CHAPTER 33

DoS からの保護の設定

この章では、Catalyst 6500 シリーズ スイッチを DoS 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 Catalyst 6500 シリーズ スイッチ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、以下のマニュアルを参照してください。

- 次の URL にある『*Catalyst Supervisor Engine 32 PISA Cisco IOS Command Reference*, Release 12.2ZY』
  http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/command/reference/cmdref.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

この章で説明する内容は、次のとおりです。

DoS からの保護の機能概要

ここでは、Policy Feature Card 3B（PFC3B; ポリシー フィーチャ カード 3B）への DoS 攻撃に対して有効な対処方法についての情報を提供し、その設定例を示します。PFC3B 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。
- CoPP：コントロール プレーンのトラフィックをフィルタおよびレート制限します。CoPP の詳細については、「CoPP の機能概要」（P.33-20）を参照してください。

ここでは、PFC3B での DoS 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 パケットを廃棄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廃棄されます。

Catalyst 6500 シリーズ 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 Catalyst 6500 シリーズ スイッチの 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、PISA 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。PISA 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 PISA データ パスに到達しないようにして、輻輳を防ぎます。PFC3B 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 PISA 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 攻撃などを受けた場合、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 PISA 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; 認定情報レート）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 マップに従って廃棄されます（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、スーパーバイザ エンジンの 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廃棄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廃棄されます。

uRPF チェックの ACL は、uRPF チェックに失敗したパケットだけに指定できます。この ACL は、パケットをただちに廃棄するか、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 PFC3B 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。

PFC3B による uRPF チェックはハードウェア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、PISA 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 トラフィックが廃棄されます。

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

Catalyst 6500 シリーズ スイッチは、すべての LAN ポートでブロードキャスト ストーム制御をサポートし、ギガビット イーサネット ポートではユニキャスト 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 PISA 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、PFC3B 上でハードウェア アシストされます。

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、PISA 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 PISA 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。
- ハードウェア転送をサポートするプラットフォーム（Catalyst 6500 シリーズ スイッチなど）では、リダイレクトの必要性が少なくされているため、リダイレクトをディセーブルにします。
- ハードウェア転送をサポートするプラットフォーム（Catalyst 6500 シリーズ スイッチなど）では、到達不能メッセージの必要性が少なくされているため、到達不能レート リミッタ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。

PFC3B のハードウェア ベース レート リミッタ

PFC3B 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。PFC3B 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（PFC3B）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、PFC3B 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。

PFC3B 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 廃棄）
- 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（ユニキャストのみ）

このレート リミッタは、入出力 ACL ブリッジの結果として PISA 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、PISA 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 PISA 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、PISA 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、PISA 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、PISA 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 PISA 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（ユニキャストのみ）

ICMP 到達不能攻撃では、攻撃対象の装置（この場合は PISA）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、PISA 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 廃棄によって PISA 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 廃棄）、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（ユニキャストのみ）

FIB 受信レート リミッタの機能は、宛先アドレスとして PISA 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（ユニキャストのみ）

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、PISA 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、PISA 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 PISA 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、PISA 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（ユニキャストのみ）

いくつかのセキュリティ機能では、パケットはまず PISA 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、PISA 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、PISA が過負荷になる恐れがあります。このような場合にレート制限を行うと効果的です。

IPSec および検査も PISA 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、IPSec、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、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（ユニキャストのみ）

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、PISA 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、PISA 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（ユニキャストのみ）

VLAN-ACL ロギングの結果によって PISA 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、PISA 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、PISA CPU に送信されます。これにより、PISA 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、PISA 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、スーパーバイザ エンジン宛てのレイヤ 2 IGMP パケットの数を制限します。IGMP スヌーピングは、ホストとスーパーバイザ エンジン間の IGMP メッセージを待ち受けます。Catalyst 6500 シリーズ 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、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、PISA CPU ではなくスーパーバイザ エンジン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。Catalyst 6500 シリーズ 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、スーパーバイザ エンジン宛てのレイヤ 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。Catalyst 6500 シリーズ 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。PFC3B 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 PISA 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、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廃棄できます。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 PISA 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 PISA 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 PISA 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
```

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 33-1 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 33-1　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
デフォルト廃棄	* (*, G/m) SSM * (*, G/m) SSM non-rpf
ルート制御	* (*, FF02::X/128)
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廃棄（**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、デフォルト廃棄（**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 33-2 は、PFC3B 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 33-2　PFC3B 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

PFC3B を使用するシステムに対して 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.33-20）を参照してください。

- 次のレート リミッタがサポートされます。
  - 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る）。
- 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 トラフィックでだけ使用できます。
  - 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。

パケット廃棄統計情報のモニタ

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 コマンドによる廃棄パケットのモニタ

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 コマンドによる廃棄パケットのモニタ

PFC3B は、ハードウェアで ACL ヒット カウンタをサポートします。**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 キャプチャによる廃棄パケットのモニタ

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。

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することはできません。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 に転送した場合は、この粒度は保存できませんスイッチ。

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#
```

CoPP の機能概要

CoPP 機能を使用すると、不要なトラフィックや DoS トラフィックから PISA を保護し、重要なコントロール プレーンおよび管理トラフィックを優先させることができるので、Catalyst 6500 シリーズ スイッチのセキュリティを強化できます。PFC3B は、CoPP をハードウェアでサポートします。CoPP は、PFC3B のレート リミッタと連携して動作します。

（注）　Supervisor Engine 2 は CoPP をサポートしません。

PFC3B は、組み込みの [special case] レート リミッタをサポートします。このレート リミッタは、IP オプション、TTL および MTU の失敗、エラーの生じたパケット、マルチキャスト パケットといった ACL の分類に該当しない、特定のシナリオで使用できます。special-case レート リミッタをイネーブルにすると、このレート リミッタは基準に適合するパケットに対し、CoPP ポリシーを上書きします。

PISA によって管理されるトラフィックは、次の 3 つの機能コンポーネント（*プレーン*）に分類されます。

- データ プレーン
- マネジメント プレーン
- コントロール プレーン

PISA の管理するトラフィックのほとんどは、コントロール プレーンおよびマネジメント プレーンによって処理されます。CoPP を使用してコントロール プレーンおよびマネジメント プレーンを保護することで、ルーティングの安定性、到達可能性、および確実なパケット配信を維持できます。CoPP では、Modular QoS CLI（MQC; モジュラ QoS コマンドライン インターフェイス）から専用のコントロール プレーン設定を使用して、コントロール プレーン パケットに対するフィルタリングおよびレート制限機能を提供します。

CoPP のデフォルト設定

CoPP はデフォルトでディセーブルにされています。

CoPP 設定時の注意事項および制約事項

CoPP を設定する場合は、次の注意事項および制約事項に従ってください。

- マルチキャストに一致するクラスは、ハードウェアではなくソフトウェアに適用されます。
- CPP によるブロードキャスト パケット処理は、ハードウェアではサポートされません。ブロードキャスト DoS 攻撃からの保護を実現するには、ACL、トラフィック ストーム制御、および CPP ソフトウェア保護を組み合わせて使用します。
- CoPP は ARP ポリシーをサポートしません。ARP ポリシング メカニズムは、ARP ストームからの保護を実現します。
- CoPP は、デフォルトの非 IP クラス以外の非 IP クラスをサポートしません。非 IP トラフィックを廃棄するには、非 IP クラスの代わりに ACL を使用できます。また、RP CPU に到達する非 IP トラフィックを制限するには、デフォルトの非 IP CoPP クラスを使用できます。
- CoPP ポリシー ACL では、**log** キーワードは使用しないでください。

- 大規模な QoS 設定を使用すると、システムの TCAM 領域が足りなくなる可能性があります。この場合は、CoPP はソフトウェア内で実行されます。
- 他のインターフェイスに対する大規模な QoS 設定があると、領域が足りなくなる可能性があります。この場合は、CoPP がソフトウェア内で完全に実行され、パフォーマンス低下や CPU サイクル消費につながる可能性があります。
- CoPP ポリシーによって、ルーティング プロトコルなどのクリティカルなトラフィック、またはスイッチへのインタラクティブなアクセスがフィルタリングされないように注意してください。このトラフィックをフィルタリングすると、スイッチへのリモート アクセスが禁止され、コンソール接続が必要となる場合があります。
- PFC3B は、組み込みの special-case レート リミッタをサポートします。これは、ACL を使用できない状況（TTL、MTU、IP オプションなど）で便利です。special-case レート リミッタをイネーブルにする場合は、このレート リミッタが基準に適合するパケットに対し、CoPP ポリシーを上書きすることに注意してください。
- **mls qos** コマンドによって MMLS QoS をグローバルにイネーブルにしないかぎり、CoPP はハードウェアでイネーブルにされません。**mls qos** コマンドを入力しないと、CoPP はソフトウェア内だけで動作し、ハードウェアに対する機能を果たせなくなります。
- 出力 CoPP、およびサイレント モードはサポートされません。CoPP は入力だけでサポートされます。サービス ポリシー出力 CoPP は、コントロール パネル インターフェイスには適用できません。
- ハードウェア内の ACE ヒット カウンタは、ACL 論理だけに対応します。CPU トラフィックのトラブルシューティングおよび評価には、ソフトウェア ACL のヒット カウンタ、および **show access-list**、**show policy-map control-plane**、**show mls ip qos** コマンドが役立ちます。
- CoPP は転送エンジン単位で実行され、ソフトウェア CoPP は集約的に実行されます。
- CoPP によるマルチキャスト パケット処理は、ハードウェアではサポートされません。マルチキャスト DoS 攻撃からの保護を実現するには、ACL、マルチキャスト CPU レート リミッタ、および CoPP ソフトウェア保護を組み合わせて使用します。
- CoPP では、ACE に **log** キーワードを使用できません。
- CoPP はハードウェア QoS TCAM リソースを使用します。TCAM の利用率を確認するには、**show tcam utilization** コマンドを入力します。

CoPP の設定

CoPP では MQC を使用することで、トラフィックの分類基準を定義し、分類したトラフィックに対して設定可能なポリシー アクションを指定します。最初にクラス マップを定義して、分類の対象となるトラフィックを識別する必要があります。クラス マップは、特定のトラフィック クラスに対するパケットを定義します。トラフィックを分類したあとは、識別したトラフィックにポリシー アクションを適用するためのポリシー マップを作成できます。**control-plane** グローバル コンフィギュレーション コマンドを使用すると、CoPP サービス ポリシーをコントロール プレーンに直接付加できます。

トラフィック分類基準を定義する方法については、「トラフィック分類の定義」（P.33-24）を参照してください。

CoPP 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 qos`	MLS QoS をグローバルにイネーブル化します。
ステップ 2	`Router(config)# ip access-list extended access-list-name` `Router(config-ext-nacl)# {permit | deny} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [established] [log | log-input] [time-range time-range-name] [fragments]`	トラフィックと一致する ACL を定義します。 • **permit** は、名前付き IP アクセス リストにパケットが適合する条件を設定します。 • **deny** は、名前付き IP アクセス リストがパケットを拒否する条件を設定します。 **（注）** ほとんどの場合は、重要なトラフィックとそうでないトラフィックの識別には ACL を設定する必要があります。
ステップ 3	`Router(config)# class-map traffic-class-name` `Router(config-cmap)# match {ip precedence} |{ip dscp} | access-group`	パケット分類基準を定義します。**match** ステートメントを使用して、クラスに関連付けるトラフィックを識別します。

ステップ 4	`Router(config)# policy-map service-policy-name`
	`Router(config-pmap)# class traffic-class-name`
	`Router(config-pmap-c)# police {bits-per-second [normal-burst-bytes] [maximum-burst-bytes] [pir peak-rate-bps]} | [conform-action action] [exceed-action action] [violate-action action]`
		サービス ポリシー マップを定義します。**class** *traffic-class-name* コマンドを使用して、サービス ポリシー マップにクラスを関連付けます。**police** ステートメントを使用して、サービス ポリシー マップにアクションを関連付けます。

ステップ 5	`Router(config)# control-plane` `Router(config-cp)#`	コントロールプレーンのコンフィギュレーション モードを有効にします。
ステップ 6	`Router(config-cp)# service-policy input service-policy-name`	QoS サービス ポリシーをコントロール プレーンに適用します。

パケット分類基準を定義する場合は、次の注意事項および制約事項に従ってください。

- 以降のクラスで設定されたフィルタリングおよびポリシングと一致することを避けるため、ポリシングは各クラスで設定します。CoPP では、police コマンドを含まないクラスにはフィルタリングを適用しません。police コマンドのないクラスは、どのトラフィックとも一致しません。
- 分類に使用する ACL は QoS ACL です。サポートされる QoS ACL は、IP 標準 ACL、拡張 ACL、および名前付き ACL です。IPv6 ACL はハードウェアではサポートされません。
- 次の一致タイプだけがサポートされます。
  - **ip precedence**
  - **ip dscp**
  - **access-group**
- ハードウェアでは、IP ACL だけがサポートされます。
- MAC ベースの一致が行われるのは、ソフトウェア上だけです。
- 1 つの **match** コマンドは、1 つのクラス マップだけに入力できます。

サービス ポリシーを定義する場合は、**police** ポリシー マップ アクションだけがサポートされます。

サービス ポリシーをコントロール プレーンに適用する場合は、**input** 方向だけがサポートされます。

CoPP のモニタ

サイト固有のポリシーを作成するには、**show policy-map control-plane** コマンドを入力することで、コントロール プレーン ポリシーの統計情報をモニタでき、CoPP のトラブルシューティングを行えます。このコマンドを使用すると、実際に適用されたポリシーについてのダイナミックな情報を表示できます。たとえば、ハードウェアおよびソフトウェア内において、設定されたポリシーに適合する、またはこれを超過するバイト数およびパケット数を表示できます。

show policy-map control-plane コマンドの出力結果は次のようになります。

```
Router# show policy-map control-plane
Control Plane Interface
  Service policy CoPP-normal
Hardware Counters:
class-map: CoPP-normal (match-all)
      Match: access-group 130
      police :
        96000 bps 3000 limit 3000 extended limit
      Earl in slot 3 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps
      Earl in slot 5 :
        0 bytes
        5 minute offered rate 0 bps
        aggregate-forwarded 0 bytes action: transmit
        exceeded 0 bytes action: drop
        aggregate-forward 0 bps exceed 0 bps

Software Counters:
    Class-map: CoPP-normal (match-all) 0 packets, 0 bytes
      5 minute offered rate 0 bps, drop rate 0 bps
      Match: access-group 130
      police:
        96000 bps, 3125 limit, 3125 extended limit
        conformed 0 packets, 0 bytes; action: transmit
        exceeded 0 packets, 0 bytes; action: drop
        conformed 0 bps, exceed 0 bps, violate 0 bps
Router#
```

ハードウェア カウンタを表示して、ポリシーによって廃棄および転送されたバイト数を確認するには、**show mls qos ip** コマンドを入力します。

```
Router# show mls qos ip
 QoS Summary [IP]:      (* - shared aggregates, Mod - switch module)

Int Mod Dir  Class-map DSCP  Agg  Trust Fl   AgForward-By   AgPoliced-By
                             Id         Id
------------------------------------------------------------------------------
CPP  5  In CoPP-normal    0    1   dscp  0         505408       83822272
CPP  9  In CoPP-normal    0    4   dscp  0              0              0
Router#
```

CoPP アクセス リストの情報を表示するには、**show access-lists coppacl-bgp** コマンドを入力します。

```
Router# show access-lists coppacl-bgp
Extended IP access list coppacl-bgp
10 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp (4 matches)
20 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
30 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp (1 match)
40 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

トラフィック分類の定義

ここでは、CoPP トラフィックを分類する方法について説明します。

トラフィック分類の概要

定義できるクラスの数に制限はありませんが、一般的にトラフィックは、相対的な重要度に基づくクラスに分類されます。次に、グループ分けの例を示します。

- Border Gateway Protocol（BGP）：BGP ルーティング プロトコルにおいて、隣接関係を維持するために重要なトラフィック。BGP キープ アライブ、ルーティング更新などです。BGP ルーティング プロトコルの維持は、ネットワーク内での接続、またはサービス プロバイダーとの接続を維持するうえで重要です。BGP を実行しないサイトでは、このクラスを使用する必要はありません。
- Interior Gateway Protocol（IGP; 内部ゲートウェイ プロトコル）：IGP ルーティング プロトコルを維持するうえで重要なトラフィック。たとえば Open Shortest Path First（OSPF）、Enhanced Interior Gateway Routing Protocol（EIGRP）、Routing Information Protocol（RIP）などです。IGP ルーティング プロトコルの維持は、ネットワーク内の接続を維持するうえで重要です。
- 管理：日常業務で必要とされ、頻繁に使用される必須トラフィック。たとえば、リモート ネットワーク アクセスに使用するトラフィックや、Cisco IOS イメージの更新および管理トラフィックです。これには、Telnet、Secure Shell（SSH; セキュア シェル）、Network Time Protocol（NTP）、Simple Network Management Protocol（SNMP; 簡易ネットワーク管理プロトコル）、Terminal Access Controller Access Control System（TACACS）、HTTP、Trivial File Transfer Protocol（TFTP; 簡易ファイル転送プロトコル）、File Transfer Protocol（FTP; ファイル転送プロトコル）などがあります。
- レポート：レポート目的で、ネットワーク パフォーマンスに関する統計情報の生成に使用されるトラフィック。たとえば、Cisco IOS IP サービス レベル アグリーメントを使用して、異なる DSCP 設定で ICMP を生成し、さまざまな QoS データ クラス内の応答時間をレポートできます。
- モニタ：スイッチのモニタに使用するトラフィック。このトラフィックは許可する必要がありますが、スイッチを危険にさらすことがあってはなりません。CoPP を使用すると、このトラフィックは許可されますが、低いレートに制限できます。たとえば、ICMP エコー要求（ping）、traceroute などです。
- クリティカルなアプリケーション：特定のカスタマー環境に固有の、クリティカルなアプリケーション トラフィック。このクラスに分類するトラフィックは、ユーザに必要なアプリケーションの要件に合わせて、特別に調整する必要があります。マルチキャストを使用するカスタマーもいれば、IPSec または Generic Routing Encapsulation（GRE; 総称ルーティング カプセル化）を使用するカスタマーもいます。このトラフィックの例としては、GRE、Hot Standby Router Protocol（HSRP）、Virtual Router Redundancy Protocol（VRRP）、Session Initiation Protocol（SIP）、データ リンク スイッチング、Dynamic Host Configuration Protocol（DHCP）、Multicast Source Discovery Protocol（MSDP）、IGMP、Protocol Independent Multicast（PIM）、マルチキャスト トラフィック、IPsec などが挙げられます。
- レイヤ 2 プロトコル：ARP に使用されるトラフィック。ARP パケットが過剰に発生すると、PISA リソースが独占され、他の重要なプロセスがリソース不足になってしまう可能性があります。CoPP を使用して ARP パケットをレート制限すると、このような状況を回避できます。現時点では、一致プロトコル分類基準を使用して明示的に分類可能な唯一のレイヤ 2 プロトコルが、ARP となります。

- 不要：PISA へのアクセスを無条件で廃棄および拒否する必要のある、不正な、または悪意あるトラフィックを明示的に指定します。この分類は、スイッチ宛ての既知のトラフィックを常に拒否する必要があり、デフォルト カテゴリに含まれないようにする場合に便利です。トラフィックを明示的に拒否した場合は、**show** コマンドを使用すると、拒否したトラフィックの概算統計情報を収集し、そのレートを見積もることができます。
- デフォルト：他に分類されない、PISA 宛ての残りのトラフィックすべてを収容。MQC はデフォルト クラスを備えているため、他のユーザ定義クラスでは明示的に識別されないトラフィックに適用する処理を指定できます。このトラフィックの PISA へのアクセス レートは、大幅に制限されます。デフォルト分類を設定しておくと、統計情報をモニタして、通常であれば識別されないコントロール プレーン宛てトラフィックのレートを決定できます。このトラフィックを識別したあとは、追加の分析を行うことで該当カテゴリに分類できます。必要であれば、このトラフィックにも対応するように、他の CoPP ポリシー エントリを更新することもできます。

トラフィックの分類が完了すると、ACL は、ポリシーの定義に使用するトラフィック クラスを作成します。CoPP 分類に使用する基本的な ACL の例については、「CoPP トラフィック分類の基本的な ACL の例」（P.33-25）を参照してください。

トラフィック分類の注意事項

トラフィック分類を定義する場合は、次の注意事項および制約事項に従ってください。

- 実際の CoPP ポリシーを作成する前に、どのトラフィックをどのクラスに分類するかを識別しておく必要があります。トラフィックは相対的な重要度に基づき、9 つのクラスに分類されます。実際に必要となるクラス数はこれとは異なる可能性があり、各自のローカルな要件、およびセキュリティ ポリシーに基づき選択する必要があります。
- 双方向的に一致するポリシーを定義する必要はありません。ポリシーは入力だけに適用されるため、トラフィックは一方向（ネットワークから PISA へ）だけで識別します。

CoPP トラフィック分類の基本的な ACL の例

ここでは、CoPP 分類の基本的な ACL の例を示します。各例では、一般的に必要とされるトラフィックを、以下の ACL によって識別します。

- ACL 120：クリティカルなトラフィック
- ACL 121：重要なトラフィック
- ACL 122：通常のトラフィック
- ACL 123：不要なトラフィックを明示的に拒否
- ACL 124：その他すべてのトラフィック

次の例では、クリティカルなトラフィックに対する ACL 120 を定義します。

```
Router(config)# access-list 120 remark CoPP ACL for critical traffic
```

次の例では、既知のピアからスイッチの BGP TCP ポートへの、BGP トラフィックを許可します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 host 10.9.9.9 eq bgp
```

次の例では、ピアの BGP ポートからこのスイッチへの BGP トラフィックを許可します。

```
Router(config)# access-list 120 permit tcp host 47.1.1.1 eq bgp host 10.9.9.9
Router(config)# access-list 120 permit tcp host 10.86.183.120 host 10.9.9.9 eq bgp
Router(config)# access-list 120 permit tcp host 10.86.183.120 eq bgp host 10.9.9.9
```

次の例では、重要なクラスに対する ACL 121 を定義します。

```
Router(config)# access-list 121 remark CoPP Important traffic
```

次の例では、TACACS ホストからのリターン トラフィックを許可します。

```
Router(config)# access-list 121 permit tcp host 1.1.1.1 host 10.9.9.9 established
```

次の例では、サブネットからスイッチへの SSH アクセスを許可します。

```
Router(config)# access-list 121 permit tcp 10.0.0.0 0.0.0.255 host 10.9.9.9 eq 22
```

次の例では、指定のサブネット内のホストからスイッチへの Telnet フル アクセスを許可し、残りのサブネットをポリシングします。

```
Router(config)# access-list 121 deny tcp host 10.86.183.3 any eq telnet
Router(config)# access-list 121 permit tcp 10.86.183.0 0.0.0.255 any eq telnet
```

次の例では、NMS ホストからスイッチへの SNMP アクセスを許可します。

```
Router(config)# access-list 121 permit udp host 1.1.1.2 host 10.9.9.9 eq snmp
```

次の例では、既知のクロック ソースからの NTP パケットの受信をスイッチに許可します。

```
Router(config)# access-list 121 permit udp host 1.1.1.3 host 10.9.9.9 eq ntp
```

次の例では、通常のトラフィック クラスに対する ACL 122 を定義します。

```
Router(config)# access-list 122 remark CoPP normal traffic
```

次の例では、スイッチから送信される traceroute トラフィックを許可します。

```
Router(config)# access-list 122 permit icmp any any ttl-exceeded
Router(config)# access-list 122 permit icmp any any port-unreachable
```

次の例では、ping を発行したスイッチへの応答を受信することを許可します。

```
Router(config)# access-list 122 permit icmp any any echo-reply
```

次の例では、スイッチへの ping の送信を許可します。

```
Router(config)# access-list 122 permit icmp any any echo
```

次の例では、不要なクラスに対する ACL 123 を定義します。

```
Router(config)# access-list 123 remark explicitly defined "undesirable" traffic
```

（注） 次の例では、ACL 123 は分類およびモニタのための許可エントリであり、トラフィックは CoPP ポリシーの結果に基づいて廃棄されます。

この例では、UDP 1434 宛てに送信され、ポリシングの対象となるすべてのトラフィックを許可します。

```
Router(config)# access-list 123 permit udp any any eq 1434
```

次の例では、他のすべてのトラフィックに対する ACL 124 を定義します。

```
Router(config)# access-list 124 remark rest of the IP traffic for CoPP
Router(config)# access-list 124 permit ip any any
```

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、エンド デバイスまたは他のスイッチにトラフィックを転送するために、ARP エントリを維持します。ARP エントリは通常、定期的に更新されます。または、ARP ブロードキャストを受信したときに変更されます。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 Supervisor Engine 32 PISA Cisco IOS System Message Guide*, Release 12.2ZY』を参照してください。

http://www.cisco.com/en/US/docs/switches/lan/catalyst6500/ios/12.2ZY/system/messages/sysmsg.html

レイヤ 3 インターフェイス上で sticky ARP 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` *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* = **ethernet**、**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#
```