CHAPTER 7

ライン インターフェイスの設定

概要

ここでは、物理ライン インターフェイス（ポート）の設定方法、トンネリング、VLAN 変換、DSCP マーキング、およびトラフィック規則に合わせてライン インターフェイスを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（サブネット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。『*Cisco SCE8000 GBE Installation and Configuration Guide*』の「Cisco SCE8000 GBE Topology and Topology-Related Parameters」に記載されているネットワーク トポロジの説明を参照してください。

ライン インターフェイスについて

SCE8000 GBE ライン インターフェイスは、スロット 3 のサブスロット 0 および 1 にインストールされている 8 ポート ギガビット イーサネット SPA にあります。各 8 ポート ギガビット イーサネット SPA には、8 個の GBE ポートがあり、サブスクライバまたはネットワーク トラフィックのインターフェイスに使用されます。このインターフェイスは、このセクションで説明する CLI コマンドを使用して個別に設定できます。

フロー制御と帯域幅に関する考慮事項

（注）　設計によっては、SCE プラットフォームがイーサネット フロー制御に反応し、アクティブ化しないことがあります。そのため、フロー制御によって SCE プラットフォーム キューのオーバーフローが発生し、それによって Rx インターフェイス上のトラフィックがドロップし、SCE プラットフォームが機能しなくなる状況になることがあります。5 秒より長くこの状況が続くと、SCE プラットフォーム内の健全性チェック メカニズムが起動し、結果として修復するために SCE プラットフォームのリロードが実行される可能性があります。

最大パケット サイズ

Cisco SCE8000 トラフィック プロセスの MTU 値は 9,238 バイトです。ただし、現在のバージョンでは、1,600 バイトよりも大きなパケットはバイパスされ、サービス コントロール アプリケーションで処理されません。

ライン インターフェイスの設定

GBE ライン インターフェイスは、ギガビット イーサネット モードで設定されます。目的のインターフェイスについてギガビット イーサネット モードを開始する必要があります。ギガビット イーサネット モードでは、そのインターフェイスに関して次の設定コマンドにアクセスできます。

- **auto-negotiate**
- **global-controller bandwidth**
- **global-controller name**

interface range コマンドを使用して、ギガビット イーサネット ライン インターフェイスの範囲を設定することもできます。このコマンドを使用して、インターフェイスの範囲を指定できます。上記の 3 つの設定コマンドのいずれかが、指定した範囲のすべてのインターフェイスに適用されます。

特定のギガビット イーサネット ライン インターフェイスを設定する方法

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 モードに移行します。

ステップ 2　SCE(config)# プロンプトに、**interface GigabitEthernet 3**/*bay number*/*port number* を入力して、**Enter** キーを押します。

選択した GBE インターフェイスについてインターフェイス コンフィギュレーション モードを開始します。

- *bay number* は選択した SPA ベイの数です（0 または 1）
- *port number* は選択したインターフェイスの数です（0 ～ 7）
- 現在、スロット番号は常に 3 です。

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

終了してグローバル コンフィギュレーション モードに移行します。このモードでは、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。

ギガビット イーサネット ライン インターフェイスの範囲を設定する方法

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 モードに移行します。

ステップ 2　SCE(config)# プロンプトに、**interface range GigabitEthernet 3**/*bay range*/*port range* を入力して、**Enter キーを押します。**

選択した範囲の GBE インターフェイスについてインターフェイス コンフィギュレーション モードに移行します。

- *bay range* には、0、1、または 0-1 を指定できます。
- *port range* には、0 ～ 7 の任意の範囲を指定できます。その範囲の特定のポート番号を指定することもできます。
- 現在、スロット番号は常に 3 です。

ステップ 3　SCE(config if range)# プロンプトに、**exit** を入力して、**Enter** キーを押します。

終了してグローバル コンフィギュレーション モードに移行します。このモードでは、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。

ギガビット イーサネット ライン インターフェイスの範囲の設定：例

次に、両方の SCE8000-SPA モジュールにポート 3 ～ 6 を設定する例を示します。

```
SCE>configure
SCE(config)interface range GigabitEthernet 3/0-1/3-6
SCE (config if range)
```

カスケード接続されたペアの指定した SCE8000 についてギガビット イーサネット ライン インターフェイスを設定する方法

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 モードに移行します。

ステップ 2　**interface range GigabitEthernet または interface GigabitEthernet** コマンドで、次のように SCE8000 の ID を指定します。

- **interface range GigabitEthernet** *sce-id*/ **3**/*bay range*/*port range*
- **interface GigabitEthernet** *sce-id*/**3**/*bay number*/*port number*

この sce-id は、カスケード接続されたペアの SCE8000 プラットフォームの ID です（0 または 1）。

指定した SCE8000 のギガビット イーサネット ライン インターフェイスの設定：例

次に、カスケード接続されたペアの SCE プラットフォーム #1 上にある両方の SCE8000-SPA モジュールについて、ポート 3 ～ 6 を設定する例を示します。

```
SCE>configure
SCE(config)interface range GigabitEthernet 1/3/0-1/3-6
SCE (config if range)
```

トンネリング プロトコル

トンネリング テクノロジーは、さまざまなネットワーク問題を解決するために、各種の電気通信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および処理でき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（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」）ことができます。トンネリング情報による分類の特殊な場合は、プライベート IP をサポートする VPN です。

表 7-1 に、多様なトンネリング プロトコルのサポート内容を示します（太字は各プロトコルのデフォルト動作です）。

表 7-1　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	対称 / 非対称
L2TP	トンネルを無視します	IP-tunnel L2TP skip	非対称
	トンネルを無視しません（外部 IP で分類します）	**no IP-tunnel**	対称
GRE	トンネルを無視します	ip-tunnel GRE skip	対称
	トンネルを無視しません（外部 IP で分類します）	**no ip-tunnel GRE skip**	対称
IPinIP	トンネルを無視します	ip-tunnel IPinIP skip	対称
	トンネルを無視しません（外部 IP で分類します）	**no ip-tunnel IPinIP skip**	対称
VLAN	トンネルを無視します	**VLAN symmetric skip**	対称
	トンネルを無視します（非対称）	VLAN a-symmetric skip	非対称
	VPN 分類に使用される VLAN タグ	VLAN symmetric classify	対称
MPLS	トンネルを無視します（ラベルを付けずに挿入）	**MPLS traffic-engineering skip**	対称
	トンネルを無視します（ラベルを付けて挿入）	MPLS VPN skip	非対称

トンネリング情報が無視されると、サブスクライバ識別情報は、トンネル内で伝送される IP パケットのサブスクライバ IP です。

非対称トンネリング

トンネリング モードには対称型と非対称型があります（表 7-1 を参照）。非対称トンネリング モードのいずれかをイネーブルにすると、システム全体が非対称フロー オープン モードへと自動的に設定されます。このモードでは、フローは対称フロー オープン モードよりも早く開かれ、フローの各方向（アップストリームとダウンストリーム）の最初のパケットがソフトウェアに到達します。これは、非対称レイヤ 2 プロトコル上のリダイレクト処理とブロック処理をサポートするために必要です。ただし、パフォーマンスと容量の両方にある程度の影響もあるため、非対称モードでは一定のパフォーマンスの低下を見込む必要があります。

また、パケット挿入（ブロック フロー処理やリダイレクト フロー処理など）の目的で、すべてのフローが非対称レイヤ 2 の特性を持つようにシステムを明示的に設定することもできます（イーサネット、VLAN、MPLS、および L2TP を含みます）。

有効なフロー オープン モードを表示するには、**show interface linecard 0 flow-open-mode** コマンドを使用します。

（注）　非対称トンネリング オプションを設定する方法については、「非対称 L2 のサポート」（P.7-12）を参照してください。

L2TP

L2TP は、IP ベースのトンネリング プロトコルです。そのため、UDP ポートを L2TP に使用する場合、L2TP フローを認識できるようにシステムを明示的に設定する必要があります。SCE プラットフォームでは、外部 IP、UDP、および L2TP の各ヘッダーをスキップし、実際のサブスクライバ トラフィックである内部 IP に到達することができます。L2TP を設定しない場合、外部 IP ヘッダーはサブスクライバ トラフィックとして扱われるため、トンネル内のすべてのフローは単一のフローと見なされます。

VLAN

1 つのパケットにつき、単一の VLAN タグがサポートされます（QinQ はサポートされません）。

VLAN タグによるサブスクライバの分類がサポートされるのは、対称 VLAN 環境の場合だけです。つまり、フローのアップストリームとダウンストリームのタグが一致している場合です。

トンネリング モードの選択

- 「L2TP トンネルの設定」（P.7-6）
- 「GRE トンネリングの設定」（P.7-6）
- 「IPinIP トンネリングの設定」（P.7-8）
- 「DSCP マーキングの設定」（P.7-9）
- 「VLAN 環境の設定」（P.7-10）
- 「MPLS 環境の設定」（P.7-11）
- 「L2TP 環境の設定」（P.7-12）

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 l2tp**
- **ip-tunnel gre**
- **ip-tunnel IPinIP**
- **ip-tunnel (GRE|IPinIP) DSCP-marking-skip**
- **vlan**
- **mpls**
- **L2TP identify-by**

L2TP トンネルの設定

注意　IP トンネリングをイネーブルまたはディセーブルにできるのは、ロードされているアプリケーションがない場合、またはラインカードがシャットダウンされている場合だけです。

L2TP トンネリングのイネーブル化

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。

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　L2TP トンネリングをイネーブルにします。

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。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

L2TP トンネリングのディセーブル化

IPinIP と GRE を除き、すべての IP トンネルをディセーブルにします。

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　L2TP トンネリングをディセーブルにします。

SCE(config if)#> プロンプトに、**no ip-tunnel l2tp skip** を入力して、**Enter** キーを押します。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

GRE トンネリングの設定

- 「GRE トンネリングのイネーブル化」（P.7-7）
- 「GRE トンネリングのディセーブル化」（P.7-7）

GRE トンネリングは、IP ベースのトンネリング プロトコルです。そのため、トンネル内のフローを認識できるようにシステムを明示的に設定する必要があります。SCE プラットフォームでは外部 IP ヘッダーがスキップされ、実際のサブスクライバ トラフィックである内部 IP に到達します。GRE スキップをディセーブルにすると、外部 IP ヘッダーはサブスクライバ トラフィックとして扱われ、すべての GRE トラフィックが一般的な IP としてレポートされます。

GRE トンネルを設定するためのガイドライン：

- GRE と他のトンネル：GRE トンネルは、プレーン IP トラフィック、および SCE プラットフォームでサポートされる他のトンネリング プロトコルと同時にサポートされます。
- 重複する IP アドレス：異なる GRE トンネル内で重複する IP アドレスについてはサポートされていません。
- DSCP マーキング：GRE トラフィックの場合、DSCP マーキングは、外部または内部の IP ヘッダーで排他的に実行できます （「DSCP マーキングの設定」（P.7-9）を参照）。

注意　IP トンネリングを設定（イネーブル、ディセーブル、または DSCP マーキングの設定）できるのは、読み込まれているアプリケーションがない場合、またはラインカードがシャットダウンされている場合のみです。

フラグメンテーション

フラグメンテーションは可能な限り回避します。フラグメンテーションを回避できない場合、内部フラグメンテーションの選択が推奨されます。内部フラグメンテーションも選択できない場合、外部フラグメンテーションの条件で SCE プラットフォームが実行される可能性があります。

GRE トンネリングのイネーブル化

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。GRE 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。

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　GRE トンネリングをイネーブルにします。

SCE(config if)#> プロンプトに、**ip-tunnel gre skip** を入力して、**Enter** キーを押します。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

GRE トンネリングのディセーブル化

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　GRE トンネリングをディセーブルにします。

SCE(config if)#> プロンプトに、**no ip-tunnel gre skip** を入力して、**Enter** キーを押します。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

IPinIP トンネリングの設定

IPinIP は、IP ベースのトンネリング プロトコルです。そのため、トンネル内のフローを認識できるようにシステムを明示的に設定する必要があります。SCE プラットフォームでは外部 IP ヘッダーがスキップされ、実際のサブスクライバ トラフィックである内部 IP に到達します。IPinIP スキップをディセーブルにすると、外部 IP ヘッダーはサブスクライバ トラフィックとして扱われ、すべての IPinIP トラフィックが一般的な IP としてレポートされます。

IPinIP トンネルを設定するためのガイドライン：

- IPinIP と他のトンネル：IPinIP は、プレーン IP トラフィック、および SCE プラットフォームでサポートされる他のトンネリング プロトコルと同時にサポートされます。
- 重複する IP アドレス：異なる IPinIP トンネル内で重複する IP アドレスについてはサポートされていません。
- DSCP マーキング：IPinIP トラフィックの場合、DSCP マーキングは、外部または内部の IP ヘッダーで排他的に実行できます （「DSCP マーキングの設定」（P.7-9）を参照）。

注意　IP トンネリングを設定（イネーブル、ディセーブル、または DSCP マーキングの設定）できるのは、読み込まれているアプリケーションがない場合、またはラインカードがシャットダウンされている場合のみです。

フラグメンテーション

フラグメンテーションは可能な限り回避します。フラグメンテーションを回避できない場合、内部フラグメンテーションの選択が推奨されます。内部フラグメンテーションも選択できない場合、外部フラグメンテーションの条件で SCE プラットフォームが実行される可能性があります。

IPinIP トンネリングのイネーブル化

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。IPinIP 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。

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　IPinIP トンネリングをイネーブルにします。

SCE(config if)#> プロンプトに、**ip-tunnel IPinIP skip** を入力して、**Enter** キーを押します。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

IPinIP トンネリングのディセーブル化

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　IPinIP トンネリングをディセーブルにします。

SCE(config if)#> プロンプトに、**no ip-tunnel IPinIP skip** を入力して、**Enter** キーを押します。

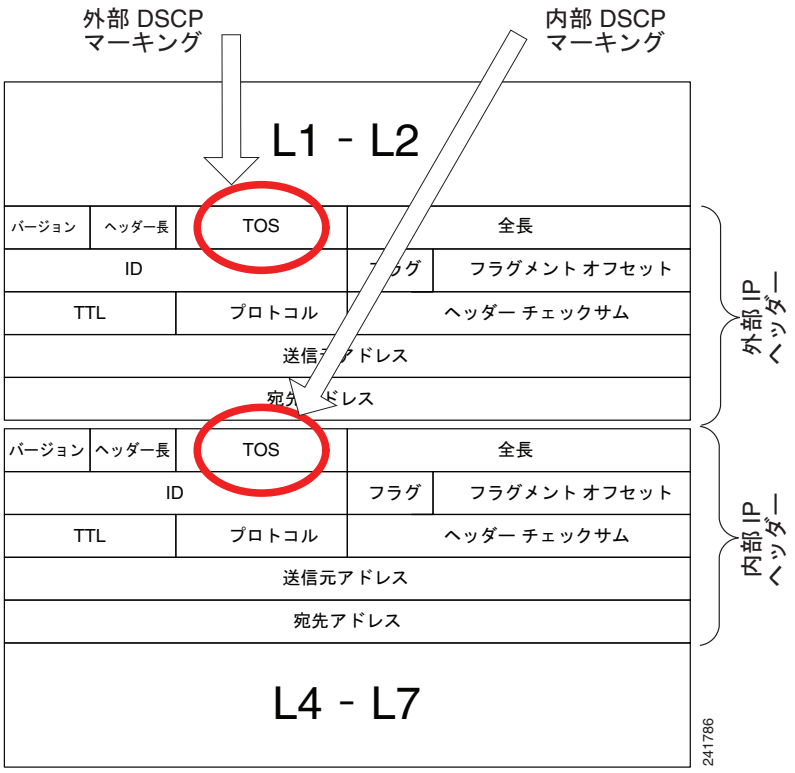
ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

DSCP マーキングの設定

DSCP マーキングによって、IPv4 ヘッダーの DSCP ビットが変更されます。GRE および IPinIP トンネルの場合、2 つ以上の IP ヘッダーがあります。デフォルトで、DSCP マーキングは外部 IP ヘッダーに対してだけ実行されます（図 7-1 を参照）。DSCP マーキングを内部ヘッダーと外部ヘッダーのどちらで実行するかを設定できます。

図 7-1　IPinIP または GRE トンネルの場合の DSCP マーキング



（注）　DSCP マーキングのイネーブル化と設定には、SCA BB コンソールを使用する必要があります。詳細については、『*Cisco Service Control Application for Broadband User Guide*』を参照してください。

内部 IP ヘッダーでの DSCP マーキングの設定

内部 IP ヘッダーの DSCP ビットをマーキングするように SCE プラットフォームを設定するには、このコマンドを使用します。このコマンドの結果を反映するには、関連するトンネリング モード（*GRE skip* または *IPinIP skip*）をイネーブルにする必要があります。

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　DSCP マーキングを設定します。

SCE(config if)#> プロンプトに、**ip-tunnel (GRE|IPinIP) DSCP-marking-skip** を入力して、**Enter** キーを押します。

IPinIP トラフィックの内部 IP ヘッダーで DSCP マーキングをイネーブルにします。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

外部 IP ヘッダーでの DSCP マーキングの設定

外部 IP ヘッダーで DSCP マーキングを実行するには、次のコマンドを使用します。

ステップ 1　ラインカードをシャットダウンします （これはルート レベル コマンドです）。

SCE(config if)#> プロンプトに、**shutdown** を入力して、**Enter** キーを押します。

ステップ 2　DSCP マーキングを設定します。

SCE(config if)#> プロンプトに、**no ip-tunnel (GRE|IPinIP) DSCP-marking-skip** を入力して、**Enter** キーを押します。

IPinIP トラフィックの外部 IP ヘッダーで DSCP マーキングをイネーブルにします。

ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに、**no shutdown** を入力して、**Enter** キーを押します。

VLAN 環境の設定

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.7-10）
- 「VLAN 環境の設定：例」（P.7-11）

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**

symmetric（対称）環境とは、アップストリーム方向とダウンストリーム方向で、トランザクションの伝送に同じ VLAN タグが使用される環境を指します。

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。これは、プライベート IP アドレスをサポートする唯一のモードです。VLAN 分類は、他のトンネルベースの分類や IP トンネルと同時に使用できません。

a-symmetric（非対称）環境とは、同じフローのアップストリーム方向とダウンストリーム方向で、VLAN タグが同じではない可能性がある環境を指します。

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に設定されています。非対称環境で SCE プラットフォームが適切に動作するには、特定のコマンドを使用し、各フローのアップストリームとダウンストリームの VLAN タグが異なる可能性があることを考慮して設定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、パフォーマンスと容量の両方に影響があります。

ステップ 1　SCE(config if)# プロンプトに、**vlan {symmetric classify | symmetric skip |a-symmetric skip}** を入力して、**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

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

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、ルーティングのために MPLS ラベルが必須ではない場合に使用します。
- **VPN skip** : すべての IP アドレスが一意で、ルーティングのために MPLS ラベルが必須の場合に使用します。

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。

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

目的の MPLS モードを指定します。

L2TP 環境の設定

L2TP 環境での外部フラグメンテーション

L2TP 環境に外部フラグメンテーションが存在する場合、*quick-forwarding-ignore* トラフィック規則（「トラフィック規則とカウンタの設定」（P.7-17）を参照）を設定する必要があります。これは、LNS または LAC IP アドレス宛てのすべての IP トラフィックをバイパスする規則です。この設定によって、L2TP ポートの情報がない（つまり最初のフラグメントではない）パケットは、トラフィック プロセッサで処理する必要はなくなります。

さらに、L2TP トンネル処理されたフラグメントの並べ替えを回避するには、すべての L2TP トラフィックについて *quick-forwarding* トラフィック規則を定義することをお勧めします。これは、（LNS の割り当てに従って）トンネルの内部 IP が使用する IP の範囲に基づいて実行するか、すべてのトラフィックについて、単純に SCE プラットフォームを通過することができます。

フローのリダイレクションとフローのブロッキングは、quick-forwarding 処理されたトラフィック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**：L2TP トンネルに LNS と LAC が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。

非対称 L2 のサポート

すべてのフローについて次の条件が該当する場合、非対称レイヤ 2 のサポートをイネーブルにする必要があります。

- フローの各方向には、異なるペアの MAC アドレスがあります。
- ルータは、他のリンクの MAC アドレスを持つパケットを受け入れません。

（注）　「非対称ルーティング トポロジ」のサポートと「非対称トンネリングのサポート」は、2 つの異なる機能です。非対称ルーティング トポロジとは、SCE プラットフォームが 1 方向（アップストリーム/ダウンストリーム）でだけ一部のフローを認識できるトポロジを指します。非対称トンネリングのサポート（非対称 L2 のサポート）とは、SCE プラットフォームがすべてのフローの両方向を認識できても、一部のフローは異なるレイヤ 2 の特性（MAC アドレス、VLAN タグ、MPLS ラベル、L2TP ヘッダーなど）を持つトポロジをサポートする機能を指します。この異なる特性については、SCE プラットフォームがパケットをトラフィックに挿入するときに考慮する必要があります。また、非対称レイヤ 2 をサポートするには、SCE プラットフォームを *asymmetric flow open* モードに切り替えます。この場合、一定のパフォーマンス ペナルティと容量の低下が生じます。これは非対称ルーティング トポロジには該当しない問題です。

ステップ 1　SCE(config if)# プロンプトに、**asymmetric-L2-support** を入力して、**Enter** キーを押します。

トンネリング設定の表示

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が表示されます。

IPinIP の設定を表示する方法

ステップ 1　SCE# プロンプトに、**show interface linecard 0 ip-tunnel IPinIP** 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が表示されます。

ログインしている VPN を表示する方法

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、現在ログインしている VPN の名前。
- **all-names**：システムに現在ログインしているすべての VPN 名を表示するには、このキーワードを使用します。

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。

非対称 L2 サポート モードを表示する方法

ステップ 1　SCE# プロンプトに、**show interface linecard 0 asymmetric-L2-support** を入力して、**Enter** キーを押します。

マネージド VPN

マネージド VPN は、サブスクライバの導入と同様の方法で導入された名前付きエンティティであり、VPN マッピングを含みます。

マネージド VPN には、単一の VLAN マッピングが含まれます。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 セットが含まれます。この IP には単一の IP アドレスまたはアドレスの範囲を指定できます。

マネージド VPN エンティティを設定するには、SM を経由する必要があります。SCE プラットフォームの CLI は、VPN 関連情報を表示するために使用できますが、VPN は設定できません。

プライベート IP アドレス

プライベート IP アドレスがサポートされるのは、次のモードだけです。このモードは、フローの IP アドレスが属する高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です。

- VLAN symmetric classify

容量

システムのサポート内容は次のとおりです。

- 2048 VPN
- VPN 上で 80,000 IP マッピング

VPN モードの制限

同時に使用できないシステム モード

システムが VPN モードで動作している場合、次のモードはサポートされません。

- DDoS
- Value Added Service(VAS; 付加価値サービス) モード

サブスクライバ関連の制限

- Push モードで動作するように SM を設定する必要があります。
- 導入されたサブスクライバのエージングは、VPN ベースのサブスクライバを使用する場合、サポートされません。

TCP 関連の要件

- アップストリーム TCP フローの数：各期間の各 PE-PE ルートで、サブスクライバ側から開始する十分な TCP フロー数が必要です。サブスクライバ側からの TCP フローの比率が高くなるほど、メカニズムの精度が高くなります。

VPN の設定要件

- VLAN ベースの VPN（VLAN 対称分類モード）では、1 つのサブスクライバが複数の VPN で複数の IP マッピングを持っている可能性があります。ただし、IP マッピングが VPN の全範囲（0.0.0.0/0）である場合だけです （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のために用意されています）。

VPN モニタリングのサポート

SCE プラットフォームの CLI では、次の操作を実行できます。

- VPN 関連マッピングの表示
- サブスクライバ カウンタの監視

VPN 関連マッピングの表示

サブスクライバ マッピングを表示するには、次の Viewer コマンドを使用します。これらのコマンドで、次の情報が表示されます。

- 指定した VPN のすべてのマッピング
- 現在ログインしているすべての VPN 一覧
- 指定した VPN 上の IP 範囲にマッピングされるすべてのサブスクライバ一覧
- 指定した VPN 上の IP 範囲にマッピングされるすべてのサブスクライバの数

指定した VPN のマッピングを表示する方法

- 「オプション」（P.7-15）
- 「指定した VPN のマッピングの表示：例」（P.7-15）

オプション

次のオプションを使用できます。

- **vpn-name**：マッピングを表示する VPN の名前。

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

指定した VPN のマッピングの表示：例

次に、VLAN ベースの VPN にこのコマンドを実行した場合の出力例を示します。

```
SCE> show interface linecard 0 VPN name vpn3
VPN name: Vpn3
VLAN: 2
Number of subscriber mappings: 0
Explicitly introduced VPN
```

次に、自動的に作成された VLAN VPN にこのコマンドを実行した場合の出力例を示します。

```
SCE> show interface linecard 0 VPN name 2
VPN name: 2
VLAN: 2
Number of subscriber mappings: 1
Automatically created VPN
```

すべての VPN 一覧を表示する方法

現在ログインしているすべての VPN 一覧を表示するには、こ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 VPN all-names** を入力して、**Enter** キーを押します。

すべての VPN 一覧の表示：例

```
SCE> show interface linecard 0 VPN all-names
```

指定した VPN 上の IP 範囲についてサブスクライバ マッピングを表示する方法

- 「オプション」（P.7-16）
- 「指定した VPN 上の IP 範囲にマッピングされたサブスクライバの表示：例」（P.7-16）

オプション

次のオプションを使用できます。

- **ip-range**：マッピングされているサブスクライバを表示する IP の範囲
- **vpn-name**：マッピングを表示する VPN の名前

ステップ 1　SCE> プロンプトに、**show interface linecard 0 subscriber mapping included-in IP** *ip-range* **VPN** *vpn-name* を入力して、**Enter** キーを押します。

この VLAN オプションを使用すると、プライベート IP マッピングでサブスクライバを検索できます。

指定した VPN 上の IP 範囲にマッピングされたサブスクライバの表示：例

```
SCE> show interface linecard 0 subscriber mapping included-in IP 10.0.0.0/0 VPN vpn1
Subscribers with IP mappings included in IP range '10.0.0.0/0'@vpn1:
Subscriber 'Sub10', mapping '10.1.4.150/32@vpn1'.
Subscriber 'Sub10', mapping '10.1.4.149/32@vpn1'.
Subscriber 'Sub10', mapping '10.1.4.145/32@vpn1'.
Subscriber 'Sub11', mapping '10.1.4.146/32@vpn1'.
Total 2 subscribers found, with 4 matching mappings
```

指定した VPN 上の IP 範囲にマッピングされたサブスクライバの数を表示する方法

- 「オプション」（P.7-16）
- 「指定した VPN 上の範囲にマッピングされるサブスクライバ数の表示：例」（P.7-17）

オプション

次のオプションを使用できます。

- **ip-range**：マッピングされているサブスクライバを表示する IP の範囲
- **vpn-name**：マッピングを表示する VPN の名前

サブスクライバ名の一覧ではなくサブスクライバの数を表示するには、「**amount** 」キーワードを使用します。

ステップ 1　SCE> プロンプトに、**show interface linecard 0 subscriber amount mapping included-in IP** *ip-range* **VPN** *vpn-name* を入力して、**Enter** キーを押します。

指定した VPN 上の範囲にマッピングされるサブスクライバ数の表示：例

```
SCE> show interface linecard 0 subscriber amount mapping included-in IP 0.0.0.0/0 VPN vpn1
There are 2 subscribers with 4 IP mappings included in IP range '0.0.0.0/0'.
```

トラフィック規則とカウンタの設定

トラフィック規則とカウンタ

トラフィック規則とカウンタの概要

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 *ciscoServiceControlTpStats* 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 種類のパケットのモニタに使用できます。
- 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通過します。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、廃棄され、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廃棄する）、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。Cisco SCE8000 の規則の最大数は 64 です。これには、SCE プラットフォームの CLI 経由で設定されるトラフィック規則だけでなく、SCA BB などの外部管理システムによって設定される追加規則も含まれます。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、この規則を示す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。

- **カウント**：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。
- **ブロック**：パケットをブロックします（反対側に渡さない）。
- **無視**：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が行われるこのパケットのサービスを提供しません）。
- **クイックフォワード**：パケットを**サービスあり**でクイックフォワードします。つまり、パケットのサービサビリティを維持しながら、高速パス経由で遅延に影響されやすいパケットを転送します。
- **クイックフォワード**：パケットを**サービスなし（quick-forwarding-ignore）**でクイックフォワードします。つまり、パケットに対してサービスを提供せずに、高速パス経由で遅延に影響されやすいパケットを転送します。

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。ある規則で**ブロック**を指定し、別の規則で**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、このカウンタを示す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**：カウントするパケットごとに、カウンタを 1 つずつインクリメントします。
- **Count bytes**：カウントするパケットごとに、カウンタをパケットのバイト数分インクリメントします。

トラフィック カウンタの設定

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 カウンタを作成する方法」（P.7-19）
- 「トラフィック カウンタを削除する方法」（P.7-19）
- 「既存のすべてのトラフィック カウンタを削除する方法」（P.7-19）

トラフィック カウンタを作成する方法

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**：カウントするパケットごとに、カウンタを 1 つずつインクリメントします。
- **Count bytes**：カウントするパケットごとに、カウンタをパケットのバイト数分インクリメントします。

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 モードでトラフィック カウンタを追加します。

トラフィック カウンタを削除する方法

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 カウンタを削除する方法

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

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。

トラフィック規則を作成する方法

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を指定します。

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

port specification:

```
all|([all-but] (port#|port-range)
```

- プロトコルが TCP または UDP の場合にだけポートを指定します。
- サブスクライバ側とネットワーク側の両方について、ポートまたはポートの範囲を指定します。
- 「MinPort:MaxPort」の形式でポートの範囲を指定します。
- 指定したポートまたはポート範囲を除外するには、**all-but** キーワードを使用します。

id specification：

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

- tunnel id は 8 ビットの 16 進値の範囲で、「(HEX) *Tunnel-id*」または「(HEX) *MinTunnelId*:(HEX) *MaxTunnelId*」という形式です。これは、VLAN タグの下位 8 ビットを反映します。
- トンネル IP ベースの規則を使用できるのは、「*VLAN symmetric classify*」モード（「VLAN 環境の設定」（P.7-10）を参照）だけです。また、*tunnel id* モードがイネーブルの場合だけ使用できます。

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

  VLAN タグ自体は 12 ビット値なので、使用する VLAN タグによっては、下位 8 ビットのエイリアシングが発生することがあります。

direction：

次のいずれかです。

```
upstream/downstream/both
```

traffic-counter：

次のいずれかです。

- **name** <*既存のトラフィック カウンタの名前*>：指定したカウンタでカウントされる規則の基準に適合するパケット。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ます。
- **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）

次のいずれかです。

- **block**：指定したトラフィックをブロックします。
- **ignore**：指定したトラフィックをバイパスし、トラフィックはサービスを受けません。
- **quick-forwarding**：パケットのサービサビリティを維持しながら、高速パス経由で遅延に影響されやすいパケットを転送します。
- **quick-forwarding-ignore**：パケットにサービスを提供せずに、高速パス経由で遅延に影響されやすいパケットを転送します。
- **flow-capture**：この規則で設定されるフローをキャプチャします。このフローにサービスは提供されません。

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* **[ports subscriber-side** <*port specification*> **network-side** <*port specification*>**] [tunnel-id** <*tunnel-id specification*>**] direction** *direction* **traffic-counter** <*traffic-counter*>**[action** *action*] **を入力します。**

トラフィック規則の設定：例

- 「例 1」（P.7-21）
- 「例 2」（P.7-22）
- 「例 3」（P.7-22）
- 「例 4」（P.7-22）

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
- 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 = all
- 方向 = both
- 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 name rule1 IP-addresses subscriber-side all network-side
10.10.10.10 protocol all 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
- ポート : サブスクライバ側 = 100-200、ネットワーク側 = all
- 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。

最初のコマンドでは tunnel id モードをイネーブルにします。

```
SCE(config if)#traffic-rule tunnel-id-mode
SCE(config if)# traffic-rule name rule2 IP-addresses subscriber-side all network-side
all-but 10.10.10.0/24 protocol tcp ports subscriber-side 100:200 network-side all
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）
- 唯一実行されるアクションは、**無視**です。

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

例 4

次に、flow-capture オプションを使用して記録規則として使用されるトラフィック規則を設定する例を示します。フローのキャプチャ プロセスが動作中は、この規則に一致するすべてのフローが記録されます。

1. 名前 = FlowCaptureRule
2. 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 = すべての IP アドレス
3. 方向 = both
4. プロトコル = 250
5. トラフィック カウンタ名 = counter2
6. アクション = flow-capture
7. 実行されるアクションは、カウントとフロー キャプチャです。

```
SCE>enable 10
Password:<cisco>
SCE#configure
SCE(config)#interface linecard 0
SCE(config if)#traffic-rule name FlowCaptureRule ip-addresses subscriber-side all
network-side all protocol 250 direction both traffic-counter name counter2 action
flow-capture
SCE(config if)#
```

トラフィック規則を削除する方法

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。

指定し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を削除する方法

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。

すべての既存のトラフィック規則を削除します。

すべてのフロー制御トラフィック規則を削除する方法

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

すべてのフロー キャプチャトラフィック規則を削除します。

トラフィック規則とカウンタの管理

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を表示する方法」（P.7-24）
- 「すべてのトラフィック規則を表示する方法」（P.7-24）
- 「指定したトラフィック カウンタを表示する方法」（P.7-24）
- 「すべてのトラフィック カウンタを表示する方法」（P.7-24）
- 「指定したトラフィック カウンタをリセットする方法」（P.7-25）
- 「すべてのトラフィック カウンタをリセットする方法」（P.7-25）

指定したトラフィック規則を表示する方法

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を表示する方法

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。

すべての既存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 カウンタを表示する方法

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。

指定したカウントの値と、それを使用するトラフィック規則の一覧を表示します。

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 カウンタを表示する方法

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。

各カウントの値と、それを使用するトラフィック規則の一覧を表示します。

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 カウンタをリセットする方法

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。

指定したトラフィック カウンタをリセットします。

すべてのトラフィック カウンタをリセットする方法

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。

すべてのトラフィック カウンタをリセットします。

DSCP マーキング

DSCP マーキングは、パケットの優先順位をシグナリングする手段として IP ネットワークに使用されます。シスコ サービス コントロール ソリューションでは、サービス別、パッケージ レベル別で、SCA BB アプリケーション経由の DSCP の分類をサポートしています。SCE プラットフォームの DSCP マーキング機能を使用すると、SCA BB コンソールで設定したポリシーに従い、各パケットの IP ヘッダーの DSCP フィールドにマーキングできます。IP ヘッダーに設定される実際の DSCP 値は、設定可能な DSCP 変換テーブルに定義されている値に従って決定されます。

DSCP マーキング設定には、SCA BB コンソールを使用します。SCE プラットフォームの CLI を使用すると、各インターフェイスの DSCP マーキングの状態（イネーブルまたはディセーブル）を表示し、DSCP 変換テーブルを表示できます。

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

（注）　リリース 3.1.5 以降の DSCP マーキングは、リリース 3.1.5 よりも前の SCOS バージョンと下位互換性がありません。

DSCP マーキングの設定を表示する方法

インターフェイス別の DSCP マーキングの状態（イネーブルまたはディセーブル）および DSCP 変換テーブルを表示するには、こ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。

ドロップされたパケットのカウント

ドロップされたパケットのカウントについて

デフォルトで、SCE プラットフォームのハードウェアは、WRED パケット（BW コントロール基準によってドロップするようにマークされたパケット）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たパケットの数を知る必要がある場合に問題になります。サービスごとにドロップされたパケット数をカウントするには、すべてのフローについてすべてのドロップされたパケットをトラフィック プロセッサが認識できる必要があります。ただし、ハードウェアが red 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たパケットをすべてカウントできません。また、ユーザは関連する MIB カウンタ（*tpTotalNumWredDiscardedPackets*）について正しい値を取得できません。

（注）　MIB オブジェクト *tpTotalNumWredDiscardedPackets* は、ドロップされたパケットをカウントします。ハードウェア パケットのドロップがディセーブル（デフォルト モードではありません）の場合にだけ、このカウンターの値が完全です。ハードウェア パケットのドロップがイネーブル（デフォルト モード）の場合、この MIB カウンタは、約 1:6 の比率で、パケット ドロップ数の動向を示す相対値だけを示します。

drop-wred-packets-by-hardware モードはディセーブルにできます。ディセーブルにすることで、アプリケーションから既存の per-flow カウンタにアクセスできます。その結果、各フローのドロップされたパケット数を取得し、ドロップされたパケットの正確な数とその分散をわかりやすく表示できるようになります。

すべてのドロップされたパケットをカウントすることは、システムのパフォーマンスに大きな影響があるため、デフォルトで、drop-wred-packets-by-hardware モードはイネーブルです。

ハードウェア パケットのドロップのディセーブル化

drop-wred-packets-by-hardware モードをディセーブルにし、ドロップされたパケットをすべてカウントするには、このコマンドを使用します。

デフォルトで、ハードウェア パケットの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、遅延とパフォーマンス低下が発生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 パケットのドロップをディセーブルにします。

ハードウェア パケットの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。

ステップ 1　SCE(config if)# プロンプトに、**accelerate-packet-drops** を入力して、**Enter** キーを押します。