

マネージドスイッチでのMACベース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。メディアアクセスコントロール(MAC)ベースのアクセスコントロールリスト(ACL)は、レイヤ2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MACアドレスのリストです。ワイヤレスアクセスポイントからローカルエリアネットワーク(LAN)ポートへ、またはその逆にパケットが着信する場合、このデバイスはパケットの送信元MACアドレスがこのリストのエントリと一致するかどうかを確認し、ACLルールとフレームの内容を照合します。次に、一致した結果を使用して、このパケットを許可または拒否します。ただし、LANからLANポートへのパケットはチェックされません。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MAC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 | ソフトウェアバージョン

- Sx350シリーズ | 2.2.0.66 (最新の[ダウンロード](#))
- SG350Xシリーズ | 2.2.0.66 (最新の[ダウンロード](#))
- Sx500シリーズ | 1.4.5.02 (最新の[ダウンロード](#))
- Sx550Xシリーズ | 2.2.0.66 (最新の[ダウンロード](#))

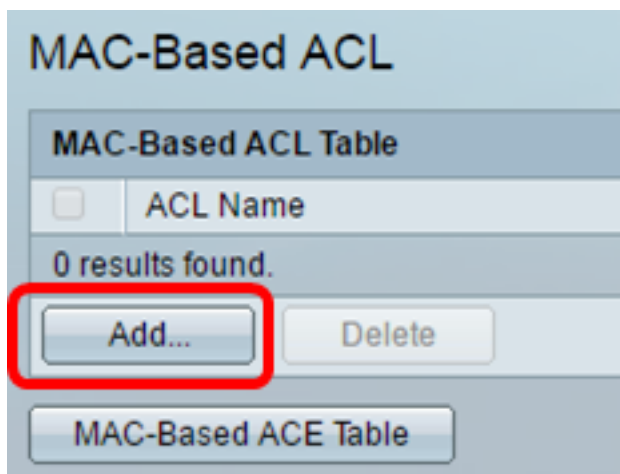
MACベースのACLとACEの設定

MACベースのACLの設定

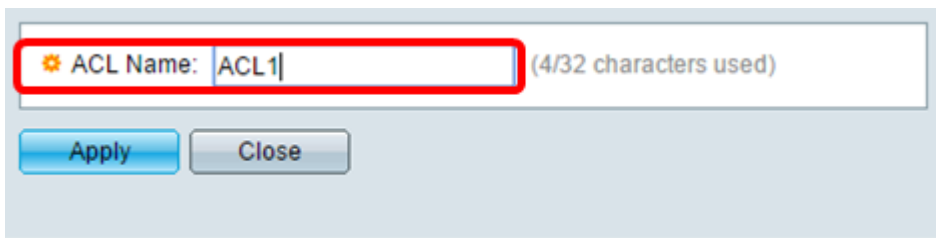
ステップ1: Webベースのユーティリティにログインし、[Access Control] > [MAC-Based ACL]に移動します。



ステップ2:[Add]ボタンをクリックします。



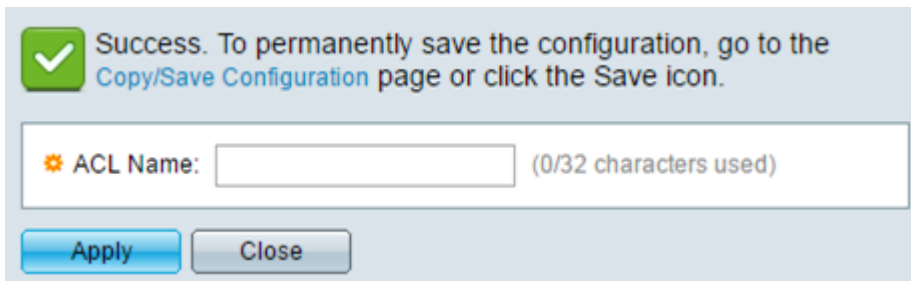
ステップ3:[ACL Name]フィールドに新しいACLの名前を入力します。



ACL Name: ACL1 (4/32 characters used)

Apply Close

ステップ4:[Apply]をクリックして、[Close]をクリックします。

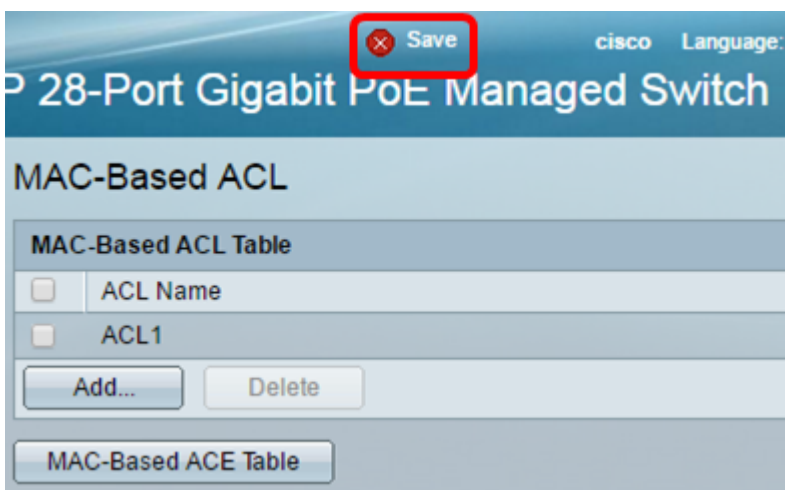


Success. To permanently save the configuration, go to the [Copy/Save Configuration](#) page or click the Save icon.

ACL Name: (0/32 characters used)

Apply Close

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。



Save cisco Language:

28-Port Gigabit PoE Managed Switch

MAC-Based ACL

MAC-Based ACL Table

<input type="checkbox"/>	ACL Name
<input type="checkbox"/>	ACL1

Add... Delete

MAC-Based ACE Table

これで、スイッチにMACベースのACLを設定できました。

MACベースのACEの設定

ポートでフレームが受信されると、スイッチは最初のACLを介してフレームを処理します。フレームが最初の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。フレームがいずれの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、フレームはデフォルトで廃棄されます。

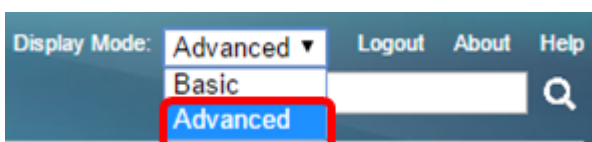
このシナリオでは、特定のユーザ定義の送信元MACアドレスから任意の宛先アドレスに送信されるトラフィックを拒否するためにACEが作成されます。

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。

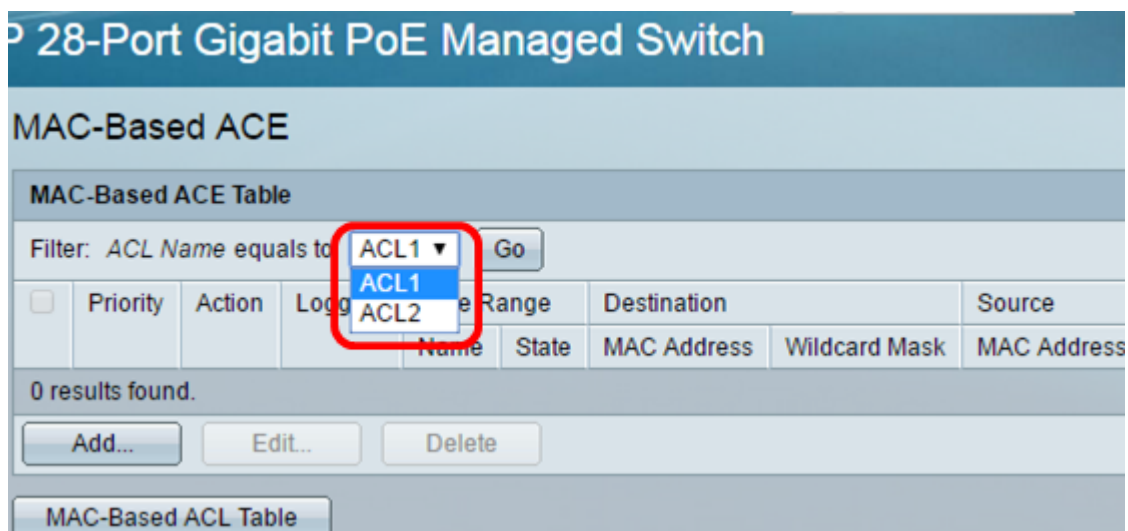
ステップ1:Webベースのユーティリティで、[Access Control] > [MAC-Based ACE]に移動します。



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。

ACL Name:	ACL1
<input type="text" value="Priority:"/>	<input type="text" value="1"/> (Range: 1 - 2147483647)
Action:	<input checked="" type="radio"/> Permit <input type="radio"/> Deny <input type="radio"/> Shutdown
Logging:	<input checked="" type="checkbox"/> Enable

ステップ5: (オプション) [Enable Logging]チェックボックスをオンにして、ACLルールに一致するロギングACLフローを有効にします。

ステップ6：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、[Deny]が選択されています。

<input type="text" value="Priority:"/>	<input type="text" value="1"/> (Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown

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。

<input type="text" value="Time Range:"/>	<input checked="" type="checkbox"/> Enable
<input type="text" value="Time Range Name:"/>	<input type="text" value="1"/> Edit

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。

<input type="text" value="Time Range:"/>	<input checked="" type="checkbox"/> Enable
<input type="text" value="Time Range Name:"/>	<input type="text" value="1"/> Edit

注：「編集」をクリックし、「時間範囲」ページに移動して時間範囲を作成できます。

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

Absolute Starting Time: Immediate
 Date 2016 Jan 01 Time 00 00 HH:MM

Absolute Ending Time: Infinite
 Date 2017 Dec 01 Time 23 59 HH:MM

Apply Close

ステップ9:[Destination MAC Address]エリアで、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。

Destination MAC Address: Any
 User Defined

※ Destination MAC Address Value:

※ Destination MAC 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MACアドレスがACEに適用されます。

「ユーザー定義」 — ACEに適用するMACアドレスとMACワイルドカードマスクを、「宛先MACアドレスの値」および「宛先MACワイルドカードマスク」フィールドに入力します。ワイルドカードマスクは、MAC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、作成するACEによってACEトラフィックが拒否されます。

ステップ10:[Source MAC 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。

ACL Name:	ACL1	
Priority:	<input type="text" value="1"/>	(Range: 1 - 2147483647)
Action:	<input type="radio"/> Permit <input checked="" type="radio"/> Deny <input type="radio"/> Shutdown	
Logging:	<input checked="" type="checkbox"/> Enable	
Time Range:	<input checked="" type="checkbox"/> Enable	
Time Range Name:	<input type="text" value="1"/> Edit	
Destination MAC Address:	<input checked="" type="radio"/> Any <input type="radio"/> User Defined	
Destination MAC Address Value:	<input type="text"/>	
Destination MAC Wildcard Mask:	<input type="text"/>	(0s for matching, 1s for no matching)
Source MAC Address:	<input type="radio"/> Any <input checked="" type="radio"/> User Defined	
Source MAC Address Value:	<input type="text" value="a2:b2:c2:d2:e2:f2"/>	
Source MAC Wildcard Mask:	<input type="text" value="000000001111"/>	(0s for matching, 1s for no matching)
VLAN ID:	<input type="text" value="2"/>	(Range: 1 - 4094)
802.1p:	<input checked="" type="checkbox"/> Include	
802.1p Value:	<input type="text" value="1"/>	(Range: 0 - 7)
802.1p Mask:	<input type="text" value="0"/>	(Range: 0 - 7)
Ethertype:	<input type="text" value="88AB"/>	(Range: 5DD - FFFF)
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

次のオプションがあります。

Any : すべての送信元MACアドレスがACEに適用されます。

「ユーザー定義」 — ACEに適用するMACアドレスとMACワイルドカードマスクを、「ソースMACアドレス値」および「ソースMACワイルドカードマスク」フィールドに入力します。ワイルドカードマスクは、MAC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。

ステップ11: (オプション) [VLAN ID]フィールドに、フレームのVLANタグと一致するVLAN IDを入力します。

ステップ12: (オプション) ACE基準に802.1p値を含めるには、[802.1pに含める]チェックボックスをオンにします。802.1pには、テクノロジークラス(CoS)が含まれています。CoSは、トラフィックの差別化に使用されるイーサネットフレームの3ビットフィールドです。

ステップ13:802.1p値が含まれている場合は、次のフィールドに入力します。

[802.1p値(802.1p Value)] : 一致させる802.1p値を入力します。802.1pは、レイヤ2スイッチ

がトラフィックの優先順位付けやダイナミックマルチキャストフィルタリングを実行できるようにする仕様です。値は次のとおりです。

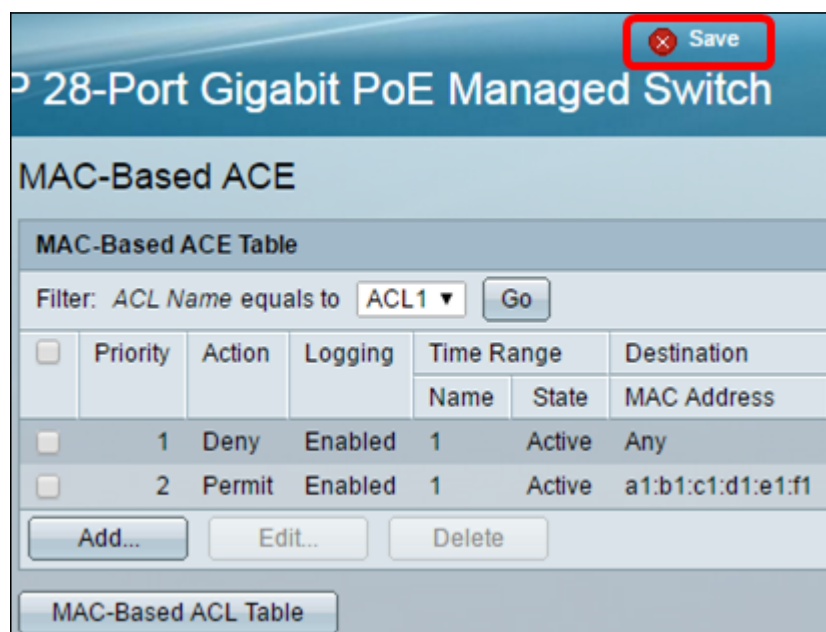
- 0 - バックグラウンド。バルク転送、ゲームなどの優先順位が最も低いデータ。
- 1 : ベストエフォート。通常のLANプライオリティでのベストエフォート配信が必要なデータ。ネットワークは配信に関する保証を提供しませんが、データはトラフィックに基づいて特定のビットレートと配信時間を取得します。
- 2 - 優れた労力。重要なユーザにベストエフォートの配信を必要とするデータ。
- 3:Linux仮想サーバ(LVS)電話セッション開始プロトコル(SIP)などの重要なアプリケーション。
- 4 - ビデオ。遅延とジッタが100ミリ秒未満
- 5 : 音声Cisco IP Phoneのデフォルト。遅延とジッタが10ミリ秒未満
- 6:Inter-network Control LVS phone Real-time Transport Protocol(RTP)。
- 7 - ネットワーク制御。ネットワークインフラストラクチャの維持とサポートに必要な要件が高い。

802.1p Mask:802.1p値のワイルドカードマスクを入力します。このワイルドカードマスクは、802.1p値の範囲を定義するために使用されます。

ステップ14: (オプション) 一致させるフレームのEthertypeを入力します。Ethertypeは、フレームのペイロードに使用されるプロトコルを示すために使用される、イーサネットフレームの2オクテットフィールドです。

ステップ14:[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15:[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。



The screenshot shows a configuration page for a "28-Port Gigabit PoE Managed Switch". The main heading is "MAC-Based ACE". Below it is a "MAC-Based ACE Table" section. A filter is set to "ACL Name equals to" with a dropdown menu showing "ACL1" and a "Go" button. The table contains two entries:

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Destination
				Name	State	MAC Address
<input type="checkbox"/>	1	Deny	Enabled	1	Active	Any
<input type="checkbox"/>	2	Permit	Enabled	1	Active	a1:b1:c1:d1:e1:f1

Below the table are buttons for "Add...", "Edit...", and "Delete". At the bottom, there is a "MAC-Based ACL Table" button. A red box highlights the "Save" button in the top right corner of the interface.

これで、スイッチにMACベースのACEが設定されているはずですが。

その他の便利なリンク：

- [350シリーズスイッチ製品ページ](#)
- [350Xシリーズスイッチ製品ページ](#)
- [550シリーズスイッチ製品ページ](#)
- [550Xシリーズスイッチ製品ページ](#)

この記事に関連するビデオを表示...

[シスコのその他のテクニカルトークを表示するには、ここをクリックしてください](#)