



IPv4 および IPv6 のアクセスコントロールリストの設定

Cisco MDS 9000 ファミリースイッチ製品は、イーサネットとファイバチャネルインターフェイスの間で IP バージョン 4 (IPv4) トラフィックをルーティングできます。IP スタティックルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリースイッチは、ネットワーク管理システム (NMS) に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス (mgmt0) での IP 転送
- IP over Fibre Channel (IPFC) 機能を使用したインバンドファイバチャネルインターフェイス上の IP 転送: IPFC は、IP フレームをカプセル化手法を利用してファイバチャネル上で転送するための方法を定義しています。IP フレームはファイバチャネルフレームにカプセル化されるため、オーバーレイイーサネットネットワークを使用しなくても、ファイバチャネルネットワーク上で NMS 情報を伝達できます。
- IP ルーティング (デフォルトルーティングおよびスタティックルーティング): 外部ルータを必要としない設定の場合は、スタティックルーティングを使用してデフォルトルートを設定できます。

スイッチは仮想ルータ冗長プロトコル (VRRP) 機能の RFC 2338 標準に準拠します。VRRP は、冗長な代替パスをゲートウェイスイッチに提供する、再起動可能なアプリケーションです。

IPv4 アクセスコントロールリスト (IPv4-ACL および IPv6-ACL) は、すべての Cisco MDS 9000 ファミリースイッチに基本的なネットワークセキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリーの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

この章は、次の項で構成されています。

- [IPv4-ACL および IPv6-ACL 設定に関する考慮事項 \(5-2 ページ\)](#)
- [フィルタの内容について \(5-3 ページ\)](#)
- [IP-ACL ログ ダンプの読み取り \(5-10 ページ\)](#)
- [インターフェイスへの IP-ACL の適用 \(5-10 ページ\)](#)
- [IP-ACL カウンタのクリーンアップ \(5-13 ページ\)](#)

IPv4 および IPv6 のアクセス コントロール リストの概要

Cisco MDS 9000 ファミリ スイッチ製品は、イーサネットとファイバチャネルインターフェイスの間で IP バージョン 4 (IPv4) トラフィックをルーティングできます。IP スタティック ルーティング機能が VSAN 間のトラフィックをルーティングします。これを行うためには、各 VSAN が異なる IPv4 サブネットワークに属していなければなりません。各 Cisco MDS 9000 ファミリ スイッチは、ネットワーク管理システム (NMS) に対して次のサービスを提供します。

- スーパーバイザ モジュールの前面パネルにある帯域外イーサネット インターフェイス (mgmt0) での IP 転送
- IP over Fibre Channel (IPFC) 機能を使用したインバンド ファイバチャネル インターフェイス上の IP 転送: IPFC は、IP フレームをカプセル化手法を利用してファイバチャネル上で転送するための方法を定義しています。IP フレームはファイバチャネルフレームにカプセル化されるため、オーバーレイ イーサネット ネットワークを使用しなくても、ファイバチャネル ネットワーク上で NMS 情報を伝達できます。
- IP ルーティング (デフォルト ルーティングおよびスタティック ルーティング): 外部ルータを必要としない設定の場合は、スタティック ルーティングを使用してデフォルト ルートを設定できます。

IPv4 アクセス コントロール リスト (IPv4-ACL および IPv6-ACL) は、すべての Cisco MDS 9000 ファミリ スイッチに基本的なネットワーク セキュリティを提供します。IPv4-ACL および IPv6-ACL は、設定された IP フィルタに基づいて IP 関連トラフィックを規制します。フィルタには IP パケットと一致させる規則が含まれています。パケットが一致すると、規則に基づいてパケットの許可または拒否が判別されます。

Cisco MDS 9000 ファミリの各スイッチには合計最大 128 の IPv4-ACL または 128 の IPv6-ACL を設定でき、各 IPv4-ACL または IPv6-ACL に最大 256 のフィルタを設定できます。

IPv4-ACL および IPv6-ACL 設定に関する考慮事項

Cisco MDS 9000 ファミリのスイッチまたはディレクタに IPv4-ACL または IPv6-ACL を設定する場合は、次の注意事項に従ってください。

- IPv4-ACL または IPv6-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビット イーサネット、およびイーサネット ポートチャネル インターフェイスに適用できます。



注意

ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL がすでに設定されている場合は、このインターフェイスをイーサネット ポートチャネル グループに追加できません。IPv4-ACL または IPv6-ACL は、ポートチャネル グループ内の 1 つのメンバーだけに適用しないでください。IPv4-ACL または IPv6-ACL はチャネル グループ全体に適用します。

- 条件の順序は正確に設定してください。IPv4-ACL または IPv6-ACL フィルタは IP フローに順番に適用されるので、最初の一致によって動作が決定されます。以降の一致は考慮されません。最も重要な条件を最初に設定してください。いずれの条件とも一致しなかった場合、パケットは廃棄されます。
- IP ACL を適用する IP ストレージのギガビット イーサネット ポートでは、暗黙的な deny は有効にならないため、明示的な deny を設定してください。

フィルタの内容について

IP フィルタには、プロトコル、アドレス、ポート、ICMP タイプ、およびサービス タイプ (TS) に基づく IP パケットの一致規則が含まれます。

この項では、次のトピックについて取り上げます。

- [プロトコル情報 \(5-3 ページ\)](#)
- [アドレス情報 \(5-3 ページ\)](#)
- [ポート情報 \(5-4 ページ\)](#)
- [ICMP 情報 \(5-5 ページ\)](#)
- [ToS 情報 \(5-5 ページ\)](#)

プロトコル情報

各フィルタには、プロトコル情報が必要です。この情報により、IP プロトコルの名前または番号を識別します。IP プロトコルは、次のいずれかの方法で指定できます。

- 0 ~ 255 の整数を指定します。この番号は IP プロトコルを表します。
- プロトコルの名前を指定しますが、インターネット プロトコル (IP)、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)、および Internet Control Message Protocol (ICMP) には限定されません。



(注) ギガビット イーサネット インターフェイスに IPv4-ACL または IPv6-ACL を設定する場合は、TCP または ICMP オプションだけを使用してください。

アドレス情報

各フィルタには、アドレス情報が必要です。アドレス情報により、次の詳細を識別します。

- 送信元: パケット送信元のネットワークまたはホストのアドレス
- 送信元ワイルドカード: 送信元に適用されるワイルドカード ビット
- 宛先: パケットの送信先となるネットワークまたはホストの番号
- 宛先ワイルドカード: 宛先に適用されるワイルドカード ビット

送信元/送信元ワイルドカードおよび宛先/宛先ワイルドカードは、次のいずれかの方法で指定します。

- 4 つに区切られたドット付き 10 進表記の 32 ビット数を使用します (10.1.1.2/0.0.0.0 はホスト 10.1.1.2 と同じ)。
 - 各ワイルドカード ビットをゼロに設定する場合には、パケットの IPv4 アドレス内の対応するビット位置と送信元の対応するビット位置で、ビット値が正確に一致している必要があります。

- 各ワイルドカード ビットを 1 に設定する場合は、パケットの IPv4 または IPv6 アドレス内の対応する位置のビット値が 0 および 1 のいずれであっても、現在のアクセス リスト エントリと一致すると見なされます。無視するビット位置に 1 を入れます。たとえば、0.0.255.255 の場合、送信元の最初の 16 ビットだけが完全に一致する必要があります。複数のワイルドカード ビットを 1 に設定する場合、これらのビットが送信元ワイルドカード内で連続している必要はありません。たとえば、送信元ワイルドカード 0.255.0.64 は有効です。
- 送信元/送信元ワイルドカードまたは宛先/宛先ワイルドカード(0.0.0.0/255.255.255.255)の短縮形として、**any** オプションを使用します。

ポート情報

ポート情報はオプションです。送信元ポートと宛先ポートを比較するためには、**eq**(等号)オプション、**gt**(より大きい)オプション、**lt**(より小さい)オプション、または **range**(ポート範囲)オプションを使用します。ポート情報は次のいずれかの方法で指定できます。

- ポート番号を指定します。ポート番号の範囲は 0 ~ 65535 です。表 5-1 に、関連 TCP ポートおよび UDP ポートについて、Cisco NX-OS ソフトウェアが認識するポート番号を示します。
- TCP または UDP ポートの名前を次のように指定します。
 - TCP ポート名は、TCP をフィルタリングする場合にかぎって使用できます。
 - UDP ポート名は、UDP をフィルタリングする場合にかぎって使用できます。

表 5-1 TCP および UDP のポート番号

プロトコル	ポート	番号
UDP	dns	53
	tftp	69
	ntp	123
	radius アカウンティング	1646 または 1813
	radius 認証	1645 または 1812
	snmp	161
	snmp-trap	162
	syslog	514
TCP ¹	ftp	20
	ftp-data	21
	ssh	22
	Telnet	23
	smtp	25
	tasacs-ds	65
	www	80
	sftp	115
http	143	

表 5-1 TCP および UDP のポート番号(続き)

プロトコル	ポート	番号
	wbem-http	5988
	wbem-https	5989

1. TCP コネクションが確立済みの場合は、**established** オプションを使用して適合するものを探してください。TCP データグラムが ACK、FIN、PSH、RST または URG のコントロールビットセットを持つ場合は、適合と見なされます。

ICMP 情報

オプションとして IP パケットは次の ICMP 条件に基づいて選別できます。

- icmp-type: ICMP メッセージタイプは 0 から 255 の番号から 1 つ選びます。
- icmp-code: ICMP メッセージコードは 0 から 255 の番号から 1 つ選びます。

表 5-2 に各 ICMP タイプの値を示します。

表 5-2 ICMP タイプの値

ICMP タイプ ¹	コード
echo	8
echo-reply	0
destination unreachable	3
traceroute	30
time exceeded	11

1. ICMP リダイレクト パケットは必ず拒否されます。

ToS 情報

オプションとして IP パケットは次の ToS 条件に基づいて選別できます。

- ToS レベル: レベルは 0 から 15 の番号で指定します。
- ToS 名: max-reliability、max-throughput、min-delay、min-monetary-cost、および normal から選択できます。

IPv4-ACL または IPv6-ACL の作成

スイッチに入ったトラフィックは、スイッチ内でフィルタが現れる順番に従って IPv4-ACL または IPv6-ACL のフィルタと比較されます。新しいフィルタは IPv4-ACL または IPv6-ACL の末尾に追加されます。スイッチは合致するまで照合を続けます。フィルタの最後に達して合致するものがなかった場合、そのトラフィックは拒否されます。そのため、フィルタの最上部にはヒットする確率の高いフィルタを置く必要があります。許可されないトラフィックに対して、*implied deny* が用意されています。1 つの拒否エントリしか持たないシングルエントリの IPv4-ACL または IPv6-ACL には、すべてのトラフィックを拒否する効果があります。

IPv4-ACL または IPv6-ACL を設定する手順は次のとおりです。

- ステップ 1** IPv4-ACL または IPv6-ACL の作成には、フィルタ名と 1 つ以上のアクセス条件を指定します。フィルタには、条件に合致する発信元と宛先のアドレスが必要です。適切な粒度を設定するために、オプションのキーワードを使用できます。



(注) フィルタのエントリは順番に実行されます。エントリは、リストの最後にだけ追加できません。正しい順番でエントリを追加するように注意してください。

- ステップ 2** 指定したインターフェイスにアクセス フィルタを適用します。

IPv4-ACL または IPv6-ACL の作成

IPv4-ACL を作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# ip access-list List1 permit ip any any	List1 と呼ばれる IPv4-ACL を設定し、任意の送信元アドレスから任意の宛先アドレスへの IP トラフィックを許可します。
	switch(config)# no ip access-list List1 permit ip any any	List1 と呼ばれる IPv4-ACL を削除します。
ステップ 3	switch(config)# ip access-list List1 deny tcp any any	送信元アドレスから宛先アドレスへの TCP トラフィックを拒否するように List1 を更新します。

IPv6-ACL を作成するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# ipv6 access-list List1 switch(config-ipv6-acl)#	List1 という IPv6-ACL を設定し、IPv6-ACL コンフィギュレーションサブモードを開始します。
	switch(config)# no ipv6 access-list List1	List1 と呼ばれる IPv6-ACL とそのエントリをすべて削除します。
ステップ 3	switch(config-ipv6-acl)# permit ipv6 any any	送信元アドレスから宛先アドレスへの IPv6 トラフィックを許可するエントリを追加します。
	switch(config-ipv6-acl)# no permit ipv6 any any	IPv6-ACL からエントリを削除します。
	switch(config-ipv6-acl)# deny tcp any any	送信元アドレスから宛先アドレスへの TCP トラフィックを拒否するエントリを追加します。

管理アクセスを規制する IPv4-ACL を定義する手順は次のとおりです。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# ip access-list restrict_mgmt permit ip 10.67.16.0 0.0.0.255 any	10.67.16.0/24 サブネットのすべてのアドレスを許可する、restrict_mgmt という名前のエントリを IPv4-ACL に定義します。
ステップ 3	switch(config)# ip access-list restrict_mgmt permit icmp any any eq 8	デバイスが MDS (icmp type 8) に ping を実行できるようにする、restrict_mgmt という名前のエントリを IPv4-ACL に追加します。
ステップ 4	switch(config)# ip access-list restrict_mgmt deny ip any any	明示的に restrict_mgmt という名前のアクセスリストへの他のすべてのアクセスをブロックします。

管理アクセスを規制する IPv6-ACL を定義する手順は次のとおりです。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# ip access-list RestrictMgmt switch(config-ipv6-acl)#	RestrictMgmt という IPv6-ACL を設定し、IPv6-ACL コンフィギュレーションサブモードを開始します。
ステップ 3	switch(config)# permit ipv6 2001:0DB8:800:200C::/64 any	2001:0DB8:800:200C::/64 プレフィックスのすべてのアドレスを許可するエントリを定義します。
ステップ 4	switch(config)# permit icmp any any eq 8	デバイスが MDS (ICMP type 8) に ping を実行できるようにするエントリを追加します。
ステップ 5	switch(config)# deny ipv6 any any	明示的に他のすべての IPv6 アクセスをブロックします。

IPv4-ACL 用のオペランドとポート オプションを使用するには、次の手順を実行してください。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# ip access-list List2 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any	1.2.3.0 から送信元ポート 5 を経由する宛先への TCP トラフィックを拒否します。

IPv6-ACL 用のオペランドとポート オプションを使用するには、次の手順を実行してください。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# ip access-list List2 deny tcp 2001:0DB8:800:200C::/64 eq port 5 any	2001:0DB8:800:200C::/64 からソースポート 5 を経由し、任意の宛先までの TCP トラフィックを拒否します。

既存の IPv4-ACL または IPv6-ACL への IP フィルタの追加

IPv4-ACL または IPv6-ACL の作成後に、続く IP フィルタを IPv4-ACL または IPv6-ACL の最後に追加できます。IPv4-ACL または IPv6-ACL の中間にはフィルタを挿入できません。設定された各エントリは、自動的に IPv4-ACL または IPv6-ACL の最後に追加されます。

既存の IPv4-ACL にエントリを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port telnet	Telnet トラフィック用の TCP を許可します。
ステップ 3	switch(config)# ip access-list List1 permit tcp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0 eq port http	HTTP トラフィック用の TCP を許可します。
ステップ 4	switch(config)# ip access-list List1 permit udp 10.1.1.2 0.0.0.0 172.16.1.1 0.0.0.0	すべてのトラフィック用の UDP を許可します。

既存の IPv6-ACL にエントリを追加するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ipv6 access-list List2 switch(config-ipv6-acl)#	IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-ipv6-acl)# permit ip 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64 eq 23	Telnet トラフィック用の TCP を許可します。
ステップ 4	switch(config-ipv6-acl)# permit tcp 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64 eq 143	HTTP トラフィック用の TCP を許可します。
ステップ 5	switch(config-ipv6-acl)# permit udp 2001:0DB8:800:200C::/64 2001:0DB8:800:2010::/64	すべてのトラフィック用の UDP を許可します。

既存の IPv4-ACL または IPv6-ACL からの IP フィルタの削除

設定されたエントリを IPv4-ACL から削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# no ip access-list List2 deny tcp 1.2.3.0 0.0.0.255 eq port 5 any	IPv4-ACL (List2) からこのエントリを削除します。
	switch(config)# no ip access-list x3 deny ip any any	IPv4-ACL (x3) からこのエントリを削除します。
	switch(config)# no ip access-list x3 permit ip any any	IPv4-ACL (x3) からこのエントリを削除します。

設定したエントリを IPv6-ACL から削除するには、次の手順を実行します。

	コマンド	目的
ステップ 1	switch# config t switch(config)#	コンフィギュレーション モードに入ります。
ステップ 2	switch(config)# ipv6 access-list List3 switch(config-ipv6-acl)#	IPv6-ACL を設定し、IPv6-ACL コンフィギュレーション サブモードを開始します。
ステップ 3	switch(config-ipv6-acl)# no deny tcp 2001:0DB8:800:2010::/64 eq port 5 any	IPv6-ACL から TCP エントリが削除されます。
ステップ 4	switch(config-ipv6-acl)# no deny ip any any	IPv6-ACL から IP エントリが削除されます。

IPv4-ACL または IPv6-ACL の設定の確認

設定された IPv4-ACL の内容を表示するには、**show ip access-list** コマンドを使用します。IPv4-ACL は 1 つ以上のフィルタを設定できます。(例 5-1 を参照)。

例 5-1 IPv4 ACL 用に設定されたフィルタの表示

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)
```

設定されたアクセス フィルタの内容を表示するには、**show ipv6 access-list** コマンドを使用します。各アクセス フィルタには、複数の条件を設定できます。(例 5-2 および例 5-3 を参照)。

例 5-2 設定した IPv6-ACL の表示

```
switch# show ipv6 access-list
switch# show ipv6 access-list

IPv6 access list copp-system-acl-bgp6
  10 permit tcp any gt 1024 any eq bgp
  20 permit tcp any eq bgp any gt 1024
IPv6 access list copp-system-acl-icmp6
  10 permit icmp any any echo-request
  20 permit icmp any any echo-reply
IPv6 access list copp-system-acl-icmp6-msgs
  10 permit icmp any any router-advertisement
  20 permit icmp any any router-solicitation
  30 permit icmp any any nd-na
  40 permit icmp any any nd-ns
  50 permit icmp any any mld-query
  60 permit icmp any any mld-report
  70 permit icmp any any mld-reduction
IPv6 access list copp-system-acl-ntp6
  10 permit udp any any eq ntp
  20 permit udp any eq ntp any
IPv6 access list copp-system-acl-ospf6
  10 permit 89 any any
IPv6 access list copp-system-acl-pim6
  10 permit 103 any ff02::d/128
```

```
20 permit udp any any eq pim-auto-rp
IPv6 access list copp-system-acl-radius6
```

例 5-3 指定した IPv6-ACL の概要の表示

```
switch# show ipv6 access-list abc
```

IP-ACL ログ ダンプの読み取り

廃棄されたエントリに合致するパケットに関する情報をログに記録するには、フィルタ条件の最後に **log-deny** オプションを使用します。ログ出力には ACL の番号、許可または拒否のステータス、およびポート情報が表示されます。



(注)

ロギング先でこれらのメッセージをキャプチャするには、カーネルおよび ipacl ファシリティに重大度 7 を設定し、ロギング先のログファイル、モニタに重大度 7 を設定する必要があります。次に例を示します。

```
switch# config t
switch(config)# logging level kernel 7
switch(config)# logging level ipacl 7
switch(config)# logging logfile message 7
```

入力 ACL に対しては、ログは無加工の MAC 情報を表示します。キーワード「MAC=」は、MAC アドレス情報を持つイーサネットの MAC フレームの表示を意味しません。ログにダンプされるレイヤ 2 の MAC レイヤ情報を意味します。出力 ACL に対しては、無加工のレイヤ 2 情報はログに記録されません。

入力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN=vsan1 OUT=
MAC=10:00:00:05:30:00:47:df:10:00:00:05:30:00:8a:1f:aa:aa:03:00:00:08:00:00:08:00:00:54:00
:00:40:00:40:01:0e:86:0b:0b:0b:0c:0b:0b:0b:02:08:00:ff:9c:01:15:05:00:6f:09:17:3f:80:02:01
:00:08:09:0a:0b:0c:0d:0e:0f:10:11:12:13:14:15:16:17:18:19:1a:1b:1c:1d:1e:1f:20:21:22:23:24
:25:26:27:28:29:2a:2b SRC=11.11.11.12 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00 TTL=64 ID=0
DF PROTO=ICMP TYPE=8 CODE=0 ID=277 SEQ=1280
```

出力 ACL ログ ダンプの例を次に示します。

```
Jul 17 20:38:44 excal-2
%KERN-7-SYSTEM_MSG:
%IPACL-7-DENY:IN= OUT=vsan1 SRC=11.11.11.2 DST=11.11.11.2 LEN=84 TOS=0x00 PREC=0x00
TTL=255 ID=38095 PROTO=ICMP TYPE=0 CODE=0 ID=277 SEQ=1280
```

インターフェイスへの IP-ACL の適用

IP-ACL は適用しなくても定義できます。しかし、IP-ACL はスイッチのインターフェイスに適用されるまで効果は出ません。IP-ACL は、VSAN インターフェイス、管理インターフェイス、IPS モジュールおよび MPS-14/2 モジュール上のギガビットイーサネット、およびイーサネットポートチャネル インターフェイスに適用できます。

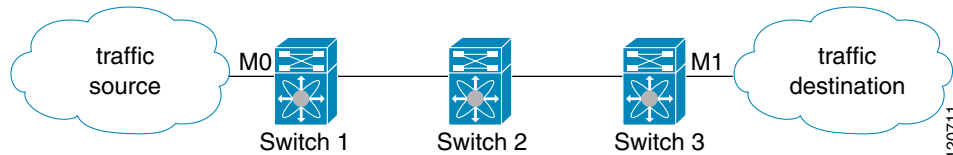


ヒント

トラフィックの送信元に一番近いインターフェイスに IP-ACL を適用してください。

送信元から宛先へ流れるトラフィックを遮断しようとする場合は、スイッチ 3 の M1 に対するアウトバンドフィルタの代わりに、スイッチ 1 の M0 にインバウンド IPv4-ACL を適用できます (図 5-1 を参照)。

図 5-1 インバウンドインターフェイス上のトラフィックの拒否



access-group オプションによりインターフェイスへのアクセスを規制できます。各インターフェイスは、1 つの方向につき 1 つの IP-ACL にしか関連付けできません。入力方向には、出力方向とは異なる IP-ACL を持たせることができます。IP-ACL はインターフェイスに適用されたときにアクティブになります。



ヒント

IP-ACL 中の条件は、インターフェイスに適用する前にすべて作成しておいてください。



注意

IP-ACL を作成前にインターフェイスに適用すると、IP-ACL が空白であるため、そのインターフェイスのすべてのパケットが排除されます。

スイッチにおいては、用語としてのイン、アウト、送信元、宛先は次の意味になります。

- イン: インターフェイスに到達してスイッチ内を通過するトラフィック。送信元はそのトラフィックが発信された場所で、宛先は送信される先(ルータの反対側で)を意味します。



ヒント

入力トラフィック用インターフェイスに適用された IP-ACL はローカルおよびリモート両方のトラフィックに作用します。

- アウト: スイッチを通過済みで、インターフェイスから離れたトラフィック。送信元はこれが送信された場所であり、宛先は送信先を意味します。



ヒント

出力トラフィック用インターフェイスに適用された IP-ACL はローカルトラフィックにだけ作用します。

インターフェイスに IPv4-ACL を適用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	switch# config t	コンフィギュレーションモードに入ります。
ステップ 2	switch(config)# interface mgmt0 switch(config-if)#	管理インターフェイスを設定します (mgmt0)。

	コマンド	目的
ステップ 3	<code>switch(config-if)# ip access-group restrict_mgmt</code>	入力および出力の両方のトラフィック (デフォルト) の <code>restrict_mgmt</code> と呼ばれる IPv4-ACL を適用します。
	<code>switch(config-if)# no ip access-group NotRequired</code>	<code>NotRequired</code> と呼ばれる IPv4-ACL を削除します。
ステップ 4	<code>switch(config-if)# ip access-group restrict_mgmt in</code>	入力トラフィックの <code>restrict_mgmt</code> という IPv4-ACL を適用します (まだ存在しない場合)。
	<code>switch(config-if)# no ip access-group restrict_mgmt in</code>	入力トラフィックの <code>restrict_mgmt</code> と呼ばれる IPv4-ACL を削除します。
	<code>switch(config-if)# ip access-group SampleName2 out</code>	出力トラフィックの <code>SampleName2</code> という IPv4-ACL を適用します (まだ存在しない場合)。
	<code>switch(config-if)# no ip access-group SampleName2 out</code>	出力トラフィックの <code>SampleName2</code> と呼ばれる IPv4-ACL を削除します。

インターフェイスに IPv6-ACL を適用する手順は、次のとおりです。

	コマンド	目的
ステップ 1	<code>switch# config t</code>	コンフィギュレーション モードに入ります。
ステップ 2	<code>switch(config)# interface mgmt0</code> <code>switch(config-if)#</code>	管理インターフェイスを設定します (mgmt0)。
ステップ 3	<code>switch(config-if)# ipv6 traffic-filter RestrictMgmt in</code>	入力トラフィックに <code>RestrictMgmt</code> という IPv6-ACL を適用します (まだ存在しない場合)。
	<code>switch(config-if)# no ipv6 traffic-filter RestrictMgmt in</code>	入力トラフィックの <code>RestrictMgmt</code> と呼ばれる IPv6-ACL を削除します。
	<code>switch(config-if)# ipv6 traffic-filter SampleName2 out</code>	出力トラフィックの <code>SampleName2</code> という IPv6-ACL を適用します (まだ存在しない場合)。
	<code>switch(config-if)# no ipv6 traffic-filter SampleName2 out</code>	出力トラフィックの <code>SampleName2</code> と呼ばれる IPv6-ACL を削除します。

mgmt0 への IP-ACL の適用

`mgmt0` と呼ばれるシステムのデフォルト ACL は、`mgmt0` インターフェイス上に存在します。この ACL はユーザに表示されないため、`mgmt0` は、ユーザが使用できない予約された ACL 名です。`mgmt0` ACL はほとんどのポートをブロックし、許可されたセキュリティ ポリシーに準拠した必須のポートへのアクセスだけを可能にします。

インターフェイスの IP-ACL 設定の確認

show interface コマンドを使用して、インターフェイスの IPv4-ACL 設定を表示します。

```
switch# show interface mgmt 0
mgmt0 is up
  Hardware is FastEthernet
  Address is 000c.30d9.fdbc
  Internet address is 172.22.31.113/24
  MTU 1500 bytes, BW 100 Mbps full Duplex
  ip access-group restrict_mgmt in
  35988 packets input, 3105539 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun 0 fifo
  2495 packets output, 430547 bytes, 0 underruns
    0 output errors, 0 collisions, 0 fifo
    0 carrier errors
```

show interface コマンドを使用して、インターフェイスの IPv6-ACL 設定を表示します。

```
switch# show interface gigabitethernet 2/1
GigabitEthernet2/1 is up
  Hardware is GigabitEthernet, address is 000e.38c6.28b0
  Internet address is 10.1.1.10/24
  MTU 1500 bytes
  Port mode is IPS
  Speed is 1 Gbps
  Beacon is turned off
  Auto-Negotiation is turned on
  ip access-group RestrictMgmt
  5 minutes input rate 1208 bits/sec, 151 bytes/sec, 2 frames/sec
  5 minutes output rate 80 bits/sec, 10 bytes/sec, 0 frames/sec
  6232 packets input, 400990 bytes
    0 multicast frames, 0 compressed
    0 input errors, 0 frame, 0 overrun 0 fifo
  503 packets output, 27054 bytes, 0 underruns
    0 output errors, 0 collisions, 0 fifo
    0 carrier errors
```

IP-ACL カウンタのクリーンアップ

指定した IPv4 ACL フィルタ エントリのカウンタをクリアするには、**clear** コマンドを使用します。



(注) このコマンドを使用して個別のフィルタのカウンタをクリアすることはできません。

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (2 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (7 matches)

switch# clear ip access-list counters abc
```

```
switch# show ip access-list abc
ip access-list abc permit tcp any any (0 matches)
ip access-list abc permit udp any any (0 matches)
ip access-list abc permit icmp any any (0 matches)
ip access-list abc permit ip 10.1.1.0 0.0.0.255 (0 matches)
ip access-list abc permit ip 10.3.70.0 0.0.0.255 (0 matches)
```

すべての IPv6-ACL のカウンタをクリアするには、**clear ipv6 access-list** コマンドを使用します。

```
switch# clear ipv6 access-list
```

指定した IPv6 ACL のカウンタをクリアするには、**clear ipv6 access-list name** コマンドを使用します。

```
switch# clear ipv6 access-list List1
```



(注)

このコマンドを使用して個別のフィルタのカウンタをクリアすることはできません。
