



ACL によるネットワーク セキュリティの設定

この章では、アクセス制御リスト(ACL)(アクセスリストとも呼ばれる)を使用して、IE 4000、IE 4010 および IE5000 スイッチにネットワークセキュリティを設定する手順について説明します。この章では、IP ACL の参考資料は IP Version 4 (IPv4) の ACL、ポート ACL、VLAN ACL、VLAN マップを対象としています。

- [ACL の概要](#)
- [IPv4 ACL の設定](#)
- [ACL によるネットワーク セキュリティの設定方法](#)
- [ACL によるネットワーク セキュリティのモニタリングとメンテナンス](#)
- [ACL によるネットワーク セキュリティの設定例](#)
- [ACL による VLAN マップの設定](#)
- [その他の関連資料](#)

ACL の概要

パケット フィルタリングは、ネットワーク トラフィックを限定し、特定のユーザまたはデバイスによるネットワークの使用を制限するうえで役立ちます。ACL はルータまたはスイッチを通過するトラフィックをフィルタリングし、特定のインターフェイスまたは VLAN でパケットを許可、または拒否します。ACL は、パケットに適用される許可条件および拒否条件の順序付けられた集まりです。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内のフィールドを適用される ACL と比較し、アクセス リストに指定された基準に基づいて、パケットが転送に必要な権限を持っているかどうかを確認します。アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは最初に一致した時点でテストを中止するので、リストに条件を指定する順序が重要です。一致する条件がない場合、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。スイッチは、VLAN 内でブリッジングされるパケットを含めて、転送されるすべてのパケットに ACL を使用します。

ネットワークに基本的なセキュリティを導入する場合は、ルータまたはレイヤ 3 スイッチにアクセス リストを設定します。ACL を設定しなければ、スイッチを通過するすべてのパケットがネットワークのあらゆる部分で許可される可能性があります。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。

ACL には、アクセス コントロール エントリ (ACE) 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。

ACL の概要

スイッチは、**IP ACL** とイーサネット (**MAC**) **ACL** をサポートしています。

- **IP ACL** は、TCP、ユーザ データグラム プロトコル (UDP)、インターネット グループ管理プロトコル (IGMP)、およびインターネット制御メッセージ プロトコル (ICMP) などの **IPv4** トラフィックをフィルタリングします。
- **イーサネット ACL** は非 **IP** トラフィックをフィルタリングします。

このスイッチは、**Quality of Service (QoS) 分類 ACL** もサポートしています。詳細については、「[QoS ACL に基づく分類 \(622 ページ\)](#)」を参照してください。

ここでは、次の概要について説明します。

- サポートされる [ACL \(578 ページ\)](#)
- フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理 ([580 ページ](#))

サポートされる ACL

注: ルータ **ACL** および **VLAN** マップは、**IP** サービスイメージが稼働しているスイッチ上でだけサポートされます。

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をアクセス コントロールします。スイッチでは、発信方向のポート **ACL** はサポートしません。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。詳細については、「[ポート ACL \(578 ページ\)](#)」を参照してください。

インターフェイスで **IEEE 802.1Q** トンネリングを設定している場合、トンネルポートで受信した **IEEE 802.1Q** カプセル化 **IP** パケットは、**MAC ACL** によってフィルタリングされますが、**IP ACL** ではフィルタリングされません。これは、スイッチが **IEEE 802.1Q** ヘッダー内部のプロトコルを認識しないためです。この制限は、ルータ **ACL** およびポート **ACL** に適用されます。

ポート ACL

ポート **ACL** は、スイッチのレイヤ 2 インターフェイスに適用される **ACL** です。ポート **ACL** がサポートされるのは物理インターフェイスだけで、**EtherChannel** インターフェイスではサポートされず、着信方向のインターフェイスだけに適用されます。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

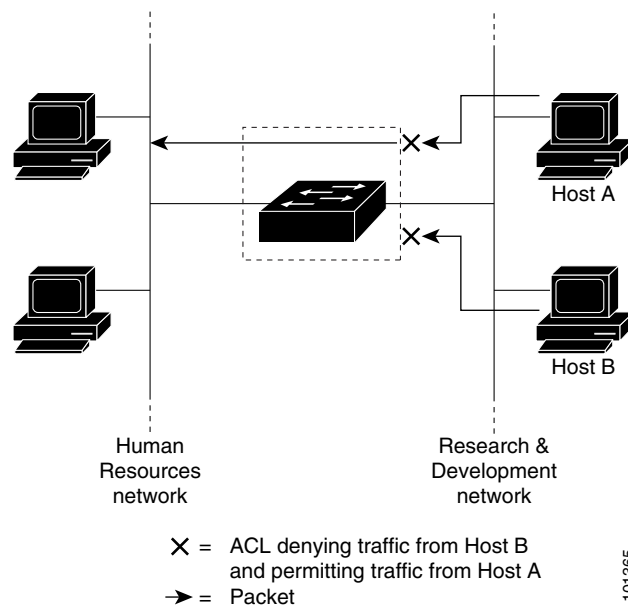
スイッチは、インターフェイスに設定されたすべての着信機能に関連付けられた **ACL** を調べ、パケットが **ACL** 内のエントリとどのように一致するかに基づいてパケットの転送を許可または拒否します。このように、**ACL** がネットワークまたはネットワークの部分へのアクセスを制御します。[図 74 \(579 ページ\)](#) に、すべてのワークステーションが同じ **VLAN** にある場合にポート **ACL** を使用してネットワークへのアクセスを制御する例を示します。レイヤ 2 入力に適用される **ACL** は、ホスト **A** に **Human Resources** ネットワークへのアクセスを許可しますが、ホスト **B** には同じネットワークへのアクセスを禁止します。ポート **ACL** は、着信方向のレイヤ 2 インターフェイスだけに適用できます。

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。ポート **ACL** を音声 **VLAN** ポートに適用すると、**ACL** はデータ **VLAN** と音声 **VLAN** の両方でトラフィックをフィルタリングします。

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: 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。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、前に設定した **ACL** が新しい **ACL** に置き換わります。

図 74 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 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。ポート ACL を音声 VLAN ポートに適用すると、ACL はデータ VLAN と音声 VLAN の両方でトラフィックをフィルタリングします。

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: 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。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、前に設定した ACL が新しい ACL に置き換わります。

ルータ ACL

VLAN へのレイヤ 3 インターフェイスであるスイッチ仮想インターフェイス (SVI)、物理層 3 インターフェイス、およびレイヤ 3 EtherChannel インターフェイスに、ルータ ACL を適用できます。ルータ ACL はインターフェイスの特定の方向 (着信または発信) に対して適用されます。1 つのインターフェイスの方向ごとに、ルータ ACL を 1 つ適用できます。

1 つの ACL をある特定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。

IPv4 トラフィックでサポートされるアクセス リストは次のとおりです。

- 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情報を使用して一致処理を行います。

ポート ACL の場合と同様、スイッチは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 が照合されます。ただし、ルータ ACL は両方向でサポートされますが、適用できるのは着信ポート ACL だけです。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 の概要

ACL は ACL 内のエントリとパケットの一致結果に応じて、パケット転送を許可するか、拒否するかを決めます。ACL を使用すると、ネットワーク全体またはネットワークの一部に対するアクセスを制御できます。図 37-1 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。

VLAN マップ

VLAN ACL または VLAN マップを使用して、すべてのトラフィックをアクセス コントロールできます。VLAN との間でルーティングされる、またはスイッチの VLAN 内でブリッジングされるすべてのパケットに、VLAN マップを適用します。

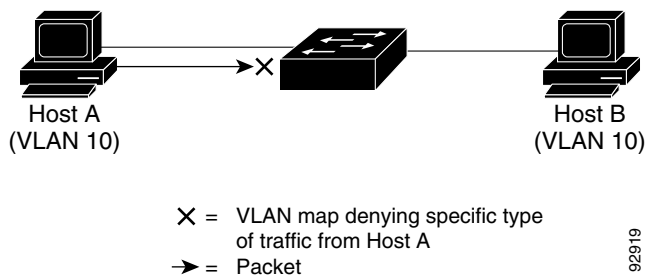
VLAN マップはセキュリティ パケット フィルタリングに使用してください。VLAN マップで方向(着信または発信)は定義されません。

VLAN マップを設定して、IPv4 トラフィックのレイヤ 3 アドレスを照合できます。

すべての非 IP プロトコルは、MAC VLAN マップを使用して、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 トラフィックは、MAC VACL マップではアクセス制御されません)。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。ハブ上またはこのスイッチに接続された別のスイッチ上のホスト間のトラフィックには、VLAN マップを適用させることができません。

VLAN マップを使用すると、マップに指定されたアクションに基づいてパケットの転送が許可または拒否されます。図 37-2 に、VLAN マップを適用して、特定のトラフィックタイプを 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。各 VLAN には、VLAN マップを 1 つだけ適用できます。

図 75 VLAN マップによるトラフィックの制御



フラグメント化されたトラフィックとフラグメント化されていないトラフィックの処理

IP パケットは、ネットワークを通過するときフラグメント化されることがあります。その場合、TCP または UDP ポート番号や ICMP タイプおよびコードなどのレイヤ 4 情報は、パケットの最初の部分があるフラグメントだけに含まれます。他のフラグメントには、この情報はありません。

ACE には、レイヤ 4 情報をチェックしないため、すべてのパケット フラグメントに適用されるものがあります。レイヤ 4 情報を調べる ACE は、フラグメント化された IP パケットのほとんどのフラグメントに標準的な方法では適用できません。フラグメントにレイヤ 4 情報が含まれておらず、ACE が一部のレイヤ 4 情報をチェックする場合、一致ルールは次のように変更されます。

- フラグメント内のレイヤ 3 情報(TCP や UDP などのプロトコル タイプを含む)をチェックする許可 ACE は、含まれていないレイヤ 4 情報の種類にかかわらず、フラグメントと一致すると見なされます。
- レイヤ 4 情報をチェックする拒否 ACE は、フラグメントにレイヤ 4 情報が含まれていない限り、フラグメントと一致しません。

IPv4 ACL の設定

次のコマンドで構成され、フラグメント化された 3 つのパケットに適用されるアクセス リスト 102 を例に取って説明します。

```
Switch(config)# access-list 102 permit tcp any host 10.1.1.1 eq smtp
Switch(config)# access-list 102 deny tcp any host 10.1.1.2 eq telnet
Switch(config)# access-list 102 permit tcp any host 10.1.1.2
Switch(config)# access-list 102 deny tcp any any
```

注:最初の 2 つの ACE には宛先アドレスの後に `eq` キーワードがありますが、これは既知の TCP 宛先ポート番号がそれぞれシンプルメール転送プロトコル (SMTP) および Telnet と一致するかどうかをチェックすることを意味します。

- パケット A は、ホスト 10.2.2.2 のポート 65000 からホスト 10.1.1.1 の SMTP ポートに送信される TCP パケットです。このパケットがフラグメント化された場合、レイヤ 4 情報がすべて揃っているため、完全なパケットである場合と同じように最初のフラグメントが最初の ACE (`permit`) と一致します。残りのフラグメントも最初の ACE と一致します。これは、それらのフラグメントに SMTP ポート情報が含まれていなくても、最初の ACE が適用されたときにレイヤ 3 情報だけをチェックするからです。この例の情報は、パケットが TCP であることと、宛先が 10.1.1.1 であることです。
- パケット B は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.2 の Telnet ポートに送信されます。このパケットがフラグメント化された場合、レイヤ 3 情報とレイヤ 4 情報がすべて揃っているため、最初のフラグメントが 2 つめの ACE (`deny`) と一致します。残りのフラグメントは、レイヤ 4 情報が含まれていないため、2 つめの ACE と一致しません。残りのフラグメントは 3 つめの ACE (`permit`) と一致します。

最初のフラグメントが拒否されたため、ホスト 10.1.1.2 は完全なパケットを再構成できず、その結果、パケット B は拒否されます。ただし、以降の許可されたフラグメントがネットワークの帯域幅を使用し、ホスト 10.1.1.2 がパケットを再構成しようとするときにホストのリソースが消費されます。

- フラグメント化されたパケット C は、ホスト 10.2.2.2 のポート 65001 からホスト 10.1.1.3 のポート ftp に送信されます。このパケットがフラグメント化された場合、最初のフラグメントが 4 つめの ACE (`deny`) と一致します。ACE はレイヤ 4 情報をチェックせず、すべてのフラグメントのレイヤ 3 情報に宛先がホスト 10.1.1.3 であることが示され、前の `permit` ACE は異なるホストをチェックしていたため、他のフラグメントもすべて 4 つめの ACE と一致します。

IPv4 ACL の設定

このスイッチで IPv4 ACL を設定する手順は、他の Cisco スイッチやルータで IPv4 ACL を設定する手順と同じです。

1. アクセス リストの番号または名前とアクセス条件を指定して、ACL を作成します。
2. その ACL をインターフェイスまたは端末回線に適用します。

設定の詳細については、以下の項を参照してください。

- [標準 IPv4 ACL および拡張 IPv4 ACL の作成](#)
- [端末回線への IPv4 ACL の適用](#)
- [インターフェイスへの IPv4 ACL アプリケーション適用の注意事項](#)
- [IP ACL のハードウェアおよびソフトウェアの処理](#)
- [ACL のトラブルシューティング](#)

標準 IPv4 ACL および拡張 IPv4 ACL の作成

ここでは、**IP ACL** について説明します。**ACL** は、許可条件と拒否条件の順序付けられた集まりです。スイッチは、アクセス リスト内の条件を 1 つずつ調べ、パケットをテストします。最初に一致した条件によって、スイッチがパケットを受け入れるか拒否するかが決定されます。スイッチは一致する最初の条件が見つかった時点でパケットのテストを停止するため、条件の順序が重要な意味を持ちます。一致する条件がない場合、スイッチはパケットを拒否します。

このソフトウェアは、**IPv4** について次の **ACL** (アクセス リスト) をサポートします。

- 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 リストでは、照合操作に送信元アドレスと宛先アドレスを使用し、任意でプロトコル タイプ情報を使用して制御のきめ細かさを高めることもできます。

スイッチは、**host** 一致条件があるエントリと **don't care** マスク **0.0.0.0** を含む一致条件があるエントリがリストの先頭に移動し、**0** 以外の **don't care** マスクを含むエントリよりも前に位置するように、標準アクセス リストの順序を書き換えます。そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、**ACE** が必ずしも入力されたとおりの順序で配置されません。

作成した番号付き標準 IPv4 ACL は、端末回線(端末回線への IPv4 ACL の適用 (595 ページ) を参照)、インターフェイス(インターフェイスへの IPv4 ACL の適用 (596 ページ) を参照)、または VLAN (ACL によるネットワーク セキュリティのモニタリングとメンテナンス (597 ページ) を参照) に適用できます。

アクセス リスト番号

ACL を識別するために使用する番号は、作成するアクセス リストのタイプを表します。表 55 (582 ページ) に、アクセス リスト番号と対応するアクセス リスト タイプを挙げ、このスイッチでサポートされているかどうかを示します。このスイッチは、IPv4 標準アクセス リストおよび拡張アクセス リスト (1 ~ 199 および 1300 ~ 2699) をサポートします。

表 55 アクセスリスト番号のサポート

アクセス リスト番号	タイプ	サポート対象
1 ~ 99	IP 標準アクセス リスト	○
100 ~ 199	IP 拡張アクセス リスト	○
200 ~ 299	プロトコル タイプコード アクセス リスト	なし
300 ~ 399	DECnet アクセス リスト	なし
400 ~ 499	XNS 標準アクセス リスト	なし
500 ~ 599	XNS 拡張アクセス リスト	なし
600 ~ 699	AppleTalk アクセス リスト	なし
700 ~ 799	48 ビット MAC アドレス アクセス リスト	なし
800 ~ 899	IPX 標準アクセス リスト	なし
900 ~ 999	IPX 拡張アクセス リスト	なし
1000 ~ 1099	IPX SAP アクセス リスト	なし
1100 ~ 1199	拡張 48 ビット MAC サマリー アドレス アクセス リスト	なし
1200 ~ 1299	IPX サマリー アドレス アクセス リスト	なし
1300 ~ 1999	IP 標準アクセス リスト (拡張範囲)	○
2000 ~ 2699	IP 拡張アクセス リスト (拡張範囲)	あり

注: 番号付き標準 ACL および番号付き拡張 ACL に加え、サポートされる番号を使用して名前付き標準 IP ACL および名前付き拡張 IP ACL も作成できます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名前は 100 ~ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

IPv4 ACL の設定

ACL のロギング

標準 IP アクセス リストによって許可または拒否されたパケットに関するログ メッセージが、スイッチのソフトウェアによって表示されます。つまり、ACL と一致するパケットがあった場合は、そのパケットに関するログ通知メッセージがコンソールに送信されます。コンソールに表示されるメッセージのレベルは、**Syslog** メッセージを制御するロギング コンソール コマンドで制御されます。

注: ルーティングはハードウェアで、ロギングはソフトウェアで実行されます。したがって、**log** キーワードを含む許可 (**permit**) または拒否 (**deny**) ACE と一致するパケットが多数存在する場合、ソフトウェアはハードウェアの処理速度に追いつくことができないため、一部のパケットはロギングされない場合があります。

ACL を起動した最初のパケットについては、ログ メッセージがすぐに表示されますが、それ以降のパケットについては、5 分間の収集時間が経過してから表示またはロギングされます。ログ メッセージにはアクセス リスト番号、パケットの許可または拒否に関する状況、パケットの送信元 IP アドレス、および直前の 5 分間に許可または拒否された送信元からのパケット数が示されます。

番号付き標準 ACL の作成

	コマンド	目的
ステップ 1	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	access-list access-list-number {deny permit} source [source-wildcard] [log]	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 <i>access-list-number</i> 値は、1 ~ 99 または 1300 ~ 1999 の範囲の 10 進数値です。 条件が一致した場合にアクセスを拒否する場合は deny 、許可する場合は permit を指定します。 <i>source</i> には、パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 ドット付き 10 進表記による 32 ビット長の値。 ■ キーワード any は 0.0.0.0 255.255.255.255 という <i>source</i> および <i>source-wildcard</i> の省略形です。 <i>source-wildcard</i> を入力する必要はありません。 ■ <i>source</i> および <i>source-wildcard</i> の値 <i>source</i> 0.0.0.0 の省略形を意味するキーワード host 。 (任意) <i>source-wildcard</i> は、ワイルドカードビットを送信元アドレスに適用します。 (任意) log を指定すると、エン트리と一致するパケットに関するログ通知メッセージがコンソールに送信されます。 (任意) log を指定すると、エン트리と一致するパケットに関するログ通知メッセージがコンソールに送信されます。
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show access-lists [number name]	アクセス リストの設定を表示します。
ステップ 5	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。

IPv4 ACL の設定

注:ACL 全体を削除するには、**no access-list access-list-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。番号付きアクセス リストから個々の ACE は削除できません。

ACL 全体を削除するには、**no access-list access-list-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。番号付きアクセス リストから個々の ACE は削除できません。

次に、IP ホスト 171.69.198.102 へのアクセスを拒否し、他のすべてのホストへのアクセスを許可し、結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
10 deny 171.69.198.102
20 permit any
```

スイッチは、**host** 一致条件があるエントリと **don't care** マスク 0.0.0.0 を含む一致条件があるエントリがリストの先頭に移動し、0 以外の **don't care** マスクを含むエントリよりも前に位置するように、標準アクセスリストの順序を書き換えます。

そのため、**show** コマンドの出力やコンフィギュレーション ファイルでは、ACE が必ずしも入力されたとおりの順序で配置されません。

番号付き拡張 ACL の作成

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさが高めることができます。番号付き拡張アクセス リストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

次の IP プロトコルがサポートされます(プロトコルキーワードはカッコ内に**太字**で示してあります)。

認証ヘッダープロトコル(**ahp**)、Enhanced IGRP(**eigrp**)、Encapsulating Security Payload(**esp**)、Generic Routing Encapsulation(**gre**)、Internet Control Message Protocol(**icmp**)、Internet Group Management Protocol(**igmp**)、任意の内部プロトコル(**ip**)、IP-in-IP トンネリング(**ipinip**)、KA9Q NOS 互換 IP over IP トンネリング(**nos**)、Open Shortest Path First ルーティング(**ospf**)、Payload Compression Protocol(**pcp**)、Protocol Independent Multicast(**pim**)、伝送制御プロトコル(**tcp**)、ユーザ データグラム プロトコル(**udp**)

注:ICMP エコー応答はフィルタ処理できません。他の ICMP コードまたはタイプは、すべてフィルタリングできます。

注:このスイッチは、ダイナミックまたはリフレクシブアクセスリストをサポートしていません。また、タイプ オブ サービス (ToS) の **minimize-monetary-cost** ビットに基づくフィルタリングもサポートしていません。

サポートされているパラメータのカテゴリは、TCP、UDP、ICMP、IGMP、その他の IP です。

ACL の作成後に(端末からの入力などによって)追加したエントリは、リストの末尾に追加されます。番号付きアクセス リストの特定の場所にはアクセス リスト エントリを追加または削除できません。

注:ACL を作成する際には、アクセスリストの末尾に暗黙の **deny** ステートメントがデフォルトで存在し、ACL の終わりに到達するまで一致が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号付き拡張 ACL は、端末回線(端末回線への IPv4 ACL の適用 (595 ページ)を参照)、インターフェイス(インターフェイスへの IPv4 ACL の適用 (596 ページ)を参照)、または VLAN (ACL によるネットワーク セキュリティのモニタリングとメンテナンス (597 ページ)を参照)に適用できます。

IPv4 ACL の設定

	コマンド	目的
ステップ 1	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 2a	<p>access-list access-list-number {deny permit} protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</p> <p>注: dscp 値を入力した場合、tos または precedence は入力できません。dscp を入力しない場合は、tos と precedence 値の両方を入力できます。</p>	<p>拡張 IPv4 アクセス リストおよびアクセス条件を定義します。access-list-number には、100 ~ 199 または 2000 ~ 2699 の 10 進数を指定します。</p> <p>条件が一致した場合にパケットを拒否する場合は deny を指定し、許可する場合は permit を指定します。protocol には、IP プロトコルの名前または番号を入力します。指定には、ahp、eigrp、esp、gre、icmp、igmp、igrp、ip、ipinip、nos、ospf、pcp、pim、tcp、udp、または IP プロトコル番号を表す 0 ~ 255 の整数を使用できます。一致条件としてインターネット プロトコル (ICMP、TCP、UDP など) を指定するには、キーワード ip を使用します。</p> <p>注: この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加のパラメータについては、ステップ 2b ~ 2e を参照してください。</p> <p>source には、パラメータの送信元であるネットワークまたはホストの番号を指定します。</p> <p>source-wildcard は、ワイルドカード ビットを送信元アドレスに適用します。</p> <p>destination には、パラメータの宛先であるネットワークまたはホストの番号を指定します。</p> <p>destination-wildcard は、ワイルドカード ビットを宛先アドレスに適用します。</p> <p>source、source-wildcard、destination、および destination-wildcard の値は、次の形式で指定します。</p> <ul style="list-style-type: none"> ■ ドット付き 10 進表記による 32 ビット長の値。 ■ 0.0.0.0 255.255.255.255 (任意のホスト) を表すキーワード any。 ■ 単一のホスト 0.0.0.0 を表すキーワード host。

IPv4 ACL の設定

	コマンド	目的
ステップ 2a、 続き		<p>その他のキーワードはオプションであり、次の意味を持ちます。</p> <ul style="list-style-type: none"> ■ precedence: パケットを 0 ～ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、routine (0)、priority (1)、immediate (2)、flash (3)、flash-override (4)、critical (5)、internet (6)、network (7) です。 ■ fragments: 2 つめ以降のフラグメントをチェックする場合に入力します。 ■ tos: パケットを 0 ～ 15 の番号または名前で指定するサービスタイプレベルと一致させる場合に入力します。指定できる値は、normal (0)、max-reliability (2)、max-throughput (4)、min-delay (8) です。 ■ log: エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。log-input を指定すると、ログエントリに入力インターフェイスが追加されます。 ■ dscp 値を入力した場合、tos または precedence は入力できません。dscp を入力しない場合は、tos と precedence 値の両方を入力できます。 ■ time-range: このキーワードの詳細については、37-17 ページの「ACL での時間範囲の使用」を参照してください。 ■ dscp: 0 ～ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符 (?) を使用すると、使用可能な値のリストが表示されます。
または	<pre>access-list access-list-number {deny permit} protocol any any [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</pre>	<p>アクセス リスト コンフィギュレーション モードで、source および source wildcard の値 0.0.0.0 255.255.255.255 の省略形と destination および destination wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。</p> <p>送信元と宛先のアドレスおよびワイルドカードの代わりに any キーワードを使用できます。</p>
または	<pre>access-list access-list-number {deny permit} protocol host source host destination [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]</pre>	<p>source および source wildcard の値 source 0.0.0.0 の省略形と destination および destination wildcard の値 destination 0.0.0.0 の省略形を使用して、拡張 IP アクセス リストを定義します。</p> <p>送信元と宛先のワイルドカードまたはマスクの代わりに host キーワードを使用できます。</p>

IPv4 ACL の設定

	コマンド	目的
ステップ 2b	access-list access-list-number {deny permit} tcp source source-wildcard [operator port] destination destination-wildcard [operator port] [established] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] [flag]	<p>(任意)拡張 TCP アクセス リストおよびアクセス条件を定義します。</p> <p>TCP の場合は tcp を入力します。</p> <p>次の例外を除き、ステップ 2a の説明にあるパラメータと同じパラメータを使用します。</p> <p>(任意)operator および port を入力すると、送信元ポート (source source-wildcard の後に入力した場合) または宛先ポート (destination destination-wildcard の後に入力した場合) が比較されます。使用可能な演算子は、eq (等しい)、gt (より大きい)、lt (より小さい)、neq (等しくない)、range (包含範囲) などです。演算子にはポート番号を指定する必要があります (range の場合は 2 つのポート番号をスペースで区切って指定する必要があります)。</p> <p>port には、10 進数 (0 ~ 65535) のポート番号または TCP ポート名を入力します。TCP ポート名を確認するには、「?」を使用するか、『Cisco IOS IP Configuration Guide, Release 12.2』の「IP Addressing and Services」の章にある「Configuring IP Services」を参照してください。TCP をフィルタリングするときには、TCP ポートの番号または名前だけを使用します。</p> <p>他のオプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> ■ established: 確立された接続と照合する場合に入力します。このキーワードは、ack または rst フラグでの照合と同じ機能を果たします。 ■ flag: 指定された TCP ヘッダービットを基準にして照合します。入力できるフラグは、ack (確認応答)、fin (終了)、psh (プッシュ)、rst (リセット)、syn (同期)、または urg (緊急) です。
ステップ 2c	access-list access-list-number {deny permit} udp source source-wildcard [operator port] destination destination-wildcard [operator port] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]	<p>(任意)拡張 UDP アクセス リストおよびアクセス条件を定義します。</p> <p>ユーザ データグラム プロトコルの場合は、udp を入力します。</p> <p>UDP パラメータは TCP の説明にあるパラメータと同じです。ただし、[operator [port]] ポート番号またはポート名は、UDP ポートの番号または名前だけでなく、flag および established パラメータは無効です。</p>

IPv4 ACL の設定

	コマンド	目的
ステップ 2d	access-list access-list-number {deny permit} icmp source source-wildcard destination destination-wildcard [icmp-type [[icmp-type icmp-code] [icmp-message]] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]	<p>(任意) 拡張 ICMP アクセス リストおよびアクセス条件を定義します。</p> <p>Internet Control Message Protocol の場合は、icmp を入力します。</p> <p>ICMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、ICMP メッセージタイプおよびコードパラメータが追加されています。オプションのキーワードの意味は次のとおりです。</p> <ul style="list-style-type: none"> ■ icmp-type: ICMP メッセージタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。 ■ icmp-code: ICMP パケットを ICMP メッセージコードタイプでフィルタリングする場合に入力します。指定できる値の範囲は、0 ~ 255 です。 ■ icmp-message: ICMP パケットを ICMP メッセージタイプ名または ICMP メッセージタイプとコード名でフィルタリングする場合に入力します。ICMP メッセージのリストを表示するには
ステップ 2e	access-list access-list-number {deny permit} igmp source source-wildcard destination destination-wildcard [igmp-type] [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp]	<p>(任意) 拡張 IGMP アクセス リストおよびアクセス条件を定義します。</p> <p>インターネット グループ管理プロトコルの場合は、igmp を入力します。</p> <p>IGMP パラメータはステップ 2a の IP プロトコルの説明にあるパラメータとほとんど同じですが、次に示すオプションのパラメータが追加されています。</p> <p>igmp-type: IGMP メッセージタイプと照合するには、0 ~ 15 の番号またはメッセージ名 (dvmrp、host-query、host-report、pim、または trace) を入力します。</p>
ステップ 3	end	特権 EXEC モードに戻ります。
ステップ 4	show access-lists [number name]	アクセス リストの設定を確認します。
ステップ 5	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。

アクセスリスト全体を削除するには、**no access-list access-list-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。番号付きアクセス リストから個々の ACE は削除できません。

次に、ネットワーク 171.69.198.0 のすべてのホストからネットワーク 172.20.52.0 のすべてのホストへの Telnet アクセスを拒否し、他のすべてのアクセスを許可する拡張アクセス リストを作成し、表示する例を示します (eq キーワードを宛先アドレスの後に指定すると、Telnet に対応する TCP 宛先ポート番号がチェックされます)。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
 10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
 20 permit tcp any any
```

IPv4 ACL の設定

ACL の作成後に(端末からの入力などによって)追加したエントリは、リストの末尾に追加されます。番号付きアクセス リストの特定の場所にはアクセス リスト エントリを追加または削除できません。

注:ACL を作成する際には、アクセスリストの末尾に暗黙の **deny** ステートメントがデフォルトで存在し、ACL の終わりに到達するまで一致が見つからなかったすべてのパケットに適用されることに注意してください。

作成した番号付き拡張 ACL は、端末回線(「[端末回線への IPv4 ACL の適用](#)」の項を参照)、インターフェイス(「[インターフェイスへの IPv4 ACL の適用](#)」の項を参照)、または VLAN(「[VLAN マップの設定](#)」の項を参照)に適用できます

ACL 内の ACE の並べ替え

アクセス リスト内のエントリのシーケンス番号は、新しい ACL の作成時に自動的に生成されます。**ip access-list resequence** グローバル コンフィギュレーション コマンドを使用して、ACL のシーケンス番号を編集したり、ACE の適用順序を変更したりできます。たとえば、ACL に新しい ACE を追加すると、その ACE はリストの末尾に配置されます。この場合、シーケンス番号を変更することで、ACE を ACL 内の別の位置に移動できます。

名前付き標準 ACL および拡張 ACL

IPv4 ACL を識別する手段として、番号ではなく英数字のストリング(名前)を使用できます。名前付き ACL を使用すると、ルータ上で番号付きアクセス リストの場合より多くの IPv4 アクセス リストを設定できます。アクセス リストの識別手段として名前を使用する場合のモードとコマンド構文は、番号を使用する場合とは多少異なります。ただし、IP アクセス リストを使用するすべてのコマンドを名前付きアクセス リストで使用できるわけではありません。

注:標準 ACL または拡張 ACL に指定する名前は、アクセスリスト番号のサポートされる範囲内の番号にすることもできます。標準 IP ACL の名前は 1 ~ 99 で、拡張 IP ACL の名前は 100 ~ 199 です。番号付きリストの代わりに名前付き ACL を使用することには、エントリを個別に削除できるという利点があります。

名前付き ACL を設定する際には、次の注意事項および制限事項に留意してください。

- 番号付き ACL で使用できるすべてのコマンドが名前付き ACL でも使用できるわけではありません。インターフェイスのパケット フィルタおよびルート フィルタ用の ACL では、名前を使用できます。
- 標準 ACL と拡張 ACL に同じ名前は使用できません。
- [番号制標準 ACL の作成\(593 ページ\)](#)で説明したとおり、番号付き ACL も使用できます。

標準 ACL または拡張 ACL を作成する際には、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準 ACL では、関連付けられた IP ホストアドレス アクセス リストの指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

ACL の作成後に追加したエントリは、リストの末尾に追加されます。ACL エントリを特定の ACL に選択的に追加できません。ただし、**no permit** および **no deny** アクセス リスト コンフィギュレーション モード コマンドを使用すると、名前付き ACL からエントリを削除できます。次に、名前付きアクセス リスト *border-list* から ACE を個別に削除する例を示します。

```
Switch(config)# ip access-list extended border-list
Switch(config-ext-nacl)# no permit ip host 10.1.1.3 any
```

番号付き ACL ではなく名前付き ACL を使用する理由の 1 つとして、名前付き ACL では行を選択して削除できることがあります。

ACL の時間範囲

time-range グローバル コンフィギュレーション コマンドを使用することによって、時刻および曜日に基づいて拡張 ACL を選択的に適用できます。まず、時間範囲の名前を定義し、その時間範囲内の時刻および日付または曜日を設定します。次に、ACL を適用してアクセス リストに制限を設定するときに時間範囲を入力します。時間範囲を使用すると、ACL の許可ステートメントまたは拒否ステートメントの有効期間(指定期間内や指定曜日など)を定義できます。

IPv4 ACL の設定

時間範囲を使用する利点の一部を次に示します。

- アプリケーションなどのリソース (IP アドレスとマスクのペア、およびポート番号で識別) へのユーザ アクセスをより厳密に許可または拒否できます。
- ログ メッセージを制御できます。ACL エントリを使用して特定の時刻に関してのみトラフィックをロギングできるため、ピーク時間に生成される多数のログを分析しなくても、簡単にアクセスを拒否できます。

時間ベースのアクセス リストを使用すると、CPU に負荷が生じます。これは、アクセス リストの新しい設定を他の機能や TCAM にロードされた結合済みの設定とマージする必要があるためです。そのため、複数のアクセス リストが短期間に連続して (互いに数分以内に) 有効となるような設定とならないように注意する必要があります。

注: 時間範囲は、スイッチのシステムクロックに基づきます。したがって、信頼できるクロックソースが必要です。ネットワーク タイム プロトコル (NTP) を使用してスイッチクロックを同期させることを推奨します。

ACL へのコメント

remark キーワードを使用すると、任意の IP 標準または拡張 ACL にエントリに関するコメント (注釈) を追加できます。コメントを使用すると、ACL の理解とスキャンが容易になります。1 つのコメント行の最大長は 100 文字です。

コメントは、**permit** ステートメントまたは **deny** ステートメントの前後どちらにでも配置できます。コメントがどの **permit** ステートメントまたは **deny** ステートメントの説明であるのかが明確になるように、コメントの位置に関して一貫性を保つ必要があります。たとえば、あるコメントは対応する **permit** または **deny** ステートメントの前にあり、他のコメントは対応するステートメントの後ろにあると、混乱を招く可能性があります。

番号付き IP 標準または拡張 ACL にコメントを挿入するには、**access-list access-list number remark remark** 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。コメントを削除するには、このコマンドの **no** 形式を使用します。

端末回線への IPv4 ACL の適用

番号付き ACL を使用して、1 つまたは複数の端末回線へのアクセスを制御できます。端末回線には名前付き ACL を適用できません。すべての仮想端末回線にユーザが接続する可能性があるため、すべてに同じ制限を設定する必要があります。

ACL をインターフェイスに適用する手順については、[インターフェイスへの IPv4 ACL の適用 \(596 ページ\)](#) を参照してください。VLAN への ACL の適用については、[ACL によるネットワーク セキュリティのモニタリングとメンテナンス \(597 ページ\)](#) を参照してください。

インターフェイスへの IPv4 ACL アプリケーション適用の注意事項

- ACL は着信レイヤ 2 ポートだけに適用してください。
- レイヤ 3 インターフェイスには、発信側または着信側のいずれかに ACL を適用してください。
- インターフェイスへのアクセスを制御する場合、名前付き ACL または番号付き ACL を使用できます。
- VLAN のメンバであるポートに ACL を適用すると、そのポートの ACL は VLAN インターフェイスに適用された ACL よりも優先されます。
- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL よりも優先します。ポートの ACL は常にレイヤ 2 ポートで受信した着信パケットをフィルタリングします。
- レイヤ 3 インターフェイスに ACL が適用され、ルーティングがイネーブルになっていない場合は、SNMP、Telnet、Web トラフィックなど、CPU で処理されるパケットだけがフィルタリングされます。レイヤ 2 インターフェイスに ACL を適用する場合、ルーティングをイネーブルにする必要はありません。
- プライベート VLAN が設定されている場合、プライマリ VLAN SVI にだけルータ ACL を適用できます。ACL はプライマリおよびセカンダリ VLAN のレイヤ 3 トラフィックに適用されます。

IPv4 ACL の設定

注: パケットがアクセスグループによって拒否された場合、デフォルトでは、ルータは **Internet Control Message Protocol (ICMP)** 到達不能メッセージを送信します。アクセスグループによって拒否されたこれらのパケットはハードウェアでドロップされず、スイッチの **CPU** にブリッジングされて、**ICMP** 到達不能メッセージを生成します。ポート **ACL** は例外です。ポート **ACL** は **ICMP** 到達不能メッセージを生成しません。

ICMP 到達不能メッセージは、ルータ **ACL** で **no ip unreachable** インターフェイス コマンドを使用してディセーブルにできます。

着信 **ACL** の場合、スイッチはパケットの受信後に **ACL** とパケットを照合します。**ACL** がパケットを許可する場合、スイッチはパケットの処理を継続します。**ACL** がパケットを拒否する場合、スイッチはパケットを廃棄します。

発信 **ACL** の場合、スイッチは、制御されたインターフェイスとの間でパケットを送受信した後に **ACL** とパケットを照合します。**ACL** がパケットを許可した場合は、スイッチはパケットを送信します。**ACL** がパケットを拒否する場合、スイッチはパケットを廃棄します。

デフォルトでは、パケットが廃棄された場合は、その原因が入力インターフェイスの **ACL** または発信インターフェイスの **ACL** のいずれであっても、常に入力インターフェイスから **ICMP** 到達不能メッセージが送信されます。**ICMP** 到達不能メッセージは通常、入力インターフェイス 1 つにつき、**0.5** 秒ごとに 1 つだけ生成されます。ただし、この設定は **ip icmp rate-limit unreachable** グローバル コンフィギュレーション コマンドを使用して変更できます。

未定義の **ACL** をインターフェイスに適用すると、スイッチは **ACL** がインターフェイスに適用されていないと判断して処理を行い、すべてのパケットが許可されてしまいます。ネットワーク セキュリティのために未定義の **ACL** を使用する場合は、このような結果が生じることに注意してください。

IP ACL のハードウェアおよびソフトウェアの処理

ACL の処理は主にハードウェアで実行されますが、トラフィック フローの中には **CPU** に転送してソフトウェア処理を行う必要があるものもあります。ハードウェアで **ACL** の設定を保存する領域が不足すると、パケットは転送のために **CPU** に送られます。ソフトウェア転送トラフィックの転送レートは、ハードウェア転送トラフィックより大幅に低くなります。

注: スwitchのリソース不足が原因でハードウェアに **ACL** を設定できない場合、影響を受ける(ソフトウェアで転送される)のは、スイッチに着信した該当 **VLAN** 内のトラフィックだけです。パケットのソフトウェア転送が発生すると、消費される **CPU** サイクル数に応じて、スイッチのパフォーマンスが低下することがあります。

ルータ **ACL** の場合は、次の場合にパケットが **CPU** に送信されることがあります。

- **log** キーワードを使用する。
- **ICMP** 到達不能メッセージを生成する。

トラフィック フローのロギングと転送の両方を行う場合、転送はハードウェアで処理されますが、ロギングはソフトウェアで処理する必要があります。ハードウェアとソフトウェアではパケット処理能力が異なるため、ロギング中であるすべてのフロー(許可フローと拒否フロー)の合計帯域幅が非常に大きい場合は、転送されたパケットの一部をロギングできません。

ルータ **ACL** の設定をハードウェアに適用できない場合、**VLAN** に着信したルーティング対象パケットはソフトウェアでルーティングされますが、ブリッジングはハードウェアで行われます。**ACL** により多数のパケットが **CPU** に送信されると、スイッチのパフォーマンスが低下する可能性があります。

show ip access-lists 特権 **EXEC** コマンドを入力した場合、表示される一致カウントには、ハードウェアでアクセスが制御されるパケットは含まれません。スイッチドおよびルーテッドパケットに関するハードウェアの **ACL** の基本的な統計情報を取得する場合は、**show access-lists hardware counters** 特権 **EXEC** コマンドを使用します。

ACL のトラブルシューティング

[chars] がアクセスリスト名となる、次の ACL マネージャのメッセージが表示された場合、スイッチは ACL のハードウェア領域を確保するためのリソースが不足しています。

```
ACLMGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

このリソースには、ハードウェア メモリおよびラベル スペースが含まれますが、CPU メモリは含まれません。この問題の原因は、使用可能な論理演算ユニットまたは専用のハードウェア リソースの不足です。論理演算ユニットは、TCP フラグの一致、または TCP、UDP、SCTP ポート番号での **eq** 以外 (**ne**、**gt**、**lt**、**range**) のテストが必要です。

次のいずれかの回避策を使用します。

- ACL 設定を変更して使用するリソースを減らします。
- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します。

専用のハードウェア リソースを識別するには、**show platform layer4 acl map** 特権 EXEC コマンドを入力します。スイッチに使用可能なリソースがない場合は、出力に **index 0 ~ index 15** が使用できないことが示されます。

十分なリソースがない ACL の設定の詳細については、Bug Toolkit の CSCsq63926 を参照してください。

名前付き MAC 拡張 ACL

VLAN またはレイヤ 2 インターフェイスで非 IPv4 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。

注: レイヤ 3 インターフェイスには、名前付き MAC 拡張 ACL を適用できません。

注: **appletalk** は、コマンドラインのヘルプ文字列に表示されますが、**deny** および **permit MAC** アクセス リスト コンフィギュレーション モード コマンドの一致条件としてサポートされていません。

レイヤ 2 インターフェイスへの MAC ACL

MAC ACL を作成し、それをレイヤ 2 インターフェイスに適用すると、そのインターフェイスに着信する非 IP トラフィックをフィルタリングできます。MAC ACL を適用するときには、次の注意事項に留意してください。

- VLAN に属しているレイヤ 2 インターフェイスに ACL を適用した場合、レイヤ 2 (ポート) ACL は VLAN インターフェイスに適用された入力方向のレイヤ 3 ACL よりも優先します。レイヤ 2 ポートで受信する着信パケットは、常にポート ACL でフィルタリングされます。
- 同じレイヤ 2 インターフェイスには、IP アクセス リストと MAC アクセス リストを 1 つずつしか適用できません。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、MAC アクセス リストは非 IP パケットをフィルタリングします。
- 1 つのレイヤ 2 インターフェイスに適用できる MAC アドレス リストは 1 つだけです。すでに MAC ACL が設定されているレイヤ 2 インターフェイスに 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。

ACLによるネットワークセキュリティの設定方法

番号制標準 ACL の作成

注:ACLを作成するときには、ACLの末尾にデフォルトで暗黙的な deny ステートメントが追加され、ACLの終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセスリストでは、関連付けられた IP ホストアドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

コマンド	目的
1. 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。
2. access-list access-list-number {deny permit} source [source-wildcard] [log] 注:ACL全体を削除するには、no access-list access-list-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。	送信元アドレスとワイルドカードを使用して標準 IPv4 アクセス リストを定義します。 access-list-number : 1 ~ 99 または 1300 ~ 1999 の 10 進数を指定します。 deny または permit : 条件が一致した場合にアクセスを拒否する場合は deny 、許可する場合は permit を指定します。 source : パケットの送信元となるネットワークまたはホストのアドレスを次の形式で指定します。 ■ ドット付き 10 進表記による 32 ビット長の値。 ■ source および source-wildcard の 0.0.0.0 255.255.255.255 の省略形を意味するキーワード any 、 source-wildcard を入力する必要はありません。 ■ source および source-wildcard の値 source 0.0.0.0 の省略形を意味するキーワード host 。 (任意) source-wildcard : ワイルドカードビットを送信元アドレスに適用します。 (任意) log : コンソールに送信されるエントリに一致するパケットに関するロギングメッセージ情報が出力されます。
3. end	特権 EXEC モードに戻ります。
4. show access-lists [number name]	アクセス リストの設定を表示します。
5. 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。

番号付き拡張 ACL の作成

標準 ACL では照合に送信元アドレスだけを使用しますが、拡張 ACL では、照合操作に送信元アドレスと宛先アドレスを使用でき、任意でプロトコル タイプ情報を使用して制御のきめ細かさが高めることができます。番号付き拡張アクセスリストの ACE を作成するときには、作成した ACE がリストの末尾に追加されることに注意してください。番号付きリストでは、ACE の順序を変更したり、リスト内の特定の場所に対して ACE を追加または削除したりできません。

一部のプロトコルには、特定のパラメータやキーワードも適用されます。

次の IP プロトコルがサポートされます(プロトコル キーワードはカッコ内に太字で示してあります)。

認証ヘッダープロトコル(ahp)、Enhanced IGRP(eigrp)、Encapsulating Security Payload(esp)、Generic Routing Encapsulation(gre)、Internet Control Message Protocol(icmp)、Internet Group Management Protocol(igmp)、任意の内部プロトコル(ip)、IP-in-IP トンネリング(ipinip)、KA9Q NOS 互換 IP over IP トンネリング(nos)、Open Shortest Path First ルーティング(ospf)、Payload Compression Protocol(pcp)、プロトコル独立型。

	コマンド	目的
1.	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。
2. a	access-list access-list-number { deny permit } protocol source source-wildcard destination destination-wildcard [precedence precedence] [tos tos] [fragments] [log] [log-input] [time-range time-range-name] [dscp dscp] 注:dscp 値を入力した場合、tos または precedence は入力できません。dscp を入力しない場合は、tos と precedence 値の両方を入力できます。	拡張 IPv4 アクセス リストおよびアクセス条件を定義します。 access-list-number : 100 ~ 199 または 2000 ~ 2699 の 10 進数を指定します。 deny または permit : 条件が一致した場合にパケットを拒否する場合は deny 、許可する場合は permit を指定します。 protocol : IP プロトコルの名前または番号を指定します。名前または番号は、 ahp eigrp 、 esp 、 gre 、 icmp 、 igmp 、 igrp 、 ip 、 ipinip 、 nos 、 ospf 、 pcp 、 pim 、 tcp 、 udp 、および IP プロトコル番号を表す 0 ~ 255 の整数です。一致条件としてインターネット プロトコル (ICMP、TCP、UDP など) を指定するには、キーワード ip を使用します。 注: この手順には、ほとんどの IP プロトコルのオプションが含まれています。TCP、UDP、ICMP、および IGMP の追加のパラメータについては、ステップ 2b ~ 2e を参照してください。 source : パラメータの送信元であるネットワークまたはホストの番号を指定します。 source-wildcard : ワイルドカードビットを送信元アドレスに適用します。 destination : パラメータの宛先であるネットワークまたはホストの番号を指定します。 destination-wildcard : ワイルドカードビットを宛先アドレスに適用します。 source 、 source-wildcard 、 destination 、および destination-wildcard の値は、次の形式で指定します。 ■ドット付き 10 進表記による 32 ビット長の値。 ■0.0.0.0 255.255.255.255 (任意のホスト) を表すキーワード any 。 ■単一のホスト 0.0.0.0 を表すキーワード host 。 その他のキーワードはオプションであり、次の意味を持ちます。 ■ precedence : パケットを 0 ~ 7 の番号または名前で指定する優先度と一致させる場合に入力します。指定できる値は、 routine (0)、 priority (1)、 immediate (2)、 flash (3)、 flash-override (4)、 critical (5)、 internet (6)、 network (7) です。 ■ fragments : 非初期フラグメントを検査します。 ■ tos : パケットを 0 ~ 15 の番号または名前で指定するサービスタイプレベルと一致させます。指定できる値は、 normal (0)、 max-reliability (2)、 max-throughput (4)、 min-delay (8) です。 ■ log : エントリと一致するパケットに関するログ通知メッセージを作成し、コンソールに送信します。 log-input を指定すると、ログエントリに入力インターフェイスが追加されます。 ■ time-range : このキーワードの詳細については、「ACL での時間範囲の使用」を参照してください。 ■ dscp : 0 ~ 63 の番号で指定された DSCP 値を使用してパケットを照合します。疑問符 (?) を使用すると、使用可能な値のリストが表示されます。

	コマンド	目的
または	access-list <i>access-list-number</i> { deny permit } <i>protocol any any</i> [precedence <i>precedence</i>] [tos <i>tos</i>] [fragments] [log] [<i>log-input</i>] [time-range <i>time-range-name</i>] [dscp <i>dscp</i>]	アクセス リスト コンフィギュレーション モードで、 source および source wildcard の値 0.0.0.0 255.255.255.255 の省略形と destination および destination wildcard の値 0.0.0.0 255.255.255.255 の省略形を使用して、拡張 IP アクセス リストを定義します。送信元と宛先のアドレスおよびワイルドカードの代わりに any キーワードを使用できます。

名前付き標準 ACL および名前付き拡張 ACL の作成

注: ACL を作成するときには、ACL の末尾にデフォルトで暗黙的な **deny** ステートメントが追加され、ACL の終わりに到達するまで一致する条件が見つからなかったすべてのパケットに適用されることに注意してください。標準アクセス リストでは、関連付けられた IP ホスト アドレス ACL の指定からマスクを省略すると、0.0.0.0 がマスクと見なされます。

<表/ステップを挿入>

ACL での時間範囲の使用

	コマンド	目的
1.	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。
2.	time-range <i>time-range-name</i>	作成する時間範囲には意味のある名前 (<i>workhours</i> など) を割り当て、時間範囲コンフィギュレーション モードを開始します。名前にスペースや疑問符を含めることはできません。また、文字から始める必要があります。
3.	absolute [<i>start time date</i>] [<i>end time date</i>] または periodic <i>day-of-the-week hh:mm to</i> [<i>day-of-the-week</i>] <i>hh:mm</i> または periodic { <i>weekdays</i> <i>weekend</i> <i>daily</i> } <i>hh:mm to hh:mm</i>	適用対象の機能がいつ動作可能になるかを指定します。 ■ 時間範囲には、 absolute ステートメントを 1 つだけ使用できます。複数の absolute ステートメントを設定した場合は、最後に設定したステートメントだけが実行されます。 ■ 複数の periodic ステートメントを入力できます。たとえば、平日と週末に異なる時間を設定できます。 設定例を参照してください。
4.	end	特権 EXEC モードに戻ります。

端末回線への IPv4 ACL の適用

この作業では、仮想端末回線と ACL 内のアドレス間の着信および発信接続を制限します。

	コマンド	目的
1.	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。
2.	line [<i>console</i> <i>vty</i>] <i>line-number</i>	設定する回線を指定し、インライン コンフィギュレーション モードを開始します。 ■ console : コンソール端末回線を指定します。コンソール ポートは DCE です。 ■ vty : リモート コンソール アクセス用の仮想端末を指定します。 <i>line-number</i> は、回線タイプを指定する場合に、設定する連続グループ内で最初の回線番号です。指定できる範囲は 0 ~ 16 です。
3.	access-class <i>access-list-number</i> { <i>in</i> <i>out</i> }	(デバイスへの) 特定の仮想端末回線とアクセス リストに指定されたアドレス間の着信接続および発信接続を制限します。
4.	end	特権 EXEC モードに戻ります。

インターフェイスへの IPv4 ACL の適用

コマンド	目的
1. 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。
2. interface interface-id	設定するインターフェイスを指定し、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。 指定するインターフェイスはレイヤ 2 インターフェイス (ポート ACL) です。
3. ip access-group {access-list-number / name} {in out}	指定されたインターフェイスへのアクセスを制御します。 out キーワードはレイヤ 2 インターフェイス (ポート ACL) ではサポートされません。
4. end	特権 EXEC モードに戻ります。

名前付き MAC 拡張 ACL の作成

コマンド	目的
1. 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。
2. 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。
3. {deny permit} {any host source MAC address / source MAC address mask} {any host destination MAC address / destination MAC address mask} [type mask isap isap mask aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp 0-65535] [cos cos]	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) 次のオプションを入力することもできます。 <ul style="list-style-type: none"> ■ type mask: Ethernet II または SNAP でカプセル化されたパケットの任意の EtherType 番号を指定します。10 進数、16 進数、または 8 進数で表記できます。一致検査の前に、任意で指定できる <i>don't care</i> ビットのマスクが EtherType に適用されます。 ■ isap isap mask: IEEE 802.2 でカプセル化されたパケットの LSAP 番号。10 進数、16 進数、または 8 進数で表記できます。任意で <i>don't care</i> ビットのマスクを指定できます。 ■ aarp amber dec-spanning decnet-iv diagnostic dsm etype-6000 etype-8042 lat lavc-sca mop-console mop-dump msdos mumps netbios vines-echo vines-ip xns-idp: IP 以外のプロトコルを指定します。 ■ cos cos: プライオリティを設定する 0 ~ 7 の IEEE 802.1Q CoS 番号を指定します。
4. end	特権 EXEC モードに戻ります。

レイヤ 2 インターフェイスへの MAC ACL の適用

コマンド	目的
1. 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。
2. interface interface-id	特定のインターフェイスを指定し、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。指定するインターフェイスは物理レイヤ 2 インターフェイス (ポート ACL) でなければなりません。
3. mac access-group {name} {in}	MAC アクセス リストを使用して、指定されたインターフェイスへのアクセスを制御します。 ポート ACL は、着信方向に限りサポートされます。
4. end	特権 EXEC モードに戻ります。

ACL によるネットワーク セキュリティのモニタリングとメンテナンス

コマンド	目的
show access-lists [number name]	最新の IP および MAC アドレス アクセス リストの全体やその一部、または特定のアクセス リスト (番号付きまたは名前付き) の内容を表示します。
show ip access-lists [number name]	最新の IP アクセス リスト全体、または特定の IP アクセス リスト (番号付きまたは名前付き) を表示します。
show ip interface interface-id	インターフェイスの詳細設定およびステータスを表示します。IP がイネーブルになっているインターフェイスに、 ip access-group 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 ACL を適用した場合は、アクセス グループも表示されます。
show running-config [interface interface-id]	スイッチまたは指定されたインターフェイスのコンフィギュレーション ファイルの内容 (設定されたすべての MAC および IP アクセス リストや、どのアクセス グループがインターフェイスに適用されたかなど) を表示します。
show mac access-group [interface interface-id]	すべてのレイヤ 2 インターフェイスまたは指定されたレイヤ 2 インターフェイスに適用されている MAC アクセス リスト を表示します。
show access-lists [number name]	アクセス リストの設定を表示します。
show time-range	時間範囲の設定を確認します。
show mac access-group [interface interface-id]	そのインターフェイスまたはすべてのレイヤ 2 インターフェイスに適用されている MAC アクセス リストを表示します。

ACL によるネットワーク セキュリティの設定例

標準 ACL の作成:例

次に、IP ホスト **171.69.198.102** へのアクセスを拒否し、他のすべてのホストへのアクセスを許可し、結果を表示する標準 ACL の作成例を示します。

```
Switch (config)# access-list 2 deny host 171.69.198.102
Switch (config)# access-list 2 permit any
Switch(config)# end
Switch# show access-lists
Standard IP access list 2
    10 deny    171.69.198.102
    20 permit any
```

拡張 ACL の作成:例

次に、ネットワーク **171.69.198.0** のすべてのホストからネットワーク **172.20.52.0** のすべてのホストへの **Telnet** アクセスを拒否し、他のすべてのアクセスを許可する拡張アクセス リストを作成し、表示する例を示します(**eq** キーワードを宛先アドレスの後に指定すると、**Telnet** に対応する **TCP** 宛先ポート番号がチェックされます)。

```
Switch(config)# access-list 102 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
Switch(config)# access-list 102 permit tcp any any
Switch(config)# end
Switch# show access-lists
Extended IP access list 102
    10 deny tcp 171.69.198.0 0.0.0.255 172.20.52.0 0.0.0.255 eq telnet
    20 permit tcp any any
```

時間範囲の設定:例

次に、**workhours**(営業時間)の時間範囲および会社の休日(2006年1月1日)を設定し、設定を確認する例を示します。

```
Switch(config)# time-range workhours
Switch(config-time-range)# periodic weekdays 8:00 to 12:00
Switch(config-time-range)# periodic weekdays 13:00 to 17:00
Switch(config-time-range)# exit
Switch(config)# time-range new_year_day_2006
Switch(config-time-range)# absolute start 00:00 1 Jan 2006 end 23:59 1 Jan 2006
Switch(config-time-range)# end
Switch# show time-range
time-range entry: new_year_day_2003 (inactive)
    absolute start 00:00 01 January 2006 end 23:59 01 January 2006
time-range entry: workhours (inactive)
    periodic weekdays 8:00 to 12:00
    periodic weekdays 13:00 to 17:00
```

時間範囲を適用するには、時間範囲を実装できる拡張 ACL 内に時間範囲名を入力します。次に、拡張アクセス リスト **188** を作成して確認する例を示します。このアクセス リストでは、定義された休業時間中はすべての送信元からすべての宛先への **TCP** トラフィックを拒否し、営業時間中はすべての **TCP** トラフィックを許可します。

```
Switch(config)# access-list 188 deny tcp any any time-range new_year_day_2006
Switch(config)# access-list 188 permit tcp any any time-range workhours
Switch(config)# end
Switch# show access-lists
Extended IP access list 188
    10 deny tcp any any time-range new_year_day_2006 (inactive)
    20 permit tcp any any time-range workhours (inactive)
```

名前付き ACL の使用:例

次に、名前付き ACL を使用して同じトラフィックを許可および拒否する例を示します。

```
Switch(config)# ip access-list extended deny_access
Switch(config-ext-nacl)# deny tcp any any time-range new_year_day_2006
Switch(config-ext-nacl)# exit
Switch(config)# ip access-list extended may_access
Switch(config-ext-nacl)# permit tcp any any time-range workhours
Switch(config-ext-nacl)# end
Switch# show ip access-lists
Extended IP access list lpip_default
  10 permit ip any any
Extended IP access list deny_access
  10 deny tcp any any time-range new_year_day_2006 (inactive)
Extended IP access list may_access
  10 permit tcp any any time-range workhours (inactive)
```

ACL へのコメントの挿入:例

次の例では、Jones のワークステーションにはアクセスを許可し、Smith のワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith through
Switch(config)# access-list 1 deny 171.69.3.13
```

名前付き IP ACL のエントリには、**remark** アクセス リスト コンフィギュレーション コマンドを使用します。コメントを削除するには、このコマンドの **no** 形式を使用します。

次の例では、Jones のサブネットには発信 Telnet の使用が許可されません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp host 171.69.2.88 any eq telnet
```

ポートへの ACL の適用:例

次に、ポートにアクセス リスト 2 を適用して、ポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group 2 in
```

インターフェイスへの ACL の適用:例

たとえば、次の ACL をインターフェイスに適用します。

```
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
permit tcp source source-wildcard destination destination-wildcard
```

なおかつ次のメッセージが表示される場合は次のようにします。

```
ACL MGR-2-NOVMR: Cannot generate hardware representation of access list [chars]
```

フラグ関連の演算子は使用できません。この問題を回避するには、

- **ip access-list resequenece** グローバル コンフィギュレーション コマンドを使用することによって、4 つめの ACE を 1 つめの ACE の前に移動させます。

```
permit tcp source source-wildcard destination destination-wildcard
permit tcp source source-wildcard destination destination-wildcard range 5 60
permit tcp source source-wildcard destination destination-wildcard range 15 160
permit tcp source source-wildcard destination destination-wildcard range 115 1660
```

または

- 他の ACL 名または番号よりも英数字順で先に表示される名前または番号に ACL の名前を変更します(たとえば、ACL 79 を ACL 1 に変更します)。

これで、ACL 内の 1 つめの ACE をインターフェイスに適用できます。スイッチは ACE を Opselect index 内の使用可能なマッピング ビットに割り当てた後、フラグ関連の演算子を割り当てて TCAM 内の同じビットを使用します。

ルータ ACL の機能は、次のとおりです。

- 標準 ACL および拡張 ACL (入力および出力) の許可アクションや拒否アクションをハードウェアで制御し、アクセス コントロールのセキュリティを強化します。
- **ip unreachable** がディセーブルの場合、log を指定しないと、セキュリティ ACL の拒否ステートメントと一致するフローがハードウェアによってドロップされます。許可ステートメントと一致するフローは、ハードウェアでスイッチングされます。
- ルータ ACL の ACE に log キーワードを追加すると、パケットのコピーが CPU に送信され、ロギングだけが行われます。ACE が許可ステートメントの場合も、パケットはハードウェアでスイッチングおよびルーティングされます。

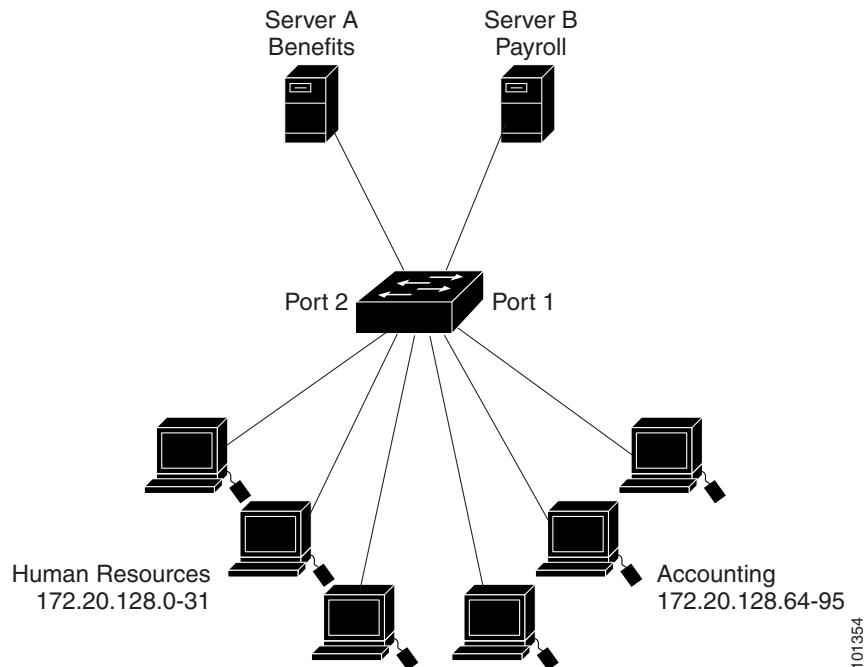
ルーテッド ACL: 例

図 76 (601 ページ) に、小規模ネットワークが構築されたオフィス環境を示します。ルーテッド ポート 2 に接続されたサーバ A には、すべての従業員がアクセスできる収益などの情報が格納されています。ルーテッド ポート 1 に接続されたサーバ B には、機密扱いの給与支払いデータが格納されています。サーバ A にはすべてのユーザがアクセスできますが、サーバ B にアクセスできるユーザは制限されています。

ルータ ACL を使用して上記のように設定するには、次のいずれかの方法を使用します。

- 標準 ACL を作成し、ポート 1 からサーバに着信するトラフィックをフィルタリングします。
- 拡張 ACL を作成し、サーバからポート 1 に着信するトラフィックをフィルタリングします。

図 76 ルータ ACL によるトラフィックの制御



次に、標準 ACL を使用してポートからサーバ B に着信するトラフィックをフィルタリングし、経理部の送信元アドレス 172.20.128.64 ~ 172.20.128.95 から送信されるトラフィックだけを許可する例を示します。この ACL は、指定された送信元アドレスを持つルーテッドポート 1 から送信されるトラフィックに適用されます。

```
Switch(config)# access-list 6 permit 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Standard IP access list 6
 permit 172.20.128.64, wildcard bits 0.0.0.31
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group 6 out
```

次に、拡張 ACL を使用してサーバ B からポートに着信するトラフィックをフィルタリングし、任意の送信元アドレス（この場合はサーバ B）から経理部の宛先アドレス 172.20.128.64 ~ 172.20.128.95 に送信されるトラフィックだけを許可する例を示します。この ACL は、ルーテッドポート 1 に着信するトラフィックに適用され、指定の宛先アドレスに送信されるトラフィックだけを許可します。拡張 ACL を使用する場合は、送信元および宛先情報の前に、プロトコル(IP)を入力する必要があります。

```
Switch(config)# access-list 106 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# end
Switch# show access-lists
Extended IP access list 106
 permit ip any 172.20.128.64 0.0.0.31
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group 106 in
```

番号付き ACL の設定:例

次の例のネットワーク **36.0.0.0** は、2 番めのオクテットがサブネットを指定するクラス **A** ネットワークです。つまり、サブネット マスクは **255.255.0.0** です。ネットワーク アドレス **36.0.0.0** の 3 番めおよび 4 番めのオクテットは、特定のホストを指定します。アクセス リスト **2** を使用して、サブネット **48** のアドレスを 1 つ許可し、同じサブネットの他のアドレスはすべて拒否します。このアクセス リストの最終行は、ネットワーク **36.0.0.0** の他のすべてのサブネット上のアドレスが許可されることを示します。この **ACL** は、ポートに着信するパケットに適用されます。

```
Switch(config)# access-list 2 permit 36.48.0.3
Switch(config)# access-list 2 deny 36.48.0.0 0.0.255.255
Switch(config)# access-list 2 permit 36.0.0.0 0.255.255.255
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group 2 in
```

拡張 ACL の設定:例

次の例の先頭行は、**1023** よりも大きい宛先ポートへの着信 **TCP** 接続を許可します。2 番めの行は、ホスト **128.88.1.2** の **SMTP** ポートへの着信 **TCP** 接続を許可します。3 番めの行は、エラー フィードバック用の着信 **ICMP** メッセージを許可します。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 gt 1023
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# access-list 102 permit icmp any any
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group 102 in
```

次の例では、インターネットに接続されたネットワークがあり、そのネットワーク上の任意のホストがインターネット上の任意のホストと **TCP** 接続を確立できるようにする場合を想定しています。ただし、**IP** ホストからは、専用メール ホストのメール (**SMTP**) ポートを除き、ネットワーク上のホストと **TCP** 接続を確立できないようにします。

SMTP は、接続の一端では **TCP** ポート **25**、もう一端ではランダムなポート番号を使用します。接続している間は、同じポート番号が使用されます。インターネットから着信するメール パケットの宛先ポートは **25** です。発信パケットのポート番号は予約されています。安全なネットワーク システムでは常にポート **25** でのメール接続が使用されているため、着信サービスと発信サービスを個別に制御できます。**ACL** は発信インターフェイスの入力 **ACL** および着信インターフェイスの出力 **ACL** として設定される必要があります。

次の例では、ネットワークはアドレスが **128.88.0.0** のクラス **B** ネットワークで、メール ホストのアドレスは **128.88.1.2** です。**established** キーワードは、確立された接続を表示する **TCP** 専用のキーワードです。**TCP** データグラムに **ACK** または **RST** ビットが設定され、パケットが既存の接続に属していることが判明すると、一致と見なされます。ギガビット イーサネット インターフェイス **1** は、ルータをインターネットに接続するインターフェイスです。

```
Switch(config)# access-list 102 permit tcp any 128.88.0.0 0.0.255.255 established
Switch(config)# access-list 102 permit tcp any host 128.88.1.2 eq 25
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group 102 in
```

名前付き ACL の作成:例

次に、**Internet_filter** という名前の標準 **ACL** および **marketing_group** という名前の拡張 **ACL** を作成する例を示します。**Internet_filter** **ACL** は、送信元アドレス **1.2.3.4** から送信されるすべてのトラフィックを許可します。

```
Switch(config)# ip access-list standard Internet_filter
Switch(config-ext-nacl)# permit 1.2.3.4
Switch(config-ext-nacl)# exit
```

marketing_group **ACL** は、宛先アドレスとワイルドカードの値 **171.69.0.0 0.0.255.255** への任意の **TCP Telnet** トラフィックを許可し、その他の **TCP** トラフィックを拒否します。**ICMP** トラフィックを許可し、任意の送信元から、宛先ポートが **1024** より小さい **171.69.0.0 ~ 179.69.255.255** の宛先アドレスへ送信される **UDP** トラフィックを拒否します。それ以外のすべての **IP** トラフィックを拒否して、結果を示すログが表示されます。


```
Switch(config)# ip access-list extended marketing_group
Switch(config-ext-nacl)# permit tcp any 171.69.0.0 0.0.255.255 eq telnet
Switch(config-ext-nacl)# deny tcp any any
Switch(config-ext-nacl)# permit icmp any any
Switch(config-ext-nacl)# deny udp any 171.69.0.0 0.0.255.255 lt 1024
Switch(config-ext-nacl)# deny ip any any log
Switch(config-ext-nacl)# exit
```

Internet_filter ACL は発信トラフィックに適用され、*marketing_group* ACL はレイヤ 3 ポートの着信トラフィックに適用されます。

```
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# no switchport
Switch(config-if)# ip address 2.0.5.1 255.255.255.0
Switch(config-if)# ip access-group Internet_filter out
Switch(config-if)# ip access-group marketing_group in
```

IP ACL への時間範囲の適用:例

次に、月曜日から金曜日の午前 8 時 ~ 午後 6 時(18 時)の間、IP の HTTP トラフィックを拒否する例を示します。UDP トラフィックは、土曜日および日曜日の正午 ~ 午後 8 時(20 時)の間だけ許可されます。

```
Switch(config)# time-range no-http
Switch(config)# periodic weekdays 8:00 to 18:00
!
Switch(config)# time-range udp-yes
Switch(config)# periodic weekend 12:00 to 20:00
!
Switch(config)# ip access-list extended strict
Switch(config-ext-nacl)# deny tcp any any eq www time-range no-http
Switch(config-ext-nacl)# permit udp any any time-range udp-yes
!
Switch(config-ext-nacl)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group strict in
```

コメント付き IP ACL エントリの作成:例

次に示す番号付き ACL の例では、Jones が所有するワークステーションにはアクセスを許可し、Smith が所有するワークステーションにはアクセスを許可しません。

```
Switch(config)# access-list 1 remark Permit only Jones workstation through
Switch(config)# access-list 1 permit 171.69.2.88
Switch(config)# access-list 1 remark Do not allow Smith workstation through
Switch(config)# access-list 1 deny 171.69.3.13
```

次に示す番号付き ACL の例では、Winter および Smith のワークステーションに Web 閲覧を許可しません。

```
Switch(config)# access-list 100 remark Do not allow Winter to browse the web
Switch(config)# access-list 100 deny host 171.69.3.85 any eq www
Switch(config)# access-list 100 remark Do not allow Smith to browse the web
Switch(config)# access-list 100 deny host 171.69.3.13 any eq www
```

次に示す名前付き ACL の例では、Jones のサブネットにアクセスを許可しません。

```
Switch(config)# ip access-list standard prevention
Switch(config-std-nacl)# remark Do not allow Jones subnet through
Switch(config-std-nacl)# deny 171.69.0.0 0.0.255.255
```

次に示す名前付き ACL の例では、Jones のサブネットに発信 Telnet の使用を許可しません。

```
Switch(config)# ip access-list extended telnetting
Switch(config-ext-nacl)# remark Do not allow Jones subnet to telnet out
Switch(config-ext-nacl)# deny tcp 171.69.0.0 0.0.255.255 any eq telnet
```

ACL ロギングの設定:例

ルータ ACL では、2 種類のロギングがサポートされています。**log** キーワードを指定すると、エントリと一致するパケットに関するログ通知メッセージがコンソールに送信されます。**log-input** キーワードを指定すると、ログエントリに入力インターフェイスが追加されます。

次の例では、名前付き標準アクセス リスト *stan1* は 10.1.1.0 0.0.0.255 からのトラフィックを拒否し、その他のすべての送信元からのトラフィックを許可します。**log** キーワードも指定されています。

```
Switch(config)# ip access-list standard stan1
Switch(config-std-nacl)# deny 10.1.1.0 0.0.0.255 log
Switch(config-std-nacl)# permit any log
Switch(config-std-nacl)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group stan1 in
Switch(config-if)# end
Switch# show logging
Syslog logging: enabled (0 messages dropped, 0 flushes, 0 overruns)
  Console logging: level debugging, 37 messages logged
  Monitor logging: level debugging, 0 messages logged
  Buffer logging: level debugging, 37 messages logged
  File logging: disabled
  Trap logging: level debugging, 39 message lines logged
```

Log Buffer (4096 bytes):

```
00:00:48: NTP: authentication delay calculation problems
```

<output truncated>

```
00:09:34:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
00:09:59:%SEC-6-IPACCESSLOGS:list stan1 denied 10.1.1.15 1 packet
00:10:11:%SEC-6-IPACCESSLOGS:list stan1 permitted 0.0.0.0 1 packet
```

次に、名前付き拡張アクセス リスト *ext1* によって、任意の送信元から 10.1.1.0 0.0.0.255 への ICMP パケットを許可し、すべての UDP パケットを拒否する例を示します。

```
Switch(config)# ip access-list extended ext1
Switch(config-ext-nacl)# permit icmp any 10.1.1.0 0.0.0.255 log
Switch(config-ext-nacl)# deny udp any any log
Switch(config-std-nacl)# exit
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# ip access-group ext1 in
```

レイヤ 2 インターフェイスへの MAC ACL の適用:例

次に、EtherType DECnet Phase IV トラフィックだけを拒否し、他のすべてのタイプのトラフィックを許可するアクセス リスト *mac1* を作成および表示する例を示します。

```
Switch(config)# mac access-list extended mac1
Switch(config-ext-macl)# deny any any decnet-iv
Switch(config-ext-macl)# permit any any
Switch(config-ext-macl)# end
Switch# show access-lists
Extended MAC access list mac1
```

ACLによるVLANマップの設定

```
10 deny any any deernet-iv
20 permit any any
```

次に、アクセスリスト `mac1` をポートに適用してポートに着信するパケットをフィルタリングする例を示します。

```
Switch(config)# interface GigabitEthernet1/17
Switch(config-if)# mac access-group mac1 in
```

注: `mac access-group` インターフェイス コンフィギュレーション コマンドは、物理レイヤ 2 インターフェイスに適用された場合に限り有効となります。このコマンドは、EtherChannel ポートチャネルには使用できません。

スイッチは、パケットを受信すると、着信 ACL とパケットを照合します。ACL がパケットを許可する場合、スイッチはパケットの処理を継続します。ACL がパケットを拒否する場合、スイッチはパケットを廃棄します。未定義の ACL をインターフェイスに適用すると、スイッチは ACL がインターフェイスに適用されていないと判断し、すべてのパケットを許可します。ネットワークセキュリティのために未定義の ACL を使用する場合は、このような結果が生じることに注意してください。

ACLによるVLANマップの設定

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。

ここで使用するコマンドの構文および使用方法の詳細については、このリリースに対応するコマンド リファレンスを参照してください。

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、次のステップを実行します。

1. VLAN に適用する標準 IPv4 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。「標準 IPv4 ACL および拡張 IPv4 ACL の作成」の項および「VLAN マップの作成」の項を参照してください。
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。
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` を入力することもできます。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 パケットまたは非 IP 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) とパケットを照合したりすることもできます。

注: パケットタイプ (IP または MAC) に対する `match` 句が VLAN マップに設定されている場合で、そのマップアクションがドロップの場合は、そのタイプに一致するすべてのパケットがドロップされます。`match` 句が VLAN マップになく、設定されているアクションがドロップの場合は、すべての IP およびレイヤ 2 パケットがドロップされます。

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。

VLAN マップの設定時の注意事項

VLAN マップを設定するときには、次の注意事項に従ってください。

- インターフェイスでトラフィックを拒否するように設定された ACL がなく、VLAN マップが設定されていない場合、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。

ACL による VLAN マップの設定

- 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 マップ内がない場合、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 マップのロギングはサポートされていません。
- レイヤ 2 インターフェイスに適用された IP アクセス リストまたは MAC アクセス リストがスイッチにあって、ポートが属する VLAN に VLAN マップを適用する場合、ポート ACL が VLAN マップに優先します。
- ハードウェアに VLAN マップの設定を適用できない場合は、その VLAN 内のすべてのパケットをソフトウェアでブリッジングおよびルーティングする必要があります。
- プライマリ VLAN およびセカンダリ VLAN で VLAN マップを設定できますただし、プライベート VLAN のプライマリおよびセカンダリ VLAN に同じ VLAN マップを設定することを推奨します。
- フレームがプライベート VLAN 内で転送されるレイヤ 2 の場合、同じ VLAN マップが入力側と出力側の両方に適用されます。フレームがプライベート VLAN の内側から外部ポートにルーティングされる場合、プライベート VLAN マップが入力側に適用されます。
 - フレームがホスト ポートから無差別ポートにアップストリームで送信される場合は、セカンダリ VLAN で設定された VLAN マップが適用されます。
 - フレームが無差別ポートからホスト ポートにダウンストリームで送信される場合は、プライマリ VLAN で設定された VLAN マップが適用されます。

プライベート VLAN の特定 IP トラフィックをフィルタリングするには、プライマリ VLAN およびセカンダリ VLAN の両方に VLAN マップを適用する必要があります。プライベート VLAN の詳細については、19 章の「プライベート VLAN の設定」を参照してください。

設定例については、「ネットワークでの VLAN マップの使用法」の項を参照してください。

ルータ ACL と VLAN マップ両方の使用の詳細については、「VLAN マップとルータ ACL の設定時の注意事項」の項を参照してください。

VLAN マップの作成

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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	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	vlan access-map name [number]	VLAN マップを作成し、名前および番号(任意)を指定します。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	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。

ACLによるVLANマップの設定

	コマンド	目的
ステップ 4	match {ip mac} address {name number} [name number]	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照合します(IP または MAC アドレスを使用)。パケットの照合は、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照合されます。非 IP 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照合されます。
ステップ 5	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	show running-config	アクセスリストの設定を表示します。
ステップ 7	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。マップ内のシーケンスエントリを1つ削除するには、**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** キーワードを使用しません。VLAN マップを使用してパケットを拒否するには、パケットを照合する ACL を作成して、アクションをドロップに設定します。ACL 内の **permit** は、一致するという意味です。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 **ip1ACL** 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、**ip2 ACL** と一致するすべてのパケットが転送されます。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。

```
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
```

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ます。標準の ACL 101 および名前付き拡張アクセス リスト `igmp-match` および `tcp-match` をこのマップと組み合わせて使用すると、次のようになります。

- 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ます。MAC 拡張アクセス リスト `good-hosts` および `good-protocols` をこのマップと組み合わせて使用すると、次のようになります。

- 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-iv` または `vines-ip` プロトコルを使用する 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 decnet-ip
Switch(config-ext-macl)# permit any any vines-ip
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、デフォルトですべてのパケット (IP および非 IP) がドロップされます。例 2 および例 3 のアクセスリスト `tcp-match` および `good-hosts` をこのマップと組み合わせて使用すると、次のようになります。

- 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、特権 EXEC モードで次の手順を実行します。

	コマンド	目的
ステップ 1	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	vlan filter mapname vlan-list list	VLAN マップを 1 つまたは複数の VLAN ID 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。 注: 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。
ステップ 3	show running-config	アクセスリストを表示します。
ステップ 4	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。

VLAN マップを削除するには、`no vlan filter mapname vlan-list list` 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。

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

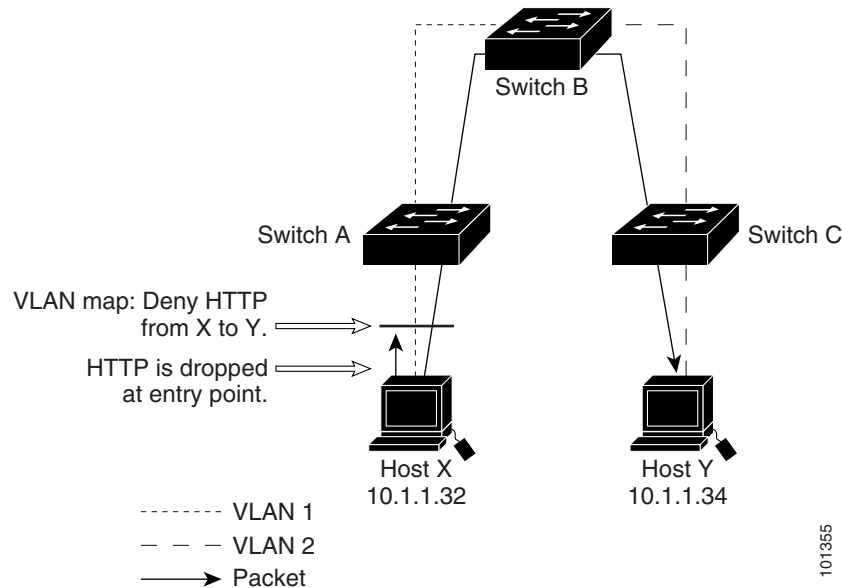
ここでは、一般的な VLAN マップの使用法について説明します。

- ワイヤリング クローゼットの設定
- 別の VLAN にあるサーバへのアクセスの拒否

ワイヤリング クローゼットの設定

ワイヤリング クローゼット構成では、ルーティングがスイッチ上で有効にされていない場合があります。ただし、この設定でも VLAN マップおよび QoS 分類 ACL はサポートされています。図 37-4 では、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 に接続されていると想定します。ホスト X からホスト Y へのトラフィックは、ルーティングがイネーブルに設定されたレイヤ 3 スイッチであるスイッチ B によって最終的に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 でアクセス制御できます。

図 77 ワイヤリング クローゼットの設定



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、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) に向かうすべての HTTP トラフィックがスイッチ A でドロップされ、スイッチ B にブリッジされないように、スイッチ A の VLAN マップを設定できます。

最初に、HTTP ポート上ですべての 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、`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、その他のすべての IP トラフィックが転送されるように、VLAN アクセスマップ `map2` を作成します。

```
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
```

その他の関連資料

その他の関連資料

ここでは、スイッチ管理に関する参考資料について説明します。

関連ドキュメント

関連項目	マニュアル タイトル
Cisco IOS 基本コマンド	『Cisco IOS Configuration Fundamentals Command Reference』
Cisco IOS マルチキャスト コマンド	『Cisco IOS IP Command Reference, Volume 3 of 3: Multicast』
Cisco IOS IP アドレッシングおよびサービス設定	『Cisco IOS IP Configuration Guide』
Cisco IOS ACL 設定	『Cisco IOS IP Command Reference, Volume 1 of 3: Addressing and Services』 『Cisco IOS Security Configuration Guide』

標準

標準	タイトル
この機能によってサポートされる新しい標準または変更された標準はありません。またこの機能による既存標準のサポートに変更はありません。	—

MIB

MIB	MIB のリンク
—	Cisco IOS XR ソフトウェアを使用して MIB を特定およびダウンロードするには、次の URL にある Cisco MIB Locator を使用し、[Cisco Access Products] メニュー (http://cisco.com/public/sw-center/netmgmt/cmtk/mibs.shtml) からプラットフォームを選択します。

RFC

RFC	タイトル
この機能によりサポートされた新規 RFC または改訂 RFC はありません。またこの機能による既存 RFC のサポートに変更はありません。	—

シスコのテクニカル サポート

説明	リンク
シスコのテクニカル サポート Web サイトでは、製品、テクノロジー、ソリューション、技術的なヒント、およびツールへのリンクなどの、数千ページに及ぶ技術情報が検索可能です。Cisco.com に登録済みのユーザは、このページから詳細情報にアクセスできます。	http://www.cisco.com/en/US/support/index.html

