

スイッチでのIPv6ベースのアクセスコントロールリスト(ACL)およびアクセスコントロールエントリ(ACE)の設定

目的

アクセスコントロールリスト(ACL)は、セキュリティの向上に使用されるネットワークトラフィックフィルタと関連付けられたアクションのリストです。ユーザが特定のリソースにアクセスするのをブロックまたは許可するACLには、ネットワークデバイスへのアクセスを許可または拒否するホストが含まれています。

IPv6の一般的なACL機能は、IPv4のACLと似ています。ACLは、どのトラフィックをブロックし、どのトラフィックをスイッチインターフェイスで転送するかを決定します。ACLでは、送信元アドレスと宛先アドレス、特定のインターフェイスへの着信および発信に基づいてフィルタリングを行うことができます。各ACLの最後には暗黙的なdeny文があります。ACLのルールは、アクセスコントロールエントリ(ACE)で設定されます。

アクセスリストを使用して、ネットワークにアクセスするための基本的なセキュリティレベルを提供する必要があります。ネットワークデバイスにアクセスリストを設定しないと、スイッチまたはルータを通過するすべてのパケットがネットワークのすべての部分に許可される可能性があります。

この記事では、スイッチでIPv6ベースのACLとACEを設定する方法について説明します。

該当するデバイス

- Sx350シリーズ
- SG350Xシリーズ
- Sx500シリーズ
- Sx550Xシリーズ

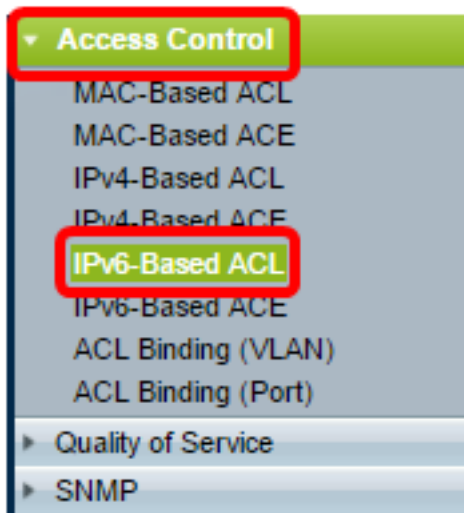
[Software Version]

- 1.4.5.02 - Sx500シリーズ
- 2.2.5.68 - Sx350シリーズ、SG350Xシリーズ、Sx550Xシリーズ

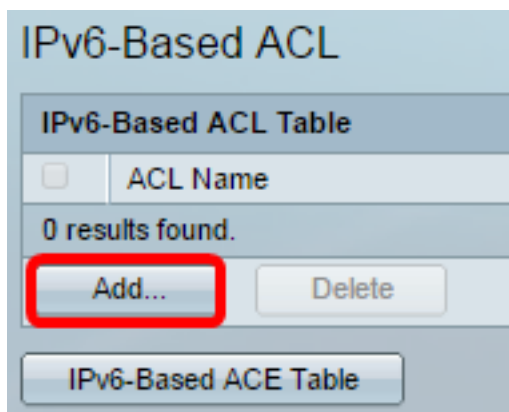
IPv6ベースのACLおよびACEの設定

IPv6ベースACLの設定

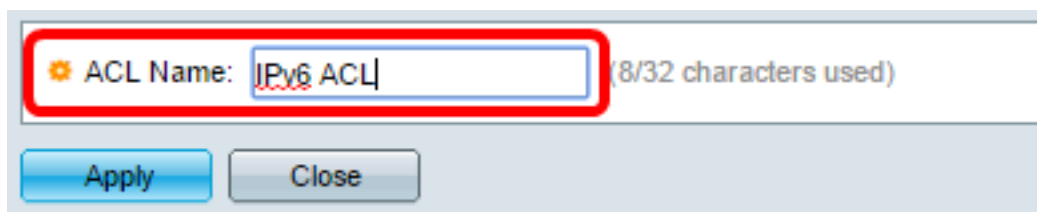
ステップ1: Webベースのユーティリティにログインし、[Access Control] > [IPv6-Based ACL]に移動します。



ステップ2:[Add]ボタンをクリックします。

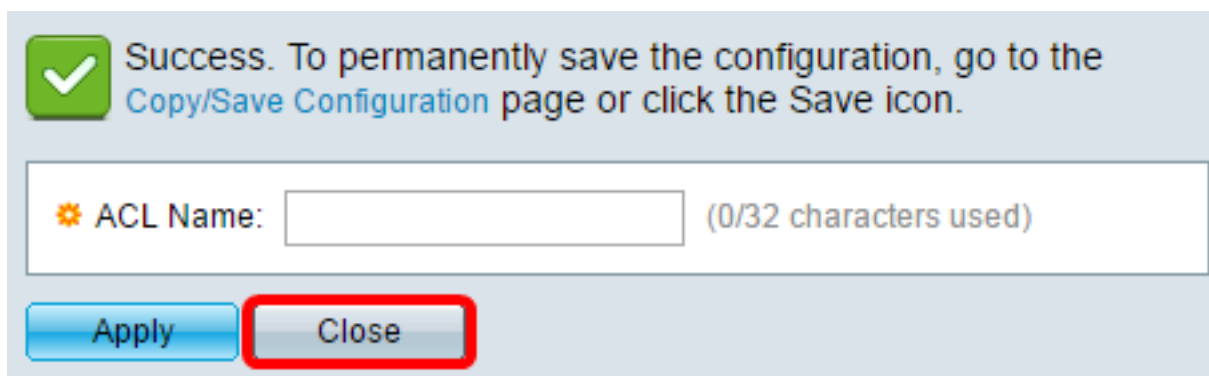


ステップ3:[ACL Name]フィールドに新しいACLの名前を入力します。



注：この例では、IPv6 ACLが使用されています。

ステップ4:[Apply]をクリックして、[Close]をクリックします。



ステップ5: (オプション) [Save]をクリックし、スタートアップコンフィギュレーションファイルに設定を保存します。



これで、スイッチにIPv6ベースのACLを設定できました。

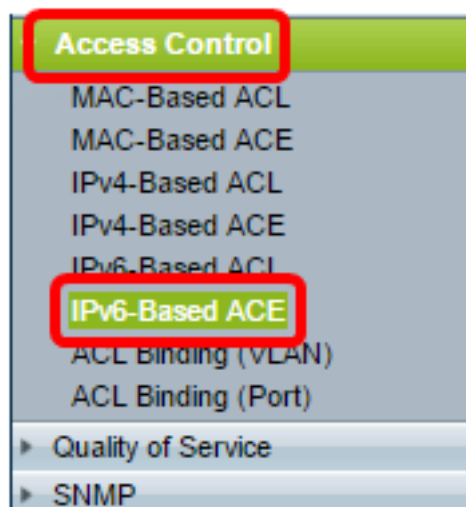
IPv6ベースのACEの設定

ポートでパケットが受信されると、スイッチは最初のACLを介してフレームを処理します。パケットが最初のACLのACEフィルタに一致すると、ACEアクションが実行されます。パケットがいずれのACEフィルタにも一致しない場合、次のACLが処理されます。関連するすべてのACLのACEに一致するものが見つからなかった場合、パケットはデフォルトで廃棄されます。

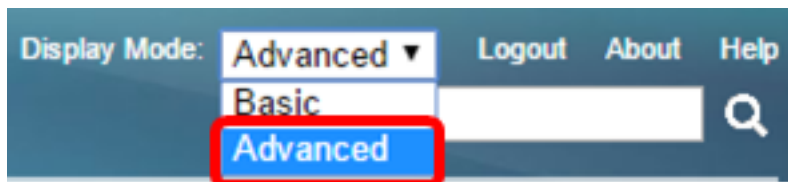
このシナリオでは、特定のユーザ定義の送信元IPv6アドレスから任意の宛先アドレスに送信されるトラフィックを拒否するためにACEが作成されます。

注：このデフォルトアクションは、すべてのトラフィックを許可する低優先度ACEを作成することで回避できます。

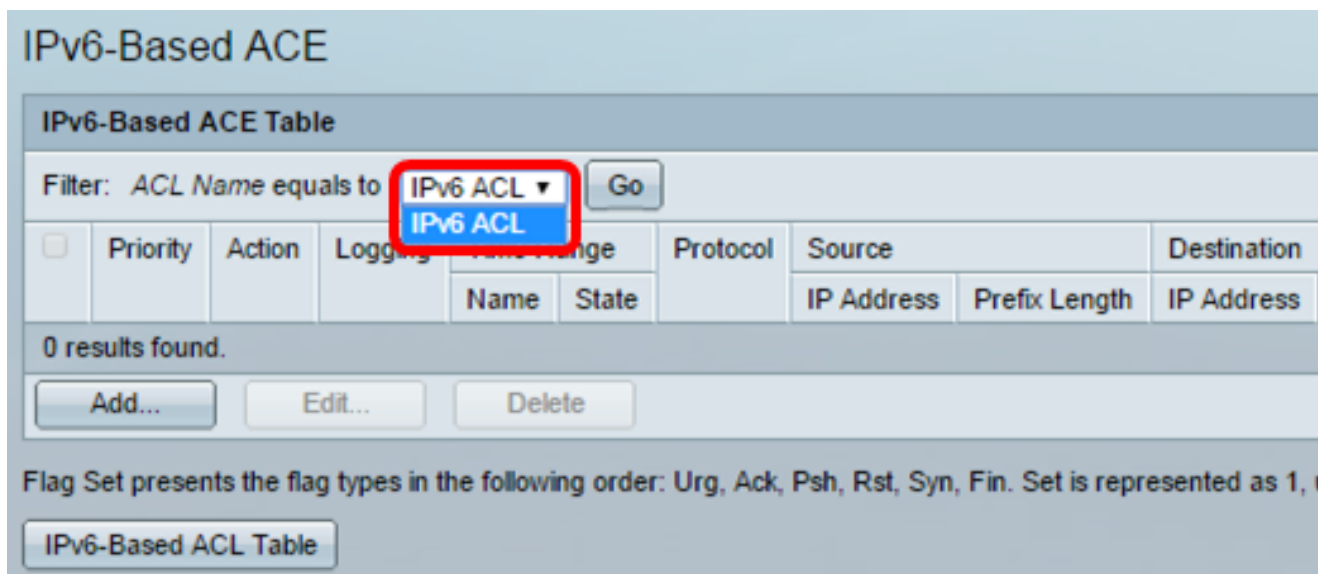
ステップ1: Webベースのユーティリティで、[Access Control] > [IPv6-Based ACE]に移動します。



重要：Sx350、SG350X、Sx550Xスイッチを使用している場合は、ページの右上隅にある[表示モード(Display Mode)]ドロップダウンリストから[詳細(Advanced)]を選択して、詳細モードに変更します。

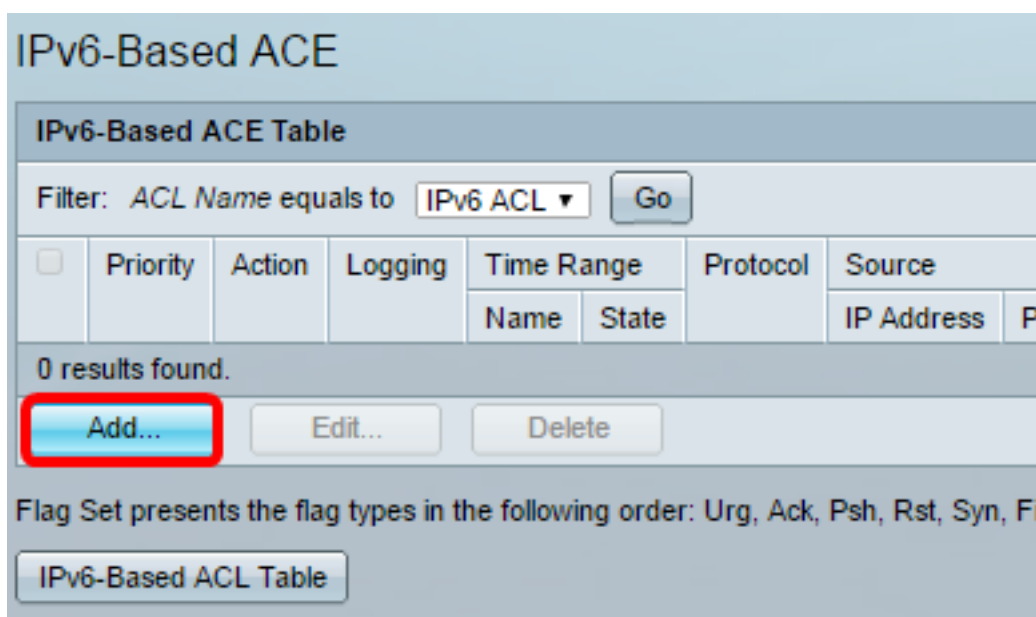


ステップ2:[ACL Name]ドロップダウンリストからACLを選択し、[Go]をクリックします。



注：ACL用にすでに設定されているACEがテーブルに表示されます。

ステップ3:[Add]ボタンをクリックして、ACLに新しいルールを追加します。



注：[ACL Name]フィールドには、ACLの名前が表示されます。

ステップ4:[Priority]フィールドにACEのプライオリティ値を入力します。プライオリティ値が大きいACEが最初に処理されます。値1が最も高い優先度です。範囲は1 ~ 2147483647です。

ACL Name: IPv6 ACL

Priority: (Range: 1 - 2147483647)

Action: Permit
 Deny
 Shutdown

Logging: Enable

Time Range: Enable

Time Range Name: [Edit](#)

Protocol: Any (IPv6)
 Select from list
 Protocol ID to match (Range: 0 - 255)

注：この例では、3 が使用されます。

ステップ5：フレームがACEの必須条件を満たしたときに実行される必要なアクションに対応するオプションボタンをクリックします。

注：この例では、[Permit]が選択されています。

- Permit：スイッチは、ACEの必須条件を満たすパケットを転送します。
- 拒否：スイッチは、ACEの必須条件を満たすパケットを廃棄します。

シャットダウン：スイッチは、ACEの必須条件を満たさないパケットをドロップし、パケットが受信されたポートをディセーブルにします。無効なポートは、[ポートの設定]ページで再アクティブ化できます。

ステップ6: (オプション) ACLルールに一致するロギングACLフローを有効にするには、[ロギングの有効化(Enable Logging)]チェックボックスをオンにします。

Logging: Enable

Time Range: Enable

Time Range Name: [Edit](#)

Protocol: Any (IP)
 Select from list
 Protocol ID to match (Range: 0 - 255)

ステップ7: (オプション) [Enable Time Range]チェックボックスをオンにして、ACEに時間範囲を設定できるようにします。時間範囲は、ACEが有効な時間を制限するために使用されます。これを無効のままにすると、ACEはいつでも動作します。

Logging: Enable

Time Range: **Enable**

Time Range Name: Time Range 1

Protocol: Any (IPv6)

Select from list

Protocol ID to match (Range: 0 - 255)

ステップ8: (オプション) [Time Range Name]ドロップダウンリストから、ACEに適用する時間範囲を選択します。

Time Range Name: Time Range 1

Protocol: Any (IPv6)

Select from list

Protocol ID to match (Range: 0 - 255)

注：「編集」をクリックし、「時間範囲」ページで時間範囲をナビゲートして作成できます。

Time Range Name: Time Range 1 (12/32 characters used)

Absolute Starting Time: Immediate

Date Time HH:MM

Absolute Ending Time: Infinite

Date Time HH:MM

ステップ9:[Protocol]領域でプロトコルタイプを選択します。ACEは、特定のプロトコルまたはプロトコルIDに基づいて作成されます。

Protocol: Any (IPv6)

Select from list

Protocol ID to match (Range: 0 - 255)

次のオプションがあります。

- [任意(IP)]：このオプションは、すべてのIPプロトコルを受け入れるようにACEを設定します。
- [リストから選択(Select from list)]：このオプションでは、ドロップダウンリストからプロトコルを選択できます。このオプションを使用する場合は、[ステップ10に進みます](#)。
- [Protocol ID to match]：このオプションでは、プロトコルIDを入力できます。このオプションを使用する場合は、[ステップ11に進みます](#)。

注：この例では、[Select from list]が選択されています。

[ステップ10:\(オプション\)](#)ステップ9で[Select from list]を選択した場合は、ドロップダウンリストからプロトコルを選択します。

Protocol:
 Any (IPv6)
 Select from list
 Protocol ID to match
 (Range: 0 - 255)

TCP
 TCP
 UDP
 ICMP

次のオプションがあります。

- TCP:Transmission Control Protocol (TCP ; 伝送制御プロトコル) :2つのホストがデータストリームを通信および交換できるようにします。TCPはパケット配信を保証し、パケットが送信順に送受信されることを保証します。
- UDP:User Datagram Protocol (UDP ; ユーザデータグラムプロトコル) はパケットを送信しますが、その配信は保証しません。
- ICMP : パケットをインターネット制御メッセージプロトコル(ICMP)に一致させます。

注 : この例では、TCPが使用されています。

[ステップ11:](#) (オプション) ステップ9で一致するプロトコルIDを選択した場合は、[一致するプロトコルID]フィールドにプロトコルIDを入力してください。

Protocol:
 Any (IP)
 Select from list

 Protocol ID to match
 (Range: 0 - 255)

注 : この例では、1 が使用されます。

ステップ12:[Source IP Address]領域で、ACEの目的の条件に対応するオプションボタンをクリックします。

Source IP Address:
 Any
 User Defined

次のオプションがあります。

- [Any] : すべての送信元IPv6アドレスがACEに適用されます。
- [User Defined]:[Source IP Address Value]フィールドと[Source IP Prefix Length]フィールドに、ACEに適用するIPアドレスとIPワイルドカードマスクを入力します。

注 : この例では、[User Defined]が選択されています。[任意]を選択した場合は、[ステップ15に進みます](#)。

ステップ13:[Source IP Address Value]フィールドに送信元IPアドレスを入力します。

Source IP Address:
 Any
 User Defined

Source IP Address Value:

注 : この例では、fe80::d0ba:7021:37f7:d68dが使用されます。

ステップ14:[Source IP Prefix Length]フィールドに送信元IPプレフィックス長を入力します。

Source IP Address: Any
 User Defined

Source IP Address Value:

Source IP Prefix Length: (Range: 0 - 128)

注：この例では、128 が使用されます。

ステップ15:[DestinationIP Address]領域で、ACEの目的の条件に対応するオプションボタンをクリックします。

Source IP Address: Any
 User Defined

Source IP Address Value:

Source IP Prefix Length: (Range: 0 - 128)

Destination IP Address: Any
 User Defined

Destination IP Address Value:

Destination IP Prefix Length: (Range: 0 - 128)

次のオプションがあります。

- [Any]：すべての宛先IPv6アドレスがACEに適用されます。
- [ユーザ定義(User Defined)]:[宛先IPアドレスの値(Destination IP Address Value)]フィールドと [宛先IPアドレスの長さ(Destination IP Prefix Length)]フィールドに、ACEに適用するIPアドレスとIPワイルドカードマスクを入力します。

注：この例では、[Any]が選択されています。このオプションを選択すると、作成されるACEは、指定されたIPv6アドレスから任意の宛先に着信するACEトラフィックを許可します。

ステップ16: (オプション) [Source Port]領域のオプションボタンをクリックします。デフォルト値は[Any]です。

Source Port: Any
 Single from list (Range: 0 - 65535)
 Single by number (Range: 0 - 65535)
 Range -

Destination Port: Any
 Single from list (Range: 0 - 65535)
 Single by number (Range: 0 - 65535)
 Range -

- Any：すべての送信元ポートに一致します。
- [Single from list]：パケットが一致する単一のTCP/UDP送信元ポートを選択できます。このフィールドは、[Select from List]ドロップダウンメニューで[800/6-TCP]または[800/17-UDP]が選択されている場合にのみアクティブになります。

- Single by number : パケットが一致する単一のTCP/UDP送信元ポートを選択できます。このフィールドは、[Select from List]ドロップダウンメニューで[800/6-TCP]または[800/17-UDP]が選択されている場合にのみアクティブになります。
- Range : パケットが一致するTCP/UDP送信元ポートの範囲を選択できます。8つの異なるポート範囲を設定できます (送信元ポートと宛先ポート間で共有)。TCPおよびUDPプロトコルには、それぞれ8つのポート範囲があります。

ステップ17: (オプション) [Destination Port (宛先ポート)]領域のオプションボタンをクリックします。デフォルト値は[Any]です。

- Any : すべての送信元ポートに一致
- [Single from list] : パケットが一致する単一のTCP/UDP送信元ポートを選択できます。このフィールドは、[Select from List]ドロップダウンメニューで[800/6-TCP]または[800/17-UDP]が選択されている場合にのみアクティブになります。
- Single by number : パケットが一致する単一のTCP/UDP送信元ポートを選択できます。このフィールドは、[Select from List]ドロップダウンメニューで[800/6-TCP]または[800/17-UDP]が選択されている場合にのみアクティブになります。
- Range : パケットが一致するTCP/UDP送信元ポートの範囲を選択できます。8つの異なるポート範囲を設定できます (送信元ポートと宛先ポート間で共有)。TCPおよびUDPプロトコルには、それぞれ8つのポート範囲があります。

ステップ18: (オプション) [TCP Flags]領域で、パケットをフィルタリングするTCPフラグを1つ以上選択します。フィルタリングされたパケットは、転送または廃棄されます。TCPフラグでパケットをフィルタリングすると、パケット制御が増加し、ネットワークセキュリティが向上します。

- Set : フラグが設定されている場合に一致します。
- Unset : フラグが設定されていない場合に一致します。
- 注意 : TCPフラグを無視します。

| | | | | | |
|---|---|--------------------------------------|---|---|---|
| Urg: | Ack: | Psh: | Rst: | Syn: | Fin: |
| <input type="radio"/> Set | <input type="radio"/> Set | <input checked="" type="radio"/> Set | <input type="radio"/> Set | <input type="radio"/> Set | <input type="radio"/> Set |
| <input type="radio"/> Unset | <input type="radio"/> Unset | <input type="radio"/> Unset | <input type="radio"/> Unset | <input type="radio"/> Unset | <input type="radio"/> Unset |
| <input checked="" type="radio"/> Don't care | <input checked="" type="radio"/> Don't care | <input type="radio"/> Don't care | <input checked="" type="radio"/> Don't care | <input checked="" type="radio"/> Don't care | <input checked="" type="radio"/> Don't care |

TCPフラグは次のとおりです。

- Urg : このフラグは、着信データをUrgentとして識別するために使用されます。
- Ack : このフラグは、パケットの正常な受信を確認するために使用されます。
- Psh : このフラグは、データに優先順位が与えられ (値する)、送信側または受信側で処理されることを保証するために使用されます。
- Rst : このフラグは、現在の接続を意図していないセグメントが到着したときに使用されます。
- Syn : このフラグはTCP通信に使用されます。
- Fin : このフラグは、通信またはデータ転送が終了したときに使用されます。

ステップ19: (オプション) Type of ServiceエリアからIPパケットのサービスタイプをクリックします。

Type of Service:

- Any
- DSCP to match (Range: 0 - 63)
- IP Precedence to match (Range: 0 - 7)

次のオプションがあります。

- Any : トラフィックの輻輳に対して任意のタイプのサービスを使用できます。
- DSCP to Match: DiffServコードポイント(DSCP to Match)は、ネットワークトラフィックを分類および管理するためのメカニズムです。6ビット(0 ~ 63)を使用して、各ノードでパケットが受けるホップごとの動作を選択します。
- IP Precedence to match: IP precedenceは、ネットワークが適切なQuality of Service(QoS)コミットメントを提供するために使用するタイプオブサービス(TOS)のモデルです。このモデルでは、RFC 791およびRFC 1349で説明されているように、IPヘッダー内のサービスタイプのバイトの最上位3ビットが使用されます。IP Preference値を持つキーワードは次のとおりです。

- 0 - ルーチン
- 1 - 優先度
- 2 - 即時
- 3 : フラッシュ
- 4 - フラッシュオーバーライド用
- 5 : 緊急
- 6 - インターネット
- 7 : ネットワーク

注 : この例では、[Any]が選択されています。

ステップ20: (オプション) ACLのIPプロトコルがICMPの場合、フィルタリングに使用するICMPメッセージタイプをクリックします。メッセージタイプを名前で選択するか、メッセージタイプ番号を入力します。

ICMP:

- Any
- Select from list (Range: 0 - 255)
- ICMP Type to match (Range: 0 - 255)

ICMP Code:

- Any
- User Defined (Range: 0 - 255)

Apply Close

- [任意(Any)] : すべてのメッセージタイプが受け入れられます。
- [リストから選択(Select from list)] : メッセージタイプを名前で選択できます。
- [一致するICMPタイプ(ICMP Type to match)] : フィルタリングのために使用されるメッセージタイプの数。

注：この例では、[Select from list]が選択されています。

ステップ21: (オプション) ステップ20で[Select from list]を選択した場合は、ドロップダウンリストの可能なオプションからフィルタリングする制御メッセージを選択します。

The screenshot shows a configuration window with several sections: TCP Flags, Urgency (Urg), Type of Service, and ICMP. The ICMP section is active, and a dropdown menu is open, listing various ICMP types. The 'Destination Unreachable (1)' option is selected and highlighted in blue. Other options include Packet Too Big (2), Time Exceeded (3), Parameter Problem (4), Echo Request (128), Echo Reply (129), MLD Query (130), MLD Report (131), MLDv2 Report (143), MLD Done (132), Router Solicitation (133), Router Advertisement (134), ND NS (135), and ND NA (136). The dropdown menu is enclosed in a red rounded rectangle.

- Destination Unreachable (1) : ホストまたはそのゲートウェイによって生成され、何らかの理由で宛先が到達不能であることをクライアントに通知します(例 : Network or Host unreachable error)。
- Packet Too Big (2) : データグラムのサイズが指定されたMTUを超えています。
- Time Exceeded(3) : 存続可能時間(TTL)フィールドがゼロに達したために廃棄されたデータグラムを送信元に通知するために、ゲートウェイによって生成されます。
- パラメータの問題(4) : 別のICMPメッセージで特にカバーされていないエラーに対する応答として生成されます。
- エコー要求(128) : これはpingであり、このpingのデータはエコー応答で受信されると想定されます。
- エコー応答(129) : エコー要求に応答して生成されます。
- MLDクエリー(130) : 接続されたリンク上でリスナーを持つマルチキャストアドレスを学習するために使用されます。10進数で130と入力します。
- MLDレポート(131) : メッセージ送信者がリッスンするIPv6マルチキャストアドレス時に生成されます。
- MLD v2 Report(143) : バージョン2のMLD Reportと同じです。
- MLD Done(132) : ホストがグループから脱退すると、ネットワーク上のマルチキャストルータにマルチキャストリスナーdoneメッセージを送信します。
- Router Solicitation(133) : ルータ検出メッセージです。ホストは、アドバタイズメントをリッスンするだけで、ネイバールータのアドレスを検出します。マルチキャストのデフォルトは224.0.0.2で、それ以外の場合は255.255.255.255です。
- ルータアドバタイズメント(134) : ルータは定期的に各マルチキャストインターフェイスからルータアドバタイズメントをマルチキャストし、そのインターフェイスのIPアドレスをアナウンスします。
- ND NS(135) : メッセージはノードによって発信され、別のノードのリンク層アドレスを要求します。また、重複アドレス検出やネイバーの到達不能検出などの機能にも使用されます。
- ND NA(136):NSメッセージに応答してメッセージが送信されます。ノードがリンク層アドレスを変更すると、未承諾のNAを送信して新しいアドレスをアドバタイズできます。

ステップ22: (オプション) ICMPメッセージには、メッセージの処理方法を示すコードフィールドを設定できます。これは、ステップ10でICMPプロトコルを選択した場合に有効になります。次のいずれかのオプションをクリックして、このコードをフィルタリングするかどうかを設定します。

ICMP: Any
 Select from list Destination Unreachable (1) ▼
 ICMP Type to match _____ (Range: 0 - 255)

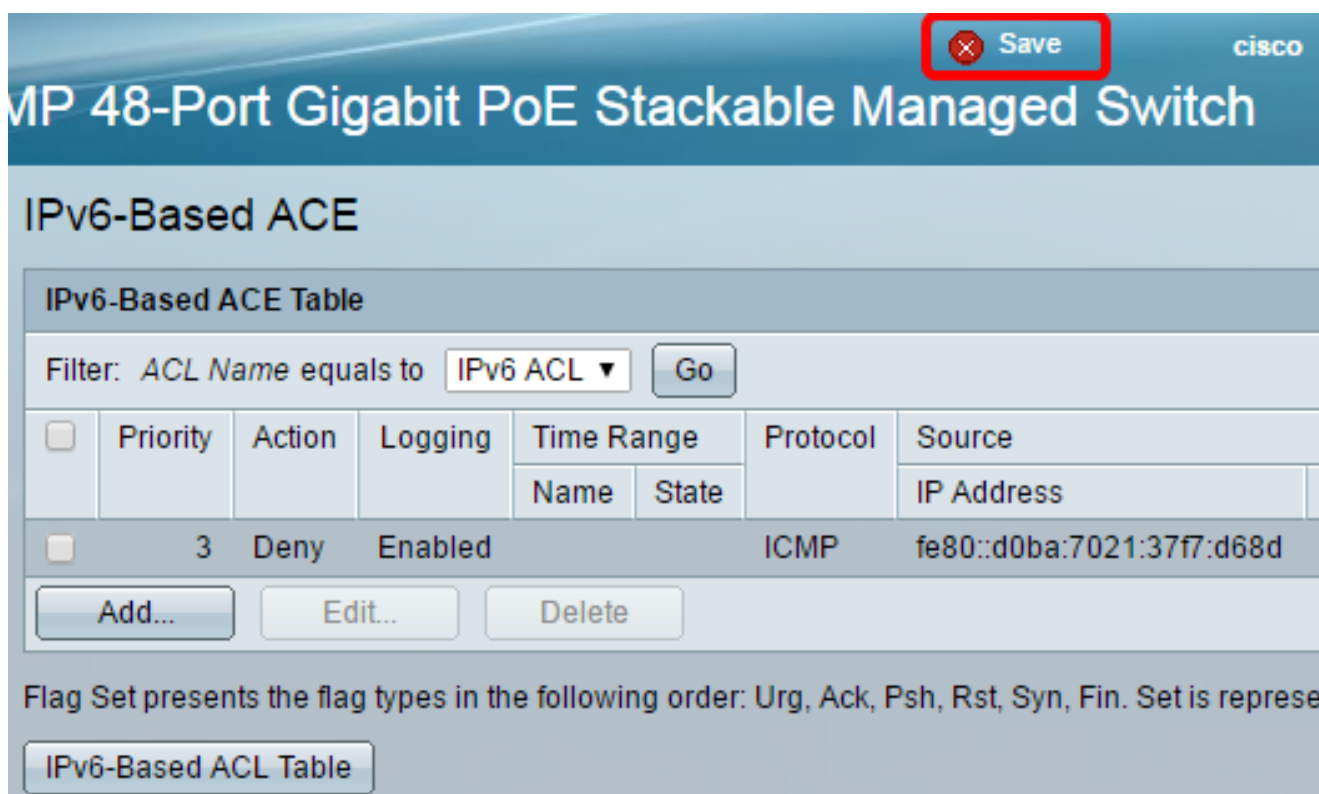
ICMP Code: Any
 User Defined _____ (Range: 0 - 255)

- Any : すべてのコードを受け入れます。
- [ユーザ定義(User Defined)] : フィルタリングの目的でICMPコードを入力できます。

注 : この例では、[Any]が選択されています。

ステップ23:[Apply]をクリックし、[Close]をクリックします。ACEが作成され、ACL名に関連付けられます。

ステップ24:[Save]をクリックし、スタートアップコンフィギュレーションファイルに設定を保存します。



MP 48-Port Gigabit PoE Stackable Managed Switch

IPv6-Based ACE

IPv6-Based ACE Table

Filter: ACL Name equals to IPv6 ACL ▼ Go

| <input type="checkbox"/> | Priority | Action | Logging | Time Range | | Protocol | Source |
|--------------------------|----------|--------|---------|------------|-------|----------|---------------------------|
| | | | | Name | State | | IP Address |
| <input type="checkbox"/> | 3 | Deny | Enabled | | | ICMP | fe80::d0ba:7021:37f7:d68d |

Add... Edit... Delete

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represe

IPv6-Based ACL Table

これで、スイッチにIPv6ベースのACEを設定できました。