IPv6 ACL の設定

IPv6 ACL の前提条件

IP Version 6（IPv6）アクセス コントロール リスト（ACL）を作成し、それをインターフェイスに適用することによって、IPv6 トラフィックをフィルタリングできます。これは、IP Version 4（IPv4）の名前付き ACL を作成し、適用する方法と同じです。 また、スイッチで IP ベース フィーチャ セットが稼働している場合、入力ルータ ACL を作成しそれを適用してレイヤ 3 管理トラフィックをフィルタリングすることもできます。

関連トピック

IPv6 ACL の作成，（6 ページ）

IPv6 ACL の制限

IPv4 では、番号制の標準 IP ACL および拡張 IP ACL、名前付き IP ACL、および MAC ACL を設定できます。 IPv6 がサポートするのは名前付き ACL だけです。

switchはCisco IOSがサポートするIPv6 ACLの大部分をサポートしますが、一部例外もあります。

- switchは、**flowlabel**、**routing header**、および **undetermined-transport** というキーワードの照合をサポートしません。
- switchは再帰 ACL（**reflect** キーワード）をサポートしません。
- switchは IPv6 フレームに MAC ベース ACL を適用しません。
- ACLを設定する場合、ACLに入力されるキーワードには、それがプラットフォームでサポートされるかどうかにかかわらず、制限事項はありません。 ハードウェア転送が必要なインターフェイス（物理ポートまたは SVI）に ACL を適用する場合、switchはインターフェイスで ACL がサポートされるかどうかを判別します。 サポートされない場合、ACL の付加は拒否されます。
- インターフェイスに適用される ACL に、サポートされないキーワードを持つアクセス コントロール エントリ（ACE）を追加しようとする場合、switchは現在インターフェイスに適用されている ACL に ACE が追加されることを許可しません。

IPv6 ACL について

アクセスコントロールリスト（ACL）は、特定のインターフェイスへのアクセスを制限するために使用される一連のルールです（たとえば、無線クライアントからコントローラの管理インターフェイスに ping が実行されるのを制限する場合などに使用されます）。 switchで設定した ACL は、管理インターフェイス、AP マネージャ インターフェイス、任意の動的インターフェイス、またはワイヤレス クライアントとやり取りするデータ トラフィックの制御用の WLAN、あるいは中央処理装置（CPU）宛のすべてのトラフィックの制御用のコントローラ CPU に適用できます。

Web 認証用に事前認証 ACL を作成することもできます。 このような ACL は、認証が完了するまでに特定のタイプのトラフィックを許可するために使用されます。

IPv6 ACL は、送信元、宛先、送信元ポート、宛先ポートなど、IPv4 ACL と同じオプションをサポートします。

（注） ネットワーク内で IPv4 トラフィックだけを有効にするには、IPv6 トラフィックをブロックします。 つまり、すべての IPv6 トラフィックを拒否するように IPv6 ACL を設定し、これを特定またはすべての WLAN 上で適用します。

IPv6 ACL の概要

スイッチは、次の 2 種類の IPv6 ACL をサポートします。

- IPv6 ルータ ACL は、ルーテッド ポート、スイッチ仮想インターフェイス（SVI）、またはレイヤ 3 EtherChannel に設定できるレイヤ 3 インターフェイスのアウトバウンド トラフィッ

クまたはインバウンド トラフィックでサポートされます。 IPv6 ルータ ACL は、ルーティングされる IPv6 パケットに対してだけ適用されます。

- IPv6 ポート ACL は、レイヤ 2 インターフェイスのインバウンド トラフィックでだけサポートされます。 IPv6 ポート ACL は、インターフェイスに着信するすべての IPv6 パケットに対して適用されます。

IP ベース フィーチャ セットが稼働しているスイッチは、入力ルータ IPv6 ACL だけをサポートします。 ポート ACL または出力ルータ IPv6 ACL はサポートされません。

（注） サポートされない IPv6 ACL を設定した場合、エラー メッセージが表示され、その設定は有効になりません。

スイッチは、IPv6 トラフィックの Virtual LAN（VLAN）ACL（VLAN マップ）をサポートしません。

1 つのインターフェイスに、IPv4 ACL および IPv6 ACL の両方を適用できます。 IPv4 ACL の場合と同様に、IPv6 ポート ACL はルータ ACL よりも優先されます。

- SVI に入力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに着信したパケットはポート ACL によってフィルタリングされます。 その他のポートに着信したルーテッド IP パケットは、ルータ ACL によってフィルタリングされます。 他のパケットはフィルタリングされません。
- SVI に出力ルータ ACL および入力ポート ACL が設定されている場合に、ポート ACL が適用されているポートに

  着信したパケットはポート ACL によってフィルタリングされます。 発信ルーテッド IPv6 パケットは、ルータ ACL によってフィルタリングされます。 他のパケットはフィルタリングされません。

（注） いずれかのポート ACL（IPv4、IPv6、または MAC）がインターフェイスに適用された場合、そのポート ACL を使用してパケットをフィルタリングし、ポート VLAN の SVI に適用されたルータ ACL は無視されます。

関連トピック

IPv6 ACL の作成，（6 ページ）
インターフェイスへの IPv6 の適用，（11 ページ）
WLAN IPv6 ACL の作成，（12 ページ）
IPv6 ACL の表示，（13 ページ）

ACL のタイプ

ユーザあたりの IPv6 ACL

ユーザあたりの ACL の場合、テキスト文字列として、完全アクセス制御エントリ（ACE）が ACS で設定されます。

ACE はコントローラで設定されません。 ACE は `ACCESS-Accept` 属性でswitchに送信され、クライアント用に直接適用されます。 ワイヤレス クライアントが外部switchにローミングするときに、ACE が、AAA 属性としてモビリティ ハンドオフ メッセージで外部switchに送信されます。 ユーザあたりの ACL を使用した出力方向はサポートされていません。

フィルタ ID IPv6 ACL

filter-Id ACL の場合、完全な ACE および `acl name(filter-id)` がswitchで設定され、`filter-id` のみが ACS で設定されます。 `filter-id` は ACCESS-Accept 属性でswitchに送信され、switchは ACE の filter-id をルックアップしてから、クライアントに ACE を適用します。 クライアント L2 が外部switchにローミングするときに、filter-id だけがモビリティ ハンドオフ メッセージで外部switchに送信されます。 ユーザあたりの ACL を使用した出力フィルタ ACL はサポートされていません。 外部switchは filter-id と ACE を事前に設定する必要があります。

ダウンロード可能 IPv6 ACL

ダウンロード可能 ACL（dACL）の場合、完全な ACE および `dacl` 名はすべて ACS だけで設定されます。

（注） コントローラは ACL を設定しません。

ACS は `dacl` 名をswitchに対しその `ACCESS-Accept` 属性で送信します。さらに `dacl` 名を使用して、ACE のために `dACL` 名が ACS に、`access-request` 属性によって戻されます。

ACS は `access-accept` 属性でswitchの対応する ACE に応答します。 ワイヤレス クライアントが外部switchにローミングするときに、`dacl` 名だけがモビリティ ハンドオフ メッセージで外部switchに送信されます。 外部switchは、`dacl` 名の ACS サーバにアクセスして ACE を取得します。

IPv6 ACL とスイッチ スタック

スタック マスターは IPv6 ACL をハードウェアでサポートし、IPv6 ACL をスタック メンバーに配信します。

（注） スイッチ スタック内で IPv6 を完全に機能させるには、すべてのスタック メンバーで拡張 IP サービス フィーチャ セットが稼働している必要があります。

新しいスイッチがスタック マスターを引き継ぐと、ACL 設定がすべてのスタック メンバーに配信されます。 メンバ スイッチは、新しいスタック マスターによって配信された設定との同期をとり、不要なエントリを一掃します。

ACL の修正、インターフェイスへの適用、またはインターフェイスからの解除が行われると、スタック マスターは変更内容をすべてのスタック メンバーに配信します。

IPv6 ACL の設定

IPv6 トラフィックをフィルタリングする場合は、次の手順を実行します

はじめる前に

IPv6 ACL を設定する場合は、事前にデュアル IPv4 および IPv6 SDM テンプレートのいずれかを選択する必要があります。

手順の概要

1. IPv6 ACL を作成し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
2. IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。
3. トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。
4. インターフェイスに IPv6 ACL を適用します。 ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	IPv6 ACL を作成し、IPv6 アクセス リスト 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	IPv6 ACL が、トラフィックをブロックする（拒否）または通過させる（許可）よう設定します。	
ステップ 3	トラフィックをフィルタリングする必要があるインターフェイスに IPv6 ACL を適用します。	
ステップ 4	インターフェイスに IPv6 ACL を適用します。 ルータ ACL では、ACL が適用されるレイヤ 3 インターフェイスにも IPv6 アドレスを設定する必要があります。	

IPv6 ACL のデフォルト設定

デフォルトでは、IPv6 ACL は設定または適用されていません。

他の機能およびスイッチとの相互作用

- IPv6 ルータ ACL がパケットを拒否するよう設定されている場合、パケットはルーティングされません。パケットのコピーがインターネット制御メッセージプロトコル（ICMP）キューに送信され、フレームに ICMP 到達不能メッセージが生成されます。
- ブリッジド フレームがポート ACL によってドロップされる場合、このフレームはブリッジングされません。
- IPv4 ACL および IPv6 ACL の両方を 1 つのスイッチまたはスイッチ スタックに作成したり、同一インターフェイスに適用できます。 各 ACL には一意の名前が必要です。設定済みの名前を使用しようとすると、エラー メッセージが表示されます。

  IPv4 ACL と IPv6 ACL の作成、および同一のレイヤ 2 インターフェイスまたはレイヤ 3 インターフェイスへの IPv4 ACL または IPv6 ACL の適用には、異なるコマンドを使用します。ACL を付加するのに誤ったコマンドを使用すると（たとえば、IPv6 ACL の付加に IPv4 コマンドを使用するなど）、エラー メッセージが表示されます。

- MAC ACL を使用して、IPv6 フレームをフィルタリングできません。 MAC ACL は非 IP フレームだけをフィルタリングできます。
- ハードウェア メモリが満杯の場合、設定済みの ACL を追加すると、パケットは CPU に転送され、ACL はソフトウェアで適用されます。 ハードウェアが一杯になると、ACL がアンロードされたことを示すメッセージがコンソールに出力され、パケットはインターフェイスでドロップされます。

（注） 追加できなかった ACL と同じタイプのパケットのみ（ipv4、ipv6、MAC）がインターフェイスでドロップされます。

IPv6 ACL の設定方法

IPv6 ACL の作成

IPv6 ACL を作成するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **ipv6 access-list** *acl_name*
3. **{deny|permit} protocol**
4. **{deny|permit} tcp**
5. **{deny|permit} udp**
6. **{deny|permit} icmp**
7. **end**
8. **show ipv6 access-list**
9. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 access-list** *acl_name* 例： `ipv6 access-list access-list-name`	名前を使用して IPv6 アクセス リストを定義し、IPv6 アクセス リスト コンフィギュレーション モードを開始します。
ステップ 3	**{deny|permit} protocol** 例： `{deny | permit} protocol {source-ipv6-prefix/prefix-length | any | host source-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |host destination-ipv6-address} [operator [port-number]][dscp value] [fragments][log] [log-input] [routing][sequence value] [time-range name]`	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。 次に、条件について説明します。 • protocol には、インターネット プロトコルの名前または番号を入力します。ahp、esp、icmp、ipv6、pcp、stcp、tcp、udp、または IPv6 プロトコル番号を表す 0 ～ 255 の整数を使用できます。 • source-ipv6-prefix/prefix-length または destination-ipv6-prefix/ prefix-length は、拒否条件または許可条件を設定する送信元または宛先 IPv6 ネットワークあるいはネットワーク クラスで、コロン区切りの 16 ビット値を使用した 16 進形式で指定します（RFC 2373 を参照）。 • IPv6 プレフィックス ::/0 の短縮形として、any を入力します。 • host source-ipv6-address または destination-ipv6-address には、拒否条件または許可条件を設定する送信元または宛先 IPv6 ホスト

	コマンドまたはアクション	目的
		アドレスを入力します。アドレスはコロン区切りの 16 ビット値を使用した 16 進形式で指定します。 • （任意）operator には、指定のプロトコルの送信元ポートまたは宛先ポートを比較するオペランドを指定します。 オペランドには、lt（より小さい）、gt（より大きい）、eq（等しい）、neq（等しくない）、range（包含範囲）があります。 source-ipv6-prefix/prefix-length 引数のあとの operator は、送信元ポートに一致する必要があります。 destination-ipv6- prefix/prefix-length 引数のあとの operator は、宛先ポートに一致する必要があります。 • （任意）port-number は、0 ～ 65535 の 10 進数または TCP あるいは UDP ポートの名前です。 TCP ポート名を使用できるのは、TCP のフィルタリング時だけです。 UDP ポート名を使用できるのは、UDP のフィルタリング時だけです。 • （任意）dscp value を入力して、各 IPv6 パケット ヘッダーの Traffic Class フィールド内のトラフィック クラス値と DiffServ コード ポイント値を照合します。 指定できる範囲は 0 ～ 63 です。 • （任意）fragments を入力して、先頭ではないフラグメントを確認します。 このキーワードが表示されるのは、プロトコルが ipv6 の場合だけです。 • （任意）log 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 メッセージがコンソールに送信されます。 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。 ロギングはルータ ACL でだけサポートされます。 • （任意）routing を入力して、IPv6 パケットのルーティングを指定します。 • （任意）sequence value を入力して、アクセス リスト ステートメントのシーケンス番号を指定します。 指定できる範囲は 1 ～ 4294967295 です。

	コマンドまたはアクション	目的
		• （任意）time-range name を入力して、拒否または許可ステートメントに適用される時間の範囲を指定します。
ステップ 4	**{deny|permit} tcp** 例： `{deny | permit} tcp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any |hostdestination-ipv6-address} [operator [port-number]][ack] [dscp value][established] [fin] [log][log-input] [neq {port |protocol}] [psh] [range{port | protocol}] [rst][routing] [sequence value] [syn] [time-range name][urg]`	（任意）TCP アクセス リストおよびアクセス条件を定義します。 TCP の場合は tcp を入力します。パラメータはステップ 3 で説明されているパラメータと同じですが、次に示すオプションのパラメータが追加されています。 • ack：確認応答（ACK）ビット セット • established：確立された接続。 TCP データグラムに ACK または RST ビットが設定されている場合、照合が行われます。 • fin：終了ビット セット。送信元からのデータはそれ以上ありません。 • neq {port | protocol}：所定のポート番号上にないパケットだけを照合します。 • psh：プッシュ機能ビット セット • range {port | protocol}：ポート番号の範囲内のパケットだけを照合します。 • rst：リセット ビット セット • syn：同期ビット セット • urg：緊急ポインタ ビット セット
ステップ 5	**{deny|permit} udp** 例： `{deny | permit} udp {source-ipv6-prefix/prefix-length | any | hostsource-ipv6-address} [operator [port-number]]{destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][dscp value] [log][log-input] [neq {port |protocol}] [range {port |protocol}] [routing][sequence value][time-range name]`	（任意）UDP アクセス リストおよびアクセス条件を定義します。 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。 UDP パラメータは TCP に関して説明されているパラメータと同じです。ただし、[operator [port]] の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でなければなりません。UDP の場合、established パラメータは無効です。
ステップ 6	**{deny|permit} icmp** 例： `{deny | permit} icmp {source-ipv6-prefix/prefix-length | any |`	（任意）ICMP アクセス リストおよびアクセス条件を定義します。 インターネット制御メッセージプロトコルの場合は、icmp を入力します。 ICMP パラメータはステップ 3a

	コマンドまたはアクション	目的
	hostsource-ipv6-address} [operator [port-number]] {destination-ipv6-prefix/prefix-length | any | hostdestination-ipv6-address} [operator [port-number]][icmp-type [icmp-code] |icmp-message] [dscpvalue] [log] [log-input] [routing] [sequence value][time-range name]	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。 • 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 メッセージのタイプ名およびコード名のリストについては、?キーを使用するか、またはこのリリースのコマンド リファレンスを参照してください。
ステップ 7	**end** 例： Switch(config)# **end**	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。
ステップ 8	**show ipv6 access-list** 例： show ipv6 access-list	アクセス リストの設定を確認します。
ステップ 9	**copy running-config startup-config** 例： 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。

関連トピック

IPv6 ACL の前提条件，（1 ページ）
IPv6 ACL の概要，（2 ページ）
インターフェイスへの IPv6 の適用，（11 ページ）
WLAN IPv6 ACL の作成，（12 ページ）
IPv6 ACL の表示，（13 ページ）

インターフェイスへの IPv6 の適用

ここでは、ネットワーク インターフェイスに IPv6 ACL を適用する手順について説明します。 レイヤ 2 およびレイヤ 3 インターフェイスの発信または着信トラフィックに IPv6 ACL を適用できます。 IPv6 ACL はレイヤ 3 インターフェイスの着信管理トラフィックにだけ適用できます。

インターフェイスへのアクセスを制御するには、特権 EXEC モードで次の手順を実行します。

手順の概要

1. **configure terminal**
2. **interface** interface_id
3. **no switchport**
4. **ipv6 address** *ipv6_address*
5. **ipv6 traffic-filter** *acl_name*
6. **end**
7. **show running-config interface tenGigabitEthernet 1/0/3**
8. **copy running-config startup-config**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**interface** interface_id 例： `Switch# interface interface-id`	アクセス リストを適用するレイヤ 2 インターフェイス（ポート ACL 用）またはレイヤ 3 スイッチ仮想インターフェイス（ルータ ACL 用）を特定して、インターフェイス コンフィギュレーション モードを開始します。
ステップ 3	**no switchport** 例： `Switch# no switchport`	レイヤ 2 モード（デフォルト）からレイヤ 3 モードにインターフェイスを変更します（ルータ ACL を適用する場合のみ）。
ステップ 4	**ipv6 address** *ipv6_address* 例： `Switch# ipv6 address ipv6-address`	レイヤ 3 インターフェイス（ルータ ACL 用）で IPv6 アドレスを設定します。 （注） このコマンドは、レイヤ 2 インターフェイスでは、またはインターフェイスに明示的な IPv6 アドレスが設定されている場合には、必要ありません。

	コマンドまたはアクション	目的
ステップ 5	**ipv6 traffic-filter** *acl_name* 例： `Switch# ipv6 traffic-filter access-list-name {in | out}`	インターフェイスの着信トラフィックまたは発信トラフィックにアクセス リストを適用します。
ステップ 6	**end** 例： `Switch(config)# end`	特権 EXEC モードに戻ります。 また、Ctrl+Z キーを押しても、グローバル コンフィギュレーション モードを終了できます。

ステップ 7	**show running-config interface tenGigabitEthernet 1/0/3**
	
	例：
	`Switch# show running-config interface tenGigabitEthernet 1/0/3`
	`.....`
	`.....`
	`Building configuration .....`
	`.....`
	`Current configuration : 98 bytes`
	`!`
	`interface TenGigabitEthernet1/0/3`
	`switchport mode trunk`
	`ipv6 traffic-filter MyFilter out`
	`end`
		設定の概要を示します。

ステップ 8	**copy running-config startup-config** 例： `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。

関連トピック

IPv6 ACL の作成，（6 ページ）
IPv6 ACL の概要，（2 ページ）
WLAN IPv6 ACL の作成，（12 ページ）
IPv6 ACL の表示，（13 ページ）

WLAN IPv6 ACL の作成

手順の概要

1. **ipv6 traffic-filter acl** *acl_name*
2. **ipv6 traffic-filter acl web**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 traffic-filter acl** *acl_name* 例： `Switch(config-wlan)# ipv6 traffic-filter acl <acl_name>`	名前付き WLAN ACL を作成します。
ステップ 2	**ipv6 traffic-filter acl web** 例： `Switch(config-wlan)# ipv6 traffic-filter acl web <acl_name-preauth>`	WLAN ACL の事前認証を作成します。

```
Switch(config-wlan)# ipv6 traffic-filter acl <acl_name>
Switch(config-wlan)#ipv6 traffic-filter acl web <acl_name-preauth>
```

関連トピック

IPv6 ACL の作成，（6 ページ）
インターフェイスへの IPv6 の適用，（11 ページ）
IPv6 ACL の概要，（2 ページ）
IPv6 ACL の表示，（13 ページ）

IPv6 ACL の確認

IPv6 ACL の表示

1 つまたは複数の特権 EXEC コマンドを使用して、設定済みのすべてのアクセス リスト、すべての IPv6 アクセス リスト、または特定のアクセス リストに関する情報を表示できます。

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**show access-list** 例： `Switch# show access-lists`	switchに設定されたすべてのアクセス リストを表示します。

	コマンドまたはアクション	目的
ステップ 2	**show ipv6 access-list** *acl_name* 例： `Switch# show ipv6 access-list [access-list-name]`	設定済みのすべての IPv6 アクセス リストまたは名前付けされたアクセス リストを表示します。

関連トピック

IPv6 ACL の作成，（6 ページ）
インターフェイスへの IPv6 の適用，（11 ページ）
WLAN IPv6 ACL の作成，（12 ページ）
IPv6 ACL の概要，（2 ページ）

IPv6 ACL の設定例

例：IPv6 ACL の作成

次に、CISCO と名前が付けられた IPv6 アクセス リストを設定する例を示します。 リスト内の最初の拒否エントリは、宛先 TCP ポート番号が 5000 より大きいパケットをすべて拒否します。 2 番めの拒否エントリは、送信元 UDP ポート番号が 5000 未満のパケットを拒否します。 また、この 2 番めの拒否エントリは、すべての一致をコンソールに表示します。 リスト内の最初の許可エントリは、すべての ICMP パケットを許可します。 リスト内の 2 番めの許可エントリは、その他のすべてのトラフィックを許可します。 暗黙の全否定の条件が各 IPv6 アクセス リストの末尾にあるため、2 番めの許可エントリは必要です。

（注） ロギングは、レイヤ 3 インターフェイスでのみサポートされます。

```
Switch(config)# ipv6 access-list CISCO
Switch(config-ipv6-acl)# deny tcp any any gt 5000
Switch (config-ipv6-acl)# deny ::/0 lt 5000 ::/0 log
Switch(config-ipv6-acl)# permit icmp any any
Switch(config-ipv6-acl)# permit any any
```

例：IPv6 ACL の適用

次に、レイヤ 3 インターフェイスの発信トラフィックに対して、アクセス リスト Cisco を適用する例を示します。

```
Switch(config-if)# no switchport
Switch(config-if)# ipv6 address 2001::/64 eui-64
Switch(config-if)# ipv6 traffic-filter CISCO out
```

例：IPv6 ACL の表示

次に、**show access-lists** 特権 EXEC コマンドの出力例を示します。 出力には、スイッチまたはスイッチ スタックに設定済みのすべてのアクセス リストが表示されます。

```
Switch #show access-lists
Extended IP access list hello
10 permit ip any any
IPv6 access list ipv6
permit ipv6 any any sequence 10
```

次に、show ipv6 access-lists 特権 EXEC コマンドの出力例を示します。 出力には、スイッチまたはスイッチ スタックに設定済みの IPv6 アクセス リストだけが表示されます。

```
Switch# show ipv6 access-list
IPv6 access list inbound
permit tcp any any eq bgp (8 matches) sequence 10
permit tcp any any eq telnet (15 matches) sequence 20
permit udp any any sequence 30

IPv6 access list outbound
deny udp any any sequence 10
deny tcp any any eq telnet sequence 20
```

例：RA スロットリングと NS 抑制の設定

このタスクでは、省電力のワイヤレス クライアントが頻繁な非請求の定期的 RA に影響されないように、RA スロットル ポリシーを作成する方法について説明します。 非請求タイプのマルチキャスト RA は、コントローラによってスロットルされます。

はじめる前に

クライアント マシンで IPv6 をイネーブルにします。

手順の概要

1. **configure terminal**
2. **ipv6 nd ra-throttler policy** Mythrottle
3. **throttle-period** 20
4. **max-through** 5
5. **allow at-least** 3 **at-most** 5
6. **switch (config)# vlan configuration 100**
7. **ipv6 nd suppress**
8. **ipv6 nd ra-th attach-policy** attach-policy_name
9. **end**

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**configure terminal** 例： `Switch# configure terminal`	グローバル コンフィギュレーション モードを開始します。
ステップ 2	**ipv6 nd ra-throttler policy** Mythrottle 例： `Switch (config)# ipv6 nd ra-throttler policy Mythrottle`	Mythrottle という RA スロットラ ポリシーを作成します。
ステップ 3	**throttle-period** 20 例： `Switch (config-nd-ra-throttle)# throttle-period 20`	スロットリングを適用する時間間隔セグメントを特定します。
ステップ 4	**max-through** 5 例： `Switch (config-nd-ra-throttle)# max-through 5`	許容する初期 RA の数を特定します。
ステップ 5	**allow at-least** 3 **at-most** 5 例： `Switch (config-nd-ra-throttle)# allow at-least 3 at-most 5`	初期RAが送信された後に、間隔セグメントの終了まで許容される RA の数を特定します。
ステップ 6	**switch (config)# vlan configuration 100** 例： `Switch (config)# vlan configuration 100`	vlan あたりの設定を作成します。
ステップ 7	**ipv6 nd suppress** 例： `Switch (config)# ipv6 nd suppress`	Vlan でネイバー探索をディセーブルにします。
ステップ 8	**ipv6 nd ra-th attach-policy** attach-policy_name 例： `Switch (config)# ipv6 nd ra-throttle attach-policy attach-policy_name`	ルータ アドバタイズメント スロットリングをイネーブルにします。
ステップ 9	**end** 例： `Switch(config)# end`	特権EXECモードに戻ります。また、Ctrl+Zキーを押しても、グローバル コンフィギュレーション モードを終了できます。

例：RA ガード ポリシーの設定

手順の概要

1. **ipv6 nd raguard policy** MyPloicy
2. **trusted-port**
3. **device-role router**
4. **interface tenGigabitEthernet** 1/0/1
5. **ipv6 nd raguard attach-policy**MyPolicy
6. **vlan configuration** 19-21,23
7. **ipv6 nd suppress**
8. **ipv6 snooping**
9. **ipv6 nd raguard attach-policy** MyPolicy
10. **ipv6 nd ra-throttler attach-policy** Mythrottle

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 nd raguard policy** MyPloicy 例： `Switch (config)# ipv6 nd raguard policy MyPolicy`	
ステップ 2	**trusted-port** 例： `Switch (config-nd-raguard)# trusted-port`	上記で作成したポリシーの信頼できるポートを設定します。

ステップ 3	**device-role router**
	
	例：
	`Switch (config-nd-raguard)# device-role [host|monitor|router|switch]`
	`Switch (config-nd-raguard)# device-role router`
		上記で作成した信頼できるポートに RA を送信可能な信頼できるデバイスを定義します。

ステップ 4	**interface tenGigabitEthernet** 1/0/1 例： `Switch (config)# interface tenGigabitEthernet 1/0/1`	信頼できるデバイスにインターフェイスを設定します。
ステップ 5	**ipv6 nd raguard attach-policy**MyPolicy 例： `Switch (config-if)# ipv6 nd raguard attach-policy Mypolicy`	ポートから受信した RA を信頼するようにポリシーを設定し、接続します。

	コマンドまたはアクション	目的
ステップ 6	**vlan configuration** 19-21,23 例： `Switch (config)# vlan configuration 19-21,23`	ワイヤレス クライアントの vlan を設定します。
ステップ 7	**ipv6 nd suppress** 例： `Switch (config-vlan-config)# ipv6 nd suppress`	無線上で ND メッセージを抑制します。
ステップ 8	**ipv6 snooping** 例： `Switch (config-vlan-config)# ipv6 snooping`	IPv6 トラフィックをキャプチャします。
ステップ 9	**ipv6 nd raguard attach-policy** MyPolicy 例： `Switch (config-vlan-config)# ipv6 nd raguard attach-policy Mypolicy`	ワイヤレス クライアントの vlan に RA ガード ポリシーを接続します。
ステップ 10	**ipv6 nd ra-throttler attach-policy** Mythrottle 例： `Switch (config-vlan-config)#ipv6 nd ra-throttler attach-policy Mythrottle`	ワイヤレス クライアントの vlan に RA スロットリング ポリシーを接続します。

例：IPv6 ネイバー バインディングの設定

手順の概要

1. **ipv6 neighbor binding** [vlan]19 2001:db8::25:4 **interface tenGigabitEthernet** 1/0/3 aaa.bbb.ccc

手順の詳細

	コマンドまたはアクション	目的
ステップ 1	**ipv6 neighbor binding** [vlan]19 2001:db8::25:4 **interface tenGigabitEthernet** 1/0/3 aaa.bbb.ccc 例： `Switch (config)# ipv6 neighbor binding vlan 19 2001:db8::25:4 interface tenGigabitEthernet 1/0/3 aaa.bbb.ccc`	送信元 MAC アドレスとして aaa.bbb.ccc が設定されたインターフェイス te1/0/3 を介して VLAN 19 で送信する場合にのみ有効なネイバー 2001:db8::25:4 を設定して検証します。

その他の関連資料

関連資料

関連項目	マニュアル タイトル
IPv6 コマンド リファレンス	*IPv6 Command Reference (Catalyst 3850 Switches)*
ACL 設定	*Security Configuration Guide (Catalyst 3850 Switches)*

エラー メッセージ デコーダ

説明	Link
このリリースのシステム エラー メッセージを調査し解決するために、エラー メッセージ デコーダ ツールを使用します。	https://www.cisco.com/cgi-bin/Support/Errordecoder/index.cgi

MIB

MIB	MIB のリンク
本リリースでサポートするすべての MIB	選択したプラットフォーム、Cisco IOS リリース、およびフィーチャ セットに関する MIB のダウンロードには、次の URL にある Cisco MIB Locator を使用します。 http://www.cisco.com/go/mibs

テクニカル サポート

説明	Link
シスコのサポート Web サイトでは、シスコの製品やテクノロジーに関するトラブルシューティングに役立てていただけるように、マニュアルやツールをはじめとする豊富なオンラインリソースを提供しています。 お使いの製品のセキュリティ情報や技術情報を入手するために、Cisco Notification Service（Field Notice からアクセス）、Cisco Technical Services Newsletter、Really Simple Syndication（RSS）フィードなどの各種サービスに加入できます。 シスコのサポート Web サイトのツールにアクセスする際は、Cisco.com のユーザ ID およびパスワードが必要です。	http://www.cisco.com/support

IPv6 ACL の機能情報

次の表に、このモジュールで説明した機能をリストし、個別の設定情報へのリンクを示します。

機能	リリース	変更内容
IPv6 ACL 機能	Cisco IOS XE 3.2SE	この機能が導入されました。