translation increment|decrement value` *value* を入力して、**Enter** キーを押します。

VLAN 変換定数を設定します。

VLAN 変換定数の設定：例

次に、変換定数を 10 に設定して、ネットワーク側でディクリメントされる例を示します。

```
SCE(config if)#vlan translation decrement value 10
```

VLAN 変換のディセーブル化の方法

ステップ 1　SCE# プロンプトに、`no vlan translation` を入力して、Enter キーを押します。

VLAN 変換をディセーブルにします。

VLAN 変換の監視方法

ステップ 1　SCE# プロンプトに、**show interface linecard 0 vlan translation** を入力して、**Enter** キーを押します。

現在の VLAN 変換設定を表示します。

トラフィック規則とカウンタの設定方法

トラフィック規則とカウンタに関する情報

トラフィック規則およびカウンタとは

ユーザは、トラフィック規則とカウンタを設定できます。この機能を使用すると、ユーザは SCE プラットフォームを流れるトラフィックに特定の処理（特定のフローのブロックまたは無視、あるいは特定のパケットのカウント）を定義できます。トラフィック規則とカウンタの設定は、SCE プラットフォームがロードしたアプリケーションに依存しません。したがって、SCE プラットフォームが実行しているアプリケーションが変更されても持続します。

トラフィック規則とカウンタの利用方法には、次のようなものがあります。

- 各種の基準に従って、ユーザによるパケットのカウントを可能にする。トラフィック カウンタは SCE SNMP MIB 経由の読み取りが可能なので、インストレーション要件に従って、最大 32 種類のパケットの監視に使用できます。
- 特定のタイプのフローを無視する。トラフィック規則が [ignore] アクションを示す場合、規則基準に一致するパケットは、新規のフローを開かずに、処理されないまま SCE プラットフォームをパススルーします。これは、特定のタイプのトラフィックを SCE プラットフォームで無視しなければならない場合に役立ちます。

  たとえば、サービスを必要としないことが明らかな特定の IP 範囲、または特定のプロトコルのトラフィックを無視できます。
- 特定のタイプのフローをブロックする。トラフィック規則が [block] アクションを示す場合、規則基準に一致し、既存のフローに属さないパケットは、ドロップされ、他のインターフェイスに渡されません。これは、特定のタイプのトラフィックを SCE プラットフォームでブロックしなければならない場合に役立ちます。

  たとえば、入力側の送信元アドレスのフィルタリングを実行したり（定義済みのサブスクライバ側サブネットに IP アドレスが属さないサブスクライバ ポートが発信元のパケットをドロップする）、特定のポートをブロックしたりできます。

トラフィック規則とカウンタの使用は、パフォーマンスに影響しません。SCE プラットフォームのパフォーマンスの劣化を発生させることなく、トラフィック規則とカウンタの両方を最大数まで定義できます。

トラフィック規則

トラフィック規則は、特定の基準に一致し、SCE プラットフォームで処理されるパケットに定義されたアクションが実行されるように指定します。規則の最大数は 128 で、SCE プラットフォームの CLI で設定されるトラフィック規則の他に、SCA BB など外部管理システムにより設定される規則も含まれます。規則を定義するときに、各規則に名前が付けられます。この名前は、この規則を言及するときに使用されます。

ユーザが定義した基準に従って、パケットが選択されます。これは、次のいずれかの組み合わせになります。

- **IP アドレス —** 各回線ポート（サブスクライバ / ネットワーク）に指定できる単一アドレスまたはサブネット範囲
- **プロトコル —** TCP/UDP/ICMP/IGRP/EIGRP/IS-IS/OSPF/other
- **TCP/UDP ポート —** 各回線ポート（サブスクライバ / ネットワーク）に指定できる単一ポートまたはポート範囲。TCP/UDP プロトコルにのみ有効です。
- **方向（アップストリーム / ダウンストリーム）**（TCP のみ）

有効なアクションは、次のとおりです。

- 特定のトラフィック カウンタでパケットを**カウント**します。
- パケットを**ブロック**します（反対側に渡さない）。
- パケットを**無視**します（帯域幅の測定、トランザクションの報告などこのパケットに対するサービスは提供されません）。
- **サービスを提供**しながらパケットを**高速転送**します　—　遅延の影響を受けやすいパケットがサービサビリティを維持されながら、高速パスを介して転送されます。
- **サービスを提供せずに**パケットを**高速転送**します **—** 遅延の影響を受けやすいパケットがサービスを受けずに、高速パスを介して転送されます。

ブロックと**無視**のアクションは、既存のフローに属さないパケットにのみ影響します。

ブロックと**無視**は、相互に排他的な関係にあります。ただし、ブロックまたは無視されたパケットはいずれもカウントできます。

単一パケットを複数の規則に照合させることができます（実際にこのような状態にするのに最も簡単な方法は、異なる名前で同一の 2 つの規則を設定することです）。この場合、システムは次のように動作します。

- カウンタは、特定のパケットを一度だけカウントします。これは、次のことを意味します。
  - 2 つの規則が同一のカウンタでパケットをカウントすることを示す場合、一度だけカウントが行われます。
  - 2 つの規則が異なるカウンタでパケットをカウントすることを示す場合、2 回カウントが行われます（それぞれのカウンタで 1 回ずつ）。
- **ブロック**は**無視**よりも優先されます **—** ある規則が**ブロック**を指定し、別の規則が**無視**を指定する場合、パケットはブロックされます。

トラフィック カウンタ

トラフィック カウンタは、トラフィック規則の指定に従って、トラフィックをカウントします。カウンタの最大数は、32 です。カウンタを定義するときに、各カウンタに名前が付けられます。この名前は、このカウンタを言及するときに使用されます。

トラフィック カウンタは、2 つの方法のどちらかに設定できます。

- **Count packets —** カウンタは、カウントする各パケットに対して 1 つずつ増分します。
- **Count bytes —** カウンタは、カウントする各パケットに対して、パケットのバイト数を増分します。

トラフィック カウンタの設定方法

トラフィック規則でトラフィック カウンタを言及できるようにするには、まずトラフィック カウンタを作成する必要があります。トラフィック カウンタの作成と削除を行うには、次のコマンドを使用します。

- トラフィック カウンタの作成方法（p.6-16）
- トラフィック カウンタの削除方法（p.6-16）
- 既存のすべてのトラフィック カウンタの削除方法（p.6-16）

トラフィック カウンタの作成方法

オプション

次のオプションを使用できます。

- **name —** カウンタの名前
- **Count packets —** カウンタは、カウントする各パケットに対して 1 つずつ増分します。
- **Count bytes —** カウンタは、カウントする各パケットに対して、パケットのバイト数を増分します。

ステップ 1　SCE(config if)# プロンプトに、`traffic-counter name` *name* `count-bytes|count-packets` を入力して、**Enter** キーを押します。

指定した名前とカウント モードのトラフィック カウントを追加します。

トラフィック カウンタの削除方法

ステップ 1　SCE(config if)# プロンプトに、`no traffic-counter name` *name* を入力して、**Enter** キーを押します。

既存のトラフィック規則で使用されている場合には、トラフィック カウンタを削除できません。

既存のすべてのトラフィック カウンタの削除方法

ステップ 1　SCE(config if)# プロンプトに、`no traffic-counter all` を入力して、**Enter** キーを押します。

すべてのトラフィック カウンタを削除します。

既存のトラフィック規則で使用されている場合には、トラフィック カウンタを削除できません。

トラフィック規則の設定方法

トラフィック規則の作成と削除を行うには、次のコマンドを使用します。

トラフィック規則の作成方法

オプション

次のオプションを使用できます。

IP specification:

```
all|([all-but] (ip-address|ip-range))
```

- *ip-address* は、10.1.2.3 などのドット付き 10 進表記の単一 IP アドレスです。
- *ip-range* は、10.1.2.0/24 など、ドット付き 10 進表記のあとに有効ビット数が続く IP サブネット範囲です。
- 指定した IP アドレスまたは IP アドレスの範囲を除外するには、***all-but*** キーワードを使用します。

protocol:

次のプロトコルのいずれかになります。

```
TCP/UDP/ICMP/IGRP/EIGRP/IS-IS/OSPF/Other
```

tunnel id specification:

```
all|([all-but] tunnel id)
```

- tunnel id は、8 ビット 16 進数の値の範囲で、[（16 進数）*Tunnel-id*] または [（16 進数）*MinTunnelId*:（16 進数）*MaxTunnelId*] の形式です。VLAN タグの下位 8 ビットを反映します。
- トンネル ID ベースの規則は、「*VLAN 対称分類*」モードで、*トンネル ID* モードがイネーブルである場合に限り使用されます（「VLAN 環境の設定方法」[p.6-7] を参照）。

  traffic-rule tunnel-id-mode コマンドを使用します。

  VLAN タグそのものが 12 ビットであるため、使用される VLAN タグによって、下位 8 ビットのエイリアシングが発生する場合があります。

direction:

次のいずれかになります。

```
upstream/downstream/both
```

traffic-counter:

次のどちらかになります。

- **name** <*name of an existing traffic counter*> — 規則の基準に一致するパケットが、指定されたカウンタでカウントされます。カウンタ名が定義されている場合は、[count] アクションも暗黙的に定義されます。カウンタの実際の名前だけでなく、***name*** キーワードも表示される必要があります。
- **none** — ***none*** が指定されている場合、action オプションを介してアクションを明示的に定義する必要があります。

action:（アクションが count だけの場合は、必要なし）

下記のいずれかになります。

- **block —** 指定されたトラフィックをブロックします。
- **ignore —** 指定されたトラフィックをバイパスします。トラフィックにサービスが提供されません。
- **quick-forwarding —** 遅延の影響を受けやすいパケットがサービサビリティを維持されながら、高速パスを介して転送されます。
- **quick-forwarding-ignore —** 遅延の影響を受けやすいパケットがサービスを受けずに、高速パスを介して転送されます。

ステップ 1　SCE(config if)# プロンプトに、**traffic-rule name** *name* `IP-addresses (all|(subscriber-side <IP specification>network-side <IP specification>)) protocol` *protocol* [tunnel-id tunnel-id specification] `direction` *direction* `traffic-counter <traffic-counter>[action` *action* `]` を入力します。

特権 EXEC モードをイネーブルにします。

トラフィック規則の設定例

例 1

次に、以下の内容のトラフィック規則を作成する例を示します。

- 名前 = rule1
- IP アドレス：サブスクライバ側 = すべての IP アドレス、ネットワーク側 = 10.10.10.10 のみ
- プロトコル = other
- 方向 = 両方
- トラフィック カウンタ = counter1
- 唯一実行されるアクションは、カウントです。

```
SCE(config if)# traffic-rule rule1 IP-addresses subscriber-side all network-side
10.10.10.10 protocol other direction both traffic-counter name counter1
```

例 2

次に、以下の内容のトラフィック規則を作成する例を示します。

- 名前 = rule2
- IP アドレス：サブスクライバ側 = すべての IP アドレス、ネットワーク側 = 10.10.10.0/24 サブネット以外のすべての IP アドレス
- プロトコル = TCP
- トンネル id = all
- 方向 = downstream
- トラフィック カウンタ = counter2
- アクション = block
- 実行されるアクションは、カウントとブロックです。

最初のコマンドでトンネル ID モードがイネーブルになります。

```
SCE(config if)#traffic-rule tunnel-id-mode
SCE(config if)# traffic-rule rule2 IP-addresses subscriber-side all network-side
all-but 10.10.10.0/24 protocol tcp tunnel-id all direction downstream traffic-counter
name counter2 action block
```

例 3

次に、以下の内容のトラフィック規則を作成する例を示します。

- 名前 = rule3
- IP アドレス：all
- プロトコル = IS-IS
- 方向 = upstream
- トラフィック カウンタ = none
- アクション = ignore（トラフィック カウンタ = none であるために必須）
- The only action performed will be **Ignore.**

```
SCE(config if)# traffic-rule rule3 IP-addresses all protocol IS-IS direction upstream
traffic-counter none action ignore
```

トラフィック規則の削除方法

ステップ 1　SCE(config if)# プロンプトに、`no traffic-rule name` *name* を入力して、**Enter** キーを押します。

指定されたトラフィック規則を削除します。

すべてのトラフィック規則の削除方法

ステップ 1　SCE(config if)# プロンプトに、`no traffic-rule all` を入力して、**Enter** キーを押します。

既存のすべてのトラフィック カウンタを削除します。

トラフィック規則とカウンタの管理方法

既存のトラフィック規則の設定、トラフィック カウンタの設定（パケット / バイトとカウンタを使用する規則名）、およびトラフィック カウンタの値を表示するには、これらのコマンドを使用します。

特定のカウンタまたはすべてのカウンタをリセットすることもできます。

- 指定したトラフィック規則の表示方法（p.6-20）
- すべてのトラフィック規則の表示方法（p.6-20）
- 指定したトラフィック カウンタの表示方法（p.6-20）
- すべてのトラフィック カウンタの表示方法（p.6-20）
- 指定したトラフィック カウンタのリセット方法（p.6-21）
- すべてのトラフィック カウンタのリセット方法（p.6-21）

指定したトラフィック規則の表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 traffic-rule name` *rule-name* を入力して、**Enter** キーを押します。

指定したトラフィック規則の設定を表示します。

すべてのトラフィック規則の表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 traffic-rule all` を入力して、**Enter** キーを押します。

既存のすべてのトラフィック規則の設定を表示します。

指定したトラフィック カウンタの表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 traffic-counter name` *counter-name* を入力して、**Enter** キーを押します。

指定されたカウンタの値を表示して、使用するトラフィック規則を一覧表示します。

トラフィック カウンタの表示：例

次に、トラフィック カウンタ [cnt] の情報を表示する例を示します。

```
SCE# show interface linecard 0 traffic-counter name cnt
Counter 'cnt' value: 0 packets. Rules using it: None.
```

すべてのトラフィック カウンタの表示方法

ステップ 1　SCE# プロンプトに、`show interface linecard 0 traffic-counter all` を入力して、**Enter** キーを押します。

各カウンタの値を表示して、使用するトラフィック規則を一覧表示します。

トラフィック カウンタの表示：例

次に、既存のすべてのトラフィック カウンタ情報を表示する例を示します。

```
SCE# show interface linecard 0 traffic-counter all
Counter 'cnt' value: 0 packets. Rules using it: None.
Counter 'cnt2' value: 0 packets. Rules using it: Rule2.
2 counters listed out of 32 available.
```

指定したトラフィック カウンタのリセット方法

ステップ 1　SCE# プロンプトに、`clear interface linecard 0 traffic-counter name` *counter-name* を入力して、**Enter** キーを押します。

指定されたカウンタの値を表示して、使用するトラフィック規則を一覧表示します。

すべてのトラフィック カウンタのリセット方法

ステップ 1　SCE# プロンプトに、`clear interface linecard 0 traffic-counter all` を入力して、**Enter** キーを押します。

各カウンタの値を表示して、使用するトラフィック規則を一覧表示します。

TOS マーキング

TOS マーキングは、ネットワーク要素間のフローのプライオリティを伝える手段として IP ネットワークで使用されます。Cisco Service Controlo ソリューションでは、SCA BB アプリケーションによるサービス単位、パッケージ レベル単位の TOS 分類をサポートしています。SCE プラットフォームの TOS マーキング機能を使用すると、SCA BB コンソール経由で設定されるポリシーに準じて各パケットの IP ヘッダーにある TOS フィールドにマーキングを行うことができます。IP ヘッダーに設定される実際の TOS 値は、設定可能な TOS 変換テーブルで定義される値によって決まります。

TOS マーキングの設定は SCA BB コンソール経由で実行されます。各インターフェイスの TOS マーキングのステート（イネーブルまたはディセーブル）および TOS 変換テーブルを表示するには、SCE プラットフォームの CLI を使用できます。

TOS マーキングの設定については、『*Cisco Service Control Application for Broadband User Guide*』Rel 3.1.5 を参照してください。

（注）　Release 3.1.5 の TOS マーキングは、以前の SCOS リリースとは下位互換性がありません。

TOS マーキング設定の表示方法

インターフェイス単位の TOS マーキングのステート（イネーブルまたはディセーブル）および TOS 変換テーブルを表示するには、次のコマンドを使用します。

ステップ 1　SCE> プロンプトに、`show interface linecard 0 ToS-marking` を入力して、**Enter** キーを押します。

ドロップされるパケットのカウント方法

ドロップされるパケットのカウントについて

SCE プラットフォーム ハードウェアはデフォルトで、レッド パケット（BW 制御基準によりドロップするようマーク付けされたパケット）をドロップします。ただし、これはサービスごとにドロップされるパケット数を把握する必要があるユーザにとっては問題があります。ドロップされるパケット数をサービスごとにカウントするには、トラフィック プロセッサがすべてのフローでドロップされる全パケットを認識しなければなりません。ただし、ハードウェアがレッド パケットをドロップする場合、トラフィック プロセッサはドロップされる全パケットをカウントできず、ユーザは関連する MIB カウンタ（*tpTotalNumWredDiscardedPackets*）で正確な値を把握できません。

（注）　MIB オブジェクト *tpTotalNumWredDiscardedPackets* がドロップされるパケットをカウントします。このカウンタの値は、ハードウェア パケット ドロップがディセーブルな場合（非デフォルト モード）に限り絶対的です。ハードウェア パケットのドロップがイネーブルの場合（デフォルト モード）、この MIB カウンタは約 1:6 の係数によりパケットのドロップ数の傾向を示す相対値のみを提供します。

ユーザは、drop-red-packets-by-hardware モードをディセーブルにできます。これにより、アプリケーションから既存のフロー単位のカウンタにアクセスできるようになります。アプリケーションは、ドロップされるパケット数をフローごとに入手して、ユーザにドロップされるパケットの正確な数およびその分配を提示できます。

ドロップされる全パケットをカウントすることは、システム パフォーマンスにかなりの影響を与えるため、デフォルトでは drop-red-packets-by-hardware mode モードがイネーブルに設定されています。

ハードウェア パケット ドロップをディセーブルにする方法

drop-red-packets-by-hardware モードをディセーブルにして、ソフトウェアでドロップされる全パケットをカウントできるようにするには、このコマンドを使用します。

デフォルトでは、ハードウェア パケット ドロップはイネーブルです。

（注）　この機能をディセーブルにすると、遅延およびパフォーマンスの両方に影響する可能性があります。

ステップ 1　SCE(config if)# プロンプトに、`no accelerate-packet-drops` を入力して、**Enter** キーを押します。

ハードウェア パケット ドロップをディセーブルにします。

- ハードウェア パケット ドロップをイネーブルにするには、次のコマンドを使用します。
  accelerate-packet-drops