



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 インターフェイスの設定方法 \(p.6-2\)](#)
- [トンネリング プロトコルの設定方法 \(p.6-5\)](#)
- [VLAN 変換の設定方法 \(p.6-9\)](#)
- [トラフィック規則とカウンタの設定方法 \(p.6-12\)](#)
- [TOS マーキングの設定方法 \(p.6-20\)](#)
- [ドロップされるパケットのカウント方法 \(p.6-22\)](#)

ライン インターフェイスの設定方法

- [ラインインターフェイス \(p.6-2\)](#)
- [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 \(p.6-2\)](#)
- [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 \(p.6-3\)](#)

ライン インターフェイス

ラインインターフェイス（サブスクリ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。

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。

サマリー 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。
2. SCE(config)# プロンプトに、`interface GigabitEthernet 0/ portnumber` を入力して、Enter キーを押します。
3. `portnumber` は選択したポート（1～4）の番号です。
4. SCE(config)# プロンプトに、`auto-negotiate` を入力して、Enter キーを押します。SCE(config)# プロンプトに、`exit` を入力して、Enter キーを押します。
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。

詳細ステップ

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)# プロンプトに、`interface GigabitEthernet 0/ portnumber` を入力して、Enter キーを押します。

ステップ 3 `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 4 SCE(config if)# プロンプトに、`auto-negotiate` を入力して、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 5 SCE(config if)# プロンプトに、`exit` 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 6 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

サマリー 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。
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。
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。
4. SCE(config if)# プロンプトに、`speed auto|100` を入力して、Enter キーを押します。
5. SCE(config if)# プロンプトに、`exit` を入力して、Enter キーを押します。
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。

詳細ステップ

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 モードを設定します。

ステップ 4 SCE(config if)# プロンプトに、`speed auto|100` 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)# プロンプトに、`exit` 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。

スピードとデュプレックス 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 \(p.6-5\)](#)
- [トンネリングモードの選択方法 \(p.6-6\)](#)
- [トンネリング設定の表示方法 \(p.6-8\)](#)

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リバ情報として扱う（「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
	サブスクリバとしての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
	サブスクリバとしてのMPLS L3 VPN	MPLS VPN auto-learn

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

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、実際のサブスクリ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リ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。

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）。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。

VLANタグによるサブスクリバ分類は、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タグが同一）でのみサポートされます。



(注)

トンネリング モードを変更するには、トンネル マッピングを使用しているすべてのサブスクリ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、CLI で `no subscriber all with-tunnel-mappings` コマンドを使用します（「トンネル マッピングを使用しているサブスクリイバを削除する方法」 [p.9-12] を参照）。

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`

トンネリング モードの選択方法

- [IP トンネルの設定方法 \(p.6-6\)](#)
- [VLAN 環境の設定方法 \(p.6-6\)](#)
- [MPLS 環境の設定方法 \(p.6-7\)](#)
- [L2TP 環境の設定方法 \(p.6-8\)](#)

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 トンネルは、トンネル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 \(p.6-6\)](#)
- [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、サブスライバとフローの分類に 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、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に設定されています。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、symmetric skip の VLAN トンネル環境を選択する例を示します。

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

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.6-7)
- 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) — トンネルを無視する (ラベルなしで挿入する)
- **VPN skip** — トンネリングを無視する (ラベル付きで挿入する)
- **VPN auto-learn** — サブスライバとしての MPLS L3 VPN

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
```

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。

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 モードのイネーブル化



(注)

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.6-12] 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。

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。

VLAN 変換の設定方法

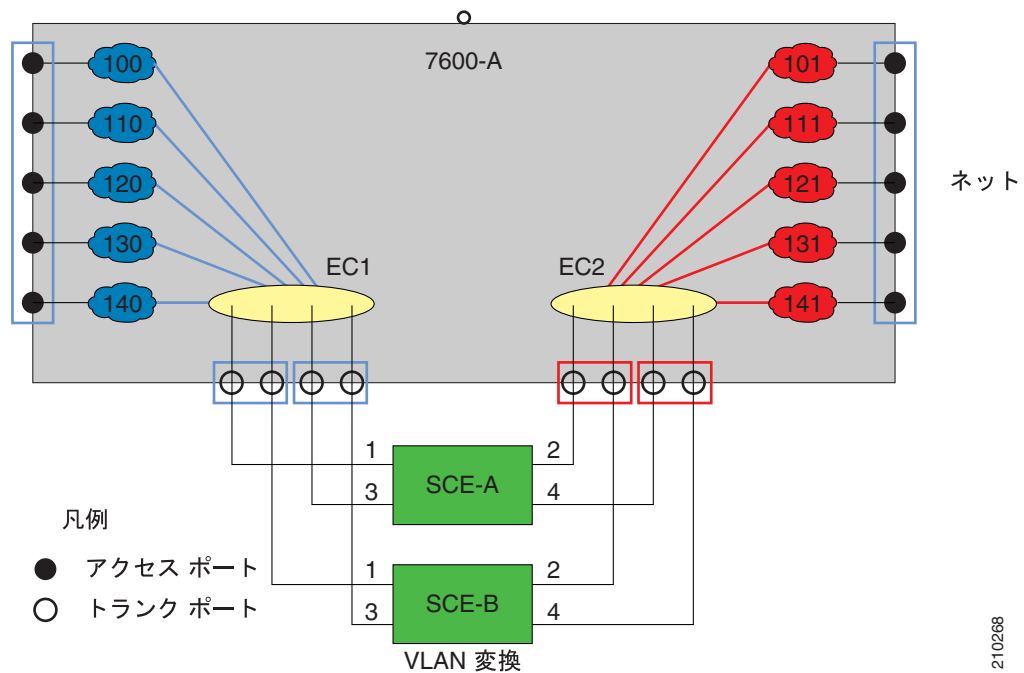
- VLAN 変換について (p.6-9)
- VLAN 変換機能および制限事項 (p.6-10)
- VLAN 変換定数の設定方法 (p.6-10)
- VLAN 変換のディセーブル化の方法 (p.6-11)
- VLAN 変換のモニタ方法 (p.6-11)

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負荷分散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、サブスライバ側では X ずつデ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 \(p.6-10\)](#)
- [VLAN 変換定数の設定：例 \(p.6-11\)](#)

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、サブスライバポートでは 5 ずつデ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 変換のモニタ方法

-
- 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 \(p.6-12\)](#)
- [トラフィック カウンタの設定方法 \(p.6-14\)](#)
- [トラフィック規則の設定方法 \(p.6-15\)](#)
- [トラフィック規則とカウンタの管理方法 \(p.6-17\)](#)

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 \(p.6-12\)](#)
- [トラフィック規則 \(p.6-12\)](#)
- [トラフィック カウンタ \(p.6-13\)](#)

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。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（サブスクリバ/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/UCP/ICMP/IGRP/EIGRP/IS-IS/OSPF/other
- **TCP/UDP ポート** — 各回線ポート（サブスクリバ/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ス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、異なる名前での同一の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つずつインクリメントします。
- **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インクリメントします。

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 \(p.6-14\)](#)
- [トラフィック カウンタの削除方法 \(p.6-14\)](#)
- [既存のすべてのトラフィック カウンタの削除方法 \(p.6-14\)](#)

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 \(p.6-15\)](#)
- [トラフィック規則の削除方法 \(p.6-17\)](#)
- [すべてのトラフィック規則の削除方法 \(p.6-17\)](#)

トラフィック規則の作成方法

- [オプション \(p.6-15\)](#)
- [トラフィック規則の設定例 \(p.6-16\)](#)

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/UCP/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.6-6]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。

■ トラフィック規則とカウンタの設定方法

- **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ス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 (p.6-16)
- 例 2 (p.6-16)
- 例 3 (p.6-17)

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)
- 唯一実行されるアクションは、無視です。

```
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 \(p.6-18\)](#)
- [すべてのトラフィック規則の表示方法 \(p.6-18\)](#)
- [指定したトラフィック カウンタの表示方法 \(p.6-18\)](#)

■ トラフィック規則とカウンタの設定方法

- すべてのトラフィック カウンタの表示方法 (p.6-18)
- 指定したトラフィック カウンタのリセット方法 (p.6-19)
- すべてのトラフィック カウンタのリセット方法 (p.6-19)

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

- トラフィック カウンタの表示 : 例 (p.6-18)

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 マーキングの設定方法

- [TOS マーキングについて \(p.6-20\)](#)
- [TOS マーキングをイネーブル化およびディセーブル化する方法 \(p.6-20\)](#)
- [TOS テーブルの変更方法 \(p.6-20\)](#)

TOS マーキングについて

SCE プラットフォームの TOS マーキング機能を使用すると、パケットの 2 つの作用属性に準じて各パケットの IP ヘッダーにある TOS フィールドにマーク付けを行うことができます。class は Class of Service (CoS; サービスクラス) であり、color は該当する場合に、パケットのコンプライアンスレベルに関連する帯域幅制限に反映します。IP ヘッダーに設定される実際の TOS 値は、class と color に基づいた設定が可能な TOS テーブルによって決まります。TOS テーブルのデフォルト値は、Diffserv 標準に基づいています。



(注)

最初のいくつかの TCP パケット (接続確立) は、デフォルトの AF4 クラスに関連付けられて、マーク付けされます。AF4 クラスは、AF-4 キューにマッピングされ、それに応じてマーク付けされます。これは、SCE プラットフォームが、フローを分類し、アプリケーションまたはサービスを特定する前に、最初のいくつかのパケットを伝送するために行われます。

TOS マーキングをイネーブル化およびディセーブル化する方法

- [TOS マーキングをイネーブル化する方法 \(p.6-20\)](#)
- [TOS マーキングをディセーブル化する方法 \(p.6-20\)](#)

TOS マーキングをイネーブル化する方法

ステップ 1 SCE(config if)# プロンプトに、ToS-marking mode diffserv を入力して、Enter キーを押します。

TOS マーキングのイネーブル化

TOS マーキングをディセーブル化する方法

ステップ 1 SCE(config if)# プロンプトに、no ToS-marking mode diffserv を入力して、Enter キーを押します。

TOS マーキングのディセーブル化

TOS テーブルの変更方法

- [オプション \(p.6-21\)](#)
- [TOS テーブルの変更例 \(p.6-21\)](#)

オプション

次のオプションを使用できます。

- **class** — パケットに適用可能なクラス (BE、AF1、AF2、AF3、AF4、EF)
- **color** — 適用可能な色 (緑、赤、または任意の色)
- **value** — パケットに割り当てる値 (IP TOS フィールドに設定された値)
value パラメータは、**0x0** ~ **0x3f** の範囲の 16 進表記である必要があります。

ステップ 1 SCE(config if)# プロンプトに、`ToS-marking set-table-entry class class color color value value` を入力して、Enter キーを押します。

TOS テーブルの変更例

次に、TOS マーキング テーブルのエントリを設定する例を示します。

```
SCE(config if)#ToS-marking set-table-entry class AF3 color green value 0x24
```

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 \(p.6-22\)](#)
- [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 \(p.6-22\)](#)

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 (管理情報ベース) カウンタで正確な値を把握できません。

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