



CHAPTER 39

ACL によるネットワーク セキュリティの設定

この章では、アクセス コントロール リスト (ACL) を使用して Catalyst 4500 シリーズ スイッチ上でネットワーク セキュリティを設定する方法について説明します。



(注)

この章のスイッチ コマンドの構文および使用方法の詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』および次の URL の関連マニュアルを参照してください。

<http://www.cisco.com/en/US/products/ps6350/index.html>

この章で説明する主な内容は、次のとおりです。

- 「ACL の概要」 (P.39-2)
- 「ハードウェアおよびソフトウェア ACL のサポート」 (P.39-5)
- 「Supervisor Engine II-Plus、Supervisor Engine IV、Supervisor Engine V、および Supervisor Engine V-10GE の TCAM プログラミングと ACL」 (P.39-6)
- 「Supervisor Engine 6-E の TCAM プログラミングおよび ACL」 (P.39-15)
- 「ACL のレイヤ 4 演算」 (P.39-15)
- 「ユニキャスト MAC アドレス フィルタリングの設定」 (P.39-19)
- 「名前付き MAC 拡張 ACL の設定」 (P.39-19)
- 「名前付き IPv6 ACL の設定」 (P.39-21)
- 「レイヤ 3 インターフェイスへの IPv6 ACL の適用」 (P.39-22)
- 「VLAN マップの設定」 (P.39-23)
- 「VLAN アクセス マップ情報の表示」 (P.39-30)
- 「ルータ ACL を VLAN マップと組み合わせて使用する方法」 (P.39-31)
- 「PACL の設定」 (P.39-33)
- 「VLAN マップおよびルータを PACL と併用する方法」 (P.39-37)



(注)

次の説明は、特に明記されていない限り、Supervisor Engine 6-E および非 Supervisor Engine 6E の設定の両方に当てはまります。

ACL の概要

ここでは、次の内容について説明します。

- 「ACL の概要」 (P.39-2)
- 「ACL を使用するサポート対象機能」 (P.39-3)
- 「ルータ ACL」 (P.39-3)
- 「ポート ACL」 (P.39-4)
- 「VLAN マップ」 (P.39-5)

ACL の概要

ACL は、パケットに適用される許可条件および拒否条件を集めて順番に並べたものです。パケットがインターフェイスに着信すると、スイッチはパケットのフィールドと適用される ACL を比較し、アクセス リストに指定されている条件に基づいて、転送に必要な許可がパケットに与えられているかどうかを調べます。スイッチはパケットをアクセス リストの条件と 1 つ 1 つ突き合わせます。最初に一致した条件によって、スイッチがパケットを許可するかまたは拒否するかが決まります。スイッチは、最初に一致した時点で条件のテストを中止するため、リストに条件を指定する順序が重要です。いずれの条件とも一致しなかった場合、スイッチはパケットを拒否します。スイッチは、制限条件がない場合はパケットを転送し、制限条件がある場合はパケットをドロップします。

従来、スイッチはレイヤ 2 で稼働し、VLAN 内でトラフィックをスイッチングしていました。一方、ルータはレイヤ 3 の VLAN 間でトラフィックをルーティングしていました。Catalyst 4500 シリーズスイッチは、レイヤ 3 スwitchングを使用して、VLAN 間のパケットルーティングの速度を向上させます。レイヤ 3 スwitchでブリッジングされたパケットは、外部ルータに送信されずに内部でルーティングされます。そのあと、再度ブリッジングされて宛先に送信されます。スイッチはこのプロセス中に、VLAN 内でブリッジングされるパケットを含めて、すべてのパケットを制御します。

トラフィックをフィルタリングし、ネットワークに基本的なセキュリティを導入するには、ルータまたはスイッチにアクセス リストを設定します。ACL を設定しないと、スイッチを通過するすべてのパケットが、ネットワーク内のすべての場所に転送されることがあります。ACL を使用すると、ネットワークの場所ごとにアクセス可能なホストを制御したり、ルータ インターフェイスで転送またはブロックされるトラフィックの種類を決定したりできます。たとえば、電子メールトラフィックの転送を許可し、Telnet トラフィックの転送を拒否することもできます。ACL を着信トラフィック、発信トラフィック、またはその両方をブロックするように設定することもできます。ただし、レイヤ 2 インターフェイスでは、ACL を適用できるのは着信方向だけです。

ACL には、Access Control Entry (ACE; アクセス コントロール エントリ) の順序付けられたリストが含まれています。各 ACE には、permit または deny と、パケットが ACE と一致するために満たす必要のある一連の条件を指定します。permit または deny の意味は、ACL が使用されるコンテキストによって変わります。

Catalyst 4500 シリーズ スwitchでは、次の 3 つの ACL タイプがサポートされています。

- TCP、ユーザ データグラム プロトコル (UDP)、Internet Group Management Protocol (IGMP)、Internet Control Message Protocol (ICMP) などの IP トラフィックをフィルタリングする IP ACL
- IPv6 ACL (Supervisor Engine 6-E にだけ該当)

ACL を使用するサポート対象機能

スイッチは、トラフィックをフィルタリングするため、次に示す 2 つの ACL 用途をサポートしています。

- ルータ ACL は、レイヤ 3 インターフェイスに適用されます。この ACL は、VLAN 間でルーティングされたトラフィックのアクセスを制御します。すべての Catalyst 4500 シリーズ スイッチでルータ ACL を作成できますが、レイヤ 3 インターフェイスに ACL を適用して、VLAN 間でルーティングされたパケットをフィルタリングするには、スイッチに Cisco IOS ソフトウェア イメージをインストールする必要があります。
- Port ACL (PACL; ポート ACL) は、レイヤ 2 インターフェイスに入るトラフィックのアクセスをコントロールします。ハードウェアの CAM (連想メモリ) エントリが十分でない場合、出力 PACL がポートに適用されず、警告メッセージがユーザに送られます (この制限は、出力 PACL のすべてのアクセス グループ モードに適用されます)。CAM エントリが十分な場合、出力ポート ACL は再適用されます。

レイヤ 2 ポートに出力 PACL が設定されている場合、レイヤ 2 ポートが属する VLAN に VACL またはルータ ACL を設定できません。その逆の場合も同じです。つまり、PACL および VLAN ベースの ACL (VACL およびルータ ACL) は、レイヤ 2 ポート上では相互に排他的です。この制限はすべてのアクセス グループ モードに適用されます。入力方向では、ポート ACL、VLAN ベース ACL、およびルータ ACL が共存できます。

1 つのレイヤ 2 インターフェイスに適用できるのは、IP アクセス リスト 1 つと MAC アクセス リスト 1 つだけです。

- VLAN ACL または VLAN マップは、すべてのパケット (ブリッジド パケットおよびルーテッド パケット) のアクセスを制御します。VLAN マップを使用すると、同じ VLAN 内のデバイス間で転送されるトラフィックをフィルタリングできます。VLAN マップを作成または適用するために、拡張イメージをインストールする必要はありません。VLAN マップは、IP のレイヤ 3 アドレスに基づいてアクセス コントロールするように設定されています。イーサネット ACE を使用する MAC アドレスにより、サポートされていないプロトコルがアクセス コントロールされます。VLAN マップを VLAN に適用すると、VLAN に入るすべてのパケット (ルーテッド パケットまたはブリッジド パケット) が VLAN マップと照合されます。パケットは、スイッチ ポートを介して、または、ルーティングされたパケットの場合、ルーテッド ポートを介して、VLAN に入ることができます。

同じスイッチ上でルータ ACL と VLAN マップを両方使用できます。

ルータ ACL

サポートされる各タイプのアクセス リスト 1 つをインターフェイスに適用できます。



(注)

Cisco IOS Release 12.2(40)SG を実行している Catalyst 4500 シリーズ スイッチは、IPv6 Port ACL (PACL) をサポートしません。

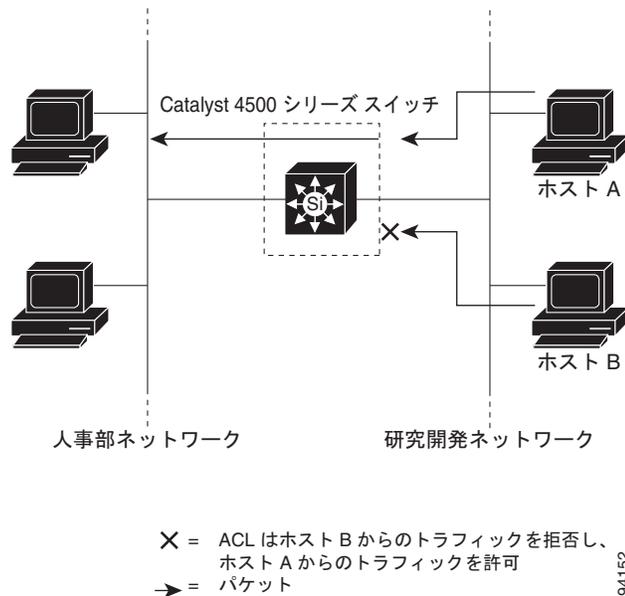
1 つの ACL を特定のインターフェイスの複数の機能に使用できます。また、1 つの機能に複数の ACL を使用することもできます。1 つのルータ ACL を複数の機能で使用する場合、そのルータ ACL は複数回、照合されます。アクセス リストのタイプによって、一致処理に対する入力が決まります。

- 標準 IP アクセス リストでは、照合操作に送信元アドレスを使用します。
- 拡張 IP アクセス リストは、送信元アドレス、宛先アドレス、およびオプションのプロトコル タイプ情報を使用して一致処理を行います。

スイッチは、特定のインターフェイスおよび方向に対する設定機能に関連付けられている ACL をテストします。パケットがスイッチのインターフェイスに着信すると、そのインターフェイスに設定されているすべての着信機能に対応する ACL が照合されます。パケットがルーティングされてからネクストホップに転送されるまでの間に、出力インターフェイスに設定された発信機能に対応するすべての ACL が照合されます。

ACL は、パケットが ACL 内のエントリとどのように一致したかに基づいてパケットの転送を許可または拒否します。たとえば、アクセス リストを使用すると、ネットワークの特定の場所へのアクセスを特定のホストに許可し、別のホストに対しては禁止できます。図 39-1 では、ルータへの入力に適用されている ACL により、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は拒否されます。

図 39-1 ACL によるネットワークへのトラフィックの制御



ポート ACL

スイッチ上のレイヤ 2 インターフェイスにも ACL を適用できます。PACL は、物理インターフェイスおよび EtherChannel インターフェイス上でサポートされています。

レイヤ 2 インターフェイス上では、次のアクセス リストがサポートされています。

- 送信元アドレスを使用する IP アクセス リスト
- 送信元および宛先のアドレスと任意でプロトコル タイプ情報を使用できる拡張 IP アクセス リスト
- 送信元および宛先の MAC アドレスと任意でプロトコル タイプ情報を使用できる MAC 拡張アクセス リスト

ルータ ACL と同様、スイッチは所定のインターフェイスに設定されている機能に関連付けられている ACL をテストし、パケットが ACL 内のエントリと一致するかどうかによって、パケットの転送を許可または拒否します。図 39-1 の例では、すべてのワークステーションが同じ VLAN 内にある場合、レイヤ 2 の入力に適用されている ACL によって、ホスト A は人事部ネットワークへのアクセスが許可されますが、ホスト B は同じネットワークへのアクセスを拒否されます。

ポート ACL をトランク ポートに適用すると、ACL はそのトランク ポート上のすべての VLAN でトラフィックをフィルタリングします。音声 VLAN があるポートに PACL を適用すると、データ VLAN と音声 VLAN の両方でその ACL によるトラフィックのフィルタリングが行われます。

ポート ACL では、IP アクセス リストを使用して IP トラフィックをフィルタリングでき、MAC アドレスを使用して非 IP トラフィックをフィルタリングできます。同じレイヤ 2 インターフェイス上で IP トラフィックと非 IP トラフィックの両方をフィルタリングするには、そのインターフェイスに IP アクセス リストと MAC アクセス リストの両方を適用します。



(注) 1 つのレイヤ 2 インターフェイスに、IP アクセス リストと MAC アクセス リストのそれぞれを 2 つ以上適用できません。すでに IP アクセス リストまたは MAC アクセス リストが設定されているレイヤ 2 インターフェイスに新しい IP アクセス リストまたは MAC アクセス リストを適用すると、設定済みの ACL が新しい ACL に置き換えられます。

VLAN マップ

VLAN マップを使用すると、VLAN のすべてのトラフィックのアクセスを制御できます。VLAN の内外でルーティングされる、または VLAN 内でブリッジングされるすべてのパケットに対して、スイッチの VLAN マップを適用できます。ルータ ACL と異なり、VLAN マップでは方向（着信または発信）は定義されません。

VLAN マップを設定すると、IP トラフィックのレイヤ 3 アドレスと照合することができます。すべての IP 以外のプロトコルは、VLAN マップの MAC ACL を使用して、MAC アドレスおよび EtherType によってアクセス コントロールされます（IP トラフィックには、VLAN マップの MAC ACL によるアクセス コントロールが行われません）。VLAN マップはスイッチを通過するパケットにだけ適用できます。ハブのホスト間、またはこのスイッチに接続された別のスイッチのホスト間を通過するトラフィックには、VLAN マップを適用できません。

VLAN マップを使用すると、パケットの転送は、マップに指定されたアクションに基づいて許可または拒否されます。図 39-2 に、VLAN マップを適用して、特定タイプのトラフィックを VLAN 10 のホスト A から転送できないように設定する例を示します。

図 39-2 VLAN マップによるトラフィックの制御



ハードウェアおよびソフトウェア ACL のサポート

ここでは、ACL をハードウェア、ソフトウェアのどちらで処理するかを決定する方法について説明します。

- 標準および拡張 ACL の拒否 (deny) 文と一致するフローは、ICMP 到達不能メッセージがディセーブルの場合、ハードウェアでドロップされます。
- 標準 ACL の (permit) 文に一致するフローは、ハードウェアで処理されます。
- ソフトウェアでは、次の ACL タイプはサポートされていません。
 - 標準 Xerox Network Systems (XNS) プロトコル アクセス リスト
 - 拡張 XNS アクセス リスト
 - DECnet アクセス リスト
 - プロトコル タイプコード アクセス リスト
 - 標準 Internet Packet Exchange (IPX) アクセス リスト
 - 拡張 IPX アクセス リスト



(注)

ロギングが必要なパケットは、ソフトウェアで処理されます。ロギング用にパケットのコピーが CPU に送信され、実際のパケットはハードウェアで転送されるので、ロギング対象外のパケットの処理は影響を受けません。

デフォルトでは、アクセス リストによりパケットが拒否されると、ICMP 到達不能メッセージが Catalyst 4500 シリーズ スイッチによって送信されます。

入力インターフェイス上でハードウェア内のアクセス リスト拒否パケットをドロップするには、**no ip unreachable** インターフェイス コンフィギュレーション コマンドを使用して ICMP 到達不能メッセージをディセーブルにする必要があります。The **ip unreachable** コマンドは、デフォルトでイネーブルになっています。



(注)

Cisco IOS Release 12.2(40)SG は、IPv6 トラフィックをルーティングするインターフェイス上での **ip unreachable** のディセーブル化をサポートしません。



(注)

すべてのレイヤ 3 インターフェイスで **no ip unreachable** コマンドを設定する場合、出力 ACL 拒否パケットは、CPU に届きません。

Supervisor Engine II-Plus、Supervisor Engine IV、Supervisor Engine V、および Supervisor Engine V-10GE の TCAM プログラミングと ACL

Catalyst 4500 シリーズ スイッチでの TCAM エントリおよびマスク利用率は、次の要素に基づきます。

- ACL 設定
- スーパーバイザ モデル
- IOS ソフトウェアのバージョン

Supervisor Engine II-Plus-10GE、Supervisor Engine V-10GE、および Catalyst 4948-10GE スイッチの場合、エントリおよびマスク利用率は、IOS ソフトウェア バージョンに関係なく、TCAM リージョンのエントリ数で割った ACL 設定の ACE 数と等しくなります。最適化された TCAM 利用率は必要ありません。

Supervisor Engine II-Plus-TS、Supervisor Engine IV、Supervisor Engine V、および Catalyst 4948 スイッチの場合、IOS ソフトウェア リリースに関係なく、8 つまでのエントリが TCAM の 1 つのマスクを共有します。したがって、TCAM 利用率は、ACL の設定によって変わります。また、各 ACL の設定順によっても変わります。ある ACL が別の ACL の前に設定された場合と、その逆の順で設定された場合では、TCAM 利用率は異なります。同じ ACL 設定を実行コンフィギュレーションにコピーしても、TCAM 利用率が変わります。



(注)

インターフェイスがダウン ステートの場合、TCAM リソースは消費されません。

Supervisor II-Plus-TS、IV、V、および Catalyst 4948 スイッチでの TCAM 利用率は、ACL 設定および IOS ソフトウェア バージョンに従って最適化されます。たとえば、Cisco IOS Release 12.2(31) SGA 以降のリリースでは、マスクを保持するために、独立した ACL エントリの順序を自動的に付け直します。1 つのパケットが 2 つの ACE のうちの 1 つだけと一致できる場合、それらの ACE は順番に依存しません。たとえば、次の 2 つの ACE は順番に依存しません。

```
permit ip host 10.1.1.10 any
permit ip host 10.1.1.20 any
```

最初の ACE と一致するパケットは、2 番めの ACE と一致しません。また、その逆も同じです。これに対して、次の 2 つの ACE は順番に依存します。

```
permit ip host 10.1.1.10 any
permit ip any host 10.1.1.20
```

送信元 IP アドレスが 10.1.1.10、宛先 IP アドレスが 10.1.1.20 のパケットは、両方の ACE に一致することができるため、その順番が問題になります。

展開する前に Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチの TCAM 利用率を見積もるときは、デフォルトの設定から開始します。マスクを共有する ACE をプログラミングするときのダイナミックな性質により、ACL がすでにプログラミングされているときの TCAM 利用率の見積もりは、予想できません。

Cisco IOS Release 12.2(31)SGA 以降では、TCAM が空である場合、IP ACL の TCAM 利用率を見積もることができます。各 IP ACL では、4 つの ACE が自動的に ACL に追加されます。4 つの ACE とは、2 つのスタティック ACE、追加された IP 全拒否 ACE、および追加された全許可 ACE です。したがって、1 つの IP ACL のマスクの最少数は 5 です。残りの ACE で利用されるマスクの数を調べるには、8 つを超える ACE を持つ別々のマスクに対して 1 つを追加して、異なるマスクの数をカウントします。

Supervisor Engine II-Plus-TS、TCAM にプログラミングされる前に、IV、V、および Release 12.2(31)SGA、ACL 前に IOS ソフトウェアを実行する Catalyst 4948 スイッチは自動的に最適化されません。ACL の設定前に同様のマスクを持つ ACE をグループ化すると、マスクの利用率が向上する場合があります。



(注)

Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチで Cisco IOS Release 12.2(31)SGA 以上にアップグレードしたあと、TCAM ACL 利用率は、独立した ACE の再順番付けのために低下することがあります。逆に、Cisco IOS Release 12.2(31)SG 以下にダウングレードすると、TCAM 利用率は上がる場合があります。

TCAM プログラミング アルゴリズム



(注)

Supervisor Engine 6-E では、TCAM プログラミング アルゴリズムは使用できません。

Cisco IOS Release 12.2(25)EWA 以降では、packed と scattered の 2 つの TCAM プログラミング アルゴリズムが Catalyst 4500 および 4900 シリーズ スイッチでサポートされます。packed モード アルゴリズムは、エントリのマスクが一致する場合、同じ 8 エントリ TCAM ブロックのエントリをプログラムします。現在のエントリのマスクが前のエントリのマスクと異なる場合、スイッチ ソフトウェアは、新しい 8 エントリ ブロックにエントリをプログラムします。マスクが変わらない場合、または設定の開始から終了まで ACL で 8 エントリごとにマスクが変わる場合、Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 シリーズ スイッチでは、TCAM が packed モードで完全に利用されます。

scattered モードでは、単一 ACL のエントリは、ACL が完全にプログラムされるまで、異なる 8 エントリ ブロックに分散されます。連続した ACL に最初の ACL と同じマスク パターンがある場合、Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 シリーズ スイッチの TCAM は、完全に利用されます。

Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチでの IP ソース ガードの設定には、scattered モードを推奨します。これは、VLAN 単位の ACL のマスク パターンが、IP ソース ガードに対して設定されたすべてのポートで同じためです。つまり、ARP パケットを許可し、ポート セキュリティが設定されていない場合はレイヤ 2 トラフィックを許可し、32 ビット マスクを持つ特定の送信元 IP アドレスからの IP トラフィックを許可し、不明を拒否し、さらにすべてを許可します。



(注) TCAM プログラミング アルゴリズムは、Cisco IOS Release 12.2(25)EWA または後続のメンテナンス リリースを実行している Supervisor Engine V-10GE および Catalyst 4948-10GE スイッチで設定できます。ただし、Supervisor Engine V-10GE および Catalyst 4948-10GE スイッチで ACL マスクが ACE 間で共有されないため、TCAM 利用率はプログラミング アルゴリズムに関係なく、設定されます。



(注) TCAM プログラミング アルゴリズムは、Supervisor Engine II-Plus-10GE または V-10GE または Cisco IOS Release 12.2(25)SG 以降を実行している Catalyst 4948-10GE スイッチでは設定できません。



(注) TCAM 利用率は、同じ TCAM プログラミング アルゴリズムを引き続き設定したあとには変更しないでください。たとえば、2 回バックされたアクセスリスト ハードウェア エントリの設定は、TCAM 利用率に影響を与えません。ただし、同じ TCAM プログラミング アルゴリズムの連続する設定間に 1 つまたは複数のコマンドが実行された場合、TCAM 利用率は変化することがあります。

TCAM 利用率を変化させるのは、次のような場合です。

- 実行コンフィギュレーションでの ACL または ACE の追加または削除
- ブートフラッシュ、TFTP サーバ、またはコンパクト フラッシュから実行コンフィギュレーションへの ACL 設定のコピーまたは再コピー
- TCAM プログラミング アルゴリズムの変更
- 実行コンフィギュレーションの NVRAM への保存とスイッチのリロード
- Cisco IOS Release 12.2(31)SGA 以上での `access-list hardware region <feature | qos> <input | output> balance percent` コマンドを使用した、TCAM の機能 ACL または QoS リージョンのサイズ変更。
- Cisco IOS Release 12.2(25)EWA に基づくイメージから Cisco IOS Release 12.2(31)SGA に基づくイメージへのアップグレード

これまでに述べたように、ACL をプログラムする際は、エントリおよびマスクの 2 種類のハードウェア リソースが消費されます。これらのリソースのいずれかが使い果たされると、ACL をそれ以上ハードウェアにプログラムすることはできません。

リソースを使い果たした場合は、次の項を参照してください。

- 「プログラミング アルゴリズムの変更」 (P.39-9)
- 「TCAM リージョンのサイズ変更」 (P.39-10)
- 「制御パケットのキャプチャのモード選択」 (P.39-12)

プログラミング アルゴリズムの変更

システム上のマスクが使い果たされても、エントリーは使用できる場合、プログラミング方式を **packed** から **scattered** に変更すると、マスクが使用可能になり、ACL をハードウェアにさらにプログラムできるようになります。



(注)

ACL プログラミング アルゴリズムを変更したり TCAM リージョンのサイズを変更したりすると、すべての ACL が一時的にハードウェアからアンロードされ、新しい TCAM パラメータに従って再ロードされます。再ロードプロセスが終了するまでは ACL は動作できません。

目的は、ACL エントリーごとのマスク数を最小化することにより、TCAM リソースをさらに有効に使用することです。

目的	コマンド
scattered または packed アルゴリズム採用時の TCAM 利用状況を比較	Switch# show platform hardware acl statistics utilization brief
アルゴリズムを packed から scattered に変更	Switch(config)# access-list hardware entries scattered
アルゴリズムを scattered から packed に変更	Switch(config)# access-list hardware entries packed



(注)

access-list hardware entries packed はデフォルト設定になっており、**show running-config** コマンドの出力には表示されません。scattered モードを設定した場合は、出力に「**access-list hardware entries scattered**」の行が表示されます。代わりに packed モードを設定した場合は、コマンド出力に何も表示されません。



(注)

TCAM プログラミング アルゴリズムのデフォルト設定は、**packed** です。

次の出力は、**packed** モードで稼働するスイッチで収集したものです。ACL エントリーの 49% だけをプログラムするために、89% のマスクが必要であることがわかります。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list hardware entries packed
Switch(config)# end
Switch#
01:15:34: %SYS-5-CONFIG_I: Configured from console by console
Switch#
```

```
Switch# show platform hardware acl statistics utilization brief
                Entries/Total(%)  Masks/Total(%)
-----
Input  Acl(PortAndVlan)  2016 / 4096 ( 49)  460 / 512 ( 89)
Input  Acl(PortOrVlan)   6 / 4096 ( 0)    4 / 512 ( 0)
Input  Qos(PortAndVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Input  Qos(PortOrVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Acl(PortAndVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Acl(PortOrVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Qos(PortAndVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Qos(PortOrVlan)  0 / 4096 ( 0)    0 / 512 ( 0)

L4Ops: used 2 out of 64
```

次の出力は、アルゴリズムが **scattered** モードに変更された後に収集したものです。エントリの 49% をプログラムするために必要なマスク数が 49% に減少したことがわかります。



(注)

シャーシ上のすべてのポートで DHCP スヌーピングおよび IP ソース ガードがイネーブルの場合は、**scattered** キーワードを使用する必要があります。

```
Switch# configure terminal
Enter configuration commands, one per line. End with CNTL/Z.
Switch(config)# access-list hardware entries scattered
Switch(config)# end
Switch#
01:39:37: %SYS-5-CONFIG_I: Configured from console by console
Switch#
Switch# show platform hardware acl statistics utilization brief
                Entries/Total(%)  Masks/Total(%)
-----
Input  Acl(PortAndVlan)  2016 / 4096 ( 49)  252 / 512 ( 49)
Input  Acl(PortOrVlan)   6 / 4096 ( 0)    5 / 512 ( 0)
Input  Qos(PortAndVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Input  Qos(PortOrVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Acl(PortAndVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Acl(PortOrVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Qos(PortAndVlan)  0 / 4096 ( 0)    0 / 512 ( 0)
Output Qos(PortOrVlan)  0 / 4096 ( 0)    0 / 512 ( 0)

L4Ops: used 2 out of 64
Switch#
```

TCAM リージョンのサイズ変更

TCAM は、異なる種類のエントリを保持するリージョンに分割されます。TCAM には、入力 ACL、出力 ACL、入力 QoS (Quality Of Service)、出力 QoS の 4 種類があります。それぞれが **PortAndVlan** リージョンと **PortOrVlan** リージョンに分割されます。デフォルトでは、**PortAndVlan** リージョンと **PortOrVlan** リージョンのサイズは同じです。

次の表に、エントリおよびマスク数をサポート対象のスーパーバイザ エンジンごとに示します。スーパーバイザ エンジンのエントリ数およびマスク数は、TCAM の種類ごとです。たとえば、入力機能 TCAM には 16,000 エントリが、出力機能 TCAM には 16,000 エントリがあります。

Supervisor Engine	エントリ	マスク
Supervisor Engine III	16,000	2,000
Supervisor Engine IV	16,000	2,000
Supervisor Engine V	16,000	2,000
Supervisor Engine II-Plus	8,000	1,000
Supervisor Engine II-Plus-TS	8,000	1,000
Supervisor Engine V-10GE	16,000	16,000
Supervisor Engine II-Plus-10GE	TBP	TBP



(注) Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチでのエントリとマスクの比率が 8:1 であるため、マスク用の TCAM スペースは、エントリ用のスペースが消費される前に消費されることがあります。



(注) TCAM タイプのあるリージョンは満杯でも他のリージョンは空いていることがあります。このような場合、リージョンの空きエントリをエントリが必要な他のリージョンに移動することによって、リージョンのサイズを変更できます。リージョンのサイズを変更するには、**access-list hardware region {feature | qos} {input | output} balance** コマンドを使用します。それぞれの TCAM タイプには固有のリージョン バランスがあります。



(注) バランス値を高くすると、PortAndVlan リージョンのエントリが増え、PortOrVlan リージョンのエントリは減ります。バランス値を低くすると、PortAndVlan リージョンのエントリが減り、PortOrVlan リージョンのエントリは増えます。バランス値を 50 にすると、PortAndVlan リージョンと PortOrVlan リージョンの割り当ては同じになります。



(注) 特定の TCAM タイプでは PortAndVlan リージョンと PortOrVlan リージョンのエントリをシフトさせることができます (たとえば、入力 ACL TCAM PortOrVlan リージョンから入力 ACL TCAM PortAndVlan リージョンへ交換できます)。TCAM タイプ間でエントリをシフトすることはできません。

リージョンのサイズ変更による効果があるかどうかを調べるには、**show platform hardware acl statistics utilization brief** コマンドを使用します。

```
Switch# show platform hardware acl statistics utilization brief
```

```
Input  Acl (PortAndVlan)      2346 / 8112 ( 29)      1014 / 1014 (100)
Input  Acl (PortOrVlan)      0 / 8112 ( 0)         0 / 1014 ( 0)
Input  Qos (PortOrVlan)     0 / 8128 ( 0)         0 / 1016 ( 0)
Input  Qos (PortOrVlan)     0 / 8128 ( 0)         0 / 1016 ( 0)
Output Acl (PortOrVlan)     0 / 8112 ( 0)         0 / 1014 ( 0)
Output Acl (PortOrVlan)     0 / 8112 ( 0)         0 / 1014 ( 0)
Output Qos (PortOrVlan)     0 / 8128 ( 0)         0 / 1016 ( 0)
Output Qos (PortOrVlan)     0 / 8128 ( 0)         0 / 1016 ( 0)
```

```
L4Ops: used 2 out of 64
```

上の出力は、入力 ACL PortAndVlan リージョンのマスクがなくなったものの入力 ACL PortOrVlan リージョンに空き容量があり、別の用途で利用できることを示しています。次に、PortAndVlan リージョンにエントリの 75% を割り当て、PortOrVlan リージョンに 25% を割り当てるように入力 ACL TCAM のリージョン バランスを変更する例を示します。

```
Switch# configure terminal
Switch(config)# access-list hardware region feature input balance 75
```

リージョン バランスの調整後は、PortAndVlan リージョンに割り当てられたリソースは増え、PortOrVlan リージョンのリソースは少なくなります。

```
Switch# show platform hardware acl statistics utilization brief

Input  Acl (PortAndVlan)      2346 / 12160 ( 19)      1014 / 1520 ( 67)
Input  Acl (PortOrVlan)      0 / 4064 ( 0)           0 / 508 ( 0)
Input  Qos (PortOrVlan)     0 / 8128 ( 0)           0 / 1016 ( 0)
Input  Qos (PortOrVlan)     0 / 8128 ( 0)           0 / 1016 ( 0)
Output Acl (PortOrVlan)     0 / 8112 ( 0)           0 / 1014 ( 0)
Output Acl (PortOrVlan)     0 / 8112 ( 0)           0 / 1014 ( 0)
Output Qos (PortOrVlan)     0 / 8128 ( 0)           0 / 1016 ( 0)
Output Qos (PortOrVlan)     0 / 8128 ( 0)           0 / 1016 ( 0)
```

```
L4Ops: used 2 out of 64
Switch#
```



(注) デフォルト値に戻すには、**access-list hardware region {feature | qos} {input | output} balance** コマンドの **no** 形式を使用するか、バランスを 50 にします。同様の設定は QoS についても実行できます。

ACL による高 CPU のトラブルシューティング

完全にプログラムされた ACL のエントリに一致するパケットは、ハードウェアで処理されます。ただし、大型 ACL および IPSG の設定は、ACL が完全にプログラムされる前に、Supervisor Engine II-Plus-TS、IV、V、および Catalyst 4948 スイッチの TCAM マスクを消費することがあります。

部分的にプログラムされた ACL のエントリに一致するパケットは、CPU を使用してソフトウェアで処理されます。これにより、CPU 使用率が高くなったりパケットがドロップされることがあります。パケットが高 CPU 使用率のためにドロップされているかどうかを判別するには、次の URL を参照してください。

http://www.cisco.com/en/US/products/hw/switches/ps663/products_tech_note09186a00804cef15.shtml

ACL または IPSG 設定がハードウェアで部分的にプログラミングされている場合、Cisco IOS Release 12.2(31) SGA 以降にアップグレードし、TCAM リージョンのサイズを変更すると、ACL の完全なプログラミングが可能になることがあります。



(注) 使用されていない TCAM エントリの削除を完了するには、何回かの CPU プロセス レビュー サイクルがかかります。これにより、TCAM エントリまたはマスク利用率が 100% かそれに近い場合、一部のパケットがソフトウェアで切り替えられます。

制御パケットのキャプチャのモード選択



(注) Supervisor Engine 6-E は、この機能をサポートしていません。

展開によっては、(CPU を犠牲にして) 制御パケットをグローバルにキャプチャしてソフトウェアで転送するのではなく、ハードウェアでブリッジします。VLAN 単位のキャプチャ モード機能により、Catalyst 4500 シリーズ スイッチは、選択した VLAN でのみ制御パケットをキャプチャし、他のすべての VLAN についてはハードウェアでトラフィックをブリッジできます。

スイッチで VLAN 単位キャプチャ モードを採用すると、内部でグローバル TCAM キャプチャ エントリを部分的にディセーブルにし、スヌーピング機能またはルーティング機能のためにイネーブルになっている VLAN 上の機能固有キャプチャ ACL を付加します (すべての IP キャプチャ エントリ、CGMP、および他の IP 以外のエントリは、引き続きグローバル TCAM を介してキャプチャされます)。この機能は、特定の制御パケットを制御するので、内部 ACL がインストールされた VLAN でだけキャプチャされます。他のすべての VLAN では、制御トラフィックは CPU に転送されるのではなく、ハードウェアでブリッジされます。

VLAN 単位のキャプチャ モードにより、制御パケットにユーザ定義 ACL および QoS ポリサー (ハードウェア内) を適用できます。さらに、CPU に入力する集約制御トラフィックをコントロールプレーン ポリシングの対象にできます。

VLAN 単位キャプチャ モードを使用するとき、次の 4 つのプロトコル グループを VLAN 単位で選択できます。各グループで代行受信されたプロトコルの詳細を参考にしてください。

- IGMP スヌーピング : CGMP、OSPF、IGMP、RIPv2、PIM、224.0.0.1、224.0.0.2、224.0.0.*
- DHCP スヌーピング : クライアントからサーバへ、サーバからクライアントへ、サーバからサーバへ
- ユニキャスト ルーティング : OSPF、RIP v2、224.0.0.1、224.0.0.2、224.0.0.*
- マルチキャスト ルーティング : OSPF、RIP v2、IGMP、PIM、224.0.0.1、224.0.0.2、224.0.0.*

グループの一部には複数の重複 ACE があるため (たとえば、224.0.0.* は、DHCP スヌーピング以外のすべてのグループに存在します)、特定のグループをオンにすると、他のグループからの一部のプロトコルの代行受信もトリガーされます。

VLAN 単位の 4 つのプロトコル グループのプログラミング トリガーは、次のとおりです。

- IGMP スヌーピングは、指定 VLAN でグローバルにイネーブルにする必要があります。
- DHCP スヌーピングは、指定 VLAN でグローバルにイネーブルにする必要があります。
- ユニキャスト ルーティングはイネーブルに、SVI (またはレイヤ 3 物理) インターフェイスはアップになり、IP プロトコル アドレスで設定されている必要があります。これは、SVI インターフェイスがアップになり、プロトコル ファミリアドレスが設定されると、インターフェイスはすぐにルーティング プロセスの一部になるためです。
- マルチキャスト ルーティングはイネーブルにされ、マルチキャスト ルーティング プロトコルの 1 つがインターフェイスで設定されている必要があります (IGMP、PIMv1、PIMv2、MBGP、MOSPF、DVMRP、および IGMP スヌーピング)。

注意事項および制限事項



(注) VLAN 単位キャプチャ モードを設定する前に設定を調べ、目的の VLAN で必要な機能だけがイネーブルになっていることを確認する必要があります。

VLAN 単位キャプチャ モードには、次の注意事項および制限事項が適用されます。

- VLAN 単位キャプチャ モードをイネーブルにすると、ACL/機能 TCAM のエントリがさらに消費されます。

使用可能な TCAM エントリ数は、スーパーバイザ エンジンの種類によって変わります。エントリ / マスク数により、ACL/機能 TCAM の利用率はさらに制限されます。

- ある種の設定では、グローバル キャプチャ モードよりも早く VLAN 単位キャプチャ モードで TCAM リソースを消費することがあります (IP ソース ガードがいくつかのインターフェイス上、またはユーザ設定 PACL 上でイネーブルにされるなど)。

TCAM リージョンのサイズを変更し、設定に基づいて PortAndVlan または PortOrVlan リージョンに対してより多くのエントリを使用可能にできます。これにより、エントリが上限に達する前にハードウェアでエントリをプログラミングできるようになります。TCAM リソースが消費されると、パケットがソフトウェアで転送されます。

- VLAN 単位キャプチャ モードでは、ACL が VLAN またはポート上で制御トラフィックを許可または拒否するように設定できます。

セキュリティ ACL は暗黙の拒否で終了されるため、機能 (プロトコル) が動作するために必要な制御パケットを許可するように ACL が設定されていることを確認する必要があります。ただし、この規則はデフォルトの動作と同じです。

設定

制御パケットのキャプチャ モードを選択するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# conf terminal	コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# [no] access-list hardware capture mode [vlan global]	制御パケットのキャプチャ モードを選択します。 access-list hardware capture mode コマンドの no 形式は、キャプチャ モードをデフォルトのグローバルに戻します。
ステップ 3	Switch(config)# end	イネーブル モードに戻ります。

次に、Catalyst 4500 シリーズ スイッチが、機能がイネーブルになっている VLAN でだけ制御パケットをキャプチャするように設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# access-list hardware capture mode vlan
Switch(config)# end
Switch#
```

次に、Catalyst 4500 シリーズ スイッチが、すべての VLAN で (デフォルト モードのスタティック ACL を使用して) 制御パケットをグローバルにキャプチャするように設定する例を示します。

```
Switch# configure terminal
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# access-list hardware capture mode global
Switch(config)# end
Switch#
```

キャプチャ モードがグローバルからパス管理に変更されると、スタティック CAM エントリは無効になります。これにより、制御パケットが代行受信されずに Catalyst 4500 シリーズ スイッチを通過して CPU に達するウィンドウ (時間) が作成されます。この一時的な状況は、新しい VLAN 単位のキャプチャ エントリがハードウェアにプログラミングされるとすぐに復元されます。

VLAN 単位キャプチャ モードを設定する場合は、個々の機能の show コマンドを調べ、適切な動作になっていることを確認する必要があります。VLAN 単位キャプチャ モードでは、無効になったスタティック CAM エントリは、**show platform hardware acl input entries static all** コマンドの出力で非アクティブ (inactive) として表示されます。たとえば、非アクティブ エントリのヒット数は、無効になって機能がイネーブルになっている VLAN ごとに適用されているので、凍結されたままになります。

CamIndex エントリの種類	アクティブ	ヒット数	CamRegion
50 PermitSharedStp	Y	3344	ControlPktsTwo
51 PermitLoopbackTest	Y	0	ControlPktsTwo
52 PermitProtTunnel	Y	0	ControlPktsTwo
53 CaptureCgmp	N	440	ControlPktsTwo
54 CaptureOspf	N	4321	ControlPktsTwo
55 CaptureIcmp	N	0	ControlPktsTwo

Supervisor Engine 6-E の TCAM プログラミングおよび ACL

Supervisor Engine 6 上の ACL と ACL ベースの機能をプログラムするときは、Mapping Table Entry (MTE)、プロファイル、および TCAM 値/マスク エントリの 3 種類のハードウェア リソースを適用します。これらのリソースのいずれかが使い果たされた場合は、パケットが CPU に送信され、ソフトウェア ベース処理が実行されます。



(注)

Supervisor Engines II-Plus から V-10GE とは異なり、Supervisor Engine 6-E は、使用可能なリソースを自動的に管理します。マスクが Supervisor Engine 6-E で共有されていないため、プログラミング アルゴリズムが 1 つしかありません。リージョンが存在しないため、リージョンのサイズを変更する必要はありません。VLAN 単位のパケット キャプチャ モードは別の実装されているため、ディセーブルにすることはできません。

Supervisor Engine 6-E でリソースが消費されてしまった場合、設定の複雑さを軽減する必要があります。



(注)

インターフェイスがダウン ステートの場合、TCAM リソースは消費されません。

ACL のレイヤ 4 演算

ここでは、レイヤ 4 ポート演算を含む ACL を設定する場合の注意事項および制約事項について説明します。

- 「レイヤ 4 演算の制約事項」 (P.39-16)
- 「レイヤ 4 演算設定時の注意事項」 (P.39-16)
- 「ACL 処理が CPU に与える影響」 (P.39-18)

レイヤ 4 演算の制約事項

次のタイプの演算子を指定できます。いずれも、ハードウェアのレイヤ 4 演算が 1 つ使用されます。

- gt (greater than : より大きい)
- lt (less than : より小さい)
- neq (not equal : 等しくない)
- range (inclusive range : 包含範囲)

Supervisor Engine 2-Plus から V-10GE の場合、1 つの ACL に指定する演算は、6 つまでにしてください。この数を超えると、超過した各演算の影響を受ける ACE が、ハードウェアで複数の ACE に変換されることがあります。また、影響を受ける ACE がソフトウェアで処理される可能性があります。

Supervisor Engine 6-E では、レイヤ 4 演算数の制限は、ACL の種類ごとに異なるうえ、他の要素によっても変わることがあります。該当する要素としては、ACL が着信または発信トラフィックに適用されているかどうか、ACL がセキュリティ ACL なのかそれとも QoS ポリシーの一致条件として使用されているのか、IPv6 ACL が圧縮フローラベル形式を使用してプログラムされているかどうか、などがあります。



(注) IPv6 圧縮フローラベル形式では、レイヤ 2 アドレステーブルを使用して、ACL の各 ACE の IPv6 送信元アドレス部分を圧縮します。フローラベルで解放された余分なスペースは、さらに多くのレイヤ 4 演算をサポートするために使用可能です。この圧縮を使用する場合、IPv6 ACL に、送信元 IPv6 アドレスの下位 48 ビットの一部だけをマスクする ACE を含めることはできません。

一般的に、同じ ACL に含めることができるレイヤ 4 演算の最大数は次のようになります。

Direction	Protocol	Type	Operations
Input	IPv4	Security	16
Input	IPv6 Compressed	Security	16
Input	IPv6 Uncompressed	Security	7
Input	IPv4	QoS	5
Input	IPv6 Compressed	QoS	12
Input	IPv6 Uncompressed	QoS	8
Output	IPv4	Security	17
Output	IPv6 Compressed	Security	17
Output	IPv6 Uncompressed	Security	8
Output	IPv4	QoS	5
Output	IPv6 Compressed	QoS	12
Output	IPv6 Uncompressed	QoS	8



(注) 16 の演算がサポートされる場合、17 番目の演算によって、拡張がトリガーされます。

使用可能なレイヤ 4 演算数を超えた場合、超過した各演算により、影響を受ける ACE がハードウェアで複数 ACE に変換されることがあります。このような変換ミスにより、パケットはソフトウェアの処理のために、CPU に送信されます。

レイヤ 4 演算設定時の注意事項

レイヤ 4 演算子を使用するときは、次の注意事項に従ってください。

- レイヤ 4 演算は、演算子またはオペランドが異なっていると、異なる演算であると見なされます。たとえば、次の ACL には 3 つの異なるレイヤ 4 演算が定義されています。gt 10 と gt 11 は 2 つの異なるレイヤ 4 演算と見なされるためです。

```
... gt 10 permit
... lt 9 deny
... gt 11 deny
```



(注) eq 演算子は、ハードウェアのレイヤ 4 演算を使用しないので、何回でも無制限に使用できません。

- 次の例のように、レイヤ 4 演算は、同じ演算子またはオペランドの組み合わせでも、送信元ポートに適用するか宛先ポートに適用するかによって異なる演算になります。

```
... Src gt 10....
... Dst gt 10
```

以下は、より詳細な例です。

```
access-list 101
... (dst port) gt 10 permit
... (dst port) lt 9 deny
... (dst port) gt 11 deny
... (dst port) neq 6 permit
... (src port) neq 6 deny
... (dst port) gt 10 deny

access-list 102
... (dst port) gt 20 deny
... (src port) lt 9 deny
... (src port) range 11 13 deny
... (dst port) neq 6 permit
```

アクセス リスト 101 および 102 で使用しているレイヤ 4 演算は、次のとおりです。

- アクセス リスト 101 のレイヤ 4 演算 : 5
 - gt 10 permit および gt 10 deny は、どちらも同じ演算です。まったく同じで、どちらも宛先ポートに適用されます。
- アクセス リスト 102 のレイヤ 4 演算 : 4
- レイヤ 4 演算の合計 : 8 (2 つのアクセス リスト間で共有されるため)
 - neq6 permit は 2 つの ACL 間で共有されます。まったく同じで、どちらも同じ宛先ポートに適用されます。
- 使用しているレイヤ 4 演算について説明します。
 - レイヤ 4 演算 1 は、ACL101 から gt 10 permit および gt 10 deny を格納します。
 - レイヤ 4 演算 2 は、ACL101 から lt 9 deny を格納します。
 - レイヤ 4 演算 3 は、ACL101 から gt 11 deny を格納します。
 - レイヤ 4 演算 4 は、ACL101 および 102 から neq 6 permit を格納します。
 - レイヤ 4 演算 5 は、ACL101 から neq 6 deny を格納します。
 - レイヤ 4 演算 6 は、ACL102 から gt 20 deny を格納します。
 - レイヤ 4 演算 7 は、ACL102 から lt 9 deny を格納します。
 - レイヤ 4 演算 8 は、ACL102 から range 11 13 deny を格納します。

ACL 処理が CPU に与える影響

ACL 処理は、次の 2 つの形で CPU に影響を与える可能性があります。

- 一部のパケットで、ハードウェア リソースを使い果たした場合、ACL との照合をソフトウェアで実行する必要があります。
 - Supervisor Engine 2-Plus から V-10GE の場合、「rst ack」と「syn fin rst」の TCP フラグの組み合わせがハードウェアで処理されます。「rst ack」は、キーワード **established** と同等です。他の TCP フラグの組み合わせは、ソフトウェアでサポートされます。
 - Supervisor Engine 6-E の場合、「rst ACK」、「syn fin rst」、「urg」、および「psh」の TCP フラグの組み合わせがハードウェアで処理されます。「rst ack」は、キーワード **established** と同等です。他の TCP フラグの組み合わせは、ソフトウェアでサポートされます。
 - Supervisor Engine 2-Plus から V-10GE の場合、すべての演算をハードウェアで処理するには、ACL に指定するレイヤ 4 演算 (lt、gt、neq、および range) を 6 つまでにする必要があります。7 つ以上のレイヤ 4 演算では、超過分の演算についてハードウェアで複数の ACE に変換しようとしています。ハードウェアで変換できなかった場合、パケットはソフトウェアで処理されます。変換プロセスは、大量のレイヤ 4 演算のある大規模 ACL や、大量の ACL が設定されたスイッチで成功の可能性が低くなります。正確な限度は、設定されている他の ACL の数と、変換対象の ACL によって使用される特定のレイヤ 4 演算によって異なります。eq 演算子は、レイヤ 4 演算を必要としないので、何回でも使用できます。
 - Supervisor Engine 6-E については、「レイヤ 4 演算の制約事項」(P.39-16) を参照してください。
 - ACL 内のレイヤ 4 演算の合計数が 6 に満たない場合、任意の形で処理を分散させることができます。

次に、例を示します。

次のアクセス リストは、すべてハードウェアで処理されます。

```
access-list 104 permit tcp any any established
access-list 105 permit tcp any any rst ack
access-list 107 permit tcp any synfin rst
```

アクセス リスト 104 および 105 は同じです。established は rst および ack の省略形です。

次のアクセス リスト 101 は、すべてソフトウェアで処理されます。

```
access-list 101 permit tcp any any syn
```

次のアクセス リスト 106 は、送信元演算が 4、宛先演算が 2 なので、ハードウェアで処理されます。

```
access-list 106 permit tcp any range 100 120 any range 120 140
access-list 106 permit tcp any range 140 160 any range 180 200
access-list 106 permit tcp any range 200 220
access-list 106 deny tcp any range 220 240
```

次のコードの場合、送信元演算と宛先演算が 3 つずつあるので、3 番目の ACE に対するレイヤ 4 演算は dst lt 1023 をハードウェアで複数の ACE に変換しようとしています。変換できなかった場合、3 番目の ACE はソフトウェアで処理されます。

```
access-list 102 permit tcp any lt 80 any gt 100
access-list 102 permit tcp any range 100 120 any range 120 1024
access-list 102 permit tcp any gt 1024 any lt 1023
```

次のアクセス リスト 103 の場合も同様に、3 番めの ACE は `dst gt 1023` をハードウェアで複数の ACE に変換しようとしています。変換できなかった場合、3 番めの ACE はソフトウェアで処理されます。送信元ポートおよび宛先ポートの演算は同じように見えますが、異なるレイヤ 4 演算と見なされます。

```
access-list 103 permit tcp any lt 80 any lt 80
access-list 103 permit tcp any range 100 120 any range 100 120
access-list 103 permit tcp any gt 1024 any gt 1023
```



(注) `source port lt 80` と `destination port lt 80` は、異なる演算と見なされるので注意してください。

- 一部のパケットはアカウントリング目的で CPU に送信する必要がありますが、アクションはそのままハードウェアで実行されます。たとえば、パケットのログが必要な場合、ログ収集のためにコピーが CPU に送信されますが、転送（またはドロップ）はハードウェアで実行されます。ロギングによって CPU の処理速度が低下しますが、転送速度は影響を受けません。この状況が発生するのは、次のような場合です。
 - `log` キーワードが使用されている場合
 - 出力 ACL でパケットが拒否された場合
 - 入力 ACL でパケットが拒否され、ACL が適用されたインターフェイス上で `ip unreachable` がイネーブルになっている場合（`ip unreachable` は、デフォルトで、すべてのインターフェイス上でイネーブルになっています）

ユニキャスト MAC アドレス フィルタリングの設定

特定の VLAN にある MAC アドレスのユニキャスト トラフィックをすべてブロックするには、次の作業を行います。

コマンド	目的
Switch(config)# <code>mac-address-table static mac_address vlan vlan_ID drop</code>	特定の VLAN にある MAC アドレスのユニキャスト トラフィックをすべてブロックします。 MAC アドレスベースのブロッキングをクリアするには、このコマンドの <code>no</code> 形式を <code>drop</code> キーワードなしで使用します。

次に、VLAN 12 にある MAC アドレス 0050.3e8d.6400 のユニキャスト トラフィックをすべてブロックする例を示します。

```
Router# configure terminal
Router(config)# mac-address-table static 0050.3e8d.6400 vlan 12 drop
```

名前付き MAC 拡張 ACL の設定



(注) ここでの説明は、Supervisor Engine II-Plus から 6-E までに該当します。

■ 名前付き MAC 拡張 ACL の設定

VLAN および物理レイヤ 2 ポートで IP 以外のトラフィックをフィルタリングするには、MAC アドレスおよび名前付き MAC 拡張 ACL を使用します。その手順は、他の名前付き拡張 ACL を設定する場合と同様です。アクセス リストの名前として番号を使用することもできますが、700 ~ 799 の MAC アドレス リスト番号はサポートされません。



(注) 名前付き MAC 拡張 ACL は、レイヤ 3 インターフェイスに適用できません。

mac access-list extended コマンドでサポートされている IP 以外のプロトコルの詳細については、『*Catalyst 4500 Series Switch Cisco IOS Command Reference*』を参照してください。

名前付きの MAC 拡張 ACL を作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# mac access-list extended name	名前を使用して MAC 拡張アクセス リストを定義します。
ステップ 3	Switch(config-ext-macl)# { deny permit } { any host source MAC address source MAC address mask } { any host destination MAC address destination MAC address mask } [protocol-family {appletalk arp-non-ipv4 decnet ipx ipv6 rarp-ipv4 rarp-non-ipv4 vines xns }]	拡張 MAC アクセス リスト コンフィギュレーション モードでは、すべての (any) 送信元 MAC アドレス、マスク付き送信元 MAC アドレス、または特定のホスト (host) 送信元 MAC アドレス、およびすべての (any) 宛先 MAC アドレス、マスク付き宛先 MAC アドレス、または特定の宛先 MAC アドレスに、 permit または deny を指定します。 (任意) • [protocol-family {appletalk arp-non-ipv4 decnet ipx ipv6 rarp-ipv4 rarp-non-ipv4 vines xns }] (注) Supervisor Engine 6-E では、IPv6 パケットは、レイヤ 2 ACL ルックアップ キーを生成せず、さらに IPv4 パケットが Supervisor Engines II-Plus から V-10GE の MAC ACL と一致しない場合と同様に、IPv6 パケットは MAC ACL に一致しません。したがって、 ipv6 キーワードは Supervisor Engine II-Plus ~ V-10GE の MAC ACL では使用可能ですが、Supervisor Engine 6-E では使用できません。
ステップ 4	Switch(config-ext-macl)# end	特権 EXEC モードに戻ります。
ステップ 5	Switch# show access-lists [<i>number</i> <i>name</i>]	アクセス リストの設定を表示します。
ステップ 6	Switch(config)# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

ACL 全体を削除するには、**no mac access-list extended name** グローバル コンフィギュレーション コマンドを使用します。名前付き MAC 拡張 ACL から ACE を個別に削除することもできます。

次に、DECnet Phase IV という EtherType のトラフィックだけを拒否し、その他のすべてのタイプのトラフィックを許可する、**macl** という名前のアクセス リストを作成、表示する例を示します。

```
Switch(config)# mac access-list extended macl
Switch(config-ext-macl)# deny any any decnet-iv (old) protocol-family decnet (new)
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch # show access-lists
Extended MAC access list macl
    deny any any decnet-iv (old) protocol-family decnet (new)
```

```
permit any any
```

アクセスリストで ACE の設定時にハードウェア統計をイネーブルまたはディセーブルにするには、次のコマンドを入力します。

```
Switch# config t
Enter configuration commands, one per line.End with CNTL/Z.
Switch(config)# mac access-list extended macl
Switch(config-ext-nacl)# hardware statistics
Switch(config-ext-nacl)# end
```

名前付き IPv6 ACL の設定



(注) この項は、Supervisor Engine 6-E にのみ適用されます。

レイヤ 3 インターフェイス上のユニキャスト、マルチキャスト、およびブロードキャスト IPv6 トラフィックをフィルタリングするために、Supervisor Engine 6-E は、ハードウェアベースの IPv6 ACL もサポートします。このようなアクセスリストは、IPv6 アドレスで設定されたレイヤ 3 インターフェイス上にものみ設定できます。

名前付き IPv6 ACL を作成するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# ipv6 access-list name	名前を使用して IPv6 アクセス リストを定義します。
ステップ 3	Switch(config-ipv6-acl)# { deny permit } { any proto } { host ipv6-addr ipv6-prefix } host ipv6-addr ipv6-prefix }	各 IPv6 ACE を指定します。 (注) このステップは、ACL の複数 ACE を定義するときに繰り返すことがあります。
ステップ 4	Switch(config-ipv6-acl)# hardware statistics	(任意) IPv6 ACL のハードウェア統計をイネーブルにします。
ステップ 5	Switch(config-ipv6-acl)# end	特権 EXEC モードに戻ります。
ステップ 6	Switch# show ipv6 access-list	IPv6 アクセス リストの設定を表示します。

IPv6 ACL を削除するには、**no ipv6 access-list name** グローバル コンフィギュレーション コマンドを使用します。IPv6 アクセス リストから個々の ACE を削除することもできます。

次の例では、1 つの特定の送信元/宛先アドレスを持つ 1 つの IPv6 トラフィックだけを拒否するが、他のすべての種類の IPv6 トラフィックは許可する *v6test* という名前の IPv6 アクセス リストを作成および表示する方法を示します。

```
Switch(config)# ipv6 access-list v6test
Switch(config-ipv6-acl)# deny ipv6 host 2020::10 host 2040::10
Switch(config-ipv6-acl)# permit any any
Switch(config-ipv6-acl)# end
Switch# show ipv6 access-list
IPv6 access list v6test
  deny ipv6 host 2020::10 host 2040::10 sequence 10
  permit ipv6 any any sequence 20
```

アクセスリスト ACE の設定時ハードウェア統計をイネーブルにするには、次のコマンドを入力します。

■ レイヤ 3 インターフェイスへの IPv6 ACL の適用

```
Switch(config)# ipv6 access-list v6test
Switch(config-ipv6-acl)# hardware statistics
Switch(config-ipv6-acl)# end
```



(注) ハードウェア統計は、デフォルトではディセーブルになっています。



(注) ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

次の条件は、RACL の故障の原因となる場合があります（回避策はありません）。

- ACL は、インターフェイスの出力方向に適用されます。
- IPv6 ACL には、ICMP オプションフィールドで一致する Ace が含まれています（ICMP タイプまたは ICMP コード）。

このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

```
IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

レイヤ 3 インターフェイスへの IPv6 ACL の適用

IPv6 ACL をレイヤ 3 インターフェイスに適用するには、次の作業を実行します。

	コマンド	目的
ステップ 1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# interface interface-type slot/interface	設定するインターフェイスを指定します。 (注) <i>interface-type</i> は、レイヤ 3 インターフェイスである必要があります。
ステップ 3	Switch(config-if)# ipv6 traffic-filter ipv6-acl {in out}	IPv6 ACL をレイヤ 3 インターフェイスに適用します。



(注) IPv6 ACL は、Supervisor VI-E 上のハードウェアでのみサポートされます。



(注) IPv6 ACL は、レイヤ 3 インターフェイスでのみサポートされます。

次の例は、拡張名前付き IPv6 ACL *simple-ipv6-acl* を SVI 300 ルーテッド入力トラフィックに適用します。

```
Switch# configure terminal
Switch(config)# interface vlan 300
Switch(config-if)# ipv6 traffic-filter simple-ipv6-acl in
```



(注) ICMP オプションで一致する Ace を持つ出力 IPv6 ACL は、スイッチ上で失敗します。

次の条件は、RACL の故障の原因となる場合があります (回避策はありません)。

- ACL は、インターフェイスの出力方向に適用されます。
- IPv6 ACL には、ICMP オプション フィールドで一致する Ace が含まれています (ICMP タイプまたは ICMP コード)。

このような機能しない RACL の例を 2 つ示します。

```
IPv6 access list a1
  permit icmp any any nd-ns sequence 10
  deny ipv6 any any sequence 20

IPv6 access list a2
  permit icmp 2020::/96 any nd-ns sequence 10
  deny ipv6 any any sequence 20
```

VLAN マップの設定

ここでは、次の内容について説明します。

- 「VLAN マップの設定時の注意事項」(P.39-24)
- 「VLAN マップの作成および削除」(P.39-25)
- 「VLAN への VLAN マップの適用」(P.39-27)
- 「ネットワークでの VLAN マップの使用法」(P.39-28)

ここでは、VLAN マップを設定する方法について説明します。この方法は、VLAN 内でフィルタリングを制御する唯一の方法です。VLAN マップには方向の指定がありません。VLAN マップを使用して、特定の方向のトラフィックをフィルタリングするには、特定の送信元または宛先アドレスが指定された ACL を追加する必要があります。VLAN マップ内に該当パケット タイプ (IP または MAC) に対する `match` 句がある場合、デフォルトでは、マップ内のどのエントリにも一致しないパケットはドロップされます。該当パケット タイプに対する `match` コマンドがない場合、デフォルトでは、パケットが転送されます。

VLAN マップを作成して、1 つまたは複数の VLAN に適用するには、次の作業を行います。

- ステップ 1** VLAN に適用する標準 IP ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。
- ステップ 2** VLAN ACL マップ エントリを作成するには、`vlan access-map` グローバル コンフィギュレーション コマンドを入力します。
- ステップ 3** アクセス マップ コンフィギュレーション モードでは、`action` として、`forward` (デフォルト) または `drop` を任意で入力できます。また、`match` コマンドを入力して、既知の MAC アドレスだけが格納された IP パケットまたは IP 以外のパケットを指定したり、1 つまたは複数の ACL (標準または拡張) とパケットを照合することもできます。`match` コマンドが指定されていない場合は、すべてのパケットにアクションが適用されます。`match` コマンドを使用すると、パケットを複数の ACL と照合できます。指定された ACL のいずれかにパケットが一致すると、アクションが適用されます。



(注) 該当パケット タイプ (IP または MAC) に対する `match` 句が VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトではパケットがドロップされます。該当タイプのパケットに対する `match` コマンドが VLAN マップ内になく、それに対するアクションが指定されていない場合、パケットは転送されます。

ステップ 4 VLAN マップを 1 つまたは複数の VLAN に適用するには、`vlan filter` インターフェイス コンフィギュレーション コマンドを使用します。



(注) レイヤ 2 インターフェイスに ACL (PACL) が適用されているスイッチ上の VLAN には、VLAN マップを適用できません。

VLAN マップの設定時の注意事項

VLAN マップを設定する際は、次の注意事項に従ってください。

- VLAN マップは IPv4 ARP パケットをフィルタリングしません。
- ルーテッド VLAN インターフェイス (入力または出力) でトラフィックを拒否するように設定されたルータ ACL が存在せず、VLAN マップが設定されていない場合は、すべてのトラフィックが許可されます。
- 各 VLAN マップは一連のエントリで構成されます。VLAN マップのエントリの順序は重要です。スイッチに着信したパケットは、VLAN マップの最初のエントリに対してテストされます。一致した場合は、VLAN マップのその部分に指定されたアクションが実行されます。一致しなかった場合、パケットはマップ内の次のエントリに対してテストされます。
- 該当パケット タイプ (IP または MAC) に対する `match` 句が VLAN マップに 1 つまたは複数ある場合でも、パケットがそれらの `match` 句に一致しない場合、デフォルトではパケットがドロップされます。該当パケット タイプに対する `match` 句が VLAN マップ内にない場合、デフォルトではパケットが転送されます。
- 多数の ACL が設定されている場合は、システムの起動に時間がかかることがあります。

VLAN マップの作成および削除

各 VLAN マップは順番に並べられた一連のエントリで構成されます。VLAN マップ エントリを作成、追加、または削除するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	Switch(config)# vlan access-map <i>name</i> [<i>number</i>]	VLAN マップを作成し、名前と、任意で番号を付けます。番号は、マップ内のエントリのシーケンス番号です。 同じ名前の VLAN マップを作成すると、10 ずつ増加する番号が順に割り当てられます。マップを変更または削除するときは、該当するマップ エントリの番号を入力できます。 このコマンドを入力すると、アクセスマップ コンフィギュレーション モードに変わります。
ステップ3	Switch(config-access-map)# action { drop forward }	(任意) マップ エントリに対するアクションを設定します。デフォルトは転送 (forward) です。
ステップ4	Switch(config-access-map)# match { ip mac } address { <i>name</i> <i>number</i> } [<i>name</i> <i>number</i>]	1 つまたは複数の標準または拡張アクセス リストに対してパケットを比較します (IP または MAC アドレスを使用)。パケットの比較は、対応するプロトコル タイプのアクセス リストに対してだけ行われます。IP パケットは、標準または拡張 IP アクセス リストに対して比較されます。IP 以外のパケットは、名前付き MAC 拡張アクセス リストに対してだけ比較されます。match コマンドが指定されていない場合は、すべてのパケットにアクションが実行されます。
ステップ5	Switch(config-access-map)# end	グローバル コンフィギュレーション モードに戻ります。
ステップ6	Switch(config)# show running-config	アクセス リストの設定を表示します。
ステップ7	Switch(config)# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。

マップを削除するには、**no vlan access-map name** グローバル コンフィギュレーション コマンドを使用します。マップ内の単一のシーケンス エントリを削除するには、**no vlan access-map name number** グローバル コンフィギュレーション コマンドを使用します。デフォルトのアクションである転送を行うには、**no action** アクセスマップ コンフィギュレーション コマンドを使用します。

VLAN マップでは、特定の **permit** または **deny** キーワードは使用されません。VLAN マップを使用してパケットを拒否するには、パケットと比較する ACL を作成して、アクションをドロップに設定します。ACL に **permit** を指定すると、一致と見なされます。ACL 内の **deny** は、一致しないという意味です。

ACL および VLAN マップの例

次に、特定の目的のための ACL および VLAN マップを作成する例を示します。

例 1

ここでは、パケットを拒否する ACL および VLAN マップを作成する例を示します。最初のマップでは、ip1 ACL (TCP パケット) に一致するすべてのパケットがドロップされます。最初に、すべての TCP パケットを許可し、それ以外のパケットをすべて拒否する ip1 ACL を作成します。VLAN マップには IP パケットに対する match 句が存在するため、デフォルトのアクションでは、どの match 句とも一致しない IP パケットがすべてドロップされます。

```
Switch(config)# ip access-list extended ip1
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
```

```
Switch(config)# vlan access-map map_1 10
Switch(config-access-map)# match ip address ip1
Switch(config-access-map)# action drop
```

次に、パケットを許可する VLAN マップを作成する例を示します。ACL ip2 は UDP パケットを許可します。ip2 ACL と一致するすべてのパケットが転送されます。

```
Switch(config)# ip access-list extended ip2
Switch(config-ext-nacl)# permit udp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map_1 20
Switch(config-access-map)# match ip address ip2
Switch(config-access-map)# action forward
```

このマップでは、これ以前のどの ACL とも一致しないすべての IP パケット (TCP でも UDP でもないパケット) がドロップされます。

例 2

次の例の VLAN マップでは、デフォルトで IP パケットがドロップされ、MAC パケットが転送されるように設定されています。標準の ACL 101、名前付き拡張アクセス リスト **igmp-match** および **tcp-match** を適用して、次のように VLAN マップを設定します。

- すべての UDP パケットが転送されます。
- すべての IGMP パケットがドロップされます。
- すべての TCP パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- すべての非 IP パケットが転送されます。

```
Switch(config)# access-list 101 permit udp any any
Switch(config)# ip access-list extended igmp-match
Switch(config-ext-nacl)# permit igmp any any
Switch(config)# ip access-list extended tcp-match
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-ip-default 10
Switch(config-access-map)# match ip address 101
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 20
Switch(config-access-map)# match ip address igmp-match
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-ip-default 30
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
```

例 3

次の例の VLAN マップでは、デフォルトで MAC パケットがドロップされ、IP パケットが転送されるように設定されています。MAC 拡張アクセス リスト **good-hosts** および **good-protocols** を適用して、次のように VLAN マップを設定します。

- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。

- DECnet または Virtual Integrated Network Service (VINES) プロトコル ファミリの MAC パケットが転送されます。
- その他のすべての非 IP パケットがドロップされます。
- すべての IP パケットが転送されます。

```
Switch(config)# mac access-list extended good-hosts
Switch(config-ext-macl)# permit host 000.0c00.0111 any
Switch(config-ext-macl)# permit host 000.0c00.0211 any
Switch(config-ext-nacl)# exit
Switch(config)# mac access-list extended good-protocols
Switch(config-ext-macl)# permit any any protocol-family decnet
Switch(config-ext-macl)# permit any any protocol-family vines
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map drop-mac-default 10
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-mac-default 20
Switch(config-access-map)# match mac address good-protocols
Switch(config-access-map)# action forward
```

例 4

次の例の VLAN マップでは、すべてのパケット (IP および IP 以外) がドロップされるように設定されています。アクセス リスト **tcp-match** および **good-hosts** を適用して、次のように VLAN マップを設定します。

- すべての TCP パケットが転送されます。
- ホスト 0000.0c00.0111 および 0000.0c00.0211 からの MAC パケットが転送されます。
- その他のすべての IP パケットがドロップされます。
- その他のすべての MAC パケットがドロップされます。

```
Switch(config)# vlan access-map drop-all-default 10
Switch(config-access-map)# match ip address tcp-match
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
Switch(config)# vlan access-map drop-all-default 20
Switch(config-access-map)# match mac address good-hosts
Switch(config-access-map)# action forward
```

VLAN への VLAN マップの適用

1 つの VLAN マップを 1 つまたは複数の VLAN に適用するには、次の作業を行います。

	コマンド	目的
ステップ1	Switch# configure terminal	グローバル コンフィギュレーション モードを開始します。
ステップ2	Switch(config)# vlan filter mapname vlan-list list	VLAN マップを 1 つまたは複数の VLAN に適用します。 list には単一の VLAN ID (22)、連続した範囲 (10 ~ 22)、または VLAN ID のストリング (12, 22, 30) を指定できます。カンマやハイフンの前後にスペースを挿入することもできます。

	コマンド	目的
ステップ 3	Switch(config)# show running-config	アクセス リストの設定を表示します。
ステップ 4	cSwitch(config)# copy running-config startup-config	(任意) コンフィギュレーション ファイルに設定を保存します。



(注) レイヤ 2 インターフェイスに ACL (PACL) が適用されているスイッチ上の VLAN には、VLAN マップを適用できません。

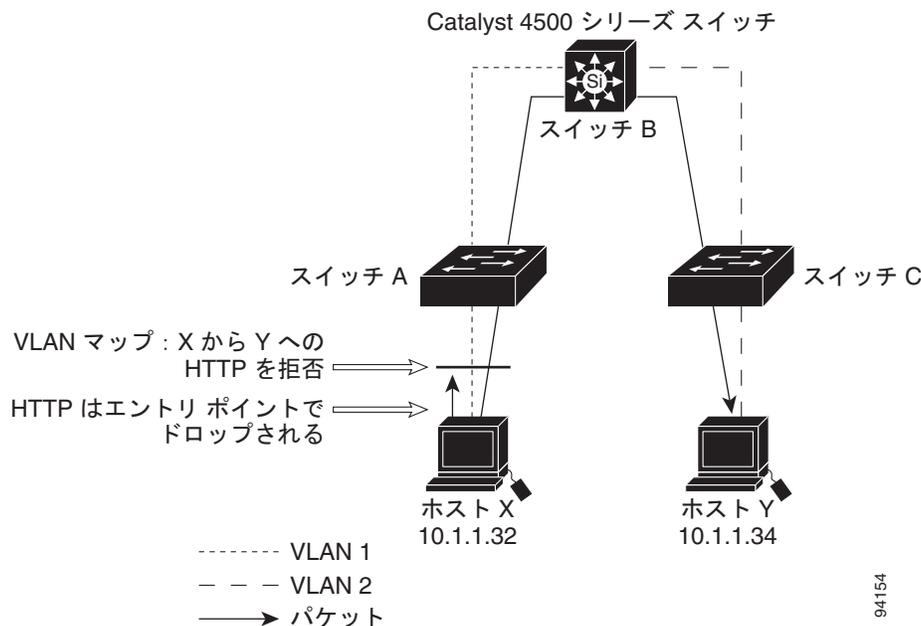
次に、VLAN マップ 1 を VLAN 20 ~ 22 に適用する例を示します。

```
Switch(config)# vlan filter map 1 vlan-list 20-22
```

ネットワークでの VLAN マップの使用法

図 39-3 に、一般的なワイヤリングクローゼットの構成を示します。ホスト X およびホスト Y は異なる VLAN 内にあり、ワイヤリングクローゼットスイッチ A およびスイッチ C に接続されています。ホスト X からホスト Y へのトラフィックは、スイッチ B によってルーティングされます。ホスト X からホスト Y へのトラフィックは、トラフィックのエントリ ポイントであるスイッチ A でアクセス コントロールできます。次の構成では、スイッチは VLAN マップと QoS 分類 ACL をサポートします。

図 39-3 ワイヤリングクローゼットの設定



たとえば、HTTP トラフィックをホスト X からホスト Y へスイッチングしない場合は、スイッチ A に VLAN マップを適用し、ホスト X (IP アドレス 10.1.1.32) からホスト Y (IP アドレス 10.1.1.34) への HTTP トラフィックがスイッチ B にブリッジングされずに、すべてスイッチ A でドロップされるようにすることもできます。このように設定するには、次の手順を実行します。

最初に、HTTP ポートですべての TCP トラフィックを許可（一致）する IP アクセス リスト `http` を定義します。

```
Switch(config)# ip access-list extended http
Switch(config-ext-nacl)# permit tcp host 10.1.1.32 host 10.1.1.34 eq www
Switch(config-ext-nacl)# exit
```

次に、VLAN アクセス マップ `map2` を作成し、`http` アクセス リストと一致するトラフィックがドロップされ、その他すべての IP トラフィックが転送されるようにします。

```
Switch(config)# vlan access-map map2 10
Switch(config-access-map)# match ip address http
Switch(config-access-map)# action drop
Switch(config-access-map)# exit
```

```
Switch(config)# ip access-list extended match_all
Switch(config-ext-nacl)# permit ip any any
Switch(config-ext-nacl)# exit
Switch(config)# vlan access-map map2 20
Switch(config-access-map)# match ip address match_all
Switch(config-access-map)# action forward
```

次に、VLAN アクセス マップ `map2` を VLAN 1 に適用します。

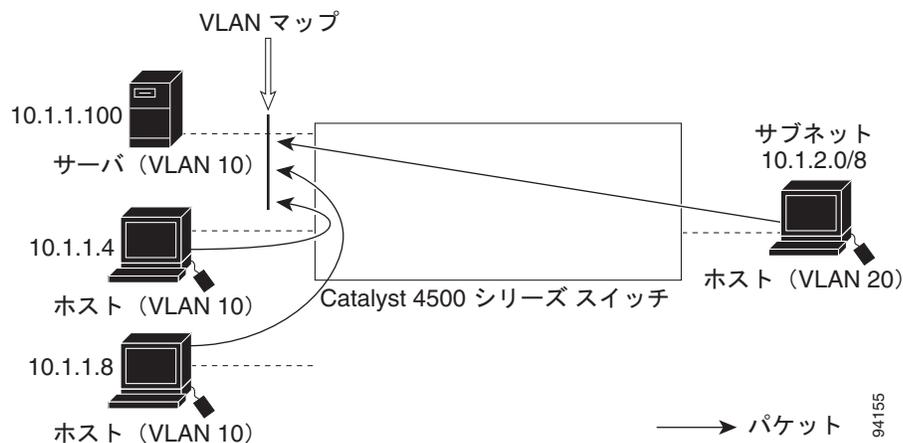
```
Switch(config)# vlan filter map2 vlan 1
```

別の VLAN にあるサーバへのアクセスの拒否

図 39-4 に、別の VLAN にあるサーバへのアクセスを制限する方法を示します。この例では、VLAN 10 内のサーバ 10.1.1.100 に対しては、次のようにアクセスが制限されています。

- VLAN 20 内のサブネット 10.1.2.0/8 にあるホストのアクセスを禁止します。
- VLAN 10 内のホスト 10.1.1.4 および 10.1.1.8 のアクセスを禁止します。

図 39-4 他 VLAN 上のサーバへのアクセス拒否



この手順では、別の VLAN にあるサーバへのアクセスを拒否するように VLAN マップを使用して ACL を設定します。VLAN マップ `SERVER_1_ACL` は、サブネット 10.1.2.0/8 内のホスト、ホスト 10.1.1.4、およびホスト 10.1.1.8 のアクセスを拒否します。一方、その他すべての IP トラフィックを許可します。ステップ 3 では、VLAN 10 に VLAN マップ `SERVER_1` を適用します。

このように設定するには次の手順を実行します。

ステップ 1 対応するパケットと照合し、許可する IP ACL を定義します。

```
Switch(config)# ip access-list extended SERVER1_ACL
Switch(config-ext-nacl)# permit ip 10.1.2.0 0.0.0.255 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.4 host 10.1.1.100
Switch(config-ext-nacl)# permit ip host 10.1.1.8 host 10.1.1.100
Switch(config-ext-nacl)# exit
```

ステップ 2 SERVER1_ACL と一致する IP パケットをドロップして、一致しない IP パケットを転送するこの ACL を使用して、VLAN マップを定義します。

```
Switch(config)# vlan access-map SERVER1_MAP
Switch(config-access-map)# match ip address SERVER1_ACL
Switch(config-access-map)# action drop
Switch(config)# vlan access-map SERVER1_MAP 20
Switch(config-access-map)# action forward
Switch(config-access-map)# exit
```

ステップ 3 VLAN 10 に VLAN マップを適用します。

```
Switch(config)# vlan filter SERVER1_MAP vlan-list 10.
```

VLAN アクセス マップ情報の表示

VLAN アクセス マップまたは VLAN フィルタに関する情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# show vlan access-map [mapname]	すべての VLAN アクセス マップまたは指定されたアクセス マップに関する情報を表示します。
Switch# show vlan filter [access-map name vlan vlan-id]	すべての VLAN フィルタに関する情報、または指定された VLAN や VLAN アクセス マップに関する情報を表示します。

次に、**show vlan access-map** コマンドの出力例を示します。

```
Switch# show vlan access-map
Vlan access-map "map_1" 10
  Match clauses:
    ip address: ip1
  Action:
    drop
Vlan access-map "map_1" 20
  Match clauses:
    mac address: mac1
  Action:
    forward
Vlan access-map "map_1" 30
  Match clauses:
  Action:
    drop
```



(注) シーケンス 30 には `match` コマンドがありません。すべてのパケット (IP および IP 以外) はこれと照合されてドロップされます。

次に、`show vlan filter` コマンドの出力例を示します。

```
Switch# show vlan filter
VLAN Map map_1 is filtering VLANs:
 20-22
```

ルータ ACL を VLAN マップと組み合わせて使用する方法

該当タイプ (IP または MAC) のパケットに対する `match` コマンドが VLAN マップにある場合でも、パケットがそのタイプに一致しない場合、デフォルトでは、パケットがドロップされます。VLAN マップ内に `match` コマンドがなく、アクションが指定されていない場合、どの VLAN マップ エントリとも一致しないパケットは転送されます。



(注) 1 つのスイッチ上で、VLAN マップまたは入力ルータ ACL を組み合わせて使用することはできません。

ルータ ACL を VLAN マップと併用する場合の注意事項

ルータ ACL と VLAN マップを同じ VLAN 上に設定する必要がある場合は、次の注意事項に従ってください。

スイッチ ハードウェアは、方向 (入力および出力) ごとに、1 回の検索を実行するので、ルータ ACL および VLAN マップを同じ VLAN に設定する場合は、これらを統合する必要があります。ルータ ACL を VLAN マップと統合すると、ACE の数が急激に増加することがあります。

できるだけ末尾のデフォルト アクションを除くすべてのエントリのアクションが同一となるように、ACL を記述します。次のいずれかの形式を使用して ACL を記述します。

```
permit...
permit...
permit...
deny ip any any
```

または

```
deny...
deny...
deny...
permit ip any any
```

ACL 内で複数の許可または拒否アクションを定義する場合は、それぞれのアクション タイプをまとめて、エントリ数を削減します。

IP ACE とレイヤ 4 情報を含む TCP/UDP/ICMP ACE が両方とも ACL 内に存在し、`full-flow` モードを指定する必要があるときは、レイヤ 4 ACE をリストの末尾に配置します。この結果、IP アドレスに基づくトラフィックのフィルタリングが優先されます。

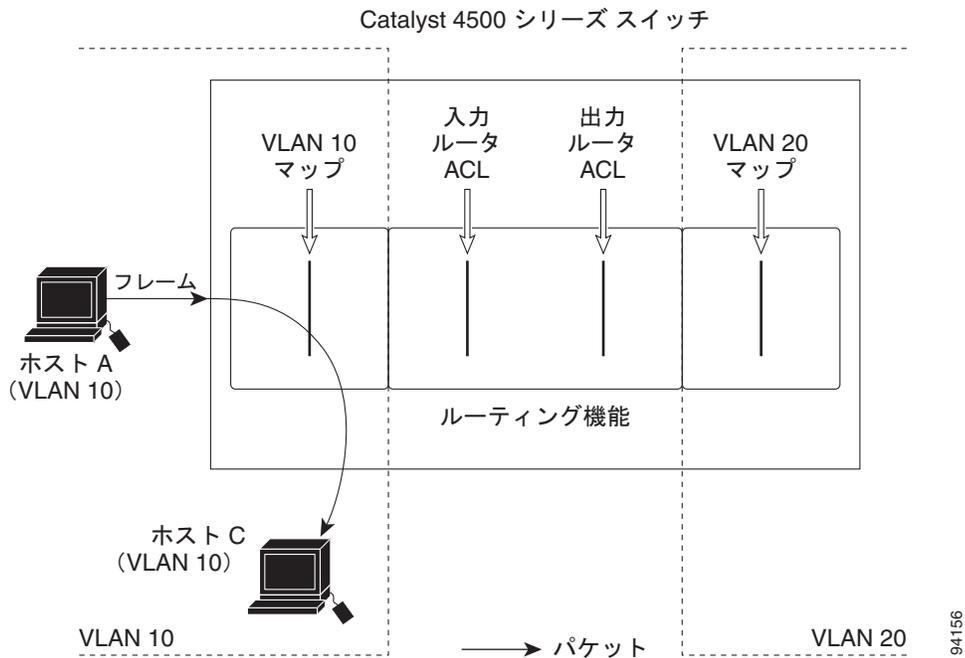
VLAN に適用されるルータ ACL と VLAN マップの例

以下の例では、ルータ ACL および VLAN マップを VLAN に適用して、スイッチド パケット、ブリッジド パケット、ルーテッド パケット、およびマルチキャスト パケットへのアクセスを制御します。次の図では、それぞれの宛先に転送されるパケットを示します。ただし、パケットのパスが VLAN マップや ACL を示す回線と交差するポイントごとに、パケットを転送しないでドロップすることもできます。

ACL およびスイッチド パケット

図 39-5 に、VLAN 内でスイッチングされるパケットを ACL が処理する方法を示します。VLAN 内でスイッチングされるパケットは、ルータ ACL では処理されません。

図 39-5 スイッチド パケットへの ACL の適用

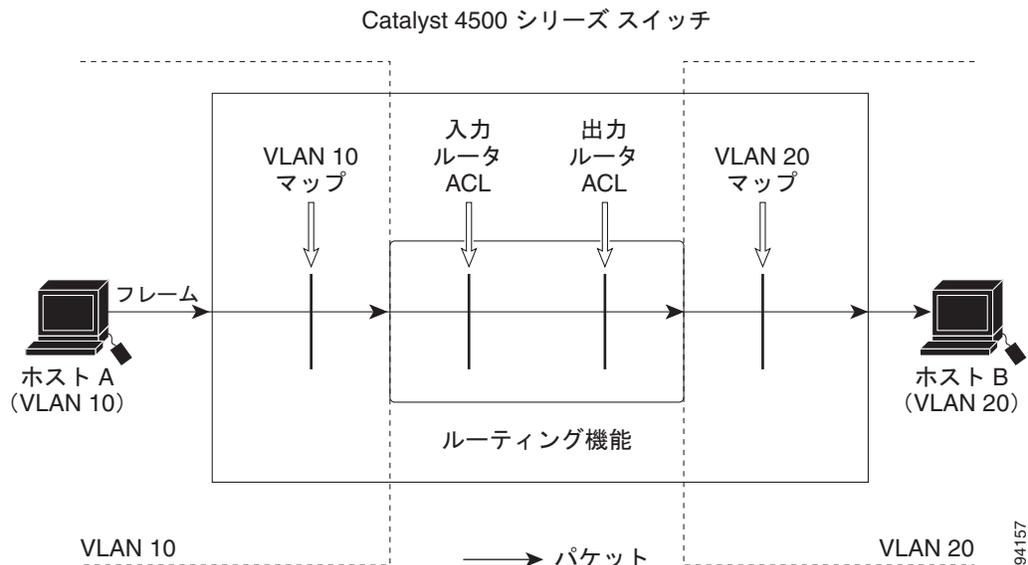


ACL およびルーテッド パケット

図 39-6 に、ルーテッド パケットに ACL を適用する方法を示します。ルーテッド パケットの場合、ACL は次の順番で適用されます。

1. 入力 VLAN の VLAN マップ
2. 入力ルータ ACL
3. 出力ルータ ACL
4. 出力 VLAN の VLAN マップ

図 39-6 ルーテッド packets への ACL の適用



PACL の設定

ここでは、PACL を設定する方法について説明します。PACL は、レイヤ 2 インターフェイス上のフィルタリングを制御するのに使用されます。PACL は、レイヤ 3 情報、レイヤ 4 ヘッダー情報または IP 以外のレイヤ 2 情報に基づいて、レイヤ 2 インターフェイスのトラフィックをフィルタリングできます。

ここでは、次の内容について説明します。

- 「PACL の作成」 (P.39-33)
- 「PACL 設定時の注意事項」 (P.39-34)
- 「レイヤ 2 インターフェイスの IP ACL および MAC ACL の設定」 (P.39-34)
- 「アクセス グループ モードを PACL と併用する方法」 (P.39-35)
- 「レイヤ 2 インターフェイス上でのアクセス グループ モードの設定」 (P.39-35)
- 「レイヤ 2 インターフェイスへの ACL の適用」 (P.39-36)
- 「レイヤ 2 インターフェイス上の ACL 設定の表示」 (P.39-36)

PACL の作成

PACL を作成して、1 つまたは複数のインターフェイスに適用するには、次の作業を行います。

-
- ステップ 1** インターフェイスに適用する標準 IP ACL または拡張 IP ACL、または名前付き MAC 拡張 ACL を作成します。
- ステップ 2** `ip access-group` または `mac access-group interface` コマンドを使用して、IP ACL または MAC ACL を 1 つまたは複数のレイヤ 2 インターフェイスに適用します。
-

PACL 設定時の注意事項

PACL を設定する場合は、次の注意事項に留意してください。

- 各方向に対して同一のレイヤ 2 インターフェイスに適用できるのは、多くても 1 つの IP アクセスリストと 1 つの MAC アクセスリストだけです。
- IP アクセスリストは、IP パケットだけをフィルタリングします。MAC アクセスリストは、IP 以外のパケットだけをフィルタリングします。
- PACL の一部として設定できる ACL と ACE の数は、スイッチのハードウェア リソースにより制限されます。これらのハードウェア リソースは、システムに設定された各 ACL 機能 (RAACL、VAACL など) で共有されます。ハードウェアに PACL をプログラミングするのに十分なハードウェア リソースがない場合、入力 PACL と出力 PACL のアクションが異なります。
 - 入力 PACL では、一部のパケットがソフトウェア転送のために CPU に転送されます。
 - 出力 PACL では、PACL がポート上でディセーブルに設定されます。
- 次の制限は、出力 PACL だけに関連します。
 - ハードウェアに PACL をプログラミングするのに十分なハードウェア リソースがない場合、出力 PACL はポートに適用されず、警告メッセージが表示されます。
 - 出力 PACL がレイヤ 2 ポート上に設定されている場合、レイヤ 2 ポートが属する VLAN に VAACL またはルータ ACL は設定できません。
レイヤ 2 ポートが属する VLAN 上に VAACL またはルータ ACL が設定されている場合、出力 PACL はレイヤ 2 ポート上に設定できません。つまり、PACL と VLAN ベースの ACL (VAACL およびルータ ACL) は、レイヤ 2 ポート上では相互に排他的です。
- 出力 IP ACL と MAC ACL ではロギングがサポートされていませんが、入力 IP ACL のロギングオプションはサポートされています。
- アクセス グループ モードを使用して、その他の ACL との PACL の対話形式を変更できます。シスコのプラットフォームにおいて動作の一貫性を保つためには、デフォルトのアクセス グループ モードを使用します。

レイヤ 2 インターフェイスの IP ACL および MAC ACL の設定

レイヤ 2 物理インターフェイスに適用できるのは、IP ACL または MAC ACL だけです。(番号付き、名前付き) 標準 IP ACL、(番号付き、名前付き) 拡張 IP ACL、および名前付き拡張 MAC ACL もサポートされています。

レイヤ 2 インターフェイス上に IP ACL または MAC ACL を適用するには、次の作業を行います。

	コマンド	目的
ステップ 1	Switch# <code>configure t</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# <code>interface interface</code>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# <code>[no] {ip mac} access-group {name number} in out</code>	レイヤ 2 インターフェイス上にアクセス グループ モードを設定します。 no プレフィックスは、レイヤ 2 インターフェイスから IP ACL または MAC ACL を削除します。
ステップ 4	Switch(config)# <code>show running-config</code>	アクセス リストの設定を表示します。

次に、すべての TCP トラフィックを許可し、暗黙的にその他すべての IP トラフィックを拒否する名前付き拡張 IP ACL `simple-ip-acl` を設定する例を示します。

```
Switch(config)# ip access-list extended simple-ip-acl
Switch(config-ext-nacl)# permit tcp any any
Switch(config-ext-nacl)# end
```

次に、送信元ホスト `000.000.011` をすべての宛先ホストで許可する、名前付き拡張 MACL `simple-mac-acl` を設定する例を示します。

```
Switch(config)# mac access-list extended simple-mac-acl
Switch(config-ext-macl)# permit host 000.000.011 any
Switch(config-ext-macl)# end
```

アクセス グループ モードを PACL と併用する方法

アクセス グループ モードを使用して、その他の ACL との PACL の対話形式を変更できます。たとえば、レイヤ 2 インターフェイスが VLAN 100 に属する場合、VACL (VLAN フィルタ) V1 は VLAN 100 上に適用され、PACL P1 がレイヤ 2 インターフェイス上に適用されます。この状況では、VLAN 100 上のレイヤ 2 インターフェイスのトラフィックに P1 と V1 がどのように影響するかを指定する必要があります。インターフェイス単位的方式では、`access-group mode` コマンドを使用して、下記に定義される動作のいずれかを指定できます。

次のモードが定義されています。

- `prefer port` モード：PACL がレイヤ 2 インターフェイス上に設定されている場合、PACL が有効になり、その他の ACL (ルータ ACL と VACL) を無効にします。レイヤ 2 インターフェイス上に PACL 機能が設定されていない場合、その他の適用可能な機能がこのインターフェイスに統合され、インターフェイス上に適用されます。これがデフォルトのアクセス グループ モードです。
- `prefer vlan` モード：ポートに VLAN ベースの ACL 機能が適用され、PACL が無効の場合は、VLAN ベースの ACL 機能が有効になります。レイヤ 2 インターフェイスに VLAN ベースの ACL 機能が適用できない場合、インターフェイス上の既存の PACL 機能が適用されます。
- `merge` モード：ハードウェアにプログラミングされる前に、適用可能な ACL 機能を統合します。



(注) 出力 PACL と、VACL およびルータ ACL は相互に排他的なので、アクセス グループ モードは出力トラフィック フィルタリングの動作を変更しません。

レイヤ 2 インターフェイス上でのアクセス グループ モードの設定

レイヤ 2 インターフェイス上にアクセス 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	Switch# <code>configure t</code>	グローバル コンフィギュレーション モードを開始します。
ステップ 2	Switch(config)# <code>interface interface</code>	インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	Switch(config-if)# <code>[no] access-group mode {prefer {port vlan} merge}</code>	レイヤ 2 インターフェイス上にアクセス グループ モードを設定します。 <code>no</code> プレフィックスは、レイヤ 2 インターフェイスから IP ACL または MAC ACL を削除します。
ステップ 4	Switch(config)# <code>show running-config</code>	アクセス リストの設定を表示します。

次に、PACL 以外の機能を統合して、インターフェイス上に適用する例を示します。

```
Switch# configure t
Switch(config)# interface interface
Switch(config-if)# access-group mode prefer port
```

次に、ハードウェアにプログラミングされる前に、適用可能な ACL 機能を統合する例を示します。

```
Switch# configure t
Switch(config)# interface interface
Switch(config-if)# access-group mode merge
```

レイヤ 2 インターフェイスへの ACL の適用

レイヤ 2 インターフェイスに IP ACL および MAC ACL を適用するには、次のいずれかの作業を行います。

コマンド	目的
Switch(config-if)# ip access-group ip-acl {in out}	レイヤ 2 インターフェイスに IP ACL を適用します。
Switch(config-if)# mac access-group mac-acl {in out}	レイヤ 2 インターフェイスに MAC ACL を適用します。



(注)

Catalyst 4500 シリーズ スイッチ上で稼働する Supervisor Engine III および Supervisor Engine IV は、インターフェイス上の入力 PACL および出力 PACL の両方をサポートしています。

次に、名前付き拡張 IP ACL simple-ip-acl をファスト イーサネット インターフェイス 6/1 の入力トラフィックに適用する例を示します。

```
Switch# configure t
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# ip access-group simple-ip-acl in
```

次に、名前付き拡張 MAC ACL simple-mac-acl をファスト イーサネット インターフェイス 6/1 の出力トラフィックに適用する例を示します。

```
Switch# configure t
Switch(config)# interface fastEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl out
```

レイヤ 2 インターフェイス上の ACL 設定の表示

レイヤ 2 インターフェイス上の ACL 設定に関する情報を表示するには、次のいずれかの作業を行います。

コマンド	目的
Switch# show ip interface [interface-name]	インターフェイス上の IP アクセス グループ設定を表示します。
Switch# show mac access-group interface [interface-name]	インターフェイス上の MAC アクセス グループ設定を表示します。
Switch# show access-group mode interface [interface-name]	インターフェイス上のアクセス グループ モード設定を表示します。

次に、IP アクセス グループ `simple-ip-acl` がインターフェイス `fa6/1` の着信方向に設定されている例を示します。

```
Switch# show ip interface fast 6/1
FastEthernet6/1 is up, line protocol is up
  Inbound access list is simple-ip-acl
  Outgoing access list is not set
```

次に、MAC アクセス グループ `simple-mac-acl` がインターフェイス `fa6/1` の着信方向に設定されている例を示します。

```
Switch# show mac access-group interface fast 6/1
Interface FastEthernet6/1:
  Inbound access-list is simple-mac-acl
  Outbound access-list is not set
```

次に、アクセス グループ統合がインターフェイス `fa6/1` に設定されている例を示します。

```
Switch# show access-group mode interface fast 6/1
Interface FastEthernet6/1:
  Access group mode is: merge
```

VLAN マップおよびルータを PACL と併用する方法

出力 PACL は、VACL または出力ルータ ACL との相互作用がありません（「PACL 設定時の注意事項」(P.39-34) で説明した制限を参照）。ただし、入力 PACL のルータ ACL および VACL との相互作用は、表 39-1 に示されるインターフェイス アクセス グループ モードによって決まります。

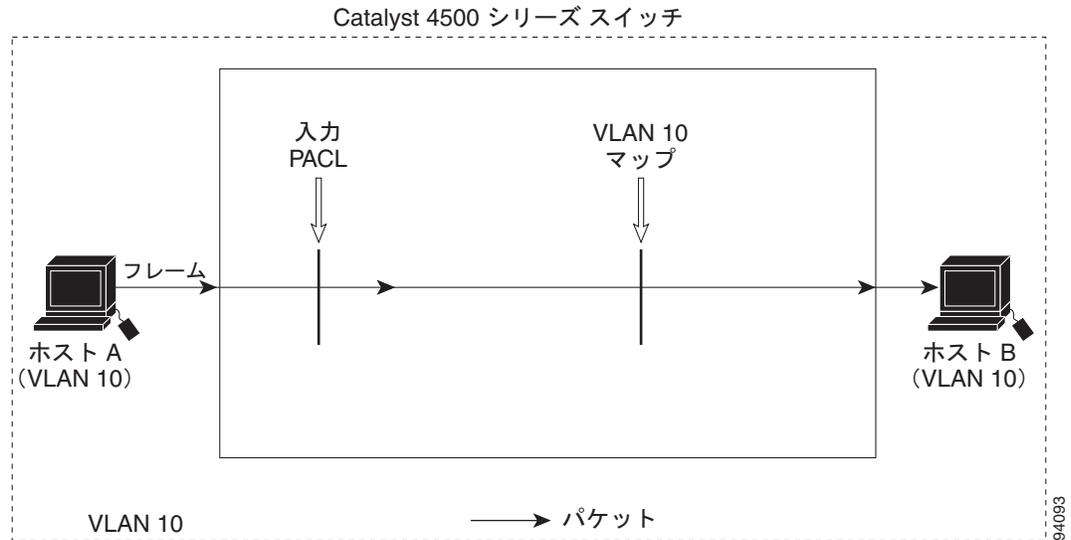
表 39-1 PACL、VACL、およびルータ ACL の相互作用

ACL タイプ	入力 PACL		
	prefer port モード	prefer vlan モード	merge モード
1. 入力ルータ ACL	PACL が適用される	入力ルータ ACL が適用される	PACL、入力ルータ ACL (統合) の順で適用される (入力側)
2. VACL	PACL が適用される	VACL が適用される	PACL、VACL (統合) の順で適用される (入力側)
3. VACL と入力ルータ ACL	PACL が適用される	VACL+ 入力ルータ ACL が適用される	PACL、VACL、入力ルータ ACL (統合) の順で適用される (入力側)

表 39-1 に示される各 ACL タイプは、次に説明する別のシナリオで同様に使用されます。

シナリオ 2：ホスト A は、VLAN 10 のインターフェイスに接続されています。図 39-8 で示すように、VLAN 10 には、VACL（VLAN マップ）と入力 PACL が設定されています。

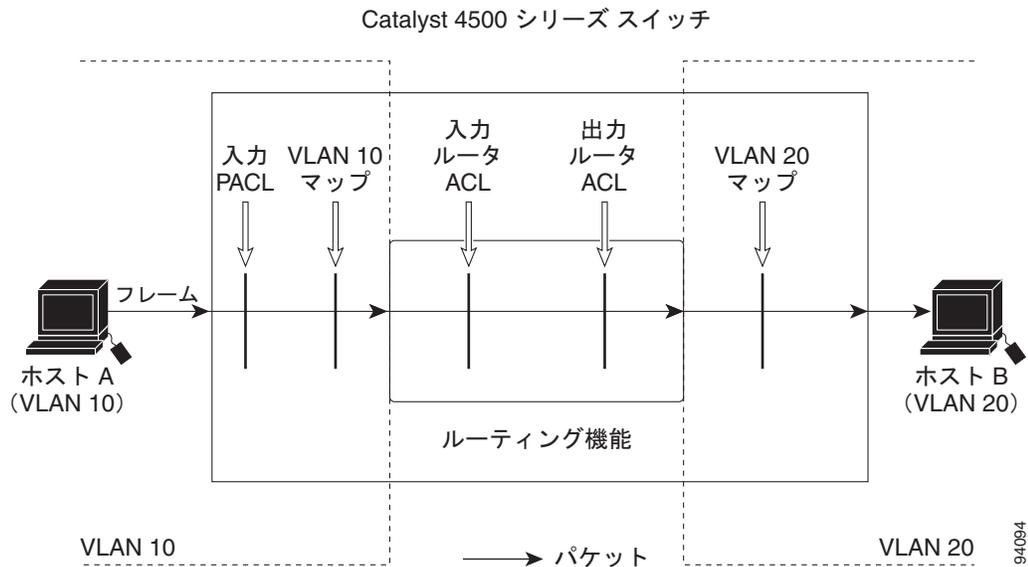
図 39-8 シナリオ 2：PACL の VACL との相互作用



インターフェイス アクセス グループ モードが **prefer port** の場合、ホスト A からの入力トラフィックに適用されるのは入力 PACL だけです。モードが **prefer vlan** の場合、VACL だけがホスト A からの入力トラフィックに適用されます。モードが **merge** の場合、最初に入力 PACL がホスト A からの入力トラフィックに適用され、その後 VACL がそのトラフィックに適用されます。

シナリオ 3：ホスト A は、VACL と SVI が設定された VLAN 10 のインターフェイスに接続されています。図 39-9 で示すように、SVI には入力ルータ ACL が設定されていて、インターフェイスには入力 PACL が設定されています。

図 39-9 シナリオ 3：VACL と入力ルータ ACL



インターフェイス アクセス グループ モードが **prefer port** の場合、ホスト A からの入力トラフィックに適用されるのは入力 PACL だけです。モードが **prefer vlan** の場合、VACL と入力ルータ ACL の統合結果がホスト A からの入力トラフィックに適用されます。モードが **merge** の場合は、入力 PACL が、最初に、ホスト A からの入力トラフィックに適用され、次に、VACL がトラフィックに適用され、最後に、入力ルータ ACL がルーティングを必要とするトラフィックに適用されます（つまり、入力 PACL、VACL、および入力ルータ ACL の統合結果がトラフィックに適用されます）。