CHAPTER 45

ポート ACL および VLAN ACL の設定

この章では、Cisco IOS Release 12.2SX で Port ACL（PACL; ポート ACL）および VLAN ACL（VACL）を設定する手順について説明します。

（注）

- この章で使用しているコマンドの構文および使用方法の詳細については、次の URL の『Cisco IOS Master Command List, Release 12.2SX』を参照してください。

  http://www.cisco.com/en/US/docs/ios/mcl/122sxmcl/12_2sx_mcl_book.html

- Optimized ACL Logging（OAL; 最適化された ACL ロギング）と VACL キャプチャには互換性がありません。スイッチに両方の機能を設定しないでください。OAL が設定されている場合は（「最適化された ACL ロギング」（P.43-8）を参照）、SPAN を使用してトラフィックをキャプチャします。
- ポート ACL は access-list キーワードである **log** または **reflexive** をサポートしません。アクセスリスト内のこれらのキーワードは無視されます。OAL は PACL をサポートしません。
- PACL はプライベート VLAN 上ではサポートされません。

ヒント

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

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

この章で説明する内容は、次のとおりです。

ACL の概要

ここでは、Cisco IOS Release 12.2SX での Access Control List（ACL; アクセス制御リスト）について説明します。

ACL の概要

ACL は、ACL に指定された条件に基づいて出力トラフィックおよび入力トラフィックをフィルタリングする機能です。

Cisco IOS Release 12.2SX では、次のタイプの ACL がサポートされます。

- Cisco IOS ACL はレイヤ 3 インターフェイスに適用され、VLAN 間でルーティングされるトラフィックをフィルタリングします。Cisco IOS ACL の詳細については、第 43 章「Cisco IOS ACL サポートの概要」を参照してください。
- VACL はすべてのパケット（ブリッジドまたはルーテッド）の VLAN へのアクセスを制御します。パケットはルーティングされたあと、レイヤ 2 ポートまたはレイヤ 3 ポートから VLAN に着信します。VACL を使用して、同じ VLAN 上のデバイス間のトラフィックをフィルタリングすることもできます。
- ポート ACL によるアクセス制御は、指定されたレイヤ 2 ポートに着信するすべてのトラフィックに対して行われます。

PACL および VACL は、レイヤ 3 アドレス（IP プロトコル向け）またはレイヤ 2 MAC アドレス（IP 以外のプロトコル向け）に基づいてアクセス制御を行います。

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 リストを 1 つと MAC アドレス リストを 1 つだけです。

VACL の概要

VLAN ACL（VACL）は、VLAN 内でブリッジされるか、VLAN または（VACL キャプチャのために）WAN インターフェイスの内側または外側へルーティングされるすべてのパケットのアクセス制御を行います。ルーティングされるパケットだけに適用される Cisco IOS ACL と異なり、VACL はすべてのパケットに適用され、どの VLAN または WAN インターフェイスにも適用できます。VACL は ACL TCAM ハードウェアで処理されます。VACL は、ハードウェアでサポートされていないすべての Cisco IOS ACL フィールドを無視します。

IP および MAC レイヤ トラフィックの場合は、VACL を設定できます。WAN インターフェイスに適用される VACL は、VACL キャプチャの IP トラフィックだけをサポートします。

VACL が特定のパケット タイプ用に設定されていて、あるパケットの該当タイプが VACL と一致しない場合、デフォルト動作では、パケットが拒否されます。

（注）　IGMP（インターネット グループ管理プロトコル）パケットは VACL と照合されません。

MAC ポリシーベース転送

Cisco IOS Release 12.2(33)SXI 以降では、MAC Policy-Based Forwarding（PBF; MAC ポリシーベース転送）がサポートされています。これは MAC ベースの VACL タイプで、これによって VLAN 間でパケットをブリッジできます。MAC PBF は、送信元と宛先の MAC アドレスだけに基づいてパケットを転送し、レイヤ 2 より上位の情報は無視します。ACL TCAM ハードウェアで処理される VACL とは異なり、MAC PBF はソフトウェアで実行され、オプションのレート リミッタで CPU の使用率を制御します。さらに PBF は、着信パケットにだけ適用されます。

（注）　レイヤ 2 ポート ACL（PACL）は、MAC PBF よりも優先されます。

ポート ACL の概要

ポート ACL 機能により、特定のレイヤ 2 ポートに対してアクセス制御を行うことができます。レイヤ 2 ポートは、VLAN に属する物理的な LAN ポートまたはトランク ポートです。ポート ACL は、入力トラフィックだけに適用されます。ポート ACL 機能は、ハードウェアだけでサポートされます（ポート ACL は、ソフトウェアでルーティングされたパケットには適用されません）。

ポート ACL を作成すると、ACL TCAM にエントリが作成されます。利用可能な TCAM スペースを確認するには、**show tcam counts** コマンドを使用します。

PACL 機能は、ポートで受信するレイヤ 2 制御パケットには影響を与えません。

PACL とその他の ACL との相互作用の方法を変更するには、**access-group mode** コマンドを使用します。

PACL は次のモードを使用します。

- 優先ポート モード : PACL がレイヤ 2 インターフェイスで設定されている場合は、PACL が有効になり、その他の ACL（Cisco IOS ACL および VACL）を無効になります。PACL 機能がレイヤ 2 インターフェイスで設定されていない場合は、そのインターフェイスに適用可能なその他の機能が結合されて適用されます。
- マージ モード : このモードでは、図 45-2 に示す論理シリアル モデルに従って、PACL、VACL、および Cisco IOS ACL が入力方向に結合されます。これはデフォルトのアクセス グループ モードです。

各インターフェイスで **access-group mode** コマンドを設定します。デフォルトはマージ モードです。

（注）　PACL は、優先ポート モードが選択された場合だけ、トランク ポート上で設定できます。トランク ポートはマージ モードをサポートしません。

アクセス グループ モードについて説明するために、VLAN100 に属する物理ポートに次の ACL が設定されているとします。

- Cisco IOS ACL R1 がルーテッド インターフェイス VLAN100 に適用されます。
- VACL（VLAN フィルタ）V1 が VLAN100 に適用されます。
- PACL P1 が物理ポートに適用されます。

この状況では、次のような ACL の相互作用が行われます。

- 優先ポート モードでは、Cisco IOS ACL R1 および VACL V1 は無視されます。
- マージ モードでは、Cisco IOS ACL R1、VACL V1、および PACL P1 は結合され、ポートに適用されます。

（注）　PACL を作成するための CLI 構文は、Cisco IOS ACL を作成する構文と同じです。レイヤ 2 ポートにマッピングされている ACL のインスタンスが PACL です。レイヤ 3 インターフェイスにマッピングされている ACL のインスタンスは Cisco IOA ACL です。同じ ACL をレイヤ 2 ポートとレイヤ 3 インターフェイスの両方にマッピングできます。

PACL 機能は MAC ACL および IPv4 ACL をサポートします。PACL 機能は IPV6、ARP、または Multiprotocol Label Switching（MPLS; マルチプロトコル ラベル スイッチング）トラフィック用の ACL をサポートしません。

次の項では、PACL の詳細について説明します。

EtherChannel と PACL の相互作用

ここでは、EtherChannel と PACL の相互作用における注意事項について説明します。

- PACL はメイン レイヤ 2 チャネル インターフェイス上でサポートされますが、ポート メンバー上ではサポートされません。PACL が設定されているポートは、EtherChannel メンバー ポートとして設定されていない場合があります。EtherChannel コンフィギュレーション コマンドは、PACL が設定されたポートでは使用できません。
- 論理ポートの設定変更は、チャネル内のすべてのポートに影響します。チャネルに属する論理ポートに ACL をマッピングすると、そのチャネル内のすべてのポートにもマッピングされます。

ダイナミック ACL（マージ モードだけに適用）

ダイナミック ACL は VLAN ベースであり、GWIP によって使用されます。マージ モードは、ダイナミック ACL と PACL の結合をサポート*しません*。マージ モードでは、次のような設定はできません。

- 対応する VLAN にダイナミック ACL がマッピングされているポートに PACL を設定しようとすること。この場合、PACL はポート上のトラフィックに適用されません。
- 構成ポートの 1 つに PACL がインストールされている VLAN にダイナミック ACL を適用しようとすること。この場合、動的 ACL は適用されません。

トランク ポート

トラック ポートで PACL を設定するには、ポート優先モードを先に設定する必要があります。**access-group mode prefer port** インターフェイス コマンドを入力してポート優先モードを設定するまで、トランク ポートまたはダイナミック ポートに PACL を適用するコンフィギュレーション コマンドは使用できません。トランク ポートはマージ モードをサポートしません。

レイヤ 2 ポートからレイヤ 3 ポートへの変換

ポートをレイヤ 2 からレイヤ 3 に再設定する場合、ポート上に設定されているすべての PACL は非アクティブになりますが、設定からは削除されません。その後ポートをレイヤ 2 として設定すると、ポート上に設定されているすべての PACL は再度アクティブになります。

ポート/VLAN アソシエーション変更

ポート/VLAN アソシエーションを変更するポート コンフィギュレーション コマンドを入力すると、ACL 再結合を開始できます。

PACL、VACL、または Cisco IOS ACL をマッピング解除したあとに再度マッピングすると、再結合が自動的に開始されます。

マージ モードでは、モジュール上のポートに PACL が設定されている場合は、スイッチング モジュールの Online Insertion and Removal（OIR; 活性挿抜）によっても再結合が開始されます。

PACL と VACL の相互作用

ここでは、さまざまなタイプの ACL 間の相互作用について説明します。

- 「PACL の VACL および Cisco IOS ACL との相互作用」（P.45-5）
- 「ブリッジド パケット」（P.45-5）
- 「ルーテッド パケット」（P.45-6）
- 「マルチキャスト パケット」（P.45-7）

PACL の VACL および Cisco IOS ACL との相互作用

ここでは、PACL の VACL および Cisco IOS ACL との相互作用における注意事項について説明します。

PACL はまず、物理ポートの着信パケットに適用されます。パケットが PACL により許可されると、次に入力 VLAN の VACL が適用されます。パケットがレイヤ 3 で転送され、VACL により許可される場合は、同じ VLAN 上の Cisco IOS ACL によりフィルタリングされます。出力方向では同じプロセスが逆に発生します。ただし、出力 PACL はハードウェアで現在サポートされていません。

ポートが優先ポート モードに設定されている場合、PACL により VACL と Cisco IOS ACL の両方が無効になります。このルールの 1 つの例外は、パケットが Route Processor（RP; ルート プロセッサ）によってソフトウェアで転送される場合です。RP は PACL モードに関係なく入力 Cisco IOS ACL を適用します。パケットがソフトウェアで転送される 2 つの例は、次のとおりです。

- 出力ブリッジド パケット（ロギングや NAT などの機能のため）
- IP オプションが指定されたパケット

ブリッジド パケット

図 45-1 に、ブリッジド パケットに適用される PACL および VACL を示します。マージ モードでは、ACL は次の順序で適用されます。

1. 入力ポートの PACL
2. 入力 VLAN の VACL
3. 出力 VLAN の VACL

図 45-1　ブリッジド パケットへの ACL の適用

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL は適用されません）。

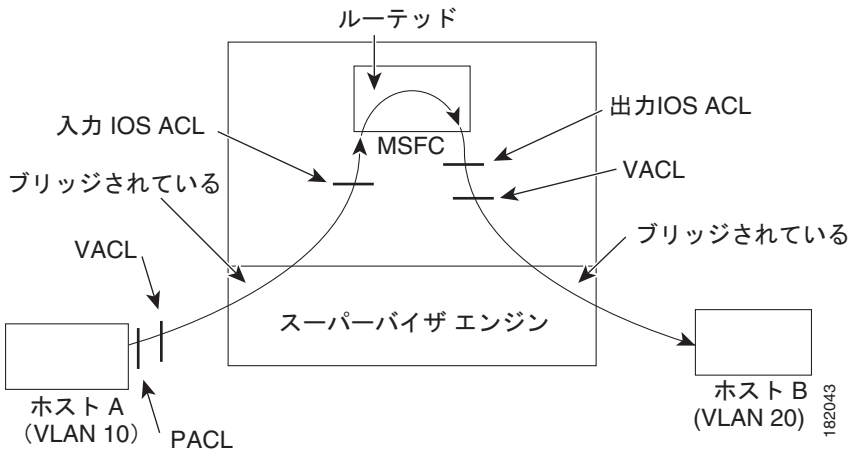
ルーテッド パケット

図 45-2 に、ルーテッド パケットおよびレイヤ 3 スイッチド パケットに ACL を適用する方法を示します。マージ モードでは、ACL は次の順序で適用されます。

1. 入力ポートの PACL
2. 入力 VLAN の VACL
3. 入力 Cisco IOS ACL
4. 出力 Cisco IOS ACL
5. 出力 VLAN の VACL

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL および Cisco IOS ACL は適用されません）。

図 45-2　ルーテッド パケットへの ACL の適用



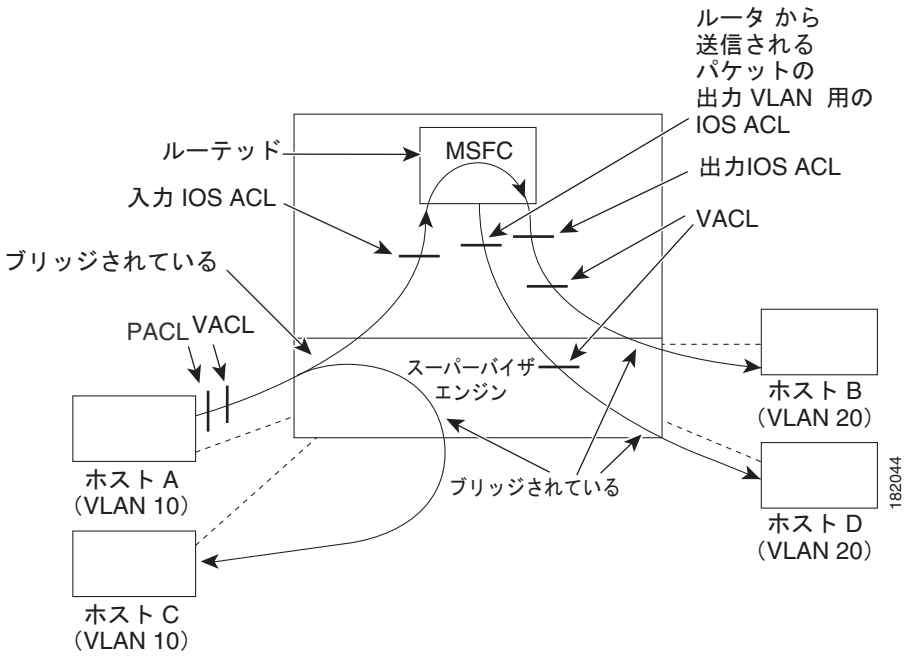
マルチキャスト パケット

図 45-3 に、マルチキャスト拡張が必要なパケットに ACL を適用する方法を示します。マルチキャスト拡張が必要なパケットに対して、ACL は次の順番で適用されます。

1. マルチキャスト拡張が必要なパケット
   a. 入力ポートの PACL
   b. 入力 VLAN の VACL
   c. 入力 Cisco IOS ACL
2. マルチキャスト拡張後のパケット
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN の VACL
3. ルータから送られるパケット
   a. 出力 Cisco IOS ACL
   b. 出力 VLAN の VACL

優先ポート モードでは、入力パケットに適用されるのは PACL だけです（入力 VACL および Cisco IOS ACL は適用されません）。

図 45-3　　マルチキャスト パケットへの ACL の適用



PACL の設定

PACL は Cisco IOS Release 12.2(33)SXH 以降のリリースでサポートされます。ここでは、PACL を設定する手順について説明します。PACL は、レイヤ 3 情報、レイヤ 4 ヘッダー情報、または非 IP レイヤ 2 情報を使用して、レイヤ 2 インターフェイスに着信するトラフィックをフィルタリングします。

PACL 機能は、ポートに適用する標準/拡張 IP ACL または名前付き拡張 MAC ACL を作成するために、既存の Cisco IOS **access-list** コマンドを使用します。

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するには、**ip access-group** コマンドまたは **mac access-group interface** コマンドを使用します。

（注）　PACL は、CDP、VTP、DTP、PAgP、UDLD、および STP などの物理リンク プロトコルおよび論理リンク プロトコルをフィルタリングできません。これらのプロトコルは ACL が有効になる前に Switch Processor（SP; スイッチ プロセッサ）にリダイレクトされるためです。

ここでは、次の内容について説明します。

PACL 設定時の注意事項

PACL を設定する場合、次の注意事項を考慮してください。

- 同じレイヤ 2 インターフェイスに方向別に適用できるのは、多くても IP アクセス リストを 1 つと MAC アクセス リストを 1 つです。
- PACL は IPv6、MPLS、または ARP メッセージに適用されません。
- IP アクセス リストは、IPv4 パケットだけをフィルタリングします。IP アクセス リストには、標準アクセス リスト、拡張アクセス リスト、または名前付きアクセス リストを定義できます。
- MAC アクセス リストは、イーサネット データグラムのフィールドに基づいて、サポートされないタイプの入力パケット（IP、IPv6、ARP、MPLS 以外のパケット）をフィルタリングします。MAC アクセス リストは、IP、IPv6、MPLS、または ARP メッセージには適用されません。定義できるのは名前付き MAC アクセス リストだけです。
- PACL の一部として設定できる ACL および Access Control Entry（ACE; アクセス制御エントリ）の数は、スイッチ上のハードウェア リソースによる制限を受けます。これらのハードウェア リソースは、システムに設定されているさまざまな ACL 機能（VACL など）により共有されます。PACL をハードウェアに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は、PACL が適用されません。
- PACL は access-list **log** および **reflect/evaluate** キーワードをサポートしません。これらのキーワードを PACL のアクセス リストに追加しても、無視されます。
- OAL は PACL をサポートしません。
- アクセス グループ モードによって、PACL とその他の ACL との相互作用の方法が変わります。シスコ プラットフォーム全体の動作を一貫させるには、デフォルトのアクセス グループ モード（マージ 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

IP ACL および MAC ACL はレイヤ 2 物理インターフェイスに適用できます。（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 がサポートされています。

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

	コマンド	目的
ステップ 1	`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*	レイヤ 2 ポートのインターフェイス 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)# {ip | mac} access-group {name | number | in | out}`	番号付き ACL または名前付き ACL をレイヤ 2 インターフェイスに適用します。
ステップ 4	`Switch(config)# show running-config`	アクセス リスト設定を表示します。

次に、すべての TCP トラフィックを許可し、他のすべての IP トラフィックを暗黙的に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 を任意の宛先ホストで許可する、名前付き拡張 MAC ACL 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
```

レイヤ 2 インターフェイスのアクセス グループ モードの設定

アクセス モードをレイヤ 2 インターフェイス上で設定するには、次の作業を行います。

	コマンド	目的
ステップ 1	`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*	レイヤ 2 ポートのインターフェイス 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)# [no] access-group mode {prefer port | merge}`	このレイヤ 2 インターフェイスのモードを設定します。**no** プレフィクスは、モードをデフォルト（マージ）に設定します。
ステップ 4	`Switch(config)# show running-config`	アクセス リスト設定を表示します。

次の例では、優先ポート モードを使用するようインターフェイスを設定します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
Switch(config-if)# access-group mode prefer port
```

次の例では、マージ モードを使用するようインターフェイスを設定します。

```
Switch# configure terminal
Switch(config)# interface gigabitEthernet 6/1
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 を適用にするには、次の作業のいずれかを行います。

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

次に、名前付き拡張 IP ACL simple-ip-acl をインターフェイス GigabitEthernet 6/1 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 gigabitEthernet 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 をインターフェイス GigabitEthernet 6/1 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 gigabitEthernet 6/1
Switch(config-if)# mac access-group simple-mac-acl in
```

ポート チャネルへの ACL の適用

ポート チャネルの論理インターフェイスに IP ACL および MAC ACL を適用にするには、次の作業を行います。

コマンド	目的
`Switch(config-if)# interface port-channel number`	ポート チャネルのコンフィギュレーション モードを開始します。
`Switch(config-if)# ip access-group ip-acl {in | out}`	IP ACL をポート チャネル インターフェイスに適用します。
`Switch(config-if)# mac access-group mac-acl {in | out}`	MAC ACL をポート チャネル インターフェイスに適用します。

次に、名前付き拡張 IP ACL simple-ip-acl をポート チャネル 3 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 port-channel 3
Switch(config-if)# ip access-group simple-ip-acl in
```

レイヤ 2 インターフェイスの ACL 設定の表示

レイヤ 2 インターフェイス上の ACL 設定の詳細を表示するには、次の作業のいずれかを行います。

コマンド	目的
Switch# **show ip access-lists** [**interface** *interface-name*]	インターフェイスの 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 をインターフェイス fa6/1 の入力方向に設定する例を示します。

```
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 をインターフェイス fa6/1 の入力方向に設定する例を示します。

```
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 グループ結合をインターフェイス fa6/1 に設定する例を示します。

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

VACL の設定

ここでは、VACL の設定手順について説明します。

VACL 設定時の注意事項

VACL を設定する場合、次の注意事項を考慮してください。

- VACL は、標準および拡張 Cisco IOS IP、MAC レイヤ名前付き ACL（「MAC ACL の設定」（P.37-79）を参照）、および VLAN アクセス マップを使用します。
- VLAN アクセス マップは、VLAN または VACL キャプチャのための WAN インターフェイスに適用されます。WAN インターフェイスに付加された VACL は、標準または拡張 Cisco IOS IP ACL だけをサポートします。
- 各 VLAN アクセス マップは、1 つまたは複数のマップ シーケンスで構成できます。各シーケンスには match 句と action 句が含まれます。match 句はトラフィック フィルタリング用の IP または MAC ACL を指定します。action 句は一致した場合に実行するアクションを指定します。フローが許可（permit）ACL エントリと一致した場合、関連付けられたアクションが実行され、それ以降の残りのシーケンスに対してフローはチェックされません。フローが拒否（deny）ACL エントリと一致した場合、同じシーケンス内の次の ACL、または次のシーケンスに対してフローがチェックされます。フローがどの ACL エントリとも一致せず、少なくとも 1 つの ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。
- ブリッジド トラフィックとルーテッド トラフィックの両方にアクセス制御を適用するには、VACL を単独で使用するか、または VACL と ACL を組み合わせて使用します。VLAN インターフェイス上で ACL を定義して、入力と出力両方のルーテッド トラフィックに対してアクセス制御を適用できます。VACL を定義して、ブリッジド トラフィックに対してアクセス制御を適用します。
- VACL とともに ACL を使用する場合は、次の点に注意してください。
  - 発信 ACL でのロギングの必要があるパケットは、VACL で拒否された場合、ロギングされません。
  - VACL は NAT 変換前のパケットに適用されます。アクセス制御されなかった変換フローは、VACL 設定により、変換後にアクセス制御される場合があります。
- 同じインターフェイス上で Policy Based Routing（PBR; ポリシー ベース ルーティング）を使用して VACL キャプチャが設定されている場合は、BDD を ACL 結合アルゴリズムとして選択しないでください。Supervisor Engine 720 のデフォルトの ACL 結合アルゴリズムである ODM を使用することを推奨します。
- VACL キャプチャが、ソフトウェアによるトラフィック処理を必要とする別の入力機能とともに入力インターフェイスに設定されている場合、重複するトラフィックのパケットは 2 回キャプチャされる可能性があります。
- ソフトウェア スイッチングされた WAN パケットは、デフォルトでは ACL TCAM の ACL ルックアップの対象ではないので、ハードウェア専用の機能の影響は受けません。したがって、ソフトウェア スイッチングされた WAN パケットの VACL キャプチャは失敗します。Cisco IOS Release 12.2(33)SXI2 以降のリリースでは、グローバル コンフィギュレーション モードで **platform cwan acl software-switched** {**egress** | **ingress**} コマンドを入力すると、ソフトウェア スイッチングされた出力および入力 WAN パケットに ACL を適用できます ソフトウェア スイッチングされた WAN パケットに ACL が適用されるかどうかを確認するには、次の例のように **show platform acl software-switched** コマンドを入力します。

```
Router (config)# platform cwan acl software-switched ingress
Router (config)# exit
Router# show platform acl software-switched
 CWAN: ACL treatment for software switched in INGRESS is enabled
 CWAN: ACL treatment for software switched in EGRESS is disabled
```

- VACL の action 句には、転送（forward）、ドロップ（drop）、キャプチャ（capture）、またはリダイレクト（redirect）を指定できます。トラフィックをロギングすることもできます。WAN インターフェイスに適用された VACL は、リダイレクトまたはログ アクションをサポートしません。
- VACL は、IGMP、MLD、または PIM トラフィックに適用できません。

（注）

- VACL のマップの最後には、暗黙的な拒否エントリがあります。パケットがどの ACL エントリとも一致せず、少なくとも 1 つ ACL がそのパケット タイプ用に設定されている場合、パケットは拒否されます。
- VACL 内で空または未定義の ACL が指定されている場合、いずれかのパケットがこの ACL に一致し、関連付けられたアクションが実行されます。

VLAN アクセス マップの定義

VLAN アクセス マップを定義するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan access-map map_name [0-65535]`	VLAN アクセス マップを定義します。任意で、VLAN アクセス マップのシーケンス番号を指定できます。
`Router(config)# no vlan access-map map_name 0-65535`	VLAN アクセス マップからマップ シーケンスを削除します。
`Router(config)# no vlan access-map map_name`	VLAN アクセス マップを削除します。

VLAN アクセス マップを定義する場合、次の点に注意してください。

- エントリを追加または変更する場合は、マップのシーケンス番号を指定します。
- マップのシーケンス番号を指定しないと、番号が自動的に割り当てられます。
- 各マップ シーケンスには、match 句および action 句をそれぞれ 1 つだけ指定できます。
- マップ シーケンスを削除する場合は、シーケンス番号を指定して **no** キーワードを使用します。
- マップを削除する場合は、シーケンス番号を指定しないで、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（P.45-16）を参照してください。

VLAN アクセス マップ シーケンスでの match 句の設定

VLAN アクセス マップ シーケンスに match 句を設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# match {ip address {1-199 | 1300-2699 | acl_name} | {mac address acl_name}}`	VLAN アクセス マップ シーケンスに match 句を設定します。
`Router(config-access-map)# no match {ip address {1-199 | 1300-2699 | acl_name} | {mac address acl_name}}`	VLAN アクセス マップ シーケンスから match 句を削除します。

VLAN アクセス マップ シーケンスに match 句を設定する場合、次の情報に注意してください。

- 1 つまたは複数の ACL を選択できます。
- WAN インターフェイスに付加された VACL は、標準または拡張 Cisco IOS IP ACL だけをサポートします。
- match 句を削除したり、match 句内の特定の ACL を削除したりする場合は、**no** キーワードを使用します。
- 名前付き MAC レイヤ ACL の詳細については、「MAC ACL の設定」（P.37-79）を参照してください。
- Cisco IOS ACL の詳細については、次の URL で『*Cisco IOS Security Configuration Guide, Release 12.2*』の「Traffic Filtering and Firewalls」を参照してください。

  http://www.cisco.com/en/US/docs/ios/12_2/security/configuration/guide/fsecur_c.html

「VLAN アクセス マップの設定および確認の例」（P.45-16）を参照してください。

VLAN アクセス マップ シーケンスでの action 句の設定

VLAN アクセス マップ シーケンスに action 句を設定するには、次の作業を行います。

コマンド	目的
`Router(config-access-map)# action {drop [log]} | {forward [capture | vlan vlan_ID]} | {redirect {{ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスに action 句を設定します。
`Router(config-access-map)# no action {drop [log]} | {forward [capture | vlan vlan_ID]} | {redirect {{ethernet | fastethernet | gigabitethernet | tengigabitethernet} slot/port} | {port-channel channel_id}}`	VLAN アクセス マップ シーケンスから action 句を削除します。

VLAN アクセス マップ シーケンスに action 句を設定する場合、次の点に注意してください。

- パケットをドロップ、転送、転送してキャプチャ、またはリダイレクトするアクションを設定できます。
- WAN インターフェイスに適用される VACL は、転送してキャプチャするアクションだけをサポートします。WAN インターフェイスに適用された VACL は、ドロップ、転送、またはリダイレクト アクションをサポートしません。
- 転送されるパケットも、設定済み Cisco IOS セキュリティ ACL の対象になります。
- **capture** アクションを指定すると、転送されるパケットのキャプチャ ビットが設定されて、キャプチャ機能がイネーブルであるポートがパケットを受信できるようになります。キャプチャできるのは、転送されたパケットだけです。**capture** アクションの詳細については、「キャプチャ ポートの設定」（P.45-17）を参照してください。
- **forward vlan** アクションは、ポリシーベース転送（PBF）を実行し、VLAN 間をブリッジします。
- WAN インターフェイスに適用された VACL は、**log** アクションをサポートしません。
- **log** アクションが指定されている場合、ドロップされたパケットがソフトウェアでロギングされます。ロギングできるのは、ドロップされた IP パケットだけです。

- **redirect** アクションを指定すると、物理インターフェイスまたは EtherChannel のインターフェイスを 5 つまで指定できます。EtherChannel メンバーまたは VLAN インターフェイスにパケットをリダイレクトするようには指定できません。
- リダイレクト インターフェイスは、VACL アクセス マップが設定されている VLAN 内に存在する必要があります。
- VACL が出力 SPAN 送信元ポートにトラフィックをリダイレクトする場合、SPAN は VACL リダイレクト トラフィックをコピーしません。
- SPAN および RSPAN 宛先ポートは、VACL リダイレクト トラフィックを送信します。
- action 句を削除するか、または指定されたリダイレクト インターフェイスを削除する場合は、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（P.45-16）を参照してください。

VLAN アクセス マップの適用

VLAN アクセス マップを適用するには、次の作業を行います。

コマンド	目的
`Router(config)# vlan filter map_name {vlan-list vlan_list | interface type[1] number[2] }`	指定した VLAN または WAN インターフェイスに VLAN アクセス マップを適用します。

1. *type* = **pos**、**atm**、または **serial**
2. number = *slot*/*port* または *slot*/*port_adapter*/*port*。サブインターフェイスまたはチャネル グループ ディスクリプタを含むことができます。

VLAN アクセス マップを適用する場合、次の点に注意してください。

- VLAN アクセス マップは、1 つまたは複数の VLAN または WAN インターフェイスに適用できます。
- *vlan_list* パラメータには単一の VLAN ID、カンマで区切った VLAN ID のリスト、または VLAN ID の範囲（*vlan_ID*-*vlan_ID*）を指定できます。
- VACL が適用された WAN インターフェイスを削除すると、インターフェイス上の VACL 設定も削除されます。
- 各 VLAN または WAN インターフェイスには、VLAN アクセス マップを 1 つだけ適用できます。
- VLAN に適用した VACL がアクティブになるのは、レイヤ 3 VLAN インターフェイスが設定されている VLAN に対してだけです。レイヤ 3 VLAN インターフェイスを持たない VLAN に VLAN アクセス マップを適用すると、VLAN アクセス マップをサポートするために、レイヤ 3 VLAN インターフェイスが、管理上のダウン状態になります。
- VLAN に適用される VACL は、レイヤ 2 VLAN が存在しないか動作していない場合は非アクティブです。
- セカンダリ プライベート VLAN に VACL を適用できません。プライマリ プライベート VLAN に適用された VACL は、セカンダリ プライベート VLAN にも適用されます。
- VLAN または WAN インターフェイスから VLAN アクセス マップを消去するには、**no** キーワードを使用します。

「VLAN アクセス マップの設定および確認の例」（P.45-16）を参照してください。

VLAN アクセス マップの設定の確認

VLAN アクセス マップの設定を確認するには、次の作業を行います。

コマンド	目的
Router# **show vlan access-map** [*map_name*]	VLAN アクセス マップの内容を表示して、VLAN アクセス マップの設定を確認します。
Router# **show vlan filter** [**access-map** *map_name* | **vlan** *vlan_id* | **interface** *type*[1] *number*[2]]	VACL と VLAN 間のマッピングの内容を表示して、VLAN アクセス マップの設定を確認します。

1. *type* = **pos**、**atm**、または **serial**
2. number = *slot*/*port* または *slot*/*port_adapter*/*port*。サブインターフェイスまたはチャネル グループ ディスクリプタを含むことができます。

VLAN アクセス マップの設定および確認の例

net_10 および **any_host** という名前の IP ACL が、次のように定義されていると想定します。

```
Router# show ip access-lists net_10
Extended IP access list net_10
    permit ip 10.0.0.0 0.255.255.255 any

Router# show ip access-lists any_host
Standard IP access list any_host
    permit any
```

次に、IP パケットを転送するよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送され、それ以外のすべての IP パケットはデフォルトのドロップ アクションによってドロップされます。このマップは VLAN 12 ～ 16 に適用されます。

```
Router(config)# vlan access-map thor 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter thor vlan-list 12-16
```

次に、IP パケットをドロップおよびロギングするよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックはドロップおよびロギングされ、それ以外のすべての IP パケットは転送されます。

```
Router(config)# vlan access-map ganymede 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action drop log
Router(config-access-map)# exit
Router(config)# vlan access-map ganymede 20
Router(config-access-map)# match ip address any_host
Router(config-access-map)# action forward
Router(config-access-map)# exit
Router(config)# vlan filter ganymede vlan-list 7-9
```

次に、IP パケットを転送およびキャプチャするよう、VLAN アクセス マップを定義および適用する例を示します。この例では、net_10 に一致する IP トラフィックは転送およびキャプチャされ、それ以外のすべての IP パケットはドロップされます。

```
Router(config)# vlan access-map mordred 10
Router(config-access-map)# match ip address net_10
Router(config-access-map)# action forward capture
Router(config-access-map)# exit
Router(config)# vlan filter mordred vlan-list 2, 4-6
```

キャプチャ ポートの設定

VACL でフィルタリングされたトラフィックをキャプチャするよう設定されたポートを、「キャプチャ ポート」といいます。

（注）　キャプチャされたトラフィックに IEEE 802.1Q または ISL（スイッチ間リンク）タグを適用するには、キャプチャ ポートで無条件にトラフィックするように設定します（「ISL または 802.1Q トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.15-11）および「DTP を使用しないようにするためのレイヤ 2 トランクの設定」（P.15-12）を参照）。

キャプチャ ポートを設定するには、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}`	設定するインターフェイスを指定します。
ステップ 2	`Router(config-if)# switchport capture allowed vlan {add | all | except | remove} vlan_list`	（任意）宛先 VLAN 単位で、キャプチャされたトラフィックをフィルタリングします。デフォルトは、**all** です。
ステップ 3	`Router(config-if)# switchport capture`	VACL フィルタリングされたトラフィックをキャプチャするよう、ポートを設定します。

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

キャプチャ ポートを設定する場合、次の点に注意してください。

- 任意のポートをキャプチャ ポートとして設定できます。
- *vlan_list* パラメータには単一の VLAN ID、カンマで区切った VLAN ID のリスト、または VLAN ID の範囲（*vlan_ID-vlan_ID*）を指定できます。
- キャプチャされたトラフィックをカプセル化するには、**switchport trunk encapsulation** コマンドをキャプチャ ポートに設定してから（「トランクとしてのレイヤ 2 スイッチング ポートの設定」（P.15-11）を参照）、**switchport capture** コマンドを入力します。
- キャプチャされたトラフィックをカプセル化しない場合は、**switchport mode access** コマンドをキャプチャ ポートに設定してから（「レイヤ 2 アクセス ポートとしての LAN インターフェイスの設定」（P.15-17）を参照）、**switchport capture** コマンドを入力します。
- キャプチャ ポートは、出力トラフィックだけをサポートします。トラフィックは、キャプチャ ポートからスイッチに入ることができません。

次に、インターフェイス GigabitEthernet 5/1 をキャプチャ ポートとして設定する例を示します。

```
Router(config)# interface gigabitEthernet 5/1
Router(config-if)# switchport capture
Router(config-if)# end
```

次に、VLAN アクセス マップの情報を表示する例を示します。

```
Router# show vlan access-map mymap
Vlan access-map "mymap"  10
        match: ip address net_10
        action: forward capture
Router#
```

次に、VACL と VLAN 間のマッピングを表示する例を示します。各 VACL マップについて、マップが設定されている VLAN、およびマップがアクティブである VLAN に関する情報が表示されます。VLAN 内にインターフェイスがない場合、VACL は、アクティブになりません。

```
Router# show vlan filter
VLAN Map mordred:
        Configured on VLANs:  2,4-6
            Active on VLANs:  2,4-6
Router#
```

MAC PBF の設定

MAC ポリシーベース転送（(PBF）を設定するには、各送信元 VLAN で次の作業を行います。

	コマンド	目的
ステップ 1	`Router(config)# mac host my_host mac_addr`	（任意）送信元ホストの MAC アドレスに名前を割り当てます。
ステップ 2	`Router(config)# mac access-list extended macl_name`	MAC ACL を設定します。
ステップ 3	`Router(config-ext-macl)# permit host my_host any`	名前を割り当てたホストから他の任意のアドレスへのトラフィックを許可するように、アクセス制御エントリ（ACE）を設定します。ホストは名前または MAC アドレスで指定できます。
	`Router(config-ext-macl)# permit host my_host host other_host`	名前を割り当てたホストからさらに別のアドレスへのトラフィックを許可するように、ACE を設定します。
ステップ 4	`Router(config-ext-macl)# exit`	ACL の設定を終了します。
ステップ 5	`Router(config)# vlan access-map map_name`	VLAN アクセス マップを定義します。
ステップ 6	`Router(config-access-map)# match mac address macl_name`	MAC ACL をこの VLAN アクセス マップに適用します。
ステップ 7	`Router(config-access-map)# action forward vlan other_vlan_ID [local]`	一致するトラフィックを他の VLAN に転送します。 **（注）** デフォルトでは、同じ VLAN 上にある PBF 指定のデバイス同士で通信できません。ホストによるローカル通信を許可するには、**local** キーワードを使用します。
ステップ 8	`Router(config-access-map)# exit`	アクセス マップの設定を終了します。
ステップ 9	`Router(config)# vlan filter map_name vlan-list my_vlan_ID`	VLAN アクセス マップを指定された VLAN に適用します。
ステップ 10	`Router(config)# interface vlan my_vlan_ID`	VLAN のインターフェイス コンフィギュレーション モードを入力します。
ステップ 11	`Router(config-if)# mac packet-classify`	この VLAN 上の着信または送信レイヤ 3 パケットをレイヤ 2 パケットとして分類します。
ステップ 12	`Router(config-if)# exit`	インターフェイス コンフィギュレーション モードを終了します。

	コマンド	目的
ステップ 13	`Router(config)# mls rate-limit unicast acl mac-pbf` *pps* [*burst_size*]	（任意）PBF パケットにレート制限を設定します。 • *pps*：1 秒あたりの最大パケット数。範囲は毎秒 10 ～ 1000000 パケットです。 • *burst_size*：バースト内の最大パケット数。範囲は 1 ～ 255 パケット です。
ステップ 14	`Router(config)# exit`	グローバル コンフィギュレーション モードを終了します。
ステップ 15	`Router# show vlan mac-pbf config`	MAC PBF の設定と統計情報を表示します。
ステップ 16	`Router# clear vlan mac-pbf counters`	（任意）MAC PBF パケット カウンタをクリアします。

MAC PBF を設定する場合、次の点に注意してください。

- 2 つの VLAN 間で両方向のトラフィックを許可するには、両方の VLAN で MAC PBF を設定する必要があります。
- MAC PBF は、異なるスイッチのホスト間に設定することができます。
- デフォルトでは、同じ VLAN 内にある MAC PBF ホスト同士で通信できません。ローカル通信を許可するには、**local** キーワードを使用します。
- **vlan filter** コマンドを設定する場合は、**vlan-list** キーワードのあとに VLAN を 1 つだけ指定します。複数の VLAN を指定すると、MAC PBF はリストの最後にある VLAN 以外はすべて無視します。
- **show vlan mac-pbf config** コマンドの出力には、設定された PBF パスに対して次のフィールドが表示されます。
  - Rcv Vlan：PBF によるパケット転送の受信側 VLAN 数。
  - Snd Vlan：PBF によるパケット転送の送信側 VLAN 数。
  - DMAC：受信側 VLAN 上の宛先ホストの MAC アドレス。
  - SMAC：送信側 VLAN 上の送信元ホストの MAC アドレス。
  - (Local)：送信側 VALN で **action forward vlan** コマンドに **local** キーワードが設定された場合は 1 を表示し、**local** キーワードが設定されていない場合は 0 を表示します。
  - (Packet counter)：送信側 VLAN から受信側 VLAN に転送されたパケット数。このカウンタをクリアするには、**clear vlan mac-pbf counters** コマンドを入力します。
  - Pkts dropped：送信側 VLAN によってドロップされたパケット数。このカウンタをクリアするには、**clear vlan mac-pbf counters** コマンドを入力します。
- 送信側 VLAN がシャットダウンされても、MAC PBF は機能します。VLAN をシャットダウンすると、レイヤ 3 の機能がディセーブルになります。MAC PBF はレイヤ 2 の機能です。

次に、別々の VLAN（「red」VLAN 100 と「blue」VLAN 200）にある 2 つのホストが同じスイッチ上でパケットを交換できるように、MAC PBF を設定および表示する例を示します。

```
Router(config)# mac host host_red3 0001.0002.0003
Router(config)# mac access-list extended macl_red
Router(config-ext-macl)# permit host host_red host host_blue
Router(config-ext-macl)# exit
Router(config)# vlan access-map red_to_blue
Router(config-access-map)# match mac address macl_red
Router(config-access-map)# action forward vlan 200 local
Router(config-access-map)# exit
Router(config)# vlan filter red_to_blue vlan-list 100
Router(config)# interface vlan 100
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router(config)#
Router(config)# mac host host_blue5 0001.0002.0005
Router(config)# mac access-list extended macl_blue
Router(config-ext-macl)# permit host host_blue host host_red
Router(config-ext-macl)# exit
Router(config)# vlan access-map blue_to_red
Router(config-access-map)# match mac address macl_blue
Router(config-access-map)# action forward vlan 100
Router(config-access-map)# exit
Router(config)# vlan filter blue_to_red vlan-list 200
Router(config)# interface vlan 200
Router(config-if)# mac packet-classify
Router(config-if)# exit
Router#
Router# show vlan mac-pbf config
 Rcv Vlan 100, Snd Vlan 200, DMAC 0001.0002.0003, SMAC 0001.0002.0005 1 15
 Rcv Vlan 200, Snd Vlan 100, DMAC 0001.0002.0005, SMAC 0001.0002.0003 0 23
 Pkts Dropped 0
Router#
```

VACL ロギングの設定

VACL ロギングが設定されているときに、次の状況で IP パケットが拒否されると、ログ メッセージが生成されます。

- 一致する最初のパケットを受信した場合
- 直前の 5 分間に、一致するパケットを受信した場合
- 5 分経過する前にしきい値に達した場合

ログ メッセージはフロー単位で生成されます。同じ IP アドレスおよびレイヤ 4（UDP または TCP）ポート番号を持つパケットが 1 つのフローと見なされます。ログ メッセージが生成されると、タイマーおよびパケット カウントがリセットされます。

VACL ロギングには、次の制限事項が適用されます。

- リダイレクトされたパケットにはレート制限機能が適用されるため、VACL ログ カウンタが不正確になることがあります。
- 拒否された IP パケットだけがロギングされます。

VACL ロギングを設定するには、VLAN アクセス マップ サブモードの **action drop log** コマンド アクションを使用し（設定情報については、「PACL の設定」（P.45-8）を参照してください）、次の作業をグローバル コンフィギュレーション モードで実行して、グローバル VACL ロギング パラメータを指定します。

	コマンド	目的
ステップ 1	`Router(config)# vlan access-log maxflow` *max_number*	ログ テーブルのサイズを設定します。maxflow の値を 0 に設定すると、ログ テーブルの内容を削除できます。デフォルトは 500、有効範囲は 0 ～ 2048 です。ログ テーブルがフルになると、新しいフローのパケットがロギングされても、ソフトウェアによってドロップされます。
ステップ 2	`Router(config)# vlan access-log ratelimit` *pps*	VACL ログ パケットの最大リダイレクト速度を設定します。デフォルトのパケット転送速度は 2000 パケット / 秒、有効範囲は 0 ～ 5000 です。制限を超えたパケットは、ハードウェアによってドロップされます。
ステップ 3	`Router(config)# vlan access-log threshold` *pkt_count*	ロギングしきい値を設定します。5 分経過する前にフローのしきい値に達すると、ログ メッセージが生成されます。デフォルトでは、しきい値は設定されていません。
ステップ 4	`Router(config)# exit`	VLAN アクセス マップ コンフィギュレーション モードを終了します。
ステップ 5	`Router# show vlan access-log config`	（任意）設定された VACL ロギング プロパティを表示します。
ステップ 6	`Router# show vlan access-log flow` *protocol* {{*src_addr src_mask*} | **any** | {**host** {*hostname* | *host_ip*}}} {{*dst_addr dst_mask*} | **any** | {**host** {*hostname* | *host_ip*}}} [**vlan** *vlan_id*]	（任意）VACL ログ テーブルの内容を表示します。
ステップ 7	`Router# show vlan access-log statistics`	（任意）パケット数、メッセージ数などの統計情報を表示します。

次に、グローバル VACL ロギングをハードウェア内で設定する例を示します。

```
Router(config)# vlan access-log maxflow 800
Router(config)# vlan access-log ratelimit 2200
Router(config)# vlan access-log threshold 4000
```

ヒント　Cisco Catalyst 6500 シリーズ スイッチの詳細（設定例およびトラブルシューティング情報を含む）については、次のページに示されるドキュメントを参照してください。
http://www.cisco.com/en/US/products/hw/switches/ps708/tsd_products_support_series_home.html

ヒント