CHAPTER 76

サービス拒否（DoS）からの保護

（注）
- この章で使用しているコマンドの構文および使用方法の詳細については、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- 次のセクションも参照してください。
  - 第 72 章「MAC アドレスベースのトラフィック ブロッキング」
  - 第 81 章「トラフィック ストーム制御」
  - 第 77 章「コントロール プレーン ポリシング（CoPP）」
  - http://www.cisco.com/en/US/docs/ios-xml/ios/security/config_library/15-sy/secdata-15-sy-library.html

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する

セキュリティ ACL および VACL

ネットワークが DoS 攻撃を受けている場合、DoS パケットがターゲットに達する前に DoS パケットをドロップする有効な方法は ACL です。特定ホストからの攻撃が検出された場合は、セキュリティ ACL を使用します。

次の例では、ホスト 10.1.1.10 およびそのホストからのすべてのトラフィックが拒否されます。

```
Router(config)# access-list 101 deny ip host 10.1.1.10 any
Router(config)# access-list 101 permit ip any any
```

セキュリティ ACL は、アドレスのスプーフィングからも保護します。たとえば送信元アドレス A がネットワーク内にあり、スイッチ インターフェイスがインターネットに向いているとします。スイッチ インターネット インターフェイスで着信 ACL を適用すれば、送信元が A（内部アドレス）になっているすべてのアドレスを拒否できます。この処理では、攻撃者が内部送信元アドレスになりすます攻撃が防止されます。パケットは、スイッチ インターフェイスに到着したとき、その ACL と一致してドロップされるので、被害は発生しません。

スイッチを Cisco Intrusion Detection Module（CIDM）で使用している場合は、感知エンジンによる攻撃の検出に対応して、セキュリティ ACL をダイナミックにインストールできます。

VACL は、レイヤ 2、レイヤ 3、レイヤ 4 の情報に基づくセキュリティ処理ツールです。パケットに対する VACL ルックアップの結果は、許可、拒否、許可および取り込み、リダイレクトのうちいずれかになります。VACL を特定 VLAN に関連付けると、すべてのトラフィックは、VACL によって許可されないと VLAN に入ることができません。VACL はハードウェア内で適用されます。したがって VLAN に VACL を適用しても、パフォーマンス ペナルティは発生しません。

第 69 章「Cisco IOS ACL のサポート」および第 74 章「VLAN ACL（VACL）」を参照してください。

QoS レート制限

QoS ACL は、RP によって処理される、特定の種類のトラフィックの量を制限します。RP に対して DoS 攻撃が開始されると、QoS ACL は DoS トラフィックが RP データ パスに到達し、輻輳を防ぎます。PFC および DFC は QoS をハードウェア内で実行します。この仕組みは、DoS トラフィックを制限して（DoS トラフィックの検知後）、スイッチが RP に影響を与えることを防ぐうえで効果的です。

たとえば、ネットワークが ping-of-death や SMURF アタックなどを受けた場合、管理者はこの DoS 攻撃に対処するため ICMP トラフィックをレート制限する必要がありますが、同時に正規のトラフィックのプロセッサ処理、または RP やホストへの転送を許可する必要があります。このレート制限設定は、レート制限が必要なフローごとに実行する必要があり、レート制限ポリシー アクションはインターフェイスに適用する必要があります。

次の例では、アクセス リスト 101 が、任意の送信元から任意の宛先への ping（エコー）ICMP メッセージを許可してトラフィックとして識別します。ポリシー マップ内では、ポリシング ルールが特定 Committed Information Rate（CIR; 認定情報速度）とバースト値（96000 bps および 16000 bps）を定義し、シャーシを経由する ping（ICMP）トラフィックをレート制限します。ポリシー マップはインターフェイスまたは VLAN に適用されます。ポリシー マップが適用されている VLAN またはインターフェイスにおいて ping トラフィックが指定したレートを超えた場合、ping トラフィックはマークダウン マップに指定されたようにドロップされます（通常バースト設定のマークダウン マップは、この例に示していません）。

```
Router(config)# access-list 101 permit icmp any any echo
Router(config)# class-map match-any icmp_class
Router(config-cmap)# match access-group 101
Router(config-cmap)# exit
Router(config)# policy-map icmp_policer
Router(config-pmap)# class icmp_class
```

```
Router(config-pmap-c)# police 96000 16000 conform-action transmit exceed-action
policed-dscp-transmit drop
Router(config-pmap-c)# exit
Router(config-pmap)# exit
```

第 63 章「分類、マーキング、およびポリシング」を参照してください。

グローバル プロトコル パケット ポリシング

グローバル プロトコル パケット ポリシングの前提条件

なし。

グローバル プロトコル パケット ポリシングの制約事項

- **platform qos protocol arp police** コマンドでサポートされている最小値は、実稼働ネットワークでは小さすぎます。
- ARP パケットの長さは約 40 バイトで、ARP 応答パケットの長さは約 60 バイトです。ポリサー レート値の単位はビット/秒です。バースト値の単位はバイト/秒です。まとめると、ARP 要求および応答は、約 800 ビットです。
- 設定したレート制限は、PFC および各 DFC に別々に適用されます。RP CPU は、設定値にフォワーディング エンジンの数を乗算した数を受け取ります。
- ポリシー ベースのプロトコル パケット ポリシングは、フォワーディング エンジン（PFC およびすべての DFC）ごとに適用されます。
- Supervisor Engine 2T を使用する場合、ポリシー ベースのプロトコル パケット ポリシングは、分散集約ポリシングをサポートします（「分散型の集約ポリシングのイネーブル化」（P.63-8）を参照）。
- プロトコル パケット ポリシング メカニズムは、ラインレート ARP 攻撃などの攻撃から RP CPU を事実上保護しますが、スイッチ へのルーティング プロトコルと ARP パケットの両方をポリシングし、CoPP を下回る粒度で、スイッチを介するトラフィックをポリシングします。
- ポリシング メカニズムとポリシング回避メカニズムは、ルート設定を共有します。ポリシング回避メカニズムでは、ルーティング プロトコルと ARP パケットが、QoS ポリサーに達したとき、ネットワークを流れます。このメカニズムは、**platform qos protocol** *protocol_name* **pass-through** コマンドを使用して設定できます。
- ポリシー ベースのプロトコル パケット ポリシングは、マイクロフロー ポリサーをサポートしていません。
- 入力ポリシー ベースのプロトコル パケット ポリシングだけがサポートされています。

- ポリシー ベースのプロトコル パケット ポリシングは、レイヤ 4 ACL 演算子（「ACL のレイヤ 4 演算の制約事項」（P.69-2）を参照）をサポートしていません。この結果、さらに、次の制限が課されます。
  - IPv4 トラフィックまたは IPv6 トラフィックで、UDP または TCP のポート範囲マッチングがサポートしません
  - IPv6 トラフィックで、優先順位または DSCP のマッチングがサポートされません
- プロトコル パケット ポリシング ポリシーでは、QoS ポリシーと、1 つの集約ポリサーを共有できます。
- 集約ポリサーは、入力トラフィックと出力トラフィックの両方には適用できません。
- Supervisor Engine 2T を使用する場合、ポリシー ベースのプロトコル パケット ポリシングでは、最大 1,000 個のグローバル TCAM エントリをサポートします。
- ポリシー ベースのプロトコル パケット ポリシングでは、**class default** and **permit** *protocol_name* **any any** コマンドをサポートしていますが、プロトコル パケット ポリシング ポリシーでは、一致するすべてのトラフィックを処理するため、トラフィック フローに大きく影響することがあります。
- Supervisor Engine 2T を使用する場合、ポリシー ベースのプロトコル パケット ポリシングは、設定されている任意のポートの信頼状態で動作します。
- 単一コマンドのプロトコル パケット ポリシングとポリシー ベースのプロトコル パケット ポリシングの両方を設定できます。単一コマンドのプロトコル パケット ポリシングが最初に適用され、次に、ポリシー ベースのプロトコル パケット ポリシングが適用されます。

（注） ソフトウェアでは、単一コマンドのプロトコル パケット ポリシングとポリシー ベースのプロトコル パケット ポリシングの間にある設定の不整合を検出せず、解決も試みません。

- ポリシー ベースのプロトコル パケット ポリシングとコントロール プレーン ポリシングの両方を設定できます（第 77 章「コントロール プレーン ポリシング（CoPP）」を参照）。ポリシー ベースのプロトコル パケット ポリシングが最初に適用され、次に、CoPP が適用されます。
- 単一コマンドのプロトコル パケット ポリシングは、入力トラフィック用に設定されたプロトコル固有のアクションをプログラムし、入力結果の出力トラフィックを維持するために、対応する出力トラフィックパススルー アクションを自動的にプログラムします。
- ポリシー ベースのプロトコル パケット ポリシングでは、出力トラフィックで入力ポリシングの結果を自動的に保持しません。
  - ポリシー ベースのプロトコル パケット ポリシングを使用して、出力トラフィックで入力ポリシングの結果を保持するには、適切な出力ポリシーを設定します。出力トラフィックを未変更で渡すには、出力ポリシー内の各入力クラスを複製し、クラス マップのアクションとして **trust dscp** を設定します。
  - 出力ポリシーマップがない場合、出力トラフィックは、設定された任意のインターフェイス ベース ポリシーマップによって処理され、入力のグローバル ポリシーの結果は上書きされます。
- PFC および任意の DFC は、**class-map match-all** クラス マップで単一の **match** コマンドをサポートします。ただし、**match protocol** コマンドは、**match dscp** または **match precedence** コマンドによってクラス マップに設定できます。
- PFC および任意の DFC は、**class-map match-any** クラス マップで複数の **match** コマンドをサポートします。
- クラス マップでは、表 76-1 に記載されている **match** コマンドを使用して、一致基準に基づくトラフィック クラスを設定できます。

表 76-1　トラフィック分類のクラス マップの match コマンドと一致基準

match コマンド	方向	一致基準
match access-group {*access_list_number* | **name** *access_list_name*}	入力	アクセス コントロール リスト（ACL）。 （注）　ACL は、次の要素の照合に使用します。 - CoS 値 - VLAN ID - パケット長
match any	入力	任意の一致基準
match cos	入力	CoS 値
match discard-class	入力	廃棄クラスの値。
match dscp （注）　**match protocol** コマンドは、**match dscp** コマンドでクラス マップに設定できます。	入力	DSCP 値。
match l2 miss	入力	現在学習されていない MAC レイヤの宛先アドレスにアドレス指定されているため、VLAN でフラッディングしたレイヤ 2 トラフィック。
match mpls experimental topmost	入力	最上位ラベルの MPLS EXP 値。
match precedence （注）　**match protocol** コマンドは、**match precedence** コマンドでクラス マップに設定できます。	入力	IP precedence 値。
match protocol {**arp** | **ip** | **ipv6**} （注）　**match protocol** コマンドは、**match dscp** コマンドまたは **match precedence** コマンドでクラス マップに設定できます。	入力	プロトコル。
match qos-group	入力	QoS グループ ID。

PFC および任意の DFC は、**match access group** コマンドで使用するために、次の ACL タイプをサポートしています。

プロトコル	番号付き ACL の有無	拡張 ACL の有無	名前付き ACL の有無
IPv4	Yes : 1 ～ 99 1300 ～ 1999	Yes : 100 ～ 199 2000 ～ 2699	Yes
IPv6	N/A	Yes（名前付き）	Yes
MAC レイヤ	N/A	N/A	Yes
ARP	N/A	N/A	Yes

グローバル プロトコル パケット ポリシングに関する情報

攻撃者はルーティング プロトコル制御パケット（ARP パケットなど）によって、RP CPU を過負荷にしようと試みることがあります。プロトコル パケット ポリシングでは、ハードウェアでこのトラフィックをレート制限します。リリース 15.1(1) SY1 以降のリリースでは、Cisco Feature Navigator にグローバル QoS ポリシー機能として表示される、ポリシー ベースのグローバル プロトコル パケット ポリシングをサポートしています。

単一コマンドのグローバル プロトコル パケット ポリシングの設定方法

platform qos protocol ? と入力して、サポートされているルーティング プロトコルを表示します。

プラットフォーム タイプ qos protocol arp police コマンドは、ARP パケットをレート制限します。次に、1 秒あたり、ARP 要求と応答を合計 200 個許可する例を示します。

```
Router(config)# platform qos protocol arp police 200000 6000
```

次に、プロトコル パケット ポリシングで使用できるプロトコルを表示する例を示します。

```
Router(config)# platform qos protocol ?
  isis
  eigrp
  ldp
  ospf
  rip
  bgp
  ospfv3
  bgpv2
  ripng
  neigh-discover
  wlccp
  arp
```

次に、**platform qos protocol** コマンドで使用できるキーワードを表示する例を示します。

```
Router(config)# platform qos protocol protocol_name ?
  pass-through  pass-through keyword
  police        police keyword
  precedence    change ip-precedence(used to map the dscp to cos value)
```

ポリシー ベースのグローバル プロトコル パケット ポリシングの設定方法

次の QoS セクションおよびグローバル プロトコル パケット ポリシング ポリシー マップ コンフィギュレーション セクションを参照してください。

- 「クラス マップの設定」（P.63-8）
- 「ポリシー マップ コンフィギュレーション」（P.63-9）
- 「グローバル プロトコル パケット ポリシング ポリシー マップの設定」（P.76-7）

グローバル プロトコル パケット ポリシング ポリシー マップの設定

グローバル プロトコル パケット ポリシング ポリシー マップを設定するには、次の作業を行います。

コマンド	目的
`Router(config)# platform qos service-policy input policy_map_name`	グローバル プロトコル パケット ポリシング ポリシー マップを設定します。 **（注）**　入力ポリシーを 1 つ設定できます。

ユニキャスト リバース パス転送（uRPF）チェック

uRPF チェックの前提条件

なし。

uRPF チェックの制約事項

- ユニキャスト RPF は、スプーフィングに対する完全な保護を提供しません。送信元 IP アドレスに戻る適切なルートが存在する場合は、スプーフィングされたパケットが、ユニキャスト RPF に対応したインターフェイスを介してネットワークに侵入する可能性があります。
- 各インターフェイスにユニキャスト RPF モードを 1 つ設定できます。
- ユニキャスト RPF モードの「allow default」オプションでは、スプーフィングを十分に防止できません。
  - Allow Default を使用したストリクト ユニキャスト RPF チェック：ルーティング テーブルに存在するプレフィックスが送信元である受信 IP トラフィックは、そのプレフィックスが入力インターフェイス経由で到達可能な場合、ユニキャスト RPF チェックに合格します。デフォルト ルートが設定されている場合、ルーティング テーブル内に存在しない送信元プレフィックスを持つ IP パケットは、入力インターフェイスがデフォルト ルートのリバース パスである場合は、ユニキャスト RPF チェックに合格します。
  - Allow Default を使用したルーズ ユニキャスト RPF チェック：デフォルト ルートが設定されている場合、すべての IP パケットがユニキャスト RPF チェックに合格します。
- ユニキャスト RPF ストリクト モード：ユニキャスト RPF ストリクト モードでは、スプーフィングされたトラフィックに対して最高のセキュリティを提供します。ユニキャスト RPF チェック対応のすべてのインターフェイスで、トラフィックのリバース パスであるインターフェイス経由で有効な IP トラフィックをスイッチが受信すると、ストリクト モードがオプションとなります。

- ユニキャスト RPF のルーズ モード：ユニキャスト RPF のルーズ モードは、ストリクト モードほど保護できない一方で、トラフィックのリバース パスでないインターフェイスで有効な IP トラフィックを受信するスイッチのオプションとなります。ユニキャスト RPF ルーズ モードでは、受信したトラフィックの送信元が、トラフィックが到着したインターフェイスに関係なく、ルーティング テーブル内に存在するプレフィックスであることを確認します。

uRPF チェックについて

ユニキャスト RPF チェックでは、受信した IP パケットの送信元アドレスが到達可能であることを確認します。ユニキャスト RPF チェックでは、検証可能な IP 送信元プレフィックス（ルート）がない IP パケットは廃棄されます。これにより、変形または偽造（スプーフィング）された IP 送信元アドレスを持つトラフィックによる問題が軽減されます。

PFC4 および DFC4 は最大 16 個のパスで、ACL フィルタリングの有無を問わず、IPv4 と IPv6 の両方のトラフィックのユニキャスト RPF チェックに対するハードウェア サポートを提供します。

17 以上のリバース パス インターフェイスが各プレフィックスのルーティング テーブルに存在しなことを確認するには、OSPF、EIGRP、または BGP の設定時に config-router モードで **maximum-paths 16** コマンドを入力します。

ユニキャスト RPF チェックの設定手順

- 「ユニキャスト RPF チェック モードの設定」（P.76-9）
- 「self-ping のイネーブル化」（P.76-10）

（注）　次のコマンドは CLI にありますが、機能しません。

- **platform ip cef rpf interface-group**
- **platform ip cef rpf multipath interface-group**
- **platform ip cef rpf multipath pass**
- **platform ip cef rpf multipath punt**

ユニキャスト RPF チェック モードの設定

ユニキャスト RPF チェック モードを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port} | {port-channel number}}`	設定するインターフェイスを選択します。 （注）　ユニキャスト RPF チェックは次の宛先にパケットを転送する前に、入力ポートに基づいて、最適なリターン パスを確認します。
ステップ 2	`Router(config-if)# ip verify unicast source reachable-via {rx | any} [allow-default] [list]`	IPv4 ユニキャスト RPF チェック モードを設定します。
ステップ 3	`Router(config-if)# ipv6 verify unicast source reachable-via {rx | any} [allow-default] [list]`	IPv6 ユニキャスト RPF チェック モードを設定します。
ステップ 4	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。
ステップ 5	`Router# show platform hardware cef ip rpf`	IPv4 の設定を確認します。
ステップ 6	`Router# show platform hardware cef ipv6 rpf`	IPv6 の設定を確認します。

- strict チェック モードをイネーブルにするには、**rx** キーワードを使用します。
- exist-only チェック モードをイネーブルにするには、**any** キーワードを使用します。
- RPF の確認にデフォルト ルートを使用できるようにするには、**allow-default** キーワードを使用します。
- アクセス リストを識別するには、*list* オプションを使用します。
  - アクセス リストによってネットワークへのアクセスが拒否された場合は、拒否されたパケットがポートでドロップされます。
  - アクセス リストによってネットワークへのアクセスが許可された場合は、パケットが宛先アドレスに転送されます。転送されたパケットは、インターフェイスの統計情報にカウントされます。
  - アクセス リストにログ アクションが含まれている場合、パケットに関する情報がログ サーバに送信されます。

次に、ギガビット イーサネット ポート 4/1 でユニキャスト RPF の exist-only チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ipv6 verify unicast source reachable-via any
Router(config-if)# ip verify unicast source reachable-via any
Router(config-if)# end
Router#
```

次に、ギガビット イーサネット ポート 4/2 でユニキャスト RPF の strict チェック モードをイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/2
Router(config-if)# ipv6 verify unicast source reachable-via rx
Router(config-if)# ip verify unicast source reachable-via rx
Router(config-if)# end
Router#
```

self-ping のイネーブル化

ユニキャスト RPF チェックがイネーブルの場合、スイッチはデフォルトで自身を ping できません。self-ping をイネーブルにするには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface {{vlan vlan_ID} | {type slot/port} | {port-channel number}}`	設定するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip verify unicast source reachable-via any allow-self-ping`	self-ping またはセカンダリ アドレスへの ping を実行できるように、スイッチをイネーブルにします。
ステップ 3	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

次に、self-ping をイネーブルにする例を示します。

```
Router(config)# interface gigabitethernet 4/1
Router(config-if)# ip verify unicast source reachable-via any allow-self-ping
Router(config-if)# end
```

スティッキ ARP の設定

スティッキ ARP では、ARP エントリ（IP アドレス、MAC アドレス、送信元 VLAN）が上書きされないようにして、MAC アドレスのスプーフィングを防止します。スイッチは ARP エントリを、エンドデバイスまたはその他のスイッチにトラフィックを転送するために維持します。ARP エントリは、一般的に定期的に更新されるか、ARP ブロードキャストを受信したときに修正されます。攻撃中に ARP ブロードキャストは、スプーフィングされた MAC アドレス（正当な IP アドレスを含む）を使用して送信されるので、スイッチは、スプーフィングされた MAC アドレスを含む正当な IP アドレスを学習し、その MAC アドレスにトラフィックを転送し始めます。スティッキ ARP をイネーブルにすると、スイッチは ARP エントリを学習し、ARP ブロードキャストで受信した修正を受け入れません。スティッキ ARP 設定を上書きしようとすると、エラー メッセージが表示されます。

sticky ARP をレイヤ 3 インターフェイス上で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# interface type[1] slot/port`	スティッキ ARP を適用するインターフェイスを選択します。
ステップ 2	`Router(config-if)# ip sticky-arp`	スティッキ ARP をイネーブルにします。
ステップ 3	`Router(config-if)# ip sticky-arp ignore`	スティッキ ARP をディセーブルにします。

1. *type* = **fastethernet**、**gigabitethernet**、または **tengigabitethernet**

次に、インターフェイス 5/1 でスティッキ ARP をイネーブルにする例を示します。

```
Router# configure terminal
Router(config)# interface gigabitethernet 5/1
Router(config-if)# ip sticky-arp
Router(config-if)# end
Router#
```

パケット ドロップ統計のモニタ

パケット ドロップ統計の前提条件

なし。

パケット ドロップ統計の制約事項

- 着信取り込みトラフィックはフィルタ処理されません。
- 着信取り込みトラフィックは、取り込み宛先にレート制限されません。

パケット ドロップ統計について

パケット ドロップ統計を表示するには、show コマンドを使用できます。トラフィックをインターフェイス上でキャプチャし、このトラフィックのコピーをポートに接続されたトラフィック アナライザに送信します。トラフィック アナライザは、パケット ドロップ統計を集約します。

ドロップされたパケットのモニタ方法

show コマンドの使用

PFC および DFC では、ハードウェア内の ACL ヒット カウンタがサポートされます。ACL TCAM におけるそれぞれのエントリを表示するには、**show platform hardware acl entry interface** コマンドを使用できます。TTL および IP のオプション カウンタを使用し、レイヤ 3 フォワーディング エンジンのパフォーマンスをモニタすることもできます。

次に、**show platform hardware acl entry interface** コマンドを使用して、レイヤ 3 フォワーディング エンジンに関連するパケット統計およびエラーを表示する例を示します。

```
Router# show platform hardware statistics

 --- Hardware Statistics for Module 6 ---


L2 Forwarding Engine
    Switched in L2 : 59624 @ 7 pps

L3 Forwarding Engine
```

```
    Processed in L3 : 59624 @ 7 pps
    Switched in L3  : 13 @ 0 pps

    Bridged         : 4602
    FIB Switched
        IPv4 Ucast : 7
        IPv6 Ucast : 1
        EoMPLS     : 1
        MPLS       : 1
        (S , *)    : 0
        IGMP MLD   : 0
        IPv4 Mcast : 2
        IPv6 Mcast : 0
        Mcast Leak : 0
    ACL Routed
        Input      : 1
        Output     : 518
    Netflow Switched
        Input      : 2
        Output     : 0
    Exception Redirected
        Input      : 0
        Output     : 1
    Mcast Bridge Disable & No Redirect
                   : 0
    Total packets with TOS Changed              : 3
    Total packets with TC  Changed              : 0
    Total packets with COS Changed              : 64
    Total packets with EXP Changed              : 0
    Total packets with QOS Tunnel Encap Changed : 1
    Total packets with QOS Tunnel Decap Changed : 1
    Total packets dropped by ACL                : 1
    Total packets dropped by Policing           : 0
Errors
    MAC/IP length inconsistencies               : 0
    Short IP packets received                   : 0
    IP header checksum errors                   : 0
    TTL failures                                : 0
    MTU failures                                : 0

Total packets L3 Processed by all Modules: 59624 @ 7 pps
```

SPAN の使用方法

次に、**monitor session** コマンドを使用して、トラフィックを取り込んで外部インターフェイスに転送する例を示します。

```
Router# configure terminal
Enter configuration commands, one per line.  End with CNTL/Z.
Router(config)# monitor session 1 source vlan 44 both
Router(config)# monitor session 1 destination interface g9/1
Router(config)# end
Router#
```

次に、**show monitor session** コマンドを使用して、宛先ポートを表示する例を示します。

```
Router# show monitor session 1
Session 1
---------
Source Ports:
    RX Only:       None
    TX Only:       None
    Both:          None
```

```
Source VLANs:
    RX Only:        None
    TX Only:        None
    Both:           44
Destination Ports: Gi9/1
Filter VLANs:       None
```

詳細については、第 56 章「ローカル SPAN、RSPAN、および ERSPAN」を参照してください。

VACL キャプチャの使用

VACL 取り込み機能では、取り込みトラフィックを転送するように設定されたポートにトラフィックを転送できます。capture アクションを指定すると、転送されたパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。

各 VLAN から別のインターフェイスにトラフィックを割り当てるには、VACL 取り込みを使用できます。

VACL 取り込みでは、HTTP などの、あるタイプのトラフィックを 1 つのインターフェイスに、DNS などの別のタイプのトラフィックを別のインターフェイスに送信できません。VACL 取り込み粒度は、ローカルにスイッチングされるトラフィックだけに適用可能です。トラフィックをリモート スイッチに転送する場合は、粒度を維持できません。

詳細については、第 74 章「VLAN ACL（VACL）」を参照してください。

ヒント Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

技術マニュアルのアイデア フォーラムに参加する