

スイッチでのIPv4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。

IPv4ベースACLは、レイヤ3情報を使用してトラフィックへのアクセスを許可または拒否する送信元IPv4アドレスのリストです。IPv4 ACLは、設定されたIPフィルタに基づいてIP関連のトラフィックを制限します。フィルタには、IPパケットに一致するルールが含まれ、パケットが一致する場合は、そのパケットを許可するか拒否するかを指定します。

アクセスコントロールエントリ(ACE)には、実際のアクセスルールの基準が含まれます。ACEが作成されると、ACEはACLに適用されます。

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、マネージドスイッチでIPv4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

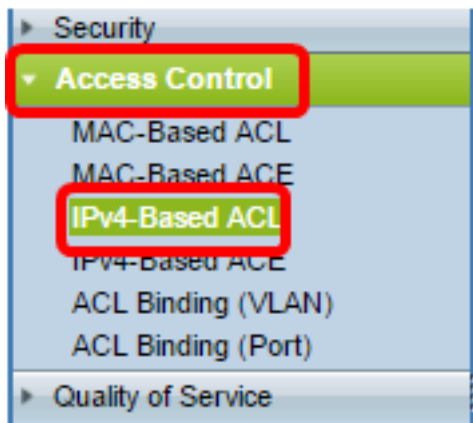
[Software Version]

- 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

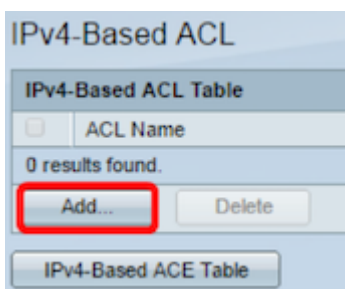
IPv4ベースのACLおよびACEの設定

IPv4ベースACLの設定

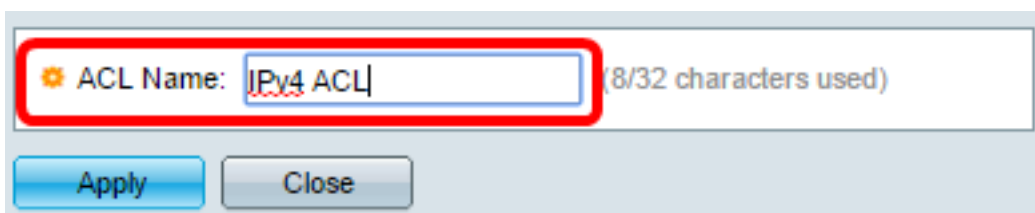
ステップ1: Webベースのユーティリティにログインし、[Access Control] > [IPv4-Based ACL]に移動します。



ステップ2:[Add]ボタンをクリックします。

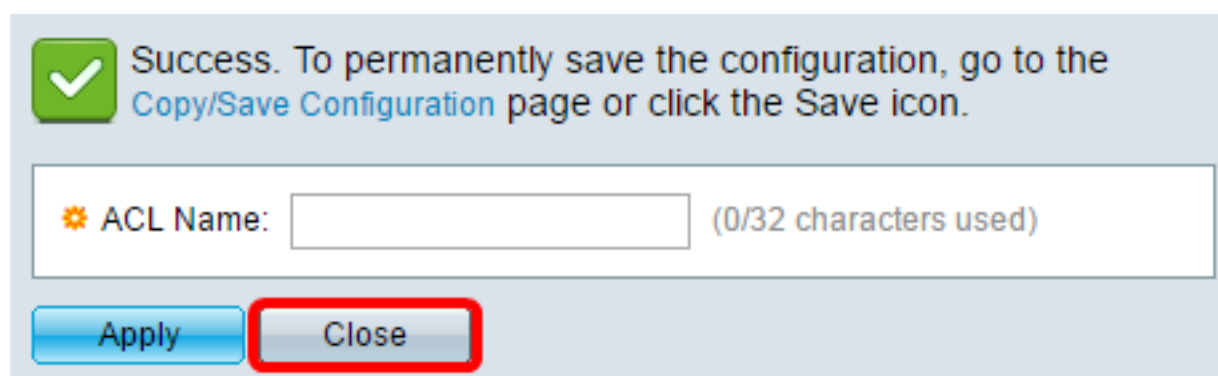


ステップ3:[ACL Name]フィールドに新しいACLの名前を入力します。



注：この例では、IPv4 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IPv4ベースのACLを設定できました。

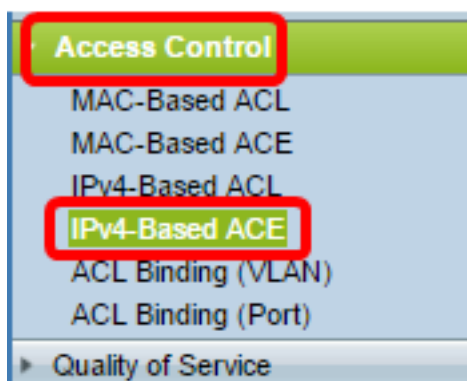
IPv4ベースのACEの設定

ポートでパケットが受信されると、スイッチは最初のACLを介してパケットを処理します。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。

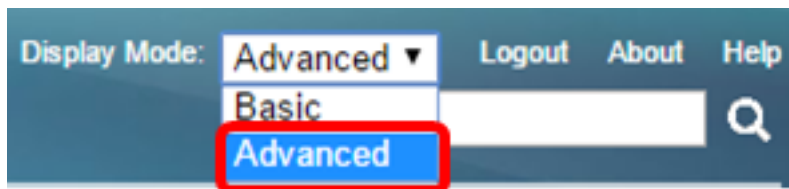
このシナリオでは、特定のユーザ定義の送信元IPv4アドレスから任意の宛先アドレスに送信されるトラフィックを拒否するためにACEが作成されます。

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。

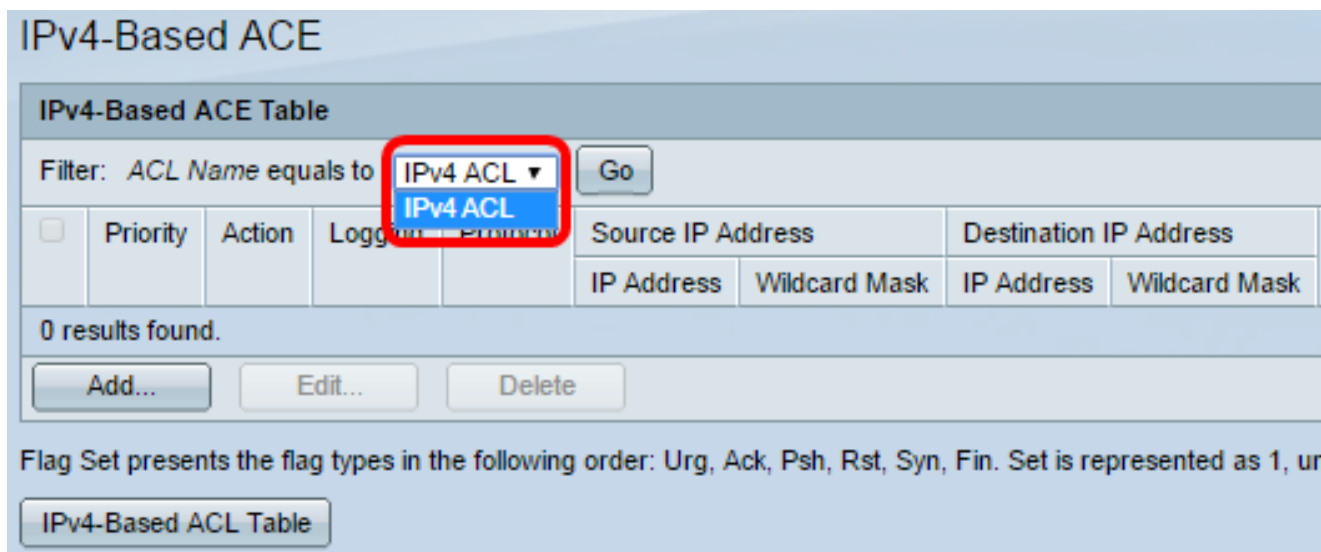
ステップ1: Webベースのユーティリティで、[Access Control] > [IPv4-Based ACE]に移動します。



重要：スイッチの使用可能な機能をフルに活用するには、ページの右上隅にある[表示モード]ドロップダウンリストから[詳細]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: IPv4 ACL

Priority: 2 (Range: 1 - 2147483647)

Action: Permit
 Deny
 Shutdown

Logging: Enable

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

注：この例では、2 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。

注：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) [Enable Logging] チェックボックスをオンにして、ACLルールに一致するACLフローのロギングを有効にします。

Logging: Enable

Time Range: Enable

Time Range Name: Time Range 1 ▼ Edit

Protocol: Any (IP)

Select from list ICMP ▼

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。

Logging: Enable

Time Range: Enable

Time Range Name: Time Range 1 ▼ Edit

Protocol: Any (IPv6)

Select from list TCP ▼

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 ▼ Edit

Protocol: Any (IPv6)

Select from list TCP ▼

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: (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 (IP)
 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、[Any (IP)]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 (IP) Select from list Protocol ID to r (Range: 0 - 255)

Source IP Address: Any User Defined

Source IP Address Value:

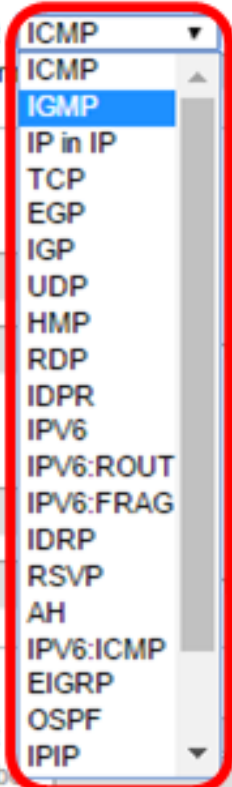
Source IP Wildcard Mask:

Destination IP Address: Any User Defined

Destination IP Address Value:

Destination IP Wildcard Mask:

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



次のオプションがあります。

- ICMP:Internet Control Message Protocol (インターネット制御メッセージプロトコル)
- IP in IP:IP in IPカプセル化
- TCP:Transmission Control Protocol (伝送制御プロトコル)
- EGP:Exterior Gateway Protocol (エクステリアゲートウェイプロトコル)
- IGP:Interior Gateway Protocol (内部ゲートウェイプロトコル)
- UDP:User Datagram Protocol (ユーザデータグラムプロトコル)
- HMP:Host Mapping Protocol
- RDP:Reliable Datagram Protocol
- IDPR : ドメイン間ポリシールーティング
- IPV6:IPv6 over IPv4トンネリング
- IPV6:ROUT : ゲートウェイを経由するIPv6 over IPv4ルートに属するパケットに一致します
- IPV6:FRAG:IPv6 over IPv4フラグメントヘッダーに属するパケットに一致します
- IDRP:IS-ISドメイン間ルーティングプロトコル
- RSVP:ReSerVation Protocol
- AH : 認証ヘッダー
- IPV6:ICMP:ICMP for IPv6
- EIGRP:Enhanced Interior Gateway Routing Protocol(EIGRP)
- OSPF:Open Shortest Path First(OSPF)
- IPIP:IP内のIP
- PIM:Protocol Independent Multicast(PIM)
- L2TP : レイヤ2トンネリングプロトコル

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を入力します。

Protocol: Any (IP) Select from list ICMP Protocol ID to match 1 (Range: 0 - 255)

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IPv4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 Wildcard Mask]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。ワイルドカードマスクは、IPアドレスの範囲を定義するために使用されます。

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: 192.168.1.1

Source IP Wildcard Mask: (0s for matching, 1s for no matching)

注 : この例では、192.168.1.1が使用されています。

ステップ14:[Source IP Wildcard Mask]フィールドに送信元ワイルドカードマスクを入力します。

Source IP Address Value: 192.168.1.1

Source IP Wildcard Mask: 0.0.0.255 (0s for matching, 1s for no matching)

注 : この例では、0.0.0.255が使用されています。

[ステップ15](#): [Destination 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

Source IP Address Value:

Source IP Wildcard Mask: (0s for matching, 1s for no matching)

Destination IP Address: Any User Defined

Destination IP Address Value:

Destination IP Wildcard Mask: (0s for matching, 1s for no matching)

次のオプションがあります。

- [Any] : すべての宛先IPv4アドレスがACEに適用されます。
- [User Defined]:[Destination IP Address Value]フィールドと[Destination IP Wildcard Mask]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。ワイルドカードマスクは、IPアドレスの範囲を定義するために使用されます。

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IPv4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]エリア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 Single by number (Range: 0 - 65535) Range -

Destination Port: Any Single from list 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)

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

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

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

次のオプションがあります。

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

- 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: DSCP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

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を選択するか、メッセ

ージタイプ番号を入力します。

- [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。範囲は0 ~ 255です。

ステップ21: (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。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。

- 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。範囲は0 ~ 255です。

ステップ22: (オプション) ACLがIGMPに基づいている場合は、フィルタリングに使用するIGMP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。

- [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)] : ドロップダウンリストから任意のオプションを選択できます。
- DVMRP : リバースパスフラッディング技術を使用し、パケットが到着したインターフェイス以外の各インターフェイスから受信パケットのコピーを送信します。
- Host-Query : 接続された各ネットワークで一般的なhost-queryメッセージを定期的を送信して情報を取得します。
- Host-Reply : クエリに応答します。
- PIM:Protocol Independent Multicast(PIM)は、マルチキャストトラフィックをマルチキャストサーバから多数のマルチキャストクライアントに転送するために、ローカルおよびリモートマルチキャストルータ間で使用されます。
- Trace:IGMPマルチキャストグループへの参加と脱退に関する情報を提供します。
- 一致するIGMPタイプ : 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。範囲は0 ~ 255です。

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。

Save cisco

MP 48-Port Gigabit PoE Stackable Managed Switch

IPv4-Based ACE

IPv4-Based ACE Table

Filter: *ACL Name equals to*

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Protocol	Source IP Address	
				Name	State		IP Address	Wildcard Mask
<input type="checkbox"/>	2	Permit	Enabled			ICMP	192.168.1.1	0.0.0.255

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

これで、スイッチにIPv4ベースのACEが設定されているはずですが。