CHAPTER 74

VLAN ACL（VACL）

（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、次の資料を参照してください。

  http://www.cisco.com/en/US/products/ps11846/prod_command_reference_list.html
- Cisco IOS Release 15.1SY は、イーサネット インターフェイスだけをサポートしています。Cisco IOS Release 15.1SY は、WAN 機能またはコマンドをサポートしていません。
- 最適化された ACL ロギング（OAL）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.69-13）を参照）、SPAN を使用してトラフィックをキャプチャします。
- 「PACL の VACL および Cisco IOS ACL との相互作用」（P.73-5）も参照してください。

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

技術マニュアルのアイデア フォーラムに参加する

VACL の前提条件

なし。

VACL の制約事項

- VACL は、標準および拡張 Cisco IOS IP、MAC レイヤ名前付き ACL（「MAC ACL」（P.69-9）を参照）、および VLAN アクセス マップを使用します。
- IGMP パケットは VACL と照合されません。
- VLAN アクセス マップは、VACL キャプチャの VLAN に適用できます。
- 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、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 トラフィックとルーテッド トラフィックの両方にアクセス コントロールを適用するには、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 コントロールを適用できます。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 コントロールを適用します。
- 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（ネットワーク アドレス変換）変換前のパケットに適用されます。アクセス コントロール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 コントロールされる場合があります。
- VACL は、OAL、合法的傍受（LI）、および IPv6 学習などのキャプチャを使用して、他の機能との競合をチェックします。
- 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。
- 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。
- VACL の action コマンドには、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。トラフィックをログに記録することもできます。

（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。
- 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。

VACL について

VLAN ACL（VACL）は、VLAN 内でブリッジされるか、VACL キャプチャのために VLAN 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 コントロールを行います。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 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 層トラフィックの場合は、VACL を設定できます。

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。

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。

VACL の設定方法

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。

- 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.74-5）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** | **ipv6**] **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 コマンドを設定します。

- Release 15.0(1)SY1 以降のリリースで、IPv6 ACL がサポートされます。
- 1 つまたは複数の ACL を選択できます。
- 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」（P.69-9）を参照してください。
- Cisco IOS ACL の詳細については、第 69 章「Cisco IOS ACL のサポート」および「VLAN アクセス マップの設定および確認の例」（P.74-5）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** | **vlan** *vlan_ID*]} | {**redirect** {{**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。

- 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。
- 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.74-6）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。
- **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記録されます。記録できるのは、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 メンバまたは VLAN 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。
- 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 リダイレクトされた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.74-5）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 アクセス マップを指定された VLAN に適用します。

- VLAN アクセス マップは、1 つまたは複数の VLAN 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 リスト、または VLAN ID 範囲（*vlan_ID-vlan_ID*）を指定できます。
- 各 VLAN に適用できるのは、1 つの VLAN アクセス マップだけです。
- 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。
- レイヤ 2 VLAN が存在しないか動作していない場合、VLAN に適用される VACL 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 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.74-5）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]`	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。

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 トラフィックはドロップおよび記録され、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

（注）

- 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。
- キャプチャされたトラフィックに IEEE 802.1Q 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（「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.20-9）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.20-10）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 slot/port}}`	設定するインターフェイスを指定します。

	コマンド	目的
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。

- 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 リスト、または VLAN ID 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.20-9）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.20-15）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、ギガビット イーサネット インターフェイス 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 分経過する前にしきい値に達している場合

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ます（「VLAN アクセス マップ シーケンスでの action コマンドの設定」（P.74-4）を参照してください）。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、ロギング 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。

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
```

設定された VACL ロギング プロパティを表示します。

```
Router# show vlan access-log config
```

VACL ログ テーブルの内容を表示します。

```
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]
```

パケット数、メッセージ数などの統計情報を表示します。

```
Router# show vlan access-log statistics
```

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

技術マニュアルのアイデア フォーラムに参加する