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 65 章「MAC アドレスベースのトラフィック ブロッキング」
  - 第 74 章「トラフィック ストーム制御」
  - 第 70 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 62 章「Cisco IOS ACL のサポート」および第 67 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 58 章「PFC QoS」を参照してください。

グローバル プロトコル パケットのポリシング

グローバル プロトコル パケットのポリシングの前提条件

なし。

グローバル プロトコル パケットのポリシングの制約事項

- **mls qos protocol arp police** コマンドでサポートされる最小値は、実稼働ネットワークで使用するには小さすぎます。
- 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。ポリサーのレート値の単位はビット / 秒です。バースト値はバイト / 秒です。ARP 要求および応答を合わせると約 800 ビットです。
- 設定したレート制限は、PFC およびすべての DFC にそれぞれ適用されます。RP CPU は設定値を転送エンジンの数だけ受け取ります。
- ポリシーベースのプロトコル パケットのポリシングは、転送エンジン（PFC およびすべての DFC）別に適用されます。
- プロトコル パケットのポリシング機能は、ラインレート ARP 攻撃などの攻撃から RP CPU を効果的に保護しますが、スイッチへのルーティング プロトコルおよび ARP パケットの両方をポリシングし、またスイッチを介して CoPP より低い精度で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、**mls qos protocol** *プロトコル名* **pass-through** コマンドで設定できます。
- ポリシーベースのプロトコル パケットのポリシングは、マイクロフロー ポリサーをサポートしません。
- 入力ポリシーベースのプロトコル パケットのポリシングのみをサポートします。

- ポリシーベースのプロトコル パケットの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.62-2）を参照）をサポートしておらず、次のような制限があります。
  - IPv4 または IPv6 トラフィックに対する UDP または TCP ポート レンジ マッチングのサポートなし
  - IPv6 トラフィックに対する優先順位または DSCP マッチングのサポートなし
- プロトコル パケットのポリシング ポリシーと QoS ポリシーは、集約ポリサーを共有できます。
- 入力トラフィックおよび出力トラフィックの両方に、集約ポリサーを適用することはできません。
- ポリシーベースのプロトコル パケットのポリシングは、**class default** および **permit** *プロトコル名* **any any** コマンドをサポートしますが、プロトコル パケットのポリシング ポリシーはすべての一致する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可能性があります。
- Supervisor Engine 720 の場合、ポリシーベースのプロトコル パケットのポリシングは信頼できないポートにのみ適用されます。
- シングルコマンドのプロトコル パケットのポリシングとポリシーベースのプロトコル パケットのポリシングの両方を設定することができます。最初にシングルコマンドのプロトコル パケットのポリシングを適用し、次にポリシーベースのプロトコル パケットのポリシングを適用します。

（注） ソフトウェアが、シングルコマンドのプロトコル パケットのポリシングとポリシーベースのプロトコル パケットのポリシングの間の設定の矛盾を検出し解決することはありません。

- ポリシーベースのプロトコル パケットの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することができます（第 70 章「コントロール プレーン ポリシング（CoPP）」を参照）。最初にポリシーベースのプロトコル パケットのポリシングを適用し、次に CoPP を適用します。
- シングルコマンドのプロトコル パケットのポリシングは、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、出力トラフィックで入力結果を保持するための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 パケットのポリシングは、出力トラフィックで入力ポリシングの結果を自動的には保持しません。
  - ポリシーベースのプロトコル パケットの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。未変更で出力トラフィックを渡すには、出力ポリシー内の各入力クラスを複製し、**trust dscp** をクラスマップのアクションとして設定します。
  - 出力ポリシーマップが存在しない場合、出力トラフィックは設定されたインターフェイスベースのポリシーマップによって処理され、入力のグローバル ポリシーの結果が上書きされます。
- PFC およびすべての DFC は **class-map match-all** クラス マップの単一の **match** コマンドをサポートしますが、**match dscp** コマンドまたは **match precedence** コマンドでクラス マップに **match protocol** コマンドを設定することができます。
- PFC およびすべての DFC は、**class-map match-any** クラス マップの複数の **match** コマンドをサポートします。
- クラス マップは、**match** コマンド（表 69-1 にリスト）を使用して、一致基準に基づくトラフィック クラスを設定することができます。

表 69-1　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 は以下を照合するために使用します。 —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** コマンドとともに、クラス マップで設定することができます。	入力	DSCP 値。
match l2 miss	入力	その時点で未学習の MAC レイヤ宛先アドレスにアドレス指定されていたために 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** コマンドとともに、クラス マップで設定することができます。	入力	IP precedence 値。
match protocol {**arp** | **ip** | **ipv6**} （注）　**match protocol** コマンドは、**match dscp** または **match precedence** コマンドとともに、クラス マップで設定することができます。	入力	プロトコル。
match qos-group	入力	QoS グループ ID。

PFC およびすべての 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 パケットの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場合があります。プロトコル パケットのポリシング レートは、ハードウェアのこのトラフィックを制限します。リリース 15.1(1)SY1 以降のリリースは、Cisco Feature Navigator にグローバル QoS ポリシー機能として示されているポリシーベースのグローバル プロトコル パケットのポリシングをサポートします。

シングルコマンド グローバル プロトコル パケットのポリシングの設定方法

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

mls qos protocol arp police コマンド レートで、ARP パケットを制限します。次に、毎秒 200 の ARP 要求および応答を割り当てる方法の例を示します。

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

次に、プロトコル パケットのポリシングを使用する場合に使用できるプロトコルを表示する方法の例を示します。

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

次に、**mls qos protocol** コマンドで、使用できるキーワードを表示する方法の例を示します。

```
Router(config)# mls 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 パケットのポリシングの設定方法

次の QoS に関するセクションおよびグローバル プロトコル パケットのポリシング ポリシー マップ設定のに関するセクションを参照してください。

- 「クラス マップの設定」（P.58-81）
- 「ポリシー マップの設定」（P.58-84）
- 「グローバル プロトコル パケットのポリシング ポリシー マップの設定」（P.69-7）

グローバル プロトコル パケットのポリシング ポリシー マップの設定

グローバル プロトコル パケットのポリシング 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)# mls qos service-policy input` *policy_map_name*	グローバル プロトコル パケットのポリシング 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。
- ユニキャスト RPF チェックによってルート プロセッサが過負荷になる設定を回避してください。
  - ACL を使用してフィルタリングするようにユニキャスト RPF を設定しないでください。
  - グローバル ユニキャスト RPF「パント」チェック モードを設定しないでください。
- PFC は、ポリシーベース ルーティング（PBR）トラフィックのユニキャスト RPF チェックをハードウェアでサポートしません。（CSCea53554）
- スイッチは、ユニキャスト RPF チェックが設定されているすべてのインターフェイスに同じユニキャスト RPF モードを適用します。任意のインターフェイス上でユニキャスト RPF モードで行ったすべての変更は、ユニキャスト RPF チェックが設定されているすべてのインターフェイスに適用されます。
- 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。
- それぞれに 6 つインターフェイスが含まれる 4 つのグループに分けられた、最大 24 のインターフェイス上で、スイッチが送信元プレフィックスごとに最大 6 つのリバース パス インターフェイスを持つ有効な IP パケットを受信した場合は、**mls ip cef rpf multipath interface-group** コマンドでユニキャスト RPF ストリクト モードを設定できます。

  このオプションでは、送信元プレフィックス、および送信元プレフィックスのリバース パスとして機能するインターフェイスを識別し、これらのリバース パス インターフェイスにインターフェイス グループを設定する必要があります。各送信元プレフィックスのリバース パス インターフェイスはすべて、同じインターフェイス グループに属している必要があります。4 つのインターフェイス グループ（それぞれ最大 6 つのリバース パス インターフェイスを含めることができる）を設定できます。インターフェイス グループがサポートできる送信元プレフィックス数に制限はありません。

  6 を超えるリバース 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い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 6** コマンドを入力します。

  これらのインターフェイス グループ外の、uPPF チェック対応インターフェイスで受信された、1 つまたは 2 つのリバース パス インターフェイスの IP トラフィックは、入力インターフェイスおよび最大 1 つの他のインターフェイスがリバース パスである場合、ユニキャスト RPF チェックに合格します。

  最大パスが 6 に設定されている場合、インターフェイス グループ外の uPPF チェック対応インターフェイスで受信された 3 つ以上のリバース パス インターフェイスを持つ IP トラフィックは、ユニキャスト RPF チェックに常に合格します。
- 任意の数のインターフェイスで､送信元プレフィックスごとに 1 つまたは 2 つのリバース パス インターフェイスを持つ有効な IP パケットをスイッチが受信した場合は、**mls ip cef rpf multipath pass** コマンドでユニキャスト RPF ストリクト モードを設定できます。

  3 つ以上のリバース 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 2** コマンドを入力します。

- パス グローバル モードでのユニキャスト RPF ルーズ モード：ユニキャスト RPF ルーズ モードはストリクト モードほど保護を提供できませんが、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。

ユニキャスト RPF チェックは RP のソフトウェアで行われ、最大 16 のリバース パス インターフェイスをサポートします。

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。

ACL フィルタリングを行わないユニキャスト RPF チェックの場合、PFC3 は、複数のインターフェイスからのトラフィックの RPF チェックをハードウェアでサポートします。

ACL フィルタリングを行うユニキャスト RPF チェックの場合、PFC はトラフィックが ACL と一致するかどうかを判別します。PFC は、RPF ACL によって拒否されたトラフィックをルート プロセッサ（RP）に送信してユニキャスト RPF チェックを行います。ACL によって許可されたパケットは、ユニキャスト RPF チェックを行わずにハードウェアで転送されます。

ユニキャスト RPF チェックの設定方法

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 mls 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。

（注） ユニキャスト RPF チェック用に設定されたすべてのポートには、最後に設定されたモードが自動的に適用されます。

- 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#
```

複数パスのユニキャスト RPF チェック モードの設定

複数パスのユニキャスト RPF 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)# mls ip cef rpf mpath {punt | pass | interface-group}`	複数パスの RPF チェック モードを設定します。
ステップ 2	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 3	`Router# show mls cef ip rpf`	設定を確認します。

複数のパス RPF チェックを設定する場合、次の情報に注意してください。

- **punt** モード（デフォルト）: PFC3 は、プレフィックス単位で最大 2 つのインターフェイスに対し、ハードウェアでユニキャスト RPF チェックを実行します。追加のインターフェイスに着信するパケットは、RP にリダイレクト（パント）され、ソフトウェアでユニキャスト RPF チェックが実行されます。
- **pass** モード : PFC3 は、single-path および two-path プレフィックスに対し、ハードウェアでユニキャスト RPF チェックを実行します。ユニキャスト RPF チェックは、3 つ以上のリバースパス インターフェイスのある multipath プレフィックスから着信するパケットに対し、ディセーブルです（これらのパケットは常にユニキャスト RPF チェックに合格します）。
- **interface-group** モード : PFC3 は、single-path および two-path プレフィックスに対し、ハードウェアでユニキャスト RPF チェックを実行します。PFC3 はプレフィックス単位で最大 4 つの追加インターフェイスに対し、ユーザが設定したマルチパス ユニキャスト RPF チェック インターフェイス グループを介して、ユニキャスト RPF チェックを実行します。ユニキャスト RPF チェック

は、3 つ以上のリバースパス インターフェイスのある他の multipath プレフィックスから着信するパケットに対し、ディセーブルです（これらのパケットは常にユニキャスト RPF チェックを合格します）。

次に、複数パスの RPF チェック モードとしてパントを設定する例を示します。

```
Router(config)# mls ip cef rpf mpath punt
```

複数パスのインターフェイス グループの設定

複数パスのユニキャスト RPF インターフェイス グループを設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mls ip cef rpf interface-group [0 | 1 | 2 | 3] interface1 [interface2 [interface3 [interface4]]]`	複数パスの RPF インターフェイス グループを設定します。
ステップ 2	`Router(config)# mls ip cef rpf interface-group group_number`	インターフェイス グループを削除します。
ステップ 3	`Router(config)# end`	コンフィギュレーション モードを終了します。
ステップ 4	`Router# show mls cef ip rpf`	設定を確認します。

次に、インターフェイス グループ 2 を設定する例を示します。

```
Router(config)# mls ip cef rpf interface-group 2 fastethernet 3/3 fastethernet 3/4
fastethernet 3/5 fastethernet 3/6
```

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
```

ハードウェア ベースのレート リミッタ

レート リミッタの前提条件

なし。

レート リミッタの制約事項

- レイヤ 2 レート リミッタは次のとおりです。
  - レイヤ 2 PDU
  - レイヤ 2 プロトコル トンネリング
  - レイヤ 2 マルチキャスト IGMP
- CoPP を使用している場合は、CEF 受信リミッタを使用しないでください。CEF 受信リミッタにより、CoPP トラフィックが無効になります。
- 設定したレート制限は、それぞれの転送エンジンに適用されます（グローバルに適用されるレイヤ 2 ハードウェア レート リミッタを除く）。
- レイヤ 2 レート リミッタは、truncated モードでサポートされません。
- 入力および出力の ACL ブリッジド パケット レート リミッタの使用時には、次の制約事項が適用されます。
  - 入力と出力の ACL ブリッジド パケット レート リミッタは、ユニキャスト トラフィックだけで使用できます。

  - 入力および出力の ACL ブリッジド パケット レート リミッタでは、単一のレート リミッタ レジスタが共有されます。ACL ブリッジ入力レート リミッタおよび ACL ブリッジ出力レート リミッタをイネーブルにする場合は、入力 ACL および出力 ACL の両方で同一レート リミッタ値を共有する必要があります。

推奨レート リミッタ設定

推奨レート リミッタ設定は次のとおりです。

- DoS 攻撃で最も使用されやすいトラフィック タイプに対し、レート リミッタをイネーブルにします。
- VACL ロギングを設定しない場合は、VACL ロギングでレート リミッタを使用しないでください。
- リダイレクトをディセーブルにします。
- 到達不能をディセーブルにします。
- すべてのインターフェイスで MTU が同一である場合は、MTU レート リミッタをイネーブルにしないでください。
- レイヤ 2 PDU レート リミッタを設定する場合は、以下に注意してください。
  - 有効な PDU の予想数またはその可能な数を計算し、その数を 2 倍か 3 倍にします。
  - PDU には、BPDU、DTP、VTP、PAgP、LACP、UDLD などが含まれます。
  - レート リミッタでは、優良フレームと不良フレームが区別されません。

入出力 ACL ブリッジド パケット（ユニキャストのみ）

コマンド：

mls rate-limit unicast acl input

mls rate-limit unicast acl output

PFC および DFC には、個別の ACL-bridge レート リミッタがあります。

このレート リミッタは、入力または出力 ACL ブリッジの結果として RP に送信されたパケットをレート制限します。スイッチはこの機能を実現するため、TCAM ブリッジの結果を表す既存および新規の ACL TCAM エントリを、RP をポイントするレイヤ 3 リダイレクトの結果に変更します。変更されたレイヤ 3 リダイレクト レート制限結果を含む TCAM エントリにヒットしたパケットは、ネットワーク管理者が CLI で設定した指示に従ってレート制限されます。ACL ブリッジ レート制限がディセーブルである場合、レイヤ 3 リダイレクト レート制限結果は、ブリッジ結果に変換されます。

バースト値では、バーストで許容されるパケット数が規制されます。各許容パケットではトークンが消費され、パケットが許容されるには、トークンが使用可能である必要があります。1 つのトークンは 1 ミリ秒ごとに生成されます。パケットが到着しない場合、トークンはバースト値まで累積されます。たとえばバースト値が 50 に設定されている場合、スイッチは 50 個までのトークンを累積し、50 個のパケットのバーストを吸収できます。

uRPF チェック エラー

コマンド：**mls rate-limit unicast ip rpf-failure**

uRPF チェック失敗のレート リミッタを使用すると、uRPF チェックに失敗したために RP に送信する必要のあるパケットのレートを設定できます。uRPF チェックでは、インターフェイスの着信パケットが有効な送信元からのものであることが検証され、スプーフィングされたアドレスを使用するユーザからの DoS 攻撃の潜在的な脅威を最小限に抑えることができます。uRPF チェックに失敗した偽装パケットは、RP に送信されることがあります。uRPF チェック レート リミッタを使用すると、uRPF チェックの失敗が発生した場合に、RP CPU にブリッジされる 1 秒あたりのパケット数をレート制限できます。

TTL エラー

コマンド：**mls rate-limit all ttl-failure**

このレート リミッタは、Time to Live（TTL）チェックに失敗したために RP に送信されるパケットをレート制限します。次の例で **all** キーワードによって示されるように、このレート リミッタは、マルチキャスト トラフィックとユニキャスト トラフィックの両方に適用されます。

（注） TTL エラー レート リミッタは、IPv6 マルチキャストでサポートされません。

ICMP 到達不能（ユニキャストのみ）

コマンド：

mls rate-limit unicast ip icmp unreachable acl-drop

mls rate-limit unicast ip icmp unreachable no-route

ICMP 到達不能攻撃では、攻撃対象の装置（この場合は RP）からは到達できない宛先アドレスを持つパケットを大量に送りつけることで、この装置を過負荷にします。ICMP 到達不能レート リミッタを使用すると、到達不能なアドレスを持ち、RP に送信されるパケットをレート制限できます。

FIB（CEF）受信ケース（ユニキャストのみ）

コマンド：**mls rate-limit unicast cef receive**

FIB 受信レート リミッタの機能は、宛先アドレスとして RP IP を保持するすべてのパケットをレート制限することです。このレート リミッタでは、優良フレームと不良フレームが区別されません。

（注） CoPP を使用している場合は、FIB 受信レート リミッタをイネーブルにしないでください。FIB 受信レート リミッタは、CoPP ポリシーを上書きします。

FIB 収集（ユニキャストのみ）

コマンド：**mls rate-limit unicast cef glean**

FIB 収集レート リミッタは ARP トラフィックを制限しません。しかし、アドレス解決（ARP）を必要とし、RP に送信されるトラフィックをレート制限する機能を備えます。この状況は、ポートに送られたトラフィックに含まれるホスト アドレスが、RP にローカル接続されているサブネット上のアドレスであり、この宛先ホストに対する ARP エントリが存在しない場合に発生します。この場合、この宛先ホストの MAC アドレスに対しては、直接接続されているサブネットが不明であるため、このサブネット上のどのホストからも回答がありません。したがって、「glean」隣接が該当し、トラフィックは RP に直接送られ、ここで ARP 解決が行われます。このレート リミッタでは、攻撃者がこのような ARP 要求で CPU に過剰な負荷をかけることが制限されます。

レイヤ 3 セキュリティ機能（ユニキャストのみ）

コマンド：**mls rate-limit unicast ip features**

いくつかのセキュリティ機能では、パケットはまず RP に送信されてから処理されます。このようなセキュリティ機能では、RP に送信されるパケットの数をレート制限することで、過負荷の可能性を抑える必要があります。このセキュリティ機能には、Authentication Proxy（auth-proxy; 認証プロキシ）、IPSEC、検査が含まれます。

認証プロキシは、入力ユーザか出力ユーザ、またはその両方を認証するために使用されます。このようなユーザは一般的にアクセス リストによってブロックされますが、auth-proxy を使用した場合、ユーザはブラウザを起動してファイアウォールを通過し、Terminal Access Controller Access Control System Plus（TACACS+）または RADIUS サーバ（IP アドレスに基づく）で認証できます。サーバは、アクセス リスト エントリをスイッチにさらに渡し、ユーザが認証後に通過できるようにします。これらの ACL はソフトウェア内で保存および処理されます。このため、認証プロキシを使用するユーザ数が多すぎると、RP が過負荷になるおそれがあります。レート制限を行うとこのような状況で効果的になります。

IP セキュリティおよび検査も RP によって実行されるので、状況によってはレート制限が必要です。レイヤ 3 セキュリティ機能レート リミッタをイネーブルにすると、認証プロキシ、IP セキュリティ、および検証すべてが同時にイネーブルになります。

ICMP リダイレクト（ユニキャストのみ）

コマンド：**mls rate-limit unicast ip icmp redirect**

ICMP リダイレクト レート リミッタを使用すると、ICMP トラフィックをレート制限できます。たとえば、最適化されていないスイッチを経由してホストがパケットを送信すると、RP はこのホストに対し、送信パスを修正するように ICMP リダイレクト メッセージを送信します。このトラフィックが連続的に発生する場合、レート制限を行わないと、RP は ICMP リダイレクト メッセージを連続的に生成します。

VACL ログ（ユニキャストのみ）

コマンド：**mls rate-limit unicast acl vacl_log**

VLAN-ACL ロギングの結果によって RP に送信されたパケットをレート制限すると、ロギング タスクによって CPU が過負荷になることを防止できます。VACL はハードウェア処理されますが、RP によるロギングが行われます。VACL ロギングをスイッチで設定すると、VACL で拒否された IP パケットによってログ メッセージが生成されます。

MTU エラー

コマンド：**mls rate-limit all mtu**

TTL エラー レート リミッタと同じように、MTU エラーのレート リミッタは、ユニキャスト トラフィックおよびマルチキャスト トラフィックの両方でサポートされます。MTU チェックに失敗したパケットは、RP CPU に送信されます。これにより、RP が過負荷になることがあります。

レイヤ 2 マルチキャスト IGMP スヌーピング

コマンド：**mls rate-limit multicast ipv4 igmp**

IGMP スヌーピング レート リミッタは、RP 宛てのレイヤ 2 IGMP パケットの数を制限します。IGMP スヌーピングは、ホストとスイッチ間の IGMP メッセージを傍受します。スイッチが truncated モードで動作している場合、レイヤ 2 PDU レート リミッタをイネーブルにはできません。スイッチにファブリック対応モジュールとファブリック非対応モジュールが両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して truncated モードが使用されます。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの最初の 64 バイト）を送信します。IGMP スヌーピング レート リミッタは、PIM メッセージをレート制限しません。

レイヤ 2 PDU

コマンド：**mls rate-limit layer2 pdu**

レイヤ 2 PDU レート リミッタを使用すると、ハードウェア スイッチングされたレイヤ 2 PDU プロトコル パケット（BPDU、DTP、PAgP、CDP、STP、および VTP パケット）の数をレート制限できます。スイッチが truncated モードで動作している場合、レイヤ 2 PDU レート リミッタをイネーブルにはできません。スイッチにファブリック対応モジュールとファブリック非対応モジュールが両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して truncated モードが使用されます。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの最初の 64 バイト）を送信します。

レイヤ 2 プロトコル トンネリング

コマンド：**mls rate-limit layer2 l2pt**

このレート リミッタは、ハードウェア スイッチングされたレイヤ 2 プロトコル トンネリング パケット（制御 PDU、CDP、STP、および VTP パケット）をレート制限します。これらのパケットはソフトウェアでカプセル化され（PDU で宛先 MAC アドレスが書き換えられ）、独自のマルチキャスト アドレス（01-00-0c-cd-cd-d0）に転送されます。スイッチが truncated モードで動作している場合、レイヤ 2 PDU レート リミッタをイネーブルにはできません。スイッチにファブリック対応モジュールとファブ

リック非対応モジュールが両方とも搭載されている場合は、ファブリック対応モジュール間のトラフィックに対して truncated モードが使用されます。このモードでは、スイッチはスイッチ ファブリック チャネルを通じて、切り捨てた形のトラフィック（フレームの最初の 64 バイト）を送信します。

IP エラー

コマンド：**mls rate-limit unicast ip errors**

このレート リミッタでは、IP チェックサムと長さにエラーがあるパケットが制限されます。PFC または DFC に到達したパケットで、IP チェックサム エラーまたは長さの整合性エラーが発生している場合は、このパケットは追加処理のために RP に送信される必要があります。攻撃者は、誤った形式のパケットを使用して DoS 攻撃を実行することがありますが、ネットワーク管理者は、このタイプのパケットにレートを設定し、制御パスを保護できます。

IPv4 マルチキャスト

コマンド：

mls rate-limit multicast ipv4 connected

mls rate-limit multicast ipv4 fib-miss

mls rate-limit multicast ipv4 igmp

mls rate-limit multicast ipv4 ip-options

mls rate-limit multicast ipv4 pim

これらのレート リミッタでは、IPv4 マルチキャスト パケットがレート制限されます。このレート リミッタでは、ハードウェアのデータ パスからソフトウェアのデータ パスに送信されるパケットをレート制限できます。このレート リミッタでは、ソフトウェアの制御パスを輻輳から保護し、設定レートを超えるトラフィックをドロップします。

IPv6 マルチキャスト

コマンド：

mls rate-limit multicast ipv6 connected

mls rate-limit multicast ipv6 control-packet

mls rate-limit multicast ipv6 mld

これらのレート リミッタでは、IPv6 マルチキャスト パケットがレート制限されます。このレート リミッタでは、ハードウェアのデータ パスからソフトウェアのデータ パスに送信されるパケットをレート制限できます。このレート リミッタでは、ソフトウェアの制御パスを輻輳から保護し、設定レートを超えるトラフィックをドロップします。

ハードウェア ベースのレート リミッタのデフォルト設定

表 69-2 に、ハードウェアベース レート リミッタの DoS からの保護のデフォルト設定を示します。

表 69-2　ハードウェア ベースのレート リミッタのデフォルト設定

レート リミッタ	デフォルト ステート	デフォルト値
CEF RECEIVE	Off	
CEF RECEIVE SECONDARY	On	pps：15000、バースト マイクロ秒：1000000
CEF GLEAN	On	pps：1000、バースト マイクロ秒：1000000
IP ERRORS	Off	
UCAST IP OPTION	On	pps：100、バースト マイクロ秒：1000000
ICMP ACL-DROP	On	pps：100、バースト マイクロ秒：1000000
ICMP NO-ROUTE	On	pps：100、バースト マイクロ秒：1000000
ICMP REDIRECT	Off	
RPF FAILURE	On	pps：100、バースト マイクロ秒：1000000
ACL VACL LOG	On	pps：2000、バースト マイクロ秒：1000000
ACL BRIDGED IN	Off	
ACL BRIDGED OUT	Off	
ARP Inspection	Off	
DHCP Snooping IN	Off	
IP FEATURES	Off	
MAC PBF IN	Off	
CAPTURE PKT	Off	
IP ADMIS.ON L2 PORT	Off	
MCAST IPV4 DIRECTLY C	Off	
MCAST IPV4 FIB MISS	Off	
MCAST IPV4 IGMP	Off	
MCAST IPV4 OPTIONS	Off	
MCAST IPV4 PIM	Off	
MCAST IPV6 DIRECTLY C	Off	
MCAST IPV6 MLD	Off	
MCAST IPV6 CONTROL PK	Off	
MTU FAILURE	Off	
TTL FAILURE	Off	
MCAST BRG FLD IP CNTR	Off	
MCAST BRG FLD IP	Off	
MCAST BRG	Off	
MCAST BRG OMF	Off	
UCAST UNKNOWN FLOOD	Off	
LAYER_2 PDU	Off	
LAYER_2 PT	Off	

表 69-2　ハードウェア ベースのレート リミッタのデフォルト設定 （続き）

レート リミッタ	デフォルト ステート	デフォルト値
LAYER_2 PORTSEC	Off	
LAYER_2 SPAN PCAP	Off	
DIAG RESERVED 0	On	pps：33554431、バースト マイクロ秒：1
DIAG RESERVED 1	On	pps：33554431、バースト マイクロ秒：1
DIAG RESERVED 2	On	pps：33554431、バースト マイクロ秒：1
DIAG RESERVED LIF 0	On	pps：33554431、バースト マイクロ秒：1
MCAST REPL RESERVED	On	pps：1、バースト マイクロ秒：0

レート リミッタ情報の表示

show mls rate-limit コマンドでは、設定したレート リミッタに関する情報が表示されます。

show mls rate-limit usage コマンドでは、レート リミッタ タイプによって使用されるハードウェア レジスタが表示されます。レジスタが、どのレート リミッタ タイプによっても使用されない場合は、出力に Free と表示されます。レジスタがレート リミッタ タイプによって使用されている場合は、Used と表示されて、レート リミッタ タイプも表示されます。

コマンド出力において、レート リミット ステータスは次のうちいずれかになります。

- On は、特定ケースのレートが設定されていることを示します。
- Off は、レート リミッタ タイプが設定されておらず、そのケースのパケットがレート制限されないことを示します。
- On/Sharing は、同一共有グループに属する別のレート リミッタの設定により、特定ケース（手動で設定していない）が影響されることを示します。
- ハイフンは、マルチキャスト部分 SC レート リミッタがディセーブルであることを示します。

コマンド出力において、レート制限共有は次の情報を示します。

- 共有がスタティックであるかダイナミックであるか
- グループ ダイナミック共有コード

設定されているレート リミッタを表示するには、**show mls rate-limit** コマンドを使用します。

```
Router# show mls rate-limit
 State : ON - enabled but not sharing, ON/S - enabled and sharing
 Share : NS - not sharing, G - group, S - static sharing, D - dynamic sharing
       : P/sec - Packets/sec, B/sec - Bytes/second, BP - Burst period (microsec)

   Rate Limiter Type   State    P/sec  P/burst      B/sec    B/burst BP      Shk
 -------------------- ----- -------- -------- ---------- ---------- ------- ---
           CEF RECEIVE   OFF        -        -          -          -       -   -
 CEF RECEIVE SECONDARY    ON    15000        -          -          - 1000000
             CEF GLEAN    ON     1000        -          -          - 1000000
            IP ERRORS   OFF        -        -          -          -       -   -
       UCAST IP OPTION    ON      100        -          -          - 1000000 G:
         ICMP ACL-DROP    ON      100        -          -          - 1000000 G:
         ICMP NO-ROUTE    ON      100        -          -          - 1000000
         ICMP REDIRECT   OFF        -        -          -          -       -   -
           RPF FAILURE    ON      100        -          -          - 1000000
          ACL VACL LOG    ON     2000        -          -          - 1000000
        ACL BRIDGED IN   OFF        -        -          -          -       -   -
       ACL BRIDGED OUT   OFF        -        -          -          -       -   -
        ARP Inspection   OFF        -        -          -          -       -   -
     DHCP Snooping IN   OFF        -        -          -          -       -   -
          IP FEATURES   OFF        -        -          -          -       -   -
           MAC PBF IN   OFF        -        -          -          -       -   -
          CAPTURE PKT   OFF        -        -          -          -       -   -
  IP ADMIS.ON L2 PORT   OFF        -        -          -          -       -   -
 MCAST IPV4 DIRECTLY C   OFF        -        -          -          -       -   -
   MCAST IPV4 FIB MISS   OFF        -        -          -          -       -   -
       MCAST IPV4 IGMP   OFF        -        -          -          -       -   -
    MCAST IPV4 OPTIONS   OFF        -        -          -          -       -   -
        MCAST IPV4 PIM   OFF        -        -          -          -       -   -
 MCAST IPV6 DIRECTLY C   OFF        -        -          -          -       -   -
        MCAST IPV6 MLD   OFF        -        -          -          -       -   -
 MCAST IPV6 CONTROL PK   OFF        -        -          -          -       -   -
          MTU FAILURE   OFF        -        -          -          -       -   -
          TTL FAILURE   OFF        -        -          -          -       -   -
 MCAST BRG FLD IP CNTR   OFF        -        -          -          -       -   -
     MCAST BRG FLD IP   OFF        -        -          -          -       -   -
            MCAST BRG   OFF        -        -          -          -       -   -
        MCAST BRG OMF   OFF        -        -          -          -       -   -
   UCAST UNKNOWN FLOOD   OFF        -        -          -          -       -   -
          LAYER_2 PDU   OFF        -        -          -          -       -   -
           LAYER_2 PT   OFF        -        -          -          -       -   -
      LAYER_2 PORTSEC   OFF        -        -          -          -       -   -
    LAYER_2 SPAN PCAP   OFF        -        -          -          -       -   -
       DIAG RESERVED 0    ON 33554431        -          -          -       1
       DIAG RESERVED 1    ON 33554431        -          -          -       1
       DIAG RESERVED 2    ON 33554431        -          -          -       1
   DIAG RESERVED LIF 0    ON 33554431        -          -          -       1
   MCAST REPL RESERVED    ON        1        -          -          -       0
Router#
```

ハードウェア レート リミッタの使用状況を表示するには、**show mls rate-limit usage** コマンドを使用します。

```
Router# show mls rate-limit usage
P/sec - Packets/sec, B/sec - Bytes/sec, BP - Burst period (microsec), U - Usee
              Rate Limiter Type     P/sec  P/burst      B/sec    B/burst BP
            -------------------- -------- -------- ---------- ---------- ------
L3 Rate Limiters:
   RL# 1: U          ACL VACL LOG     2000        -          -          - 100000
   RL# 2: F                     -        -        -          -          -      -
   RL# 3: F                     -        -        -          -          -      -
```

```
   RL# 4: F                      -       -       -         -         -      -
   RL# 5: F                      -       -       -         -         -      -
   RL# 6: F                      -       -       -         -         -      -
   RL# 7: F                      -       -       -         -         -      -
   RL# 8: F                      -       -       -         -         -      -
   RL# 9: F                      -       -       -         -         -      -
   RL#10: U       UCAST IP OPTION        -       -     10000       100     60
                    ICMP ACL-DROP        -       -     10000       100     60
   RL#11: U         ICMP NO-ROUTE      100       -         -         - 100000
   RL#12: F                      -       -       -         -         -      -
   RL#13: F                      -       -       -         -         -      -
   RL#14: F                      -       -       -         -         -      -
   RL#15: F                      -       -       -         -         -      -
   RL#16: F                      -       -       -         -         -      -
   RL#17: F                      -       -       -         -         -      -
   RL#18: F                      -       -       -         -         -      -
   RL#19: F                      -       -       -         -         -      -
   RL#20: F                      -       -       -         -         -      -
   RL#21: F                      -       -       -         -         -      -
   RL#22: F                      -       -       -         -         -      -
   RL#23: F                      -       -       -         -         -      -
   RL#24: F                      -       -       -         -         -      -
   RL#25: F                      -       -       -         -         -      -
   RL#26: F                      -       -       -         -         -      -
   RL#27: F                      -       -       -         -         -      -
   RL#28: F                      -       -       -         -         -      -
   RL#29: F                      -       -       -         -         -      -
   RL#30: F                      -       -       -         -         -      -
   RL#31: F                      -       -       -         -         -      -

L2 Input Rate Limiters:
   RL#32: U       DIAG RESERVED 0 33554431       -         -         -      1
   RL#33: U       DIAG RESERVED 1 33554431       -         -         -      1
   RL#34: U       DIAG RESERVED 2 33554431       -         -         -      1
   RL#35: U   DIAG RESERVED LIF 0 33554431       -         -         -      1
   RL#36: U   MCAST REPL RESERVED        1       -         -         -      0
   RL#37: F                      -       -       -         -         -      -
   RL#38: F                      -       -       -         -         -      -
   RL#39: F                      -       -       -         -         -      -
   RL#40: F                      -       -       -         -         -      -
   RL#41: F                      -       -       -         -         -      -
   RL#42: F                      -       -       -         -         -      -
   RL#43: F                      -       -       -         -         -      -
   RL#44: F                      -       -       -         -         -      -
   RL#45: F                      -       -       -         -         -      -
   RL#46: F                      -       -       -         -         -      -
   RL#47: U             CEF GLEAN     1000       -         -         - 100000
   RL#48: U           RPF FAILURE      100       -         -         - 100000
   RL#49: U CEF RECEIVE SECONDARY    15000       -         -         - 100000
   RL#50: F                      -       -       -         -         -      -
   RL#51: F                      -       -       -         -         -      -

L2 Output Rate Limiters:
   RL#52: F                      -       -       -         -         -      -
   RL#53: F                      -       -       -         -         -      -
   RL#54: F                      -       -       -         -         -      -
   RL#55: F                      -       -       -         -         -      -
   RL#56: F                      -       -       -         -         -      -
   RL#57: F                      -       -       -         -         -      -
Router#
```

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 tcam interface** コマンドを使用できます。

次に、**show tcam interface** コマンドを使用して、エントリがヒットした回数を表示する例を示します。

```
Router# show tcam interface fa5/2 acl in ip detail

------------------------------------------------------------------------------------------------------------------------
DPort - Destination Port   SPort - Source Port        TCP-F - U -URG Pro   - Protocol
I     - Inverted LOU       TOS   - TOS Value                - A -ACK rtr   - Router
MRFM  - M -MPLS Packet     TN    - T -Tcp Control           - P -PSH COD   - C -Bank Care Flag
      - R -Recirc.Flag           - N -Non-cachable          - R -RST       - I -OrdIndep.Flag
      - F -Fragment Flag   CAP   - Capture Flag             - S -SYN       - D -Dynamic Flag
      - M -More Fragments  F-P   - FlowMask-Prior.          - F -FIN T     - V(Value)/M(Mask)/R(Result)
X     - XTAG               (*)   - Bank Priority
------------------------------------------------------------------------------------------------------------------------


Interface: 1018   label: 1   lookup_type: 0
protocol: IP   packet-type: 0

+-+-----+---------------+---------------+---------------+---------------+-------+---+----+-+---+--+---+---+
|T|Index|  Dest Ip Addr | Source Ip Addr|     DPort     |     SPort     | TCP-F|Pro|MRFM|X|TOS|TN|COD|F-P|
+-+-----+---------------+---------------+---------------+---------------+------+---+----+-+---+--+---+---+
 V 18396         0.0.0.0         0.0.0.0       P=0             P=0       ------   0 ---- 0   0 -- --- 0-0
 M 18404         0.0.0.0         0.0.0.0         0               0               0 ---- 0   0
 R rslt: L3_DENY_RESULT                rtr_rslt: L3_DENY_RESULT


 V 36828         0.0.0.0         0.0.0.0       P=0             P=0        ------  0 ---- 0   0 -- --- 0-0
 M 36836         0.0.0.0         0.0.0.0         0               0               0 ---- 0   0
 R rslt: L3_DENY_RESULT (*)            rtr_rslt: L3_DENY_RESULT (*)
Router#
```

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 mls statistics** 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 mls statistics
```

```
Statistics for Earl in Module 6

L2 Forwarding Engine
  Total packets Switched                : 25583421

L3 Forwarding Engine
  Total packets L3 Switched             : 25433414 @ 24 pps

  Total Packets Bridged                 : 937860
  Total Packets FIB Switched            : 23287640
  Total Packets ACL Routed              : 0
  Total Packets Netflow Switched        : 0
  Total Mcast Packets Switched/Routed   : 96727
  Total ip packets with TOS changed     : 2
  Total ip packets with COS changed     : 2
  Total non ip packets COS changed      : 0
  Total packets dropped by ACL          : 33
  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 Switched by all Modules: 25433414 @ 24 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 53 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 67 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