CHAPTER 7

ライン インターフェイスの設定

概要

この章では、物理的なライン インターフェイス（ポート）の設定方法と、これらのインターフェイスにトンネリング、VLAN 変換、DSCP マーキング、トラフィック規則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（サブスクライバとネットワーク）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します。『*Cisco SCE8000 10GBE Installation and Configuration Guide*』の「Cisco SCE8000 Topology and Topology-Related Parameters」の章に書か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 10GBE 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 ～ 3 にインストールされている、1 ポートの 10 ギガビット イーサネット SPA 上にあります。それぞれの 1 ポート 10 ギガビット イーサネット SPA は、サブスクライバまたはネットワーク トラフィックとインターフェイスする、10GBE のポート 1 つを提供します。これら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の考慮事項

（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に反応するものであり、これをアクティブ化することはしません。したがって、SCE プラットフォームのキューがオーバーフローしてしまい、フロー制御によって SCE プラットフォームの動作が停止して、Rx インターフェイスでトラフィックが廃棄されるという状況が生じる可能性があります。この状況が 5 秒以上続くと、SCE プラットフォームで内部の健全性チェック メカニズムが起動され、さらにここから復旧を試みる際に SCE プラットフォームがリロードされることがあります。

最大パケット サイズ

Cisco SCE8000 のトラフィック処理に対する MTU 値は、9238 バイトです。しかし、現在のバージョンでは、大きさが 1600 バイトを超える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は処理されません。

10 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には

10 GBE ライン インターフェイスは、TenGigabitEthernet モードで設定します。

ステップ 1　SCE# プロンプトに対して、**configure** 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 モードが開始されます。

ステップ 2　SCE(config)# プロンプトに対して、**interface TenGigabitEthernet 3**/*bay number*/**0** と入力し、**Enter** キーを押します。ここで、*bay number* は選択した SPA ベイの番号（0 ～ 3）です。現在、スロット番号は常に 3 であり、ポート番号は常に 0 です。

選択した 10 GBE インターフェイスのインターフェイス コンフィギュレーション モードが開始されます。

ステップ 3　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 モードに戻ります。ここからまた別のギガビット イーサネット インターフェイスにアクセスできます。

10 ギガビット イーサネット ライン インターフェイスでトラフィックの向きを変更する

SCE8000 10G プラットフォームのハードウェアは、SPA 0 および 2 で送受信されるトラフィックが、各方向とも合計 16Gbps に制限されるように設計されており、SPA 1 および 3 で送受信されるトラフィックも同様です。10GBE のインストレーションではデフォルトで、SPA 0 および 2 がサブスクライバ側ポート、SPA 1 および 3 がネットワーク側ポートとなっているため、各方向（アップストリームおよびダウンストリーム）の合計トラフィックが効果的に 16Gbps に制限されます。そのため、1 方向（アップストリームまたはダウンストリーム）の合計トラフィックが 16Gbps を超えるサイトは、この制限を超えるためにパケット損失が発生してしまいます。

このコマンドを使用して、リンク 1 のポートの役割を入れ替えれば、高容量トラフィックの一部を反対側の SPA のペアに切り替えて、いずれの SPA のペアも 16Gbps の制限を超えないようにすることができます。

制限事項

- このコマンドはリンク 1 だけでサポートされています（3/2/0 および 3/3/0）。リンク 0 ではサポートされていません。

  リンクには 1 つのインターフェイスだけが明示的に設定されます。逆のトラフィック側には、対応するインターフェイスが自動的に設定されます。

- 接続モードは、インラインまたは受信専用でなければなりません。このコマンドはカスケード モードではサポートされていません。
- このコマンドは、アプリケーションがいずれもロードされておらず、shutdown モードにもなっていない場合にだけ実行できます。

リンク 1 のトラフィックの向きを指定するには

ステップ 1　SCE# プロンプトに対して、**configure** 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 モードが開始されます。

ステップ 2　SCE(config)# プロンプトで、**interface TenGigabitEthernet 3/2/0** または **interface TenGigabitEthernet 3/3/0** と入力し、**Enter** キーを押します。

選択した 10 GBE インターフェイスのインターフェイス コンフィギュレーション モードが開始されます。

ステップ 3　SCE(config if)# プロンプトで、**traffic-side (subscriber | network)** と入力し、**Enter** キーを押します。

トラフィックが、設定中のインターフェイスについては指定した方向に、対応するインターフェイスについては自動的に逆方向に設定されます。

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、各種のトンネリング プロトコルをいくつかの方法で認識および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か（ヘッダーの「スキップ」）、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」）ことができます。トンネリング情報による分類の特殊なケースは、プライベート IP をサポートする VPN の場合です。

表 7-1 は、サポートしている各種のトンネリング プロトコルを表しています（各プロトコルのデフォルトの動作は太字で表しています）。

表 7-1　トンネリング プロトコルの概要

プロトコル	サポートしている処理	モード名	対称 / 非対称
L2TP	トンネルの無視	IP-tunnel L2TP skip	非対称
	トンネルの無視は不可：外部 IP による分類	**No IP-Tunnel**	対称
GRE	トンネルの無視	ip-tunnel GRE skip	対称
	トンネルの無視は不可：外部 IP による分類	**no ip-tunnel GRE skip**	対称
IPinIP	トンネルの無視	ip-tunnel IPinIP skip	対称
	トンネルの無視は不可：外部 IP による分類	**no ip-tunnel IPinIP skip**	対称
VLAN	トンネルの無視	**VLAN symmetric skip**	対称
	トンネルの無視 – 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	トンネルの無視（ラベルなしインジェクト）	**MPLS traffic-engineering skip**	対称
	トンネルの無視（ラベルありインジェクト）	MPLS VPN skip	非対称

トンネリング情報が無視されるとき、サブスクライバの識別情報は、トンネル内を伝送される IP パケットのサブスクライバ IP になります。

非対称トンネリング

トンネリングモードには、対称のものと非対称のものがあります（表 7-1 を参照）。いずれかの非対称トンネリング モードがイネーブルになると、システム全体が自動的に非対称フロー オープン モードに設定されます。このモードでは、対称フロー オープン モードよりも速くフローがオープンされ、フローの各方向の最初のパケット（アップストリームおよびダウンストリーム）がソフトウェアに到達します。これは、非対称レイヤ 2 のプロトコル上で処理をリダイレクトおよびブロックするのに必要です。しかし、パフォーマンスと容量のどちらにもいくらかの影響はあるため、どの非対称モードでもある程度のパフォーマンス低下が予測されます。

また、パケットのインジェクションの目的で（フローのブロックやフローのリダイレクトの処理）、すべてのフローが非対称レイヤ 2 の特性を持つ（イーサネット、VLAN、MPLS、および L2TP）としてシステムを明示的に設定することもできます。

効果的なフロー オープン モードを調べるには、**show interface linecard 0 flow-open-mode** コマンドを使用してください。

（注）　非対称トンネリング オプションの設定方法については、「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、システムは L2TP フローや、L2TP のために使用する UDP ポートを認識するよう、明確に設定する必要があります。その結果、SCE プラットフォームは外部 IP、UDP、および L2TP ヘッダーをスキップするようになり、実際のサブスクライバのトラフィックである内部 IP に到達します。L2TP が設定されていないと、システムは外部 IP ヘッダーをサブスクライバのトラフィックとして扱うため、トンネル内のすべてのフローが 1 つのフローに見えます。

VLAN

パケットごとに 1 つの VLAN タグをサポートしています（QinQ はサポートせず）。

VLAN タグによるサブスクライバの分類は、対称 VLAN 環境でのみサポートされています。この環境では、フローのアップストリーム タグとダウンストリーム タグが同一であるためです。

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.7-11）

トンネリングを設定するには、ここで説明する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 トンネリングは、アプリケーションがまったくロードされていないとき、あるいはラインカードがシャットダウンされているときにだけ、イネーブル化またはディセーブル化できます。

L2TP トンネリングをイネーブルにする

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、ここで説明する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 root レベルのコマンドです）。

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

L2TP トンネリングをディセーブルにする

IPinIP と GRE を除くすべての 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 root レベルのコマンドです）。

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

GRE トンネリングの設定

- 「GRE トンネリングをイネーブルにする」（P.7-7）
- 「GRE トンネリングをディセーブルにする」（P.7-7）

GRE トンネリングは IP ベースのトンネリング プロトコルであるため、システムはトンネル内のフローを認識するよう明確に設定する必要があります。その結果、SCE プラットフォームは外部 IP ヘッダーをスキップし、実際のサブスクライバのトラフィックである内部 IP に到達します。GRE スキップがディセーブルのとき、システムは外部 IP ヘッダーをサブスクライバのトラフィックとして取り扱い、結果としてすべての GRE トラフィックが汎用 IP として報告されます。

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、SCE プラットフォームでサポートされている単純な IP トラフィックや他のトンネリング プロトコルと同時にサポートされています。
- IP アドレスの重複：異なる GRE トンネル内での IP アドレスの重複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 ヘッダーのいずれかで排他的に行うことができます（「DSCP マーキングの設定」（P.7-9）を参照）。

注意　IP トンネリングは、アプリケーションがまったくロードされていないとき、あるいはラインカードがシャットダウンされているときにだけ設定（イネーブル化、ディセーブル化、DSCP マーキング）できます。

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する必要があります。フラグメンテーションを回避できない場合は、内部でのフラグメンテーションを選ぶことを推奨します。これも不可能な場合は、SCE プラットフォームを外部フラグメンテーションが生じている状態で運用することもできます。

GRE トンネリングをイネーブルにする

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、ここで説明する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 root レベルのコマンドです）。

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

GRE トンネリングをディセーブルにする

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 root レベルのコマンドです）。

SCE(config if)#> プロンプトに対して、**shutdown** と入力し、**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)#> プロンプトに対して、**no ip-tunnel gre skip** と入力し、**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)#> プロンプトに対して、**no shutdown** と入力し、**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 プロトコルであるため、システムはトンネル内のフローを認識するよう明確に設定する必要があります。その結果、SCE プラットフォームは外部 IP ヘッダーをスキップし、実際のサブスクライバのトラフィックである内部 IP に到達します。IPinIP スキップがディセーブルのとき、システムは外部 IP ヘッダーをサブスクライバのトラフィックとして取り扱い、結果としてすべての IPinIP トラフィックが汎用 IP として報告されます。

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、SCE プラットフォームでサポートされている単純な IP トラフィックや他のトンネリング プロトコルと同時にサポートされています。
- IP アドレスの重複：異なる IPinIP トンネル内での IP アドレスの重複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 ヘッダーのいずれかで排他的に行うことができます（「DSCP マーキングの設定」（P.7-9）を参照）。

注意　IPinIP トンネリングは、アプリケーションがまったくロードされていないとき、あるいはラインカードがシャットダウンされているときにだけ設定（イネーブル化、ディセーブル化、DSCP マーキング）できます。

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する必要があります。フラグメンテーションを回避できない場合は、内部でのフラグメンテーションを選ぶことを推奨します。これも不可能な場合は、SCE プラットフォームを外部フラグメンテーションが生じている状態で運用することもできます。

IPinIP トンネリングをイネーブルにする

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、ここで説明する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 root レベルのコマンドです）。

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

IPinIP トンネリングをディセーブルにする

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 root レベルのコマンドです）。

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

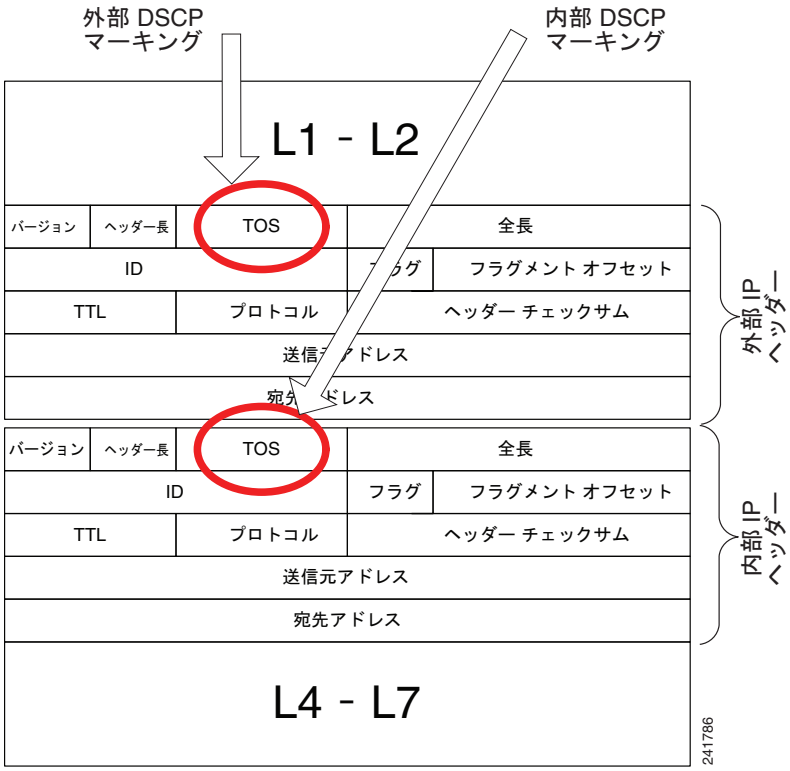
ステップ 3　ラインカードを再起動します。

SCE(config if)#> プロンプトに対して、**no shutdown** と入力し、**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 トンネルおよび IPinIP トンネルには、少なくとも 2 つの IP ヘッダーがあります。デフォルトでは、DSCP マーキングは外部 IP ヘッダーに対してのみ行われます（図 7-1）。内部ヘッダーまたは外部ヘッダーで DSCP マーキングが行われるかどうかは設定可能です。

図 7-1　IPinIP トンネルまたは GRE トンネルに対する DSCP マーキングの設定



（注）　DSCP マーキングは、SCA BB コンソールからイネーブルにし、設定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 ヘッダーに対する DSCP マーキングの設定

内部 IP ヘッダーの DSCP ビットをマーク付けするよう SCE プラットフォームを設定するには、ここで説明するコマンドを使用します。このコマンドは、該当するトンネリング モード（*GRE skip* または *IPinIP skip*）がイネーブルになっている場合のみ有効です。

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 root レベルのコマンドです）。

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

IPinIP トラフィックの内部 IP ヘッダーに対する DSCP マーキングがイネーブルになります。

ステップ 3　ラインカードを再起動します。

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

外部 IP ヘッダーに対する DSCP マーキングの設定

外部 IP ヘッダーに対する DSCP マーキングを実行するには、ここで説明する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 root レベルのコマンドです）。

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

IPinIP トラフィックの外部 IP ヘッダーに対する DSCP マーキングがイネーブルになります。

ステップ 3　ラインカードを再起動します。

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

VLAN 環境の設定

VLAN 環境を設定するには、ここで説明する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**

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の両方で、トランザクションの伝送に同じ VLAN タグが使用されている環境を意味します。

分類のための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 の分類の使用は、他のトンネルベースの分類または IP トンネルと相互に排他的な関係にあります。

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意味します。

SCE プラットフォームは、デフォルトでは対称環境で動作するよう設定されています。非対称環境で SCE プラットフォームが正しく動作するようにするには、特別なコマンドを使用して、各フローのアップストリーム側とダウンストリーム側で VLAN タグが異なる場合があることを考慮するよう指示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出ます。

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

希望する VLAN モードを指定します。

VLAN 環境の設定例

次の例では、VLAN ベースの分類を選択しています。

```
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 アドレスが一意であり、ルーティングに MPLS ラベルが必要でない場合に使用します。
- **VPN skip** : すべての IP アドレスは一意だが、ルーティングに MPLS ラベルが必要な場合に使用します。

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)# プロンプトに対して、**mpls {traffic-engineering skip|vpn skip}** と入力し、**Enter** キーを押します。

希望する 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」（P.7-12）
- 「オプション」（P.7-12）

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ある場合には、LNS または LAC IP アドレスのいずれかに宛てられたすべての 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（「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。これによって、トラフィック プロセッサで L2TP ポートの指示がないパケット（非初期フラグメントなど）を処理する必要がなくなります。

さらに、L2TP トンネル化されたフラグメントの並び替えが行われないようにするには、すべての L2TP トラフィックに対して *quick-forwarding* トラフィック規則を定義することを推奨します。これは、トンネル内の内部 IP で使用されている IP の範囲に基づいて実行されるか、あるいは単に SCE プラットフォームを通過するすべてのトラフィックに対して実行されます。

フローのリダイレクションおよびフローのブロッキングは、クイック転送が設定されたトラフィックには実行できないことに注意してください。

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 トンネル用に使用しているポート番号です。

  デフォルトのポート番号は 1701 です。

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

非対称 L2 のサポート

あらゆるフローに対して次の状態が生じている場合は、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。

- フローの各方向で異なる MAC アドレスのペアが使用されている。
- ルータで他のリンクの MAC アドレスを持つパケットが受け入れられない。

（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、別個の機能です。非対称ルーティング トポロジとは、SCE プラットフォームで一方向の一部のフロー（アップストリームまたはダウンストリーム）しか検出できないトポロジです。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 プラットフォームですべてのフローの両方向を検出できるトポロジをサポートできることを意味します。しかし、一部のフローは異なるレイヤ 2 特性（MAC アドレス、VLAN タグ、MPLS ラベル、および L2TP ヘッダーなど）を持つ可能性があるため、SCE プラットフォームではパケットをトラフィックにインジェクトするときに（ブロックやリダイレクトなどの処理の際）これを考慮する必要があります。また、非対称レイヤ 2 をサポートするためには、SCE プラットフォームが*非対称フロー オープン モード*に切り替わり、これによってある程度のパフォーマンス ペナルティが生じるとともに、容量も減少することに注意してください。これは非対称ルーティング トポロジに関するものではありません。

ステップ 1　SCE(config if)# プロンプトに対して、**asymmetric-L2-support** と入力し、**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# プロンプトに対して、**show interface linecard 0 (MPLS|VLAN|L2TP|IP-tunnel)** と入力し、**Enter** キーを押します。

指定したトンネル オプションに対する現在の設定が表示されます。

IPinIP の設定を表示するには

ステップ 1　SCE# プロンプトに対して、**show interface linecard 0 ip-tunnel IPinIP** と入力し、**Enter** キーを押します。

指定したトンネル オプションに対する現在の設定が表示されます。

ログイン中の VPN を表示するには

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特定の VPN の名前。
- **all-names**：このキーワードを使用すると、現在システムにログインしているすべての VPN 名を表示できます。

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 のサポート モードを表示するには

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

マネージド VPN

マネージド VPN は、サブスクライバと同様の方法で導入される、VPN マッピングを含む名前付きエンティティです。

1 つのマネージド VPN には、1 つの 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 という形式の一連のマッピングが含まれており、ここで IP は単一の IP アドレスかまたはアドレスの範囲になります。

マネージド VPN エンティティは、SM を介してのみ設定できます。SCE プラットフォームの CLI は、VPN 関連情報の表示に使用できますが、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、次のモードでのみサポートされています。これはこのモードで、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）関連の情報が提供されるためです。

- VLAN symmetric classify

容量

このシステムのサポート内容は次のとおりです。

- 2048 の VPN
- VPN を介した 80,000 の IP マッピング

VPN モードの制限事項

相互排他的なシステム モード

システムが VPN モードで稼動しているときは、次のモードはサポートされません。

- DDoS
- 付加価値サービス（VAS）モード

サブスクライバ関連の制限事項

- 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。
- 導入されたサブスクライバ エージングは、VPN ベースのサブスクライバの使用時に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 フローの数：各時間範囲において、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

- VLAN ベースの VPN（VLAN 対称分類モード）では、サブスクライバが複数の VPN に渡る IP マッピングを有している場合がありますが、これは IP マッピングが VPN 全体に渡る場合に限ります（0.0.0.0/0）（このオプションは後方互換性のために提供されており、レガシーのマルチ VLAN サブスクライバをサポートしています）。

VPN サポートのモニタリング

SCE プラットフォームの CLI は、次の目的に使用できます。

- VPN 関連のマッピングの表示
- サブスクライバ カウンタの監視

VPN 関連のマッピングを表示する

サブスクライバ マッピングを表示するには、ここで説明するビューア 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 のリスト
- 指定した VPN 上の特定の IP 範囲にマッピングされたすべてのサブスクライバのリスト
- 指定した VPN 上の特定の IP 範囲にマッピングされた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

次の例は、VLAN ベースの VPN におけるこのコマンドの出力を示しています。

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

次の例は、自動的に作成された VLAN VPN におけるこのコマンドの出力を示しています。

```
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 のリストを表示する方法

現在ログインしているすべての VPN のリストを表示するには、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** と入力して、**Enter** キーを押します。

全 VPN のリストの表示：例

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

指定した VPN 上の特定の IP 範囲のサブスクライバ 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 上の特定の 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**：マッピングされたサブスクライバを表示する IP 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* と入力して、**Enter** キーを押します。

VPN オプションを使用すると、プライベート IP のマッピングのあるサブスクライバを検索できます。

指定した VPN 上の特定の 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 上の特定の 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 上の特定の範囲にマッピングされたサブスクライバ数の表示：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**：マッピングされたサブスクライバを表示する IP 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リスト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* と入力して、**Enter** キーを押します。

指定した VPN 上の特定の範囲にマッピングされた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対して特定の処理（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 による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リングに使用できます。
- 特定のタイプのフローを無視する。トラフィック規則に「ignore」アクションが指定されていると、規則基準に一致するパケットは、新規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する必要がある場合に役立ちます。

  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。トラフィック規則に「block」アクションが指定されていると、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する必要がある場合に役立ちます。

  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（サブスクライバ ポートが送信元であるパケットのうち、その IP アドレスが、定義されているサブスクライバ側のサブネットのいずれにも属さないものを廃棄する）、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。そのため、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、SCE プラットフォームで処理されるパケットのうち特定の基準を満たすものに、定義したアクションが実行されるように指定します。Cisco SCE8000 の場合の規則の最大数は 64 であり、これには SCE プラットフォームの CLI によって設定されたトラフィック規則だけでなく、SCA BB のような外部の管理システムで設定された規則も含まれます。各規則には定義したときに名前を付けます。その後、この規則を参照するときにはこの名前を使用します。

パケットはユーザが定義した基準に従って選択されます。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）に指定できる単一のアドレスまたはサブネットの範囲。
- **プロトコル**：TCP/UDP/ICMP/IGRP/EIGRP/IS-IS/OSPF/ その他。
- **TCP/UDP ポート**：各回線ポート（サブスクライバ/ネットワーク）に指定できる単一のポートまたはポートの範囲。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を行うサービスをこのパケットに提供しません）。
- **サービスを行う**パケットの**クイック転送**：遅延に影響されやすいパケットを高速パスから転送し、これらのパケットに対するサービサビリティを維持します。
- **サービスを行わない**パケットの**クイック転送**（quick-forwarding-ignore）：遅延に影響されやすいパケットを、これらのパケット用に提供されているサービスを行わず高速パスから転送します。

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。

1 つの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する。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指定している場合、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指定している場合、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**に優先する。ある規則によって**ブロック**が指定され、別の規則によって**無視**が指定されていると、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。各カウンタには定義したときに名前を付けます。その後、このカウンタを参照するときにはこの名前を使用します。

トラフィック カウンタは、次の 2 つの方法のどちらかで設定できます。

- **Count packets**：カウンタは、カウントする各パケットごとに 1 ずつ増分されます。
- **Count bytes**：カウンタは、カウントする各パケットごとに、そのパケットのバイト数だけ増分されます。

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 カウンタを参照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、ここで説明する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には」（P.7-19）
- 「トラフィック カウンタを削除するには」（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には」（P.7-19）

トラフィック カウンタを作成するには

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ごとに 1 ずつ増分されます。
- **Count bytes**：カウンタは、カウントする各パケットごとに、そのパケットのバイト数だけ増分されます。

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

指定した名前とカウンタのモードでトラフィック カウンタが追加されます。

トラフィック カウンタを削除するには

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

トラフィック カウンタが既存のトラフィック規則で使用されている場合、そのトラフィック カウンタは削除できません。

既存のすべてのトラフィック カウンタを削除するには

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

すべてのトラフィック カウンタが削除されます。

トラフィック カウンタが既存のトラフィック規則で使用されている場合、そのトラフィック カウンタは削除できません。

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、ここで説明するコマンドを使用します。

トラフィック規則を作成するには

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 進表記の単一の IP アドレスです。
- *ip-range* は、10.1.2.0/24 など、ドット付き 10 進表記の後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/all
```

port specification：

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

- プロトコルが TCP または UDP の場合にのみ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ポートまたはポートの範囲を指定します。
- ポートの範囲は MinPort:MaxPort という形式で指定します。
- 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)
```

- トンネル ID は 8 ビットの 16 進数の値の範囲であり、「(HEX) *Tunnel-id*」または「(HEX) *MinTunnelId* :(HEX) *MaxTunnelId*」という形式で表します。これは VLAN タグの下位 8 ビットを表します。
- トンネル ID をベースとする規則は、「*VLAN 対称分類*」モード（「VLAN 環境の設定」（P.7-10）を参照）で、かつ *トンネル ID* モードがイネーブルになっているときにのみ使用できます。

  traffic-rule tunnel-id-mode コマンドを使用してください。

  VLAN タグ自体は 12 ビットの値であり、使用されている VLAN タグによっては、下位 8 ビットのエイリアシングが行われます。

direction：

次のいずれかになります。

```
upstream/downstream/both
```

traffic-counter：

次のいずれかになります。

- **name** <*既存のトラフィック カウントの名前*>：規則の条件を満たすパケットが、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** キーワードも指定する必要があります。
- **none**：**none** を指定する場合、action オプションを使用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 だけの場合は不要）

次のいずれかになります。

- **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ます。トラフィックはサービスを受けません。
- **quick-forwarding**：遅延に影響されやすいパケットを高速パスから転送し、これらのパケットに対するサービサビリティを維持します。
- **quick-forwarding-ignore**：遅延に影響されやすいパケットを高速パスから転送し、これらのパケットにはサービスを提供しません。
- **flow-capture**：この規則によって定義されたフローをキャプチャします。このフローにサービスは適用されません。

ステップ 1　SCE(config if)# プロンプトに対して、**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***]** と入力します。

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

この例では、次の内容のトラフィック規則を作成します。

- 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 = 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

この例では、次の内容のトラフィック規則を作成します。

- 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。

最初のコマンドによって、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 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

この例では、次の内容のトラフィック規則を作成します。

- 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

次の例では、flow-capture オプションを使用する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方法を示します。フロー キャプチャ プロセスが動作中は、この規則を満たすフローがすべて記録されます。

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には

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

指定したトラフィック規則が削除されます。

すべてのトラフィック規則を削除するには

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

既存のすべてのトラフィック規則が削除されます。

すべてのフロー制御トラフィック規則を削除するには

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

すべてのフロー キャプチャ トラフィック規則が削除されます。

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 カウンタの値の表示には、ここで説明する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には

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

指定したトラフィック規則の設定が表示されます。

すべてのトラフィック規則を表示するには

ステップ 1　SCE# プロンプトに対して、**show interface linecard 0 traffic-rule all** と入力し、**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が表示されます。

指定したトラフィック カウンタを表示するには

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

指定したカウンタの値が表示され、これを使用しているトラフィック規則が一覧表示されます。

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には

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

各カウンタの値が表示され、これを使用しているトラフィック規則が一覧されます。

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には

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

指定したトラフィック カウンタがリセットされます。

すべてのトラフィック カウンタをリセットするには

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

すべてのトラフィック カウンタがリセットされます。

DSCP マーキング

DSCP マーキングは、IP ネットワークでパケットのプライオリティを示す手段として使用されます。Cisco Service Control ソリューションでは、サービス単位、パケット単位のレベルに対して、SCA BB アプリケーションを通じて DSCP 分類をサポートしています。SCE プラットフォームの DSCP マーキング機能により、SCA BB コンソールで設定されたポリシーに基づいて、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るようになります。IP ヘッダーに設定されている実際の DSCP 値は、設定変更が可能な DSCP 変換テーブルで定義されている値に従って決定されます。

DSCP マーキング設定は、SCA BB から行います。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についての DSCP マーキングの状態（イネーブルまたはディセーブル）を確認したり、DSCP 変換テーブルを表示したりすることができます。

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 バージョンとの後方互換性はありません。

DSCP マーキングの設定を表示するには

インターフェイスごとの DSCP マーキングの状態（イネーブルまたはディセーブル）や、DSCP 変換テーブルを表示するには、ここで説明するコマンドを使用します。

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

廃棄されたパケットのカウント

廃棄されたパケットのカウントについて

デフォルトでは、SCE プラットフォームのハードウェアでは、WRED パケット（BW 制御基準に即して廃棄されることがマーキングされたパケット）を廃棄します。しかし、これによって、サービスごとに廃棄されたパケットの数を知る必要があるユーザには、ある問題が生じます。サービスごとに廃棄されたパケットの数をカウントできるようにするには、トラフィック プロセッサで、すべてのフローを対象として、廃棄されたすべてのパケットを調べる必要があります。しかし、ハードウェアによって WRED パケットが廃棄されているとき、トラフィック プロセッサは廃棄されたパケットすべてをカウントできず、ユーザは関係する MIB カウンタ（*tpTotalNumWredDiscardedPackets*）についての正しい値を知ることができなくなります。

（注） MIB オブジェクト *tpTotalNumWredDiscardedPackets* では、廃棄されたパケットをカウントします。このカウンタの値が確実なのは、ハードウェア パケットの廃棄がディセーブルになっている（デフォルト モードではない）ときだけです。ハードウェア パケットの廃棄がイネーブル（デフォルト モード）のとき、この MIB カウンタは、パケットの廃棄数の傾向を示す相対的な値（約 1:6 の係数）だけを示します。

ユーザは drop-wred-packets-by-hardware モードをディセーブルにできます。これによって、アプリケーションが既存のフローごとのカウンタにアクセスできるようになります。その後、このアプリケーションから各フローごとの廃棄されたパケットの数を入手して、廃棄されたパケットの正確な数とその分布をユーザにわかりやすく表示できるようになります。

廃棄されたすべての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相当の影響を与えるため、デフォルトでは drop-wred-packets-by-hardware モードがイネーブルにされていることに注意してください。

ハードウェアによるパケット廃棄のディセーブル化

drop-wred-packets-by-hardware モードをディセーブルにして、廃棄されたすべてのパケットのソフトウェアによるカウントをイネーブルにするには、ここで説明するコマンドを使用します。

デフォルトでは、ハードウェアによるパケットの廃棄がイネーブルになっています。

（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の両方に影響が生じることがあります。

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

ハードウェアによるパケット廃棄がディセーブルになります。

ハードウェアによるパケット廃棄をイネーブルにするには、ここで説明するコマンドを使用します。

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