CHAPTER 36

VACL の設定

この章では、Catalyst 6500 シリーズ スイッチで VLAN（仮想 LAN）Access Control List（ACL; アクセス制御リスト）（VACL）を設定する手順を説明します。

（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 で『*Catalyst 6500 Series Switch Cisco IOS Command Reference*』Release 12.2SX を参照してください。
  http://www.cisco.com/univercd/cc/td/doc/product/lan/cat6000/122sx/cmdref/index.htm
- Supervisor Engine 720 および Release 12.2(17d)SXB よりも前のリリースの場合、VACL キャプチャは、WS-SVC-IDSM2-K9 Intrusion Detection System Module 2（IDSM2; 侵入検知システム モジュール 2）および WS-SVC-NAM-2/WS-SVC-NAM-1 ネットワーク解析モジュールとともに使用する場合にのみサポートされます。この制限事項は、Release 12.2(17d)SXB 以降では解消されています。
- Optimized ACL Logging（OAL; 最適化された ACL ロギング）キャプチャと 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混在させないでください。OAL が設定されている場合は（「PFC3 での OAL」[p.35-4] を参照）、SPAN を使用してトラフィックをキャプチャします。

この章で説明する内容は、次のとおりです。

- VACL の概要（p.36-2）
- VACL の設定（p.36-5）
- VACL ログ機能の設定（p.36-11）

VACL の概要

ここでは VACL について説明します。

- VACL の概要（p.36-2）
- ブリッジド パケット（p.36-3）
- ルーティング対象パケット（p.36-3）
- マルチキャスト パケット（p.36-4）

VACL の概要

VACL は、VLAN 内でブリッジされるか、VLAN または VACL キャプチャの WAN インターフェイスとの間でルーティングされているすべてのパケットのアクセス制御を行います。ルータ インターフェイスでのみ設定され、ルーティング対象パケットにのみ適用される通常の Cisco IOS 標準または拡張 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 はハードウェアで処理されます。VACL は Cisco IOS ACL を使用します。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、Internetwork Packet Exchange（IPX）、および MAC（メディア アクセス制御）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 トラフィックのみをサポートします。

VACL を設定して VLAN に適用すると、VLAN に着信するすべてのパケットが、この VACL と照合されます。VACL を VLAN に適用し、ACL を VLAN 内のルーティング対象インターフェイスに適用すると、VLAN に着信するパケットは最初に VACL と照合されます。そこで許可されると、次に入力 ACL と照合され、それからルーティング対象インターフェイスで処理されます。別の VLAN にルーティングされるパケットは、最初に、ルーティング対象インターフェイスに適用される出力 ACL と照合されます。そこで許可されると、宛先 VLAN 用に設定された VACL が適用されます。VACL が特定のパケット タイプ用に設定されていて、VACL と該当タイプのパケットとが一致しない場合、デフォルト動作では、パケットが拒否されます。

（注）
- TCP インターセプトおよび再帰 ACL は、VACL と同じインターフェイスに設定されている場合、VACL よりも優先されます。
- VACL および Context-Based Access Control（CBAC; コンテキスト ベースのアクセス制御）は、同じインターフェイス上に設定できません。
- Internet Group Management Protocol（IGMP）パケットは VACL と照合されません。

ブリッジド パケット

図 36-1 に、ブリッジド パケットに適用される VACL を示します。

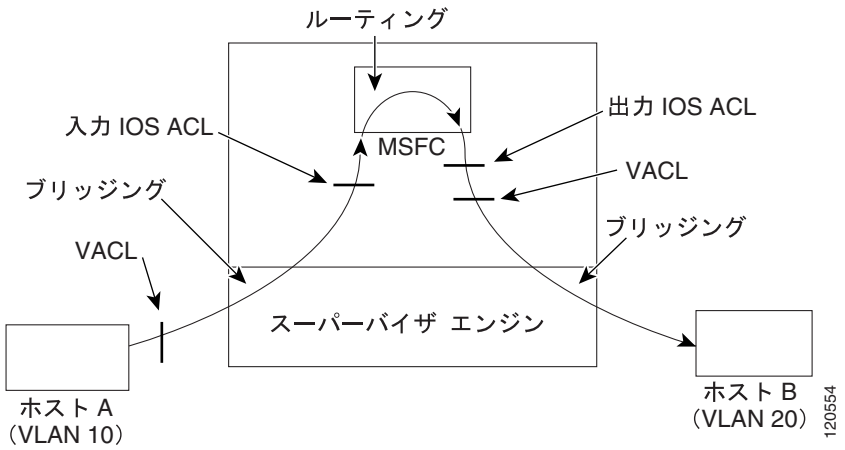
図 36-1　ブリッジド パケットへの VACL の適用

ルーティング対象パケット

図 36-2 に、ルーティング対象パケットおよびレイヤ 3 スイッチング対象パケットに ACL を適用する方法を示します。ルーティング対象パケットおよびレイヤ 3 スイッチング対象パケットに対して、ACL は次の順番で適用されます。

1. 入力 VLAN 用 VACL
2. 入力 Cisco IOS ACL
3. 出力 Cisco IOS ACL
4. 出力 VLAN 用 VACL

図 36-2　ルーティング対象パケットへの VACL の適用

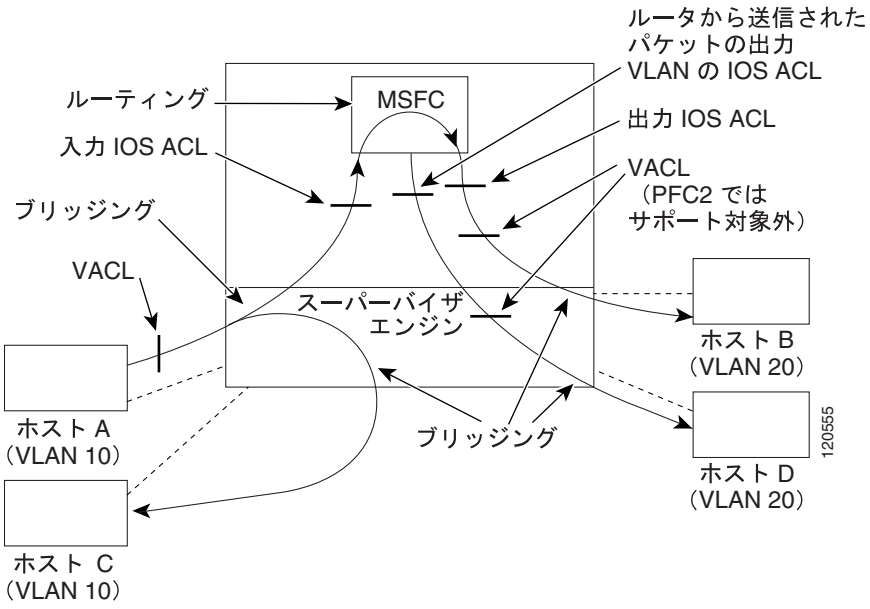


マルチキャスト パケット

図 36-3 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 VLAN 用 VACL
   b. 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 用 VACL
3. ルータから送信されるパケット — 出力 VLAN 用 VACL

図 36-3　マルチキャスト パケットへの VACL の適用



VACL の設定

ここでは、VACL の設定手順について説明します。

- VACL の設定の概要（p.36-5）
- VLAN アクセス マップの定義（p.36-6）
- VLAN アクセス マップ シーケンスでの match コマンドの設定（p.36-6）
- VLAN アクセス マップ シーケンスでの action コマンドの設定（p.36-7）
- VLAN アクセス マップの適用（p.36-8）
- VLAN アクセス マップの設定の確認（p.36-8）
- VLAN アクセス マップの設定および確認の例（p.36-9）
- キャプチャ ポートの設定（p.36-9）

VACL の設定の概要

VACL は標準および拡張 Cisco IOS IP と IPX ACL、MAC レイヤ名前付き ACL（「MAC ACL の設定」[p.42-66] 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 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 のみをサポートします。

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 コマンドと action コマンドが含まれます。match コマンドはトラフィック フィルタリング用の IP、IPX、または MAC ACL を指定します。action コマンド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、1 つまたは複数の 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 トラフィックおよびルーティング対象トラフィックの両方にアクセス制御を使用するには、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、入力と出力のルーティング対象トラフィックに対してアクセスを制御できます。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使用します。

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 での記録の必要があるパケットは、VACL で拒否された場合、記録されません。
- 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。

VACL の action コマンドには、転送（forward）、廃棄（drop）、キャプチャ（capture）、またはリダイレクト（redirect）を指定できます。トラフィックをログに記録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。

（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、1 つまたは複数の 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。
- 空または未定義の ACL が VACL 内で指定されている場合、すべてのパケットはこの 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、次の情報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 コマンドおよび action コマンドをそれぞれ 1 つのみ指定できます。
- 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.36-9）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 コマンドの設定

VLAN アクセス マップ シーケンスに match コマンドを設定するには、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} | ipx address {800-999 | acl_name}| mac address acl_name}`	VLAN アクセス マップ シーケンスに match コマンドを設定します。
`Router(config-access-map)# no match {ip address {1-199 | 1300-2699 | acl_name} | ipx address {800-999 | acl_name}| mac address acl_name}`	VLAN アクセス マップ シーケンスから match コマンドを削除します。

VLAN アクセス マップ シーケンスに match コマンドを設定する場合、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 のみをサポートします。
- match コマンドを削除したり、match コマンド内の特定の 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.42-66）を参照してください。
- Cisco IOS ACL の詳細については、次の URL にある『*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/univercd/cc/td/doc/product/software/ios122/122cgcr/fsecur_c/ftrafwl/index.htm

「VLAN アクセス マップの設定および確認の例」（p.36-9）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 コマンドの設定

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

コマンド	目的
`Router(config-access-map)# action {drop [log]} | {forward [capture]} | {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 コマンドを設定します。
`Router(config-access-map)# no action {drop [log]} | {forward [capture]} | {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 コマンドを削除します。

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

- パケットを廃棄、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のみをサポートします。WAN インターフェイスに適用された VACL は、廃棄、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。
- 転送されたパケットも、設定済み Cisco IOS セキュリティ ACL による制約を受けます。
- **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のみです。**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.36-9）を参照してください。
- 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、廃棄されたパケットがソフトウェアで記録されます。記録できるのは、廃棄された 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 のいずれか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指定することはできません。
- 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。
- PFC3 では、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した場合、SPAN は VACL リダイレクト トラフィックをコピーしません。
- PFC2 では、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した場合、SPAN は VACL リダイレクト トラフィックをコピーします。
- 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 コマンドを削除するか、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.36-9）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。
`Router(config)# no vlan filter map_name [vlan-list vlan_list | interface type[1] number[2]]`	指定した VLAN または WAN インターフェイスから VLAN アクセス マップを削除します。

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、次の情報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で作成されます。
- 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 を適用することはできません。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.36-9）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廃棄アクションによって廃棄されます。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 パケットを廃棄および記録するよう、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 トラフィックは廃棄および記録され、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 パケットは廃棄されます。

```
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 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ン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.11-9] 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.11-10] 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。
	`Router(config-if)# no switchport capture allowed vlan`	設定された宛先 VLAN リストを消去して、デフォルト値に戻します（**all**）。
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。
	`Router(config-if)# no switchport capture`	インターフェイス上のキャプチャ機能をディセーブルにします。

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

キャプチャ ポートを設定する場合、次の情報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** コマンドでキャプチャ ポートを設定してから（「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.11-9] 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** コマンドでキャプチャ ポートを設定してから（「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.11-15] を参照）、**switchport capture** コマンドを入力します。
- キャプチャ ポートは、出力トラフィックのみをサポートします。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 mordred
Vlan access-map "mordred"  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 マップでは、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 についての情報があります。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#
```

VACL ログ機能の設定

VACL ログ機能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 分経過する前にスレッシュホールドに達している場合

ログ メッセージはフロー単位で生成されます。フローは、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として定義されます。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 ログ機能には、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ので、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 パケットだけが記録されます。

VACL ログ機能を設定するには、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ます（設定情報については、「VACL の設定」[p.36-5] を参照）。こ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 テーブルが満杯になると、新しいフローのパケットが記録されても、ソフトウェアによって廃棄されます。
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廃棄されます。
ステップ 3	`Router(config)# vlan access-log threshold` *pkt_count*	ログ スレッシュホールドを設定します。5 分経過する前にフローのスレッシュホールドに達すると、ログ メッセージが生成されます。デフォルトでは、スレッシュホールド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 ログ機能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
```