CHAPTER 46

DoS からの保護の設定

この章では、スイッチを Denial of Service（DoS; サービス拒絶）攻撃から保護する手順について説明します。この章で説明する内容は Cisco IOS Release 12.2SX に固有のものであり、このマニュアルの「ネットワーク セキュリティの設定」の章で説明するネットワーク セキュリティ情報とその手順、および以下のマニュアルでのネットワーク セキュリティ情報とその手順を補完します。

- 次の URL の『*Cisco IOS Security Configuration Guide*, Release 12.2』
  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html
- 次の URL の『*Cisco IOS Security Command Reference*, Release 12.2』
  http://www.cisco.com/en/US/docs/ios/12_2/security/command/reference/fsecur_r.html

（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、次のマニュアルを参照してください。

- 次の URL にある『Cisco IOS Master Command List, Release 12.2SX』
  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html
- 次の URL にある Release 12.2 のマニュアル
  http://www.cisco.com/en/US/products/sw/iosswrel/ps1835/products_installation_and_configuration_guides_list.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

この章で説明する内容は、次のとおりです。

DoS 攻撃からの保護の概要

ここでは、DoS 攻撃に対して有効な対処方法についての情報を説明し、その設定例を示します。PFC3 は、次の方法を使用して、DoS 攻撃に対する多層防御を実現します。

- CPU レート リミッタ：トラフィックの種類を制御します。
- Control Plane Policing（CoPP; コントロール プレーン ポリシング）：コントロール プレーンのトラフィックをフィルタリングおよびレート制限します。CoPP の詳細については、第 47 章「コントロール プレーン ポリシングの設定」を参照してください。

ここでは、DoS 攻撃からの保護について説明します。

セキュリティ ACL および VACL

ネットワークが実際に DoS 攻撃を受けた場合は、ターゲットに到達する前に DoS パケットをドロップするための有効な手段として、ACL を使用できます。セキュリティ ACL は、特定のホストから攻撃が検出されたときに使用します。

次の例では、ホスト 10.1.1.10 と、このホストからのすべてのトラフィックを拒否します。

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

また、セキュリティ ACL はアドレスのスプーフィングも防止します。たとえば、ネットワークの内側、およびインターネットをポイントするスイッチ インターフェイスの内側に、A という送信元アドレスがあるとします。この場合は、スイッチのインターネット インターフェイスに、送信元 A（内部アドレス）からのすべてのアドレスを拒否する入力 ACL を適用します。これで、内部のこの送信元アドレスを偽装する攻撃を防止できます。このようなパケットがスイッチ インターフェイスに到達すると、このパケットは ACL と一致するため、被害が発生する前にドロップされます。

スイッチとともに Cisco Intrusion Detection Module（CIDM）を使用すると、検知エンジンが攻撃を検知した時点で、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、およびレイヤ 4 情報に基づくセキュリティ強化ツールです。VACL によるパケット検索の結果は、許可（permit）、拒否（deny）、許可およびキャプチャ（permit and capture）、またはリダイレクト（redirect）のいずれかになります。VACL を特定の VLAN に関連付けると、トラフィックがこの VLAN に許可されるには、すべてのトラフィックが VACL によって許可されなければならなくなります。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。

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。PFC3 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上で効果的です。

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。このレート制限は、レート制限の必要な個々のフローに設定し、レート制限ポリシー アクションをインターフェイスに適用する必要があります。

次の例に示すアクセス リスト 101 は、すべての送信元からすべての宛先にトラフィックとして流れる ping（エコー）ICMP メッセージを許可および識別します。ポリシー マップ内では、ポリシー ルールによって指定の Committed Information Rate（CIR; 認定情報速度）およびバースト値（96000 bps、16000 bps）を定義し、シャーシを通過する ping（ICMP）トラフィックをレート制限します。このポリシー マップは、インターフェイスまたは VLAN に適用されます。ping トラフィックがポリシー マップの適用された VLAN またはインターフェイスで指定のレートを超えると、このトラフィックはマークダウン マップに従ってドロップされます（この例では、通常のバースト設定に対するマークダウン マップは掲載していません）。

```
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
```

uRPF チェック

unicast Reverse Path Forwarding（uRPF）チェックをイネーブルにすると、スプーフィングされた IP 送信元アドレスなど、確認可能な送信元 IP アドレスを持たないパケットが廃棄されます。送信元アドレスと、これが受信されたインターフェイスとが、Switch Processor（SP; スイッチ プロセッサ）の FIB テーブルと一致しているかどうかを確認するには、Cisco Express Forwarding（CEF）テーブルが使用されます。

インターフェイス上で uRPF チェックをイネーブルにすると（VLAN 単位）、受信パケットは逆引き参照によって CEF テーブルと比較されます。いずれかのリバース パス ルートから受信されたパケットは転送されます。受信パケットに対し、インターフェイス上にリバース パス ルートが 1 つも存在しない場合は、このパケットは uRPF チェックに失敗したことになります。このパケットは、uRPF チェックに失敗したトラフィックに ACL が適用されるかどうかに応じてドロップまたは転送されます。CEF テーブルに ACL が指定されていない場合は、偽装パケットはただちにドロップされます。

uRPF チェックの ACL は、uRPF チェックに失敗したパケットにだけ指定できます。この ACL は、パケットをただちにドロップするか、または転送するかをチェックします。ACL による uRPF チェックは、ハードウェア内の PFC3 ではサポートされません。uRPF ACL で拒否されたパケットは、ハードウェア内で転送されます。許可されたパケットは CPU に送信されます。

uRPF チェックはハードウェア内でサポートされます。ただし、uRPF チェックに失敗し、適用された ACL によって転送されるすべてのパケットは、RP に送信およびレート制限され、ICMP 到達不能メッセージを生成します。これらの動作は、すべてソフトウェアによって制御されます。ハードウェアでの uRPF チェックは、最大 2 つのリターン パス（インターフェイス）を持つルートに対してサポートされ、インターフェイス グループが設定された場合は最大 6 つのリターン パス（2 つは FIB テーブルから、4 つはインターフェイス グループから）を持つルートに対してサポートされます。

トラフィック ストーム制御

トラフィック ストームは、パケットが LAN でフラッディングする場合に発生するもので、過剰なトラフィックを生成し、ネットワークのパフォーマンスを低下させます。トラフィック ストーム制御機能は、ネットワーク設定の誤り、またはユーザによる DoS 攻撃の開始が原因となり、物理インターフェイス上のブロードキャスト、マルチキャスト、またはユニキャスト トラフィック ストームによって LAN ポートが中断されるのを防ぎます。トラフィック ストーム制御（トラフィック抑制とも呼ぶ）は、1 秒間のトラフィック ストーム制御インターバルにおいて受信するトラフィックのレベルをモニタします。このインターバルの間、設定済みのトラフィック ストーム制御レベルに対し、トラフィック レベルが比較されます。トラフィック ストーム制御レベルは、ポートの利用可能な帯域幅全体に対するパーセンテージです。各ポートには、すべてのタイプのトラフィック（ブロードキャスト、マルチキャスト、およびユニキャスト）用に使用されている単一のトラフィック ストーム制御レベルがあります。

トラフィック ストーム制御はインターフェイスに対して設定され、デフォルトではディセーブルにされています。次の設定例では、インターフェイス FastEthernet 2/3 上で、レベル 20% のブロードキャスト アドレス ストーム制御をイネーブルにしています。1 秒間のトラフィック ストーム制御インターバルで、ブロードキャスト トラフィックが、設定されたレベルであるポートの有効帯域幅合計の 20% を超えると、このトラフィック ストーム制御インターバルが終了するまで、すべてのブロードキャスト トラフィックがドロップされます。

```
Router(config-if)# storm-control broadcast level 20
```

スイッチは、すべての LAN ポート上でブロードキャストのストーム制御をサポートし、ギガビット イーサネット ポート上ではマルチキャストとユニキャストのストーム制御をサポートします。

2 つまたは 3 つの抑制モードを同時に設定する場合は、同じレベル設定が共有されます。ブロードキャスト抑制をイネーブルにした場合に、マルチキャスト抑制もイネーブルにし、そのしきい値を 70% に設定すると、ブロードキャスト抑制にもこの 70% の設定が適用されます。

SYN 攻撃を受けたネットワーク

SYN 攻撃を受けたネットワークは、簡単に見分けることができます。ターゲット ホストは極端に低速になるか、クラッシュするか、または処理が中断されます。ターゲット ホストから返されたトラフィックによって RP に問題が生じることもあります。これは、リターン トラフィックが、元のパケットからランダムに抽出された送信元アドレスに送信され、「本物」の IP トラフィックのローカル性が失われることで、ルート キャッシュまたは CEF テーブルでオーバーフローが生じる可能性があるためです。

ネットワークが SYN 攻撃を受けると、TCP インターセプト機能がアグレッシブな防御モードに変わります。スイッチ上でアグレッシブな動作が開始および終了するタイミングは、次の 2 つの要素によって決定されます。

- 未完了接続の合計数
- 最後の 1 分間のサンプリング期間における接続要求数

両方の要素には、最小値と最大値の両方を設定します。

未完了接続の数が 1,100 を超えると、または最後の 1 分間の接続数が 1,100 に達すると、新たな接続が確立されるたびに、最も古い部分接続（ランダム接続）が削除されるようになります。これはデフォルト値であり、変更できます。いずれかのしきい値が超過すると、サーバが攻撃を受けたと見なされ、TCP インターセプト機能はアグレッシブ モードに変わり、以下が行われます。

- 新たに接続が確立するたびに、最も古い部分接続（ランダムな部分接続）が削除されます。
- 最初の再送信タイムアウトが半減されて 0.5 秒となり、この結果、接続の確立を試みる合計時間も半減します。
- ウォッチ モードでは、ウォッチ タイムアウトも半減されます。

（注） 設定した最小値を両方のしきい値が下回ると、アグレッシブ モードは終了します（デフォルト値はいずれも 900）。

TCP フローは、PFC3 においてハードウェア補助される機能です。

ARP ポリシング

悪意あるユーザが攻撃を仕掛ける際、ルーティング プロトコルや ARP パケットなどの制御パケットによって、RP CPU を過負荷にしようと試みる場合があります。このような特殊な制御パケットは、特定のルーティング プロトコルおよび ARP ポリシング機能によって、ハードウェアでレート制限することができます。これは、**mls qos protocol** コマンドによって設定します。RIP、BGP、LDP、OSPF、IS-IS、IGRP、EIGRP といったルーティング プロトコルがサポートされます。たとえば **mls qos protocol arp police 32000** というコマンドは、ARP パケットをハードウェア内で 32,000 bps にレート制限します。こ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 パケットのポリシングだけにとどまらず、CoPP より低い粒度で機器を通過するトラフィックもポリシングします。

ポリシング メカニズムは、ポリシング回避メカニズムとルート設定を共有します。ポリシング回避メカニズムは、QoS ポリサーに到達したルーティング プロトコルおよび ARP パケットに対し、ネットワークの通過を許可します。このメカニズムを設定するには、**mls qos protocol** *protocol* **pass-through** コマンドを使用します。

次の例では、ARP ポリシングで使用可能なプロトコルを一覧表示する方法を示します。

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

次の例では、**mls qos protocol arp** コマンドで使用可能なキーワードを一覧表示する例を示します。

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

推奨されるレート リミッタ設定

レート リミッタは、次のように設定することを推奨します。

- DoS 攻撃で使用される可能性が最も高い種類のトラフィックに対し、レート リミッタをイネーブルにします。
- VACL ロギングを設定していない場合は、VACL ロギングにレート 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の MTU が同じである場合は、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 Protocol Data Unit（PDU; プロトコル データ ユニット）レート リミッタを設定する場合は、次の点に注意してください。
  - 有効な PDU の予測値（可能な値）を計算し、この値を 2 倍または 3 倍にします。
  - PDU には、BPDU、DTP、VTP、PAgP、LACP、UDLD などが含まれます。
  - 各レート リミッタは、正しいフレーム（good frame）と不正なフレーム（bad frame）を区別しません。

PFC3 のハードウェア ベース レート リミッタ

PFC3 では、ハードウェア ベースのレート リミッタを追加で使用できます。PFC3 は、新たなレート リミッタに対応する 8 つのレート リミッタ レジスタを備えています。これらはすべて、スイッチ上でグローバルに設定します。これらのレート リミッタ レジスタはレイヤ 3 転送エンジン（PFC）上にあり、使用可能なさまざまな設定済みレート リミッタと一致した各パケットに関する、レート制限情報の格納を行います。

8 つのレート リミッタ レジスタは、PFC3 に実装されているため、異なる複数のレート制限シナリオで、同一レジスタが強制的に共有される場合もあります。各レジスタは、先着順に割り当てられます。すべてのレジスタが使用されている場合、もう 1 つのレート リミッタを新たに設定する唯一の方法は、いずれか 1 つのレジスタを解放することです。

PFC3 で使用可能なハードウェア ベースのレート リミッタは、次のとおりです。

- 入力および出力 ACL ブリッジド パケット
- uRPF チェックの失敗
- FIB 受信
- FIB 収集
- レイヤ 3 セキュリティ機能
- ICMP リダイレクト
- ICMP 到達不能（ACL ドロップ）
- ルートなし（FIB 不一致）
- VACL ログ
- TTL 失敗
- MTU 失敗
- マルチキャスト IPv4
- マルチキャスト IPv6

入出力 ACL ブリッジド パケット（ユニキャストだけ）

このレート リミッタは、入出力 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。TCAM エントリが、変更したレイヤ 3 リダイレクト レート制限の結果と一致するパケットは、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。入力値および出力値は、いずれも同一のレート リミッタ レジスタを共有するため、同じ値となります。ACL ブリッジの入出力レート制限をディセーブルにすると、レイヤ 3 リダイレクトによるレート制限の結果は、ブリッジの結果に変換されます。

入力または出力 ACL ブリッジド パケットのレート制限は、1 つのレート リミッタ レジスタを共有します。この機能をオンにすると、入力および出力 ACL にはいずれも、同じレート リミッタ値が使用されます。

バースト値は、1 度のバーストで許可されるパケット数を制限します。許可される個々のパケットは、それぞれ 1 つのトークンを使用します。1 つのパケットに対し 1 つのトークンが使用可能である必要があります。1 ミリ秒ごとに 1 つのトークンが生成されます。パケットが送られて来ないと、トークンは最大バースト値まで蓄積されます。たとえば、バースト値を 50 に設定している場合は、スイッチは最大 50 のトークンを蓄積でき、50 パケットのバーストを吸収できます。

次の例では、入力 ACL ブリッジの結果からのユニキャスト パケットを 50000 pps（パケット/秒）に制限し、バースト値を 50 に制限します。

```
Router(config)# mls rate-limit unicast acl input 50000 50
```

次の例では、入力 ACL ブリッジの結果からのユニキャスト パケットを、出力 ACL ブリッジの結果と同じレート（50000 pps、バースト値 50）に制限します。

```
Router(config)# mls rate-limit unicast acl output 50000 50
```

入力または出力のいずれかでレート リミッタの値が変更されると（両方がイネーブルになっている場合）、両方の値が新しい値に変更されます。次の例では、出力レートが 40000 pps に変更されます。

```
Router(config)# mls rate-limit unicast acl output 40000 50
```

show mls rate-limit コマンドを入力すると、ACL ブリッジド入力（ACL BRIDGED IN）および出力（ACL BRIDGED OUT）の値がどちらも 40000 pps に変わっていることを確認できます。

```
Router# show mls rate-limit
  Rate Limiter Type       Status      Packets/s   Burst
---------------------   ----------    ---------   -----
MCAST NON RPF           Off           -           -
MCAST DFLT ADJ          On            100000      100
MCAST DIRECT CON        Off           -           -
ACL BRIDGED IN          On            40000       50
ACL BRIDGED OUT         On            40000       50
IP FEATURES             Off
…
```

uRPF チェックの失敗

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 チェックは、インターフェイスの受信したパケットが有効な送信元からのものであるかどうかを検証する機能です。これにより、偽装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にできます。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。

次の例では、uRPF チェックに失敗し、RP に送信されるパケットを、100000 pps およびバースト パケット 100 にレート制限します。

```
Router(config)# mls rate-limit unicast ip rpf-failure 100000 100
```

TTL 失敗

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。次の例の **all** キーワードからもわかるように、このレート リミッタはマルチキャストおよびユニキャスト トラフィックの両方に適用されます。

（注） TTL 失敗のレート リミッタは、IPv6 マルチキャストではサポートされません。

次の例では、TTL に失敗したパケットを 70000 pps、およびバースト値 150 にレート制限します。

```
Router(config)# mls rate-limit all ttl-failure 70000 150
```

ICMP 到達不能（ユニキャストだけ）

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。

次の例では、ACL ドロップによって RP に送信されるパケットを、10000 pps およびバースト値 100 にレート制限します。

```
Router(config)# mls rate-limit unicast ip icmp unreachable acl-drop 10000 100
```

次の例では、FIB との不一致によって到達不能 ICMP メッセージの生成が必要となるパケットを、80000 pps およびバースト値 70 にレート制限します。

```
Router(config)# mls rate-limit unicast ip icmp unreachable no-route 80000 70
```

ICMP 到達不能（ルートなし）、ICMP 到達不能（ACL ドロップ）、IP エラー、および IP RPF 失敗の 4 つのレート リミッタは、同一のレート リミッタ レジスタを共有します。このいずれかのリミッタをイネーブルにすると、4 つのリミッタすべては同じ値を共有し、状況によっては同じ状態を共有します（ON/ON/ON など）。レート リミッタの内容を確認すると、このレジスタのメンバーが別の機能の設定によってイネーブルにされている場合は、ステータスは ON ではなく ON-Sharing と表示されます。ただし、TTL 失敗のレート リミッタは例外です。この機能を手動でイネーブルにしている場合は、この値はレジスタ内の他のメンバーと同じ値を共有します。

FIB（CEF）受信（ユニキャストだけ）

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。レート リミッタは、正しいフレーム（good frame）と不正なフレーム（bad frame）を区別しません。

（注）　CoPP を使用する場合は、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。

次の例では、トラフィックを 25000 pps、およびバースト値 60 にレート制限します。

```
Router(config)# mls rate-limit unicast cef receive 25000 60
```

FIB 収集（ユニキャストだけ）

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、「収集（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 リミッタは、このような ARP 要求によって CPU を過負荷にする攻撃の可能性を制限します。

次の例では、RP に送信されるトラフィックを 20000 pps、およびバースト値 60 に制限します。

```
Router(config)# mls rate-limit unicast cef glean 20000 60
```

レイヤ 3 セキュリティ機能（ユニキャストだけ）

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。これは、認証プロキシ（auth-proxy）、IPSEC、検査などのセキュリティ機能です。

認証プロキシは、入力ユーザまたは出力ユーザ、またはその両方の認証に使用されます。通常これらのユーザはアクセス リストによってブロックされますが、認証プロキシを使用すると、ユーザはブラウザを開いてファイアウォールを通過し、IP アドレスに基づき Terminal Access Controller Access Control System Plus（TACACS+）または RADIUS サーバの認証を受けることができます。このサーバは追加のアクセス リスト エントリをスイッチに渡し、認証を受けたユーザの通過を許可します。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。このような場合にレート制限を行うと効果的です。

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。

次の例では、RP のセキュリティ機能を 100000 pps、およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit unicast ip features 100000 10
```

ICMP リダイレクト（ユニキャストだけ）

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。

次の例では、ICMP リダイレクトを 20000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit unicast ip icmp redirect 20000 20
```

VACL ログ（ユニキャストだけ）

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。スイッチで VACL ロギングを設定しておくと、VACL で拒否された IP パケットに対するログ メッセージが生成されます。

次の例では、ロギング要求を 5000 pps（このレート リミッタの有効範囲は 10 ～ 5000 pps）に制限します。

```
Router(config)# mls rate-limit unicast acl vacl-log 5000
```

MTU 失敗

MTU 失敗のレート リミッタは TTL 失敗のレート リミッタと似ており、ユニキャスト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。

次の例では、MTU チェックに失敗し、RP に送信されるパケットを、10000 pps およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit all mtu 10000 10
```

レイヤ 2 マルチキャスト IGMP スヌーピング

Internet Group Management Protocol（IGMP）スヌーピング レート リミッタは、SP 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は、レイヤ 2 PDU レート リミッタはイネーブルにできません。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の両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックに truncated モードを使用します。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（フレームの初めの 64 バイト）を送信します。Cisco IOS Release 12.2(33)SXH よりも前のリリースでは、IGMP スヌーピング レート リミッタにより、PIM メッセージもレート制限されます。Cisco IOS Release 12.2(33)SXH 以降の IGMP スヌーピング レート リミッタでは、PIM メッセージはレート制限されません。

次の例では、IGMP スヌーピング トラフィックをレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 igmp 20000 40
```

レイヤ 2 PDU

レイヤ 2 PDU レート リミッタを使用すると、RP CPU ではなく SP 宛てに送信されたレイヤ 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は、レイヤ 2 PDU レート リミッタはイネーブルにできません。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の両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックに truncated モードを使用します。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（フレームの初めの 64 バイト）を送信します。

次の例では、レイヤ 2 PDU を 20000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit layer2 pdu 20000 20
```

レイヤ 2 プロトコル トンネリング

このレート リミッタは、SP 宛てのレイヤ 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によってカプセル化（PDU 内の宛先 MAC アドレスを書き換え）されてから、専用のマルチキャスト 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は、レイヤ 2 PDU レート リミッタはイネーブルにできません。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の両方が搭載されている場合、スイッチはファブリック モジュール間のトラフィックに truncated モードを使用します。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（フレームの初めの 64 バイト）を送信します。

次の例では、レイヤ 2 プロトコル トンネリング パケットを 10000 pps、およびバースト パケット 10 にレート制限します。

```
Router(config)# mls rate-limit layer2 l2pt 10000 10
```

IP エラー

このレート リミッタは、IP チェックサム エラーおよび長さのエラーが生じたパケットを制限します。PFC3 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。このように形式に誤りのあるパケットは、攻撃者によって DoS 攻撃の実行に悪用されることがありますが、ネットワーク管理者はこのようなパケットのレートを設定することで、制御パスを保護できます。

次の例では、RP に送信される IP エラーの生じたパケットを、1000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit unicast ip errors 1000 20
```

IPv4 マルチキャスト

このレート リミッタは、IPv4 マルチキャスト パケットを制限します。このレート リミッタでは、ハードウェア内のデータ パスから、ソフトウェア内のデータ パスまで送信されたパケットをレート制限できます。これを使用することで、ソフトウェア内の制御パスが輻輳することを防止し、設定したレートを超えたトラフィックをドロップできます。IPv4 マルチキャスト レート リミッタは、設定可能な 3 つのレート リミッタから構成されます。FIB 不一致に対するレート リミッタ、マルチキャストで部分的にスイッチされるフローのレート リミッタ、およびマルチキャスト直接接続レート リミッタです。

FIB 不一致に対するレート リミッタを使用すると、mroute テーブル内のエントリと一致しないマルチキャスト トラフィックをレート制限できます。

部分的にスイッチされたフローに対するレート リミッタを使用すると、転送および複製のために RP 宛てに送信されるフローをレート制限できます。マルチキャスト トラフィック フローにおいて、少なくとも 1 つの発信レイヤ 3 インターフェイスが多層的にスイッチングされ、少なくとも 1 つの発信インターフェイスが多層的にスイッチングされていない場合（ハードウェア スイッチの H ビットが設定されていない）は、このフローは部分的にスイッチングされたフロー、つまりパーシャル SC（パーシャル ショートカット）と見なされます。H ビット フラグが設定された発信インターフェイスはハードウェア内でスイッチングされ、残りのトラフィックは RP により、ソフトウェア内でスイッチングされます。このため、転送および複製のために RP に送信されるフローをレート制限することを推奨します。レート制限をしないと、このフローによって CPU の稼動率が高くなる可能性があります。

マルチキャスト直接接続レート リミッタは、直接接続された送信元からのマルチキャスト パケットを制限します。

次の例では、マルチキャスト パケットを 30000 pps、およびバースト値 30 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 connected 30000 30
```

ip-option キーワード、および ip-option レート リミッタは、PFC3A モードではサポートされません。

次の例では、uRPF チェックに失敗した IPv4 マルチキャスト パケットのレート制限を設定する方法を示します。

```
Router(config)# mls rate-limit multicast ipv4 non-rpf 100
```

次の例では、マルチキャスト FIB 不一致パケットを 10000 pps、およびバースト値 10 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 fib-miss 10000 10
```

次の例では、パーシャル ショートカット フローを 20000 pps、およびバースト パケット 20 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 partial 20000 20
```

次の例では、マルチキャスト パケットを 30000 pps、およびバースト値 20 にレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 connected 30000 20
```

次の例では、IGMP スヌーピング トラフィックをレート制限します。

```
Router(config)# mls rate-limit multicast ipv4 igmp 20000 40
```

IPv6 マルチキャスト

このレート リミッタは、IPv6 マルチキャスト パケットを制限します。表 46-1 は、IPv6 レート リミッタの一覧、および各レート リミッタが対応するトラフィック クラスを示します。

表 46-1　IPv6 レート リミッタ

レート リミッタ	レート制限するトラフィック クラス
接続済み	直接接続された送信元トラフィック
デフォルト ドロップ	* (*, G/m) SSM * (*, G/m) SSM non-rpf
ルート制御	* (*, FF02::X/128)

表 46-1　IPv6 レート リミッタ （続き）

レート リミッタ	レート制限するトラフィック クラス
Starg ブリッジ	* (*, G/128) SM * (*, G) が存在する場合は SM 非 rpf トラフィック
Starg-M ブリッジ	* (*, G/m) SM * (*, FF/8) * (*, G) が存在しない場合は SM 非 rpf トラフィック

IPv6 マルチキャスト トラフィックのレート リミッタを設定するには、次のいずれかの方法を使用できます。

- レート リミッタをトラフィック クラスに直接関連付け：レートを選択して、このレートをレート リミッタに関連付けます。次の例では、1000 pps および 20 バースト パケットを選択して、このレートをデフォルト ドロップ（**default-drop**）レート リミッタに関連付けます。

  ```
  Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
  ```

- レート リミッタを、設定済みの別のレート リミッタとスタティックに共有：隣接関係に基づくレート リミッタが十分に確保できない場合は、すでに設定されたレート リミッタ（ターゲット レート リミッタ）とレート リミッタを共有できます。次の例では、ルート制御（**route-cntl**）レート リミッタを、デフォルト ドロップ（**default-drop**）ターゲット レート リミッタと共有します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
  ```

  ターゲット レート リミッタが未設定の場合は、ターゲット レート リミッタを別のレート リミッタと共有するには、ターゲット レート リミッタが設定されている必要があることを通知するメッセージが表示されます。

- レート リミッタをダイナミックに共有：どのレート リミッタを共有すべきか判断しにくい場合は、**share auto** キーワードを使用して、ダイナミック共有をイネーブルにします。ダイナミック共有をイネーブルにすると、事前設定されたレート リミッタが選択され、このレート リミッタが指定のレート リミッタと共有されます。次の例では、ルート制御（route-cntrl）レート リミッタに対してダイナミック共有を選択します。

  ```
  Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
  ```

次の例では、直接接続された送信元からの IPv6 マルチキャスト パケットのレート制限を設定する方法を示します。

```
Router(config)# mls rate-limit multicast ipv6 connected 1500 20
```

次の例では、レート リミッタをトラフィック クラスに直接関連付ける設定方法を示します。

```
Router(config)# mls rate-limit multicast ipv6 default-drop 1000 20
```

次の例では、事前設定された別のレート リミッタとレート リミッタをスタティックに共有する方法を示します。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share default-drop
```

次の例では、ルート制御レート リミッタに対してダイナミック共有をイネーブルにします。

```
Router(config)# mls rate-limit multicast ipv6 route-cntl share auto
```

DoS 攻撃から保護するためのデフォルト設定

表 46-2 は、PFC3 の各種のハードウェア ベース レート リミッタにおける、DoS 攻撃から保護するためのデフォルト設定を示します。

表 46-2　PFC3 のハードウェア ベース 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 ステータス（ON/OFF）	デフォルト値
入力および出力 ACL ブリッジド パケット	OFF	
RPF 失敗	ON	100 pps、バースト パケット 10
FIB 受信	OFF	
FIB 収集	OFF	
レイヤ 3 セキュリティ機能	OFF	
ICMP リダイレクト	OFF	
ICMP 到達不能	ON	100 pps、バースト パケット 10
VACL ログ	ON	2000 pps、バースト パケット 10
TTL 失敗	OFF	
MTU 失敗	OFF	
レイヤ 2 PDU	OFF	
レイヤ 2 プロトコル トンネリング	OFF	
IP エラー	ON	100 pps、バースト パケット 10
マルチキャスト IGMP	OFF	
マルチキャスト FIB 不一致	ON	100000 pps、バースト パケット 100
マルチキャスト パーシャル SC	ON	100000 pps、バースト パケット 100
マルチキャスト直接接続	OFF	
マルチキャスト非 RPF	OFF	
マルチキャスト IPv6	ON	*packets-in-burst* を設定しない場合は、マルチキャスト関連のレート リミッタではデフォルト値 **100** がプログラミングされます。

DoS 攻撃からの保護における設定時の注意事項および制約事項

DoS 攻撃からの保護を設定する場合は、CPU レート リミッタに関する次の注意事項および制約事項に従ってください。

（注）　CoPP に関する注意事項および制約事項については、「CoPP 設定時の注意事項および制約事項」（P.47-2）を参照してください。

- PFC3A を使用して構成したシステムでマルチキャストをイネーブルにしている場合は、以下のレート リミッタは使用しないでください。
  - TTL 失敗
  - MTU 失敗
- 以下のレート リミッタは、PFC3A モードではサポートされません。
  - ユニキャスト IP オプション
  - マルチキャスト IP オプション
- レイヤ 2 レート リミッタは以下のとおりです。
  - 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
- 8 つのレイヤ 3 レジスタ、および 2 つのレイヤ 2 レジスタを CPU レート リミッタとして使用できます。
- CoPP を使用している場合は、CEF 受信リミッタは使用しないでください。CEF 受信リミッタは、CoPP トラフィックを上書きします。
- レート リミッタは CoPP トラフィックを上書きします。
- 設定したレート制限は、個々の転送エンジンに適用されます（レイヤ 2 ハードウェア レート リミッタは例外的にグローバルに適用されます）。
- レイヤ 2 レート リミッタは、truncated モードではサポートされません。
- 入力および出力 ACL ブリッジド パケット レート リミッタを使用する場合は、次の制約事項があります。
  - 入力および出力 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 ACL ブリッジド パケット レート リミッタは、1 つのレート リミッタ レジスタを共有します。ACL ブリッジ入出力レート リミッタをイネーブルにすると、入出力 ACL はどちらも同一のレート リミッタ値を共有します。
- ユニキャスト トラフィックをレート制限するには、**mls rate-limit unicast** コマンドを使用します。
- マルチキャスト トラフィックをレート制限するには、**mls rate-limit multicast** コマンドを使用します。
- レイヤ 2 マルチキャスト トラフィックをレート制限するには、**mls rate-limit multicast layer 2** コマンドを使用します。

パケット ドロップ統計情報のモニタ

着信または送信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外部インターフェイスに送信して、トラフィック アナライザでモニタできます。トラフィックをキャプチャして外部インターフェイスに転送するには、**monitor session** コマンドを使用します。

トラフィックをキャプチャする場合は、次の制約事項が適用されます。

- キャプチャした着信トラフィックはフィルタリングされません。
- キャプチャする着信トラフィックは、キャプチャの実行場所までの転送時にレート制限されません。

monitor session コマンドによるドロップ パケットのモニタ

次の例では、**monitor session** コマンドを使用してトラフィックをキャプチャし、外部インターフェイスに転送する方法を示します。

```
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#
2w0d: %SYS-5-CONFIG_I: Configured from console by console
```

次の例では、**show monitor session** コマンドを使用して、宛先ポートの場所を表示する方法を示します。

```
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
```

show tcam interface コマンドによるドロップ パケットのモニタ

PFC3A モードを除くすべてのモードでは、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。**show tcam interface** コマンドを使用すると、ACL TCAM 内の各エントリを表示できます。

次の例では、**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 または IP オプション カウンタを使用して、レイヤ 3 転送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。

次の例では、**show mls statistics** コマンドを使用して、レイヤ 3 転送エンジンに関連付けられたパケット統計情報およびエラーを表示します。

```
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
<----------------- TTL counters
  MTU failures                          : 0
<------------------MTU failure counters

Total packets L3 Switched by all Modules: 25433414 @ 24 pps
```

VACL キャプチャによるドロップ パケットのモニタリング

VACL キャプチャ機能を使用すると、キャプチャした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、転送される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。

VACL キャプチャを使用すると、各 VLAN からのトラフィックを別のインターフェイスに割り当てることができます。

VACL キャプチャでは、ある種類のトラフィック（たとえば HTTP）をあるインターフェイスに、別の種類のトラフィック（たとえば DNS）を別のインターフェイスに送信できません。また、VACL キャプチャ粒度は、ローカルにスイッチされたトラフィックだけに適用できます。トラフィックをリモート スイッチに転送した場合は、この粒度は保存できません。

次の例では、VACL キャプチャを使用してトラフィックをキャプチャし、ローカル インターフェイスに転送する方法を示します。

```
Router(config-if)# switchport capture
Router(config-if)# switchport capture allowed vlan add 100
```

レート リミッタ情報の表示

show mls rate-limit コマンドを使用すると、設定したレート リミッタに関する情報を表示できます。

show mls rate-limit usage コマンドを使用すると、特定の種類のレート リミッタが使用したハードウェア レジスタを表示できます。どの種類のレート リミッタからも使用されていないレジスタの場合は、出力結果には Free と表示されます。ある種類のレート リミッタによって使用されているレジスタの場合は Used と表示され、このレート リミッタの種類が表示されます。

コマンドの結果、レート制限ステータスは次のいずれかとして出力されます。

- 特定の条件に対するレートが設定されている場合は「On」
- この種類のレート リミッタが未設定であり、この条件に適合するパケットがレート制限されていない場合は「Off」
- ある特定の条件（手動設定したものではない条件）が、同一の共有グループに属する別のレート リミッタの設定によって影響を受ける場合は「On/Sharing」
- マルチキャスト パーシャル SC レート リミッタがディセーブルになっている場合は「-（ハイフン）」

コマンドの結果、レート制限共有については次の情報が出力されます。

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

設定したレート リミッタの情報を表示するには、**show mls rate-limit** コマンドを使用します。

```
Router# show mls rate-limit
 Sharing Codes: S - static, D - dynamic
 Codes dynamic sharing: H - owner (head) of the group, g - guest of the group

   Rate Limiter Type       Status     Packets/s   Burst  Sharing
 ----------------------   ----------   ---------   -----  -------
         MCAST NON RPF   Off                  -       -     -
        MCAST DFLT ADJ   On              100000     100  Not sharing
      MCAST DIRECT CON   Off                  -       -     -
        ACL BRIDGED IN   Off                  -       -     -
       ACL BRIDGED OUT   Off                  -       -     -
           IP FEATURES   Off                  -       -     -
```

```
          ACL VACL LOG   On                2000       1  Not sharing
           CEF RECEIVE   Off                  -        -     -
             CEF GLEAN   Off                  -        -     -
       MCAST PARTIAL SC   On              100000      100  Not sharing
         IP RPF FAILURE   On                 100       10  Group:0 S
            TTL FAILURE   Off                  -        -     -
 ICMP UNREAC. NO-ROUTE   On                 100       10  Group:0 S
 ICMP UNREAC. ACL-DROP   On                 100       10  Group:0 S
          ICMP REDIRECT   Off                  -        -     -
            MTU FAILURE   Off                  -        -     -
        MCAST IP OPTION   Off                  -        -     -
        UCAST IP OPTION   Off                  -        -     -
            LAYER_2 PDU   Off                  -        -     -
             LAYER_2 PT   Off                  -        -     -
              IP ERRORS   On                 100       10  Group:0 S
            CAPTURE PKT   Off                  -        -     -
             MCAST IGMP   Off                  -        -     -
 MCAST IPv6 DIRECT CON   Off                  -        -     -
 MCAST IPv6 *G M BRIDG   Off                  -        -     -
  MCAST IPv6 *G BRIDGE   Off                  -        -     -
  MCAST IPv6 SG BRIDGE   Off                  -        -     -
 MCAST IPv6 ROUTE CNTL   Off                  -        -     -
  MCAST IPv6 DFLT DROP   Off                  -        -     -
 MCAST IPv6 SECOND. DR   Off                  -        -     -
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
                             Rate Limiter Type     Packets/s   Burst
                           ----------------------  ---------   -----
Layer3 Rate Limiters:
             RL# 0: Free                           -           -       -
             RL# 1: Free                           -           -       -
             RL# 2: Free                           -           -       -
             RL# 3: Used
                                  MCAST DFLT ADJ      100000     100
             RL# 4: Free                           -           -       -
             RL# 5: Free                           -           -       -
             RL# 6: Used
                                IP RPF FAILURE         100      10
                           ICMP UNREAC. NO-ROUTE       100      10
                           ICMP UNREAC. ACL-DROP       100      10
                                       IP ERRORS       100      10
             RL# 7: Used
                                  ACL VACL LOG        2000       1
             RL# 8: Rsvd for capture               -           -       -

Layer2 Rate Limiters:
             RL# 9: Reserved
             RL#10: Reserved
             RL#11: Free                           -           -       -
             RL#12: Free                           -           -       -
Router#
```

sticky ARP の設定

sticky ARP 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保証することで、MAC アドレスのスプーフィングを防止します。スイッチは、トラフィックをエンド デバイスまたは他のスイッチに転送する目的で、ARP エントリを維持します。ARP エントリは通常、定期的に更新されるか、または ARP ブロードキャスト受信時に修正されます。攻撃が開始されると、偽装した MAC アドレスと正規の IP アドレスを持つ ARP ブロードキャストが送信されます。この結果、スイッチは偽装した MAC アドレスによる正規の IP アドレスを学習し、トラフィックのこの MAC アドレスへの転送を開始します。sticky 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 ブロードキャストから受信した変更は受け付けなくなります。ARP 設定を上書きしようとすると、エラー メッセージが発行されます。システム エラー メッセージの完全な詳細については、次の URL の『*Catalyst 6500 Series Switch Cisco IOS System Message Guide*, Release 12.2SX』を参照してください。

http://www.cisco.com/en/US/docs/ios/12_2sx/system/messages/122sxsms.html

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*	sticky 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`	sticky ARP をイネーブルにします。
	`Router(config-if)# no ip sticky-arp ignore`	以前に設定した sticky ARP コマンドを削除します。
ステップ 3	`Router(config-if)# ip sticky-arp ignore`	sticky 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 sticky 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#
```

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

ヒント