SG350XGおよびSG550XGでのMACベースACLの作成

目的

アクセスコントロールリスト(ACL)は、特定の基準を満たしているかどうかに応じてパケットを操作するために作成できる一連のルールです。これらの基準は、送信元アドレスまたは宛先アドレス、ヘッダーフィールド、およびパケットのさまざまなコンポーネントです。パケットがACLの指定された基準に一致する場合、パケットは廃棄されるか、続行されます。MACベースのACLは、MACアドレス、VLAN ID、Ethertype値など、パケットのレイヤ2ヘッダーを分析するルールを使用します。MACベースのACLを実装すると、レイヤ2レベルでスイッチを通過するパケットを制御できます。

このドキュメントの目的は、SG350XGおよびSG550XGスイッチでMACベースのACLを作成および設定する方法を示すことです。

該当するデバイス

- SG350XG
- SG550XG

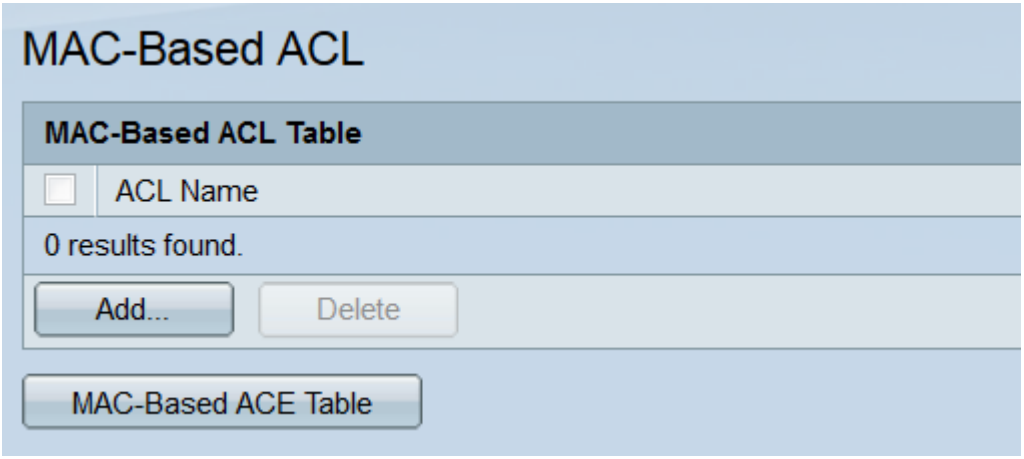
[Software Version]

- v2.0.0.73

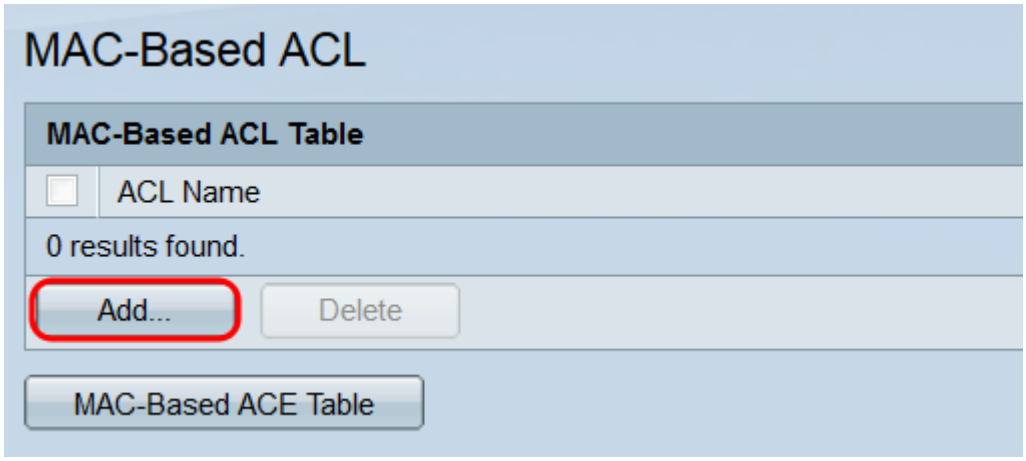
Fast SSID Changing の設定 MACベースのACL

作成 ACLとルール

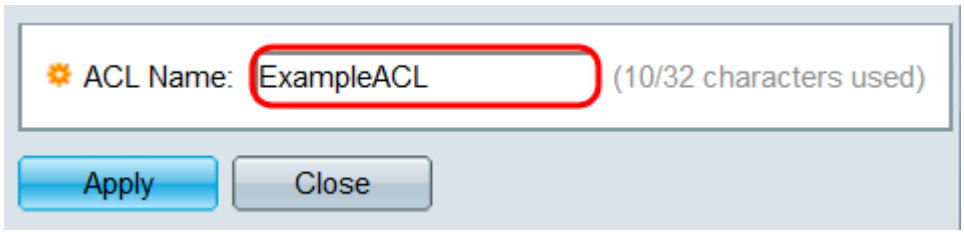
ステップ1:Web設定ユーティリティにログインし、[Access Control] > [MAC-Based ACL]を選択します。[*MAC-Based ACL]ページが*開きます。



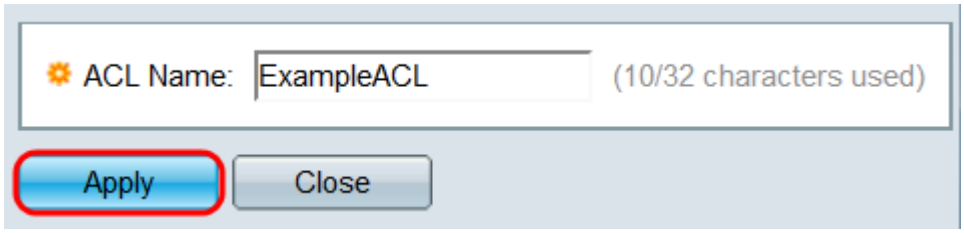
ステップ2:MACベース*のACLテーブル*には、スイッチ上のすべてのMACベースのACLが表示されます。新しいACLを作成するには、[Add...]ボタン**をクリック**します。[*Add MAC-Based ACL*]*ウィンドウが*開きます。



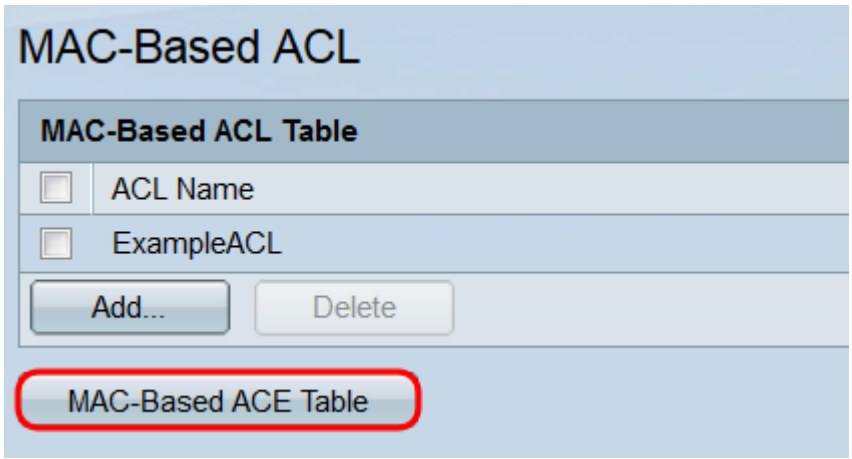
ステップ3:[*ACL Name*]フィールドに、新しいACLの名前を入力します。この名前はACLの機能に影響を与えず、識別のためだけに使用されます。



ステップ4:[Apply]をクリックします。新しいACLがMACベースのACLテーブルに追加されます。[閉じる]をクリックして[*MAC-Based ACL*]ページに戻るか、前の手順を繰り返して別のACLを作成します。

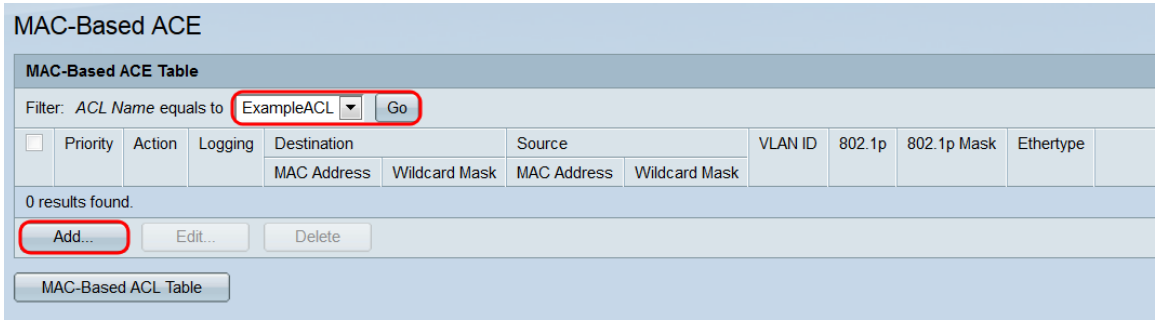


ステップ5：新しく作成されたACLはすべて空になります。つまり、MACアドレスに基づいてパケットをブロックまたは許可するルールは含まれていません。これらのルールを作成するには、アクセスコントロールエントリ(ACE)をACLに追加する必要があります。これを行うには、[MAC-Based ACE Table]ボタンをクリックし、[*MAC-Based ACE*]ページに移動します。

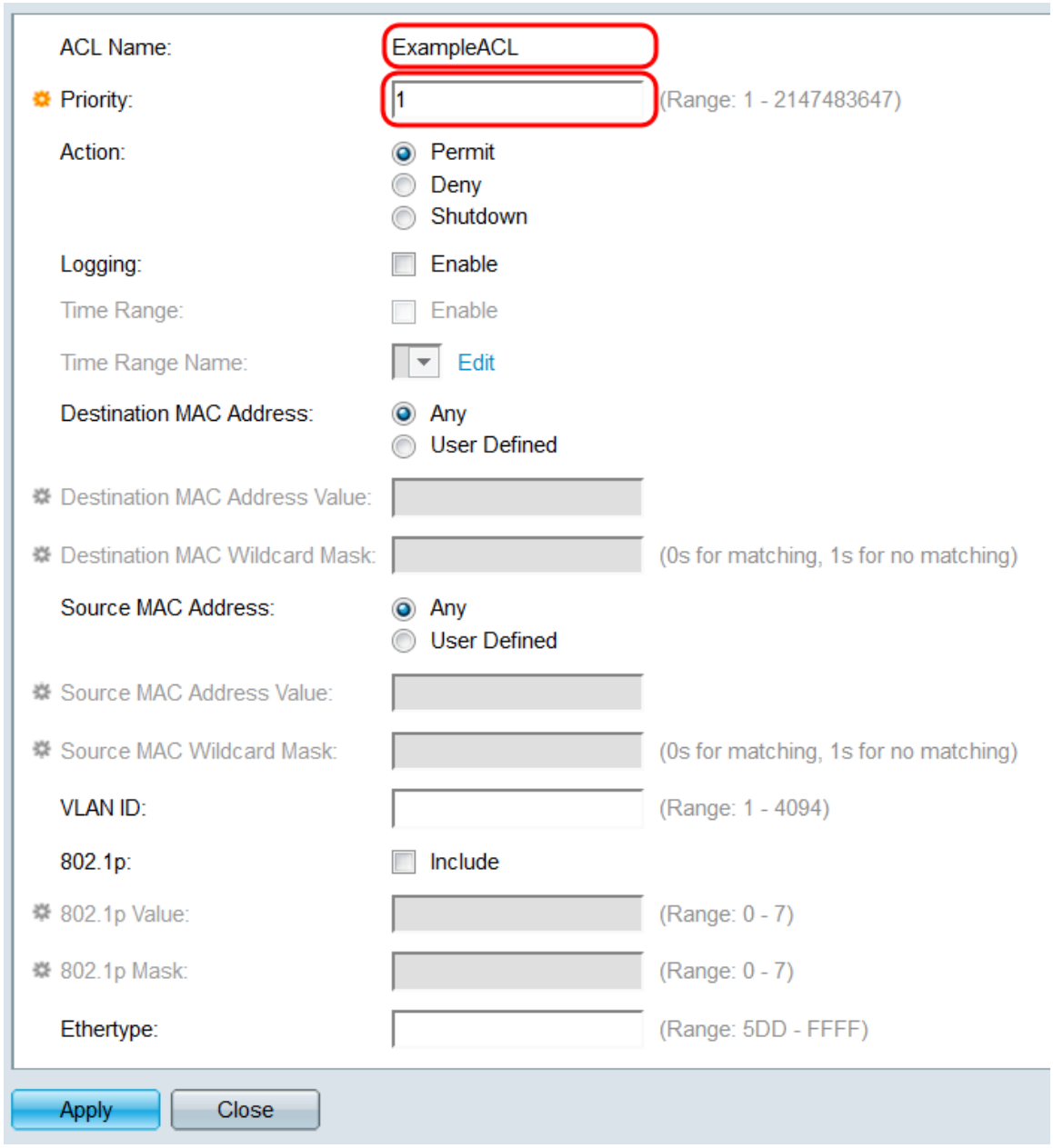


ステップ6:[*MAC-Based ACE（MACベースACE）*]ページで、MACベースACEテーブルの上部にあるドロップダウンリストからACEを追加するACLを選択し、[Go]をクリックします。

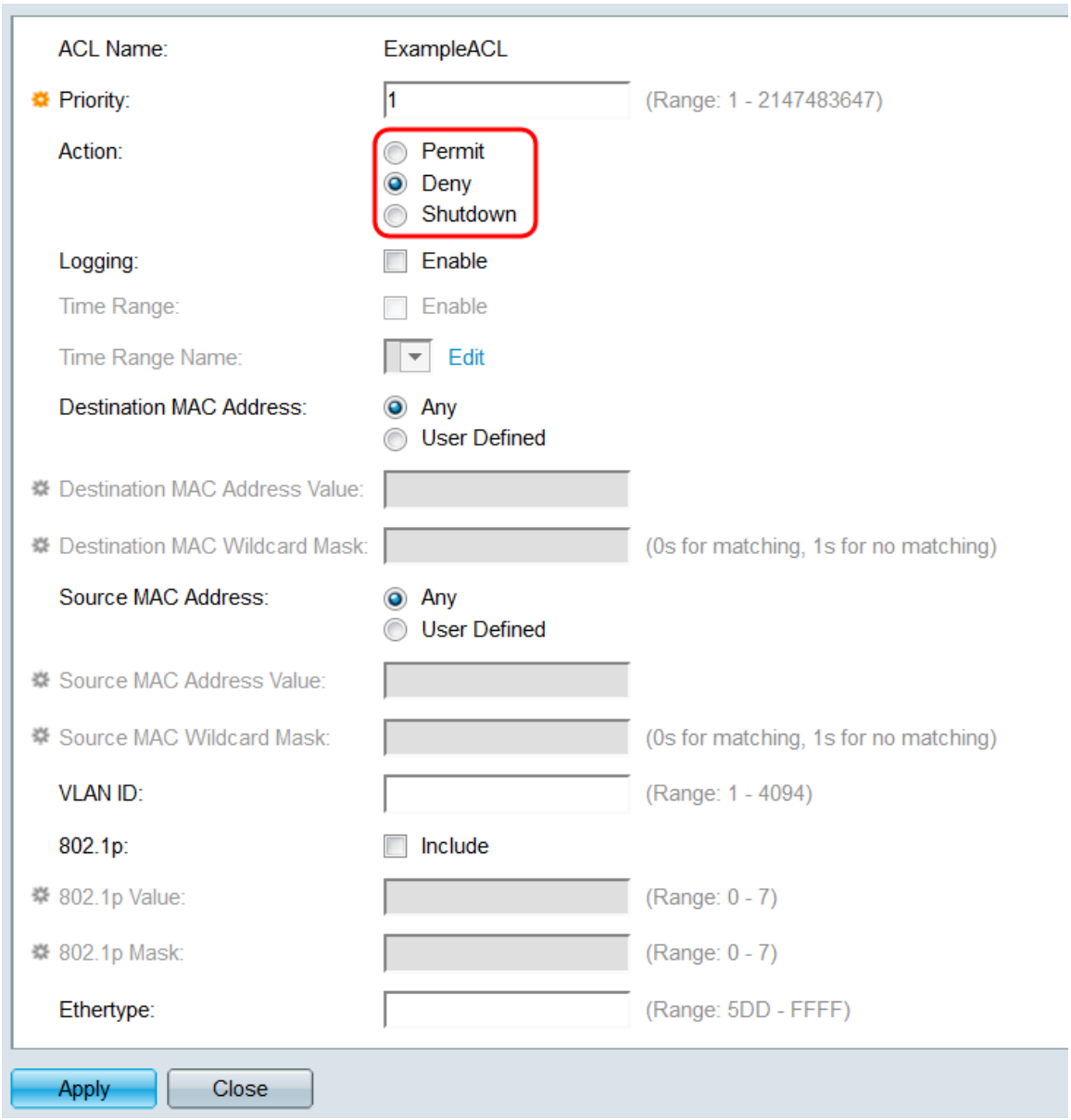
この表には、選択したACLに現在関連付けられているACEが表示されます。ACEを追加するには、[**Add**...]ボタンをクリックします。[*Add MAC-Based ACE*]ウィンドウが開きます。



ステップ7:[*ACL Name*]フィールドに、ACEを追加するACLの名前が表示されます。[Priority]フィールドに、ACEのプライオリティ番号を入力します。ACEの優先度が高いほど、処理が早くなります。範囲は1 ~ 2147483647で、1が最も高い優先度です。



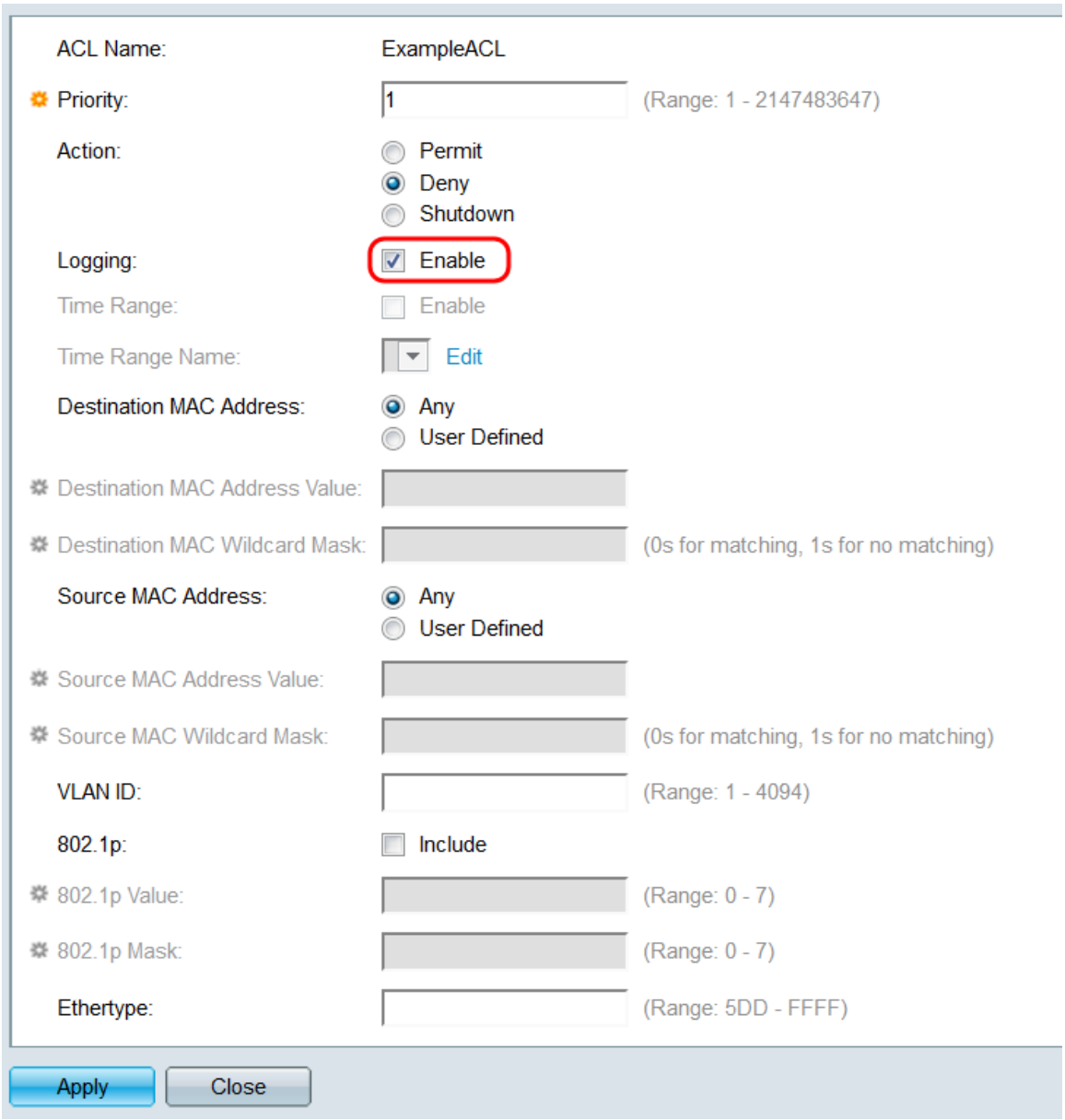
ステップ8:[*Action*]フィールドで、*ACEの基準を満たしたときに何が起こるかを決定するラジオ・ボタンを選択します。*



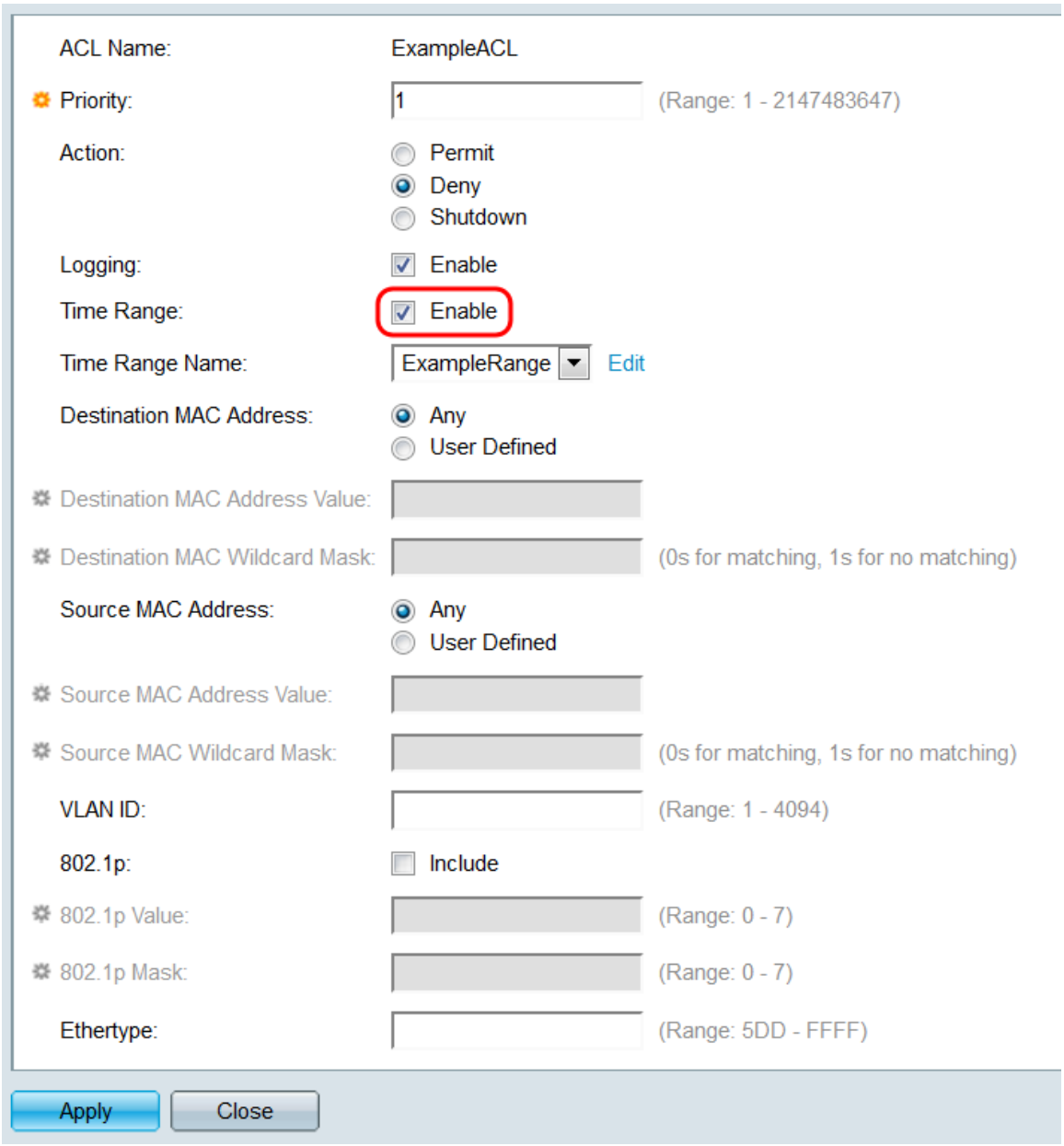
次のオプションがあります。

- Permit：条件を満たすパケットを転送します。
- 拒否：基準を満たすパケットをドロップします。
- Shutdown：基準を満たすパケットをドロップしてから、ポートをディセーブルにします。

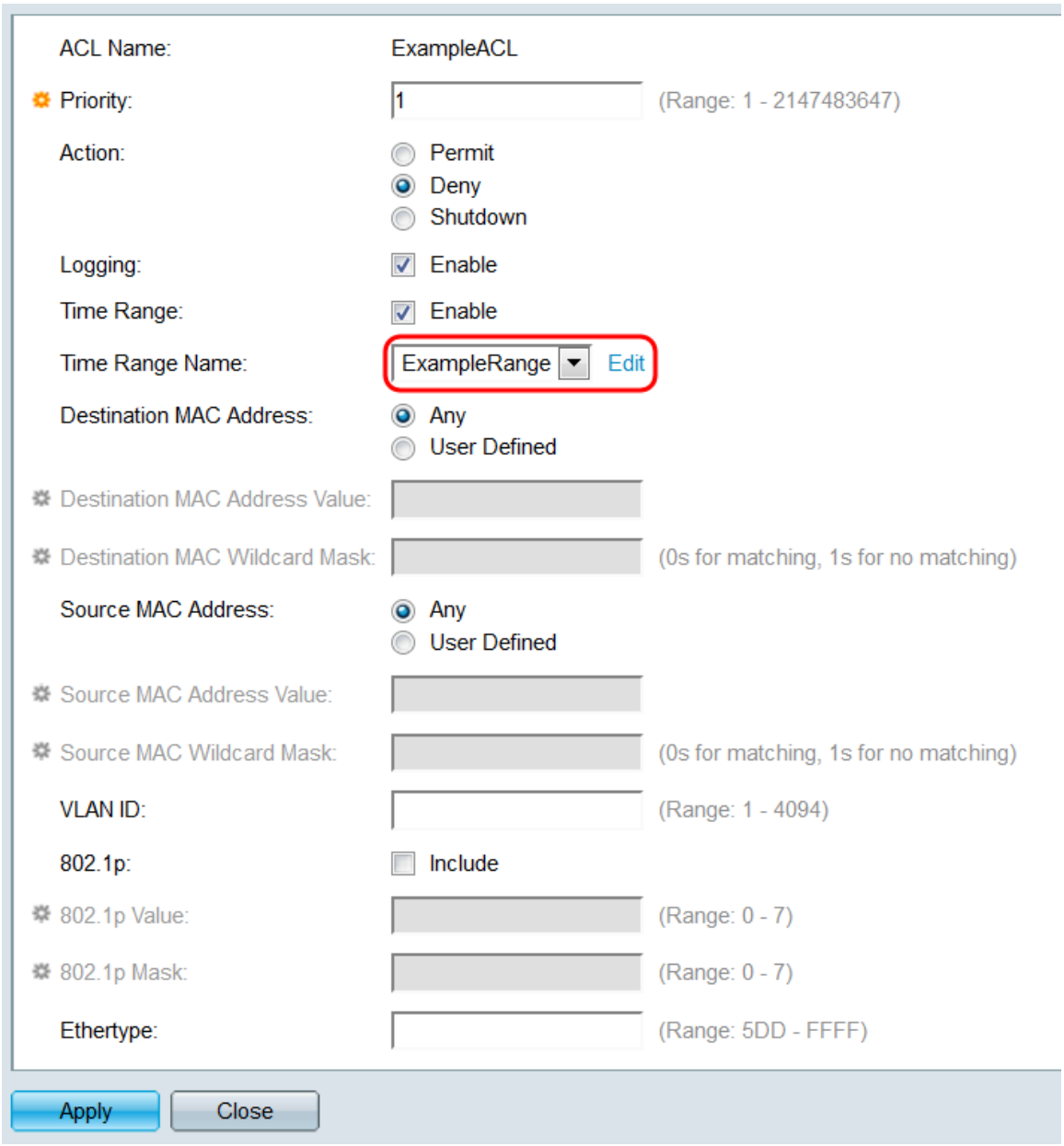
ステップ9:[*Logging*]フィールドで、[**Enable**]チェックボックスをオンにして、ACEルールに一致するロギングACLフローを有効にします。基本表示モードを使用している場合は、ステップ[12に進みます](#)。表示モードは、Webユーティリティの右上隅にあるドロップダウンリストから変更できます。



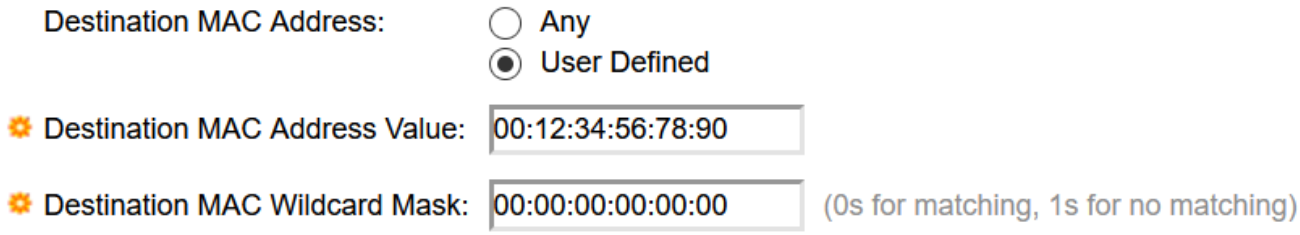
ステップ10:[時間の範囲(*Time Range)]フィールド*で、[有効(**Enable)]チェックボックスをオンにすると、指定した時間範囲内でのみ**ACEがアクティブになります。スイッチに設定されている時間範囲がない場合、このフィールドは使用できません。



ステップ11：このACEの時間範囲を有効にしている場合は、[時間範囲名*(Time Range Name)]*フィールドを使用できます。ドロップダウンリストを使用して、ACEに適用するスイッチですでに設定されている時間範囲を選択します。スイッチに時間範囲がない場合、このフィールドは使用できません。[編集]リンクをクリックして、[時間範*囲]*ページに移動し、時間範囲を作成または変更します。詳細については、「*SG350XGおよびSG550XGの時間範囲の設定」を参照してください*。



ステップ12:[Destination MAC Address]フィールドで、オプションボタンを選択して、一致する宛先MACアドレスを決定します。任意の宛先アドレスを一致させる場合は[任意]を選択し、アドレスまたはアドレスの範囲を指定する場合は[ユーザ定義]を選択します。

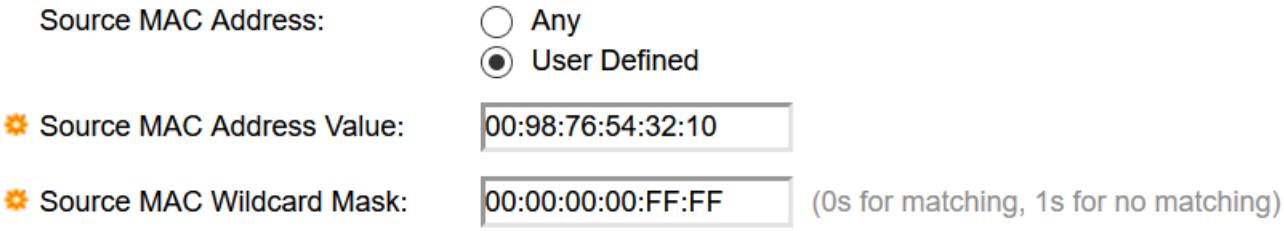


「ユーザー定義」を選択した場合、次のフィールドに入力します。

- Destination MAC Address Value：宛先MACアドレスを入力します。パケットにこの宛先アドレスが含まれている場合、ACEは一致を考慮します。
- 宛先MACワイルドカードマスク：アドレスの範囲を定義するマスクを入力します。ビットを1に設定すると、MACアドレスの対応するビットが無視され、0は一致するビットになります。

注:0000 0000 000 000 000 0000 000 000 0000000000 111111のマスクを指定します（ビット上で一致することを意味します）0と1のビットでは一致しません)。 1を16進数に変換し、4個のゼロごとに0を記述する必要があります。この例では、1111 111 = FFなので、マスクは次のように書かれます。00:00:00:00:00:FFと表示されます。

ステップ13:[*Source MAC Address*]フィールドで、オプションボタンを選択して、一致する送信元MACアドレスを決定します。任意の**送信元**アドレスを一致させる場合は[任意]を選択し、アドレスまたは**アドレスの範**囲を指定する場合は[ユーザ定義]を選択します。



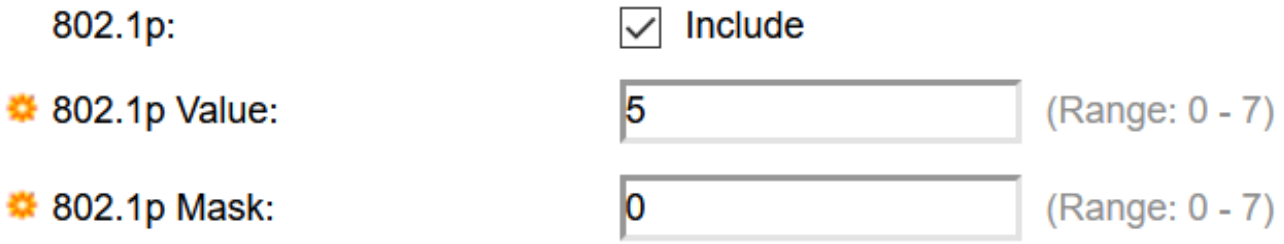
「ユーザー定義」を選**択した場**合、次のフィールドに入力します。

- Source MAC Address Value：送信元MACアドレスを入力します。パケットにこの送信元アドレスが含まれている場合、ACEは一致を考慮します。
- 送信元MACワイルドカードマスク：アドレスの範囲を定義するマスクを入力します。ビットを1に設定すると、MACアドレス内の対応するビットが無視され、0は一致するビット(例：00:00:00:00:00:11)になります。

注:0000 0000 000 000 000 0000 000 000 0000000000 111111のマスクを指定します（ビット上で一致することを意味します）0と1のビットでは一致しません)。 1を16進数に変換し、4個のゼロごとに0を記述する必要があります。この例では、1111 111 = FFなので、マスクは次のように書かれます。00:00:00:00:00:FFと表示されます。

ステップ14:[VLAN ID]フィールドに、1 ~ 4094のVLAN IDを入力します。パケットにこのVLAN IDが含まれている場合、ACEはそのVLAN IDが一致すると見なします。このフィールドは必須ではありません。空白のままにすると、ACEはパケットを検査するときにVLAN IDを考慮しなくなります。

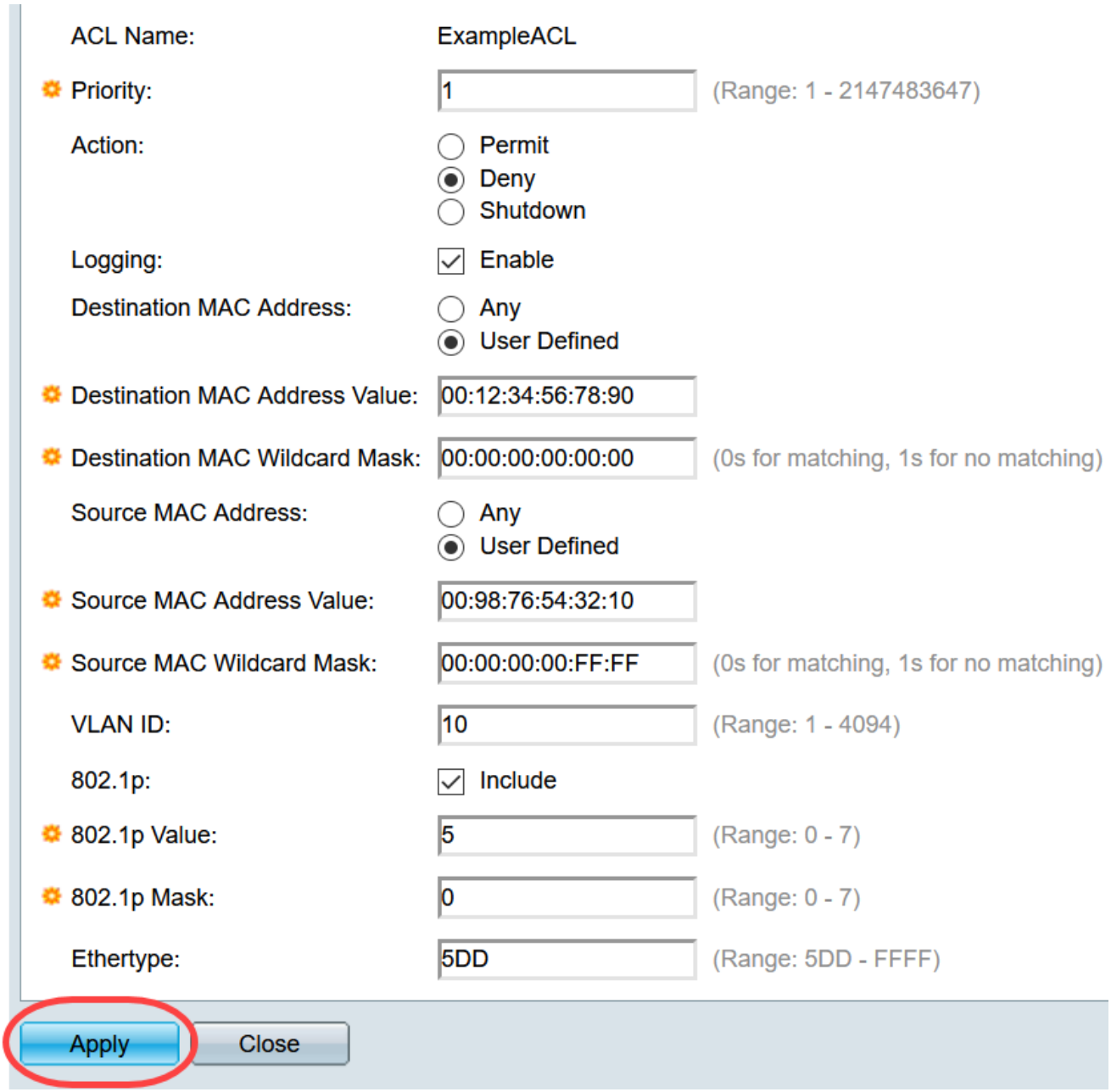
ステップ15:[*802.1p]フィールド*で、[**Include**]チェックボックスをオンにして、ACEに802.1p基準を含めます。802.1p基準を含めた場合は、802.1p値フィールドに802.1p値を、802.1pマスク*フィールド*にマスクをそれぞれ入力します。両方のフィールドの範囲は0 ~ 7です。パケットに対応する802.1p値が含まれ、マスクに適合する場合、ACEはそれを一致と見なします。



ステップ16:[*Ethertype*]フィールドに、着信パケットと比較するEthertype値を入力します。

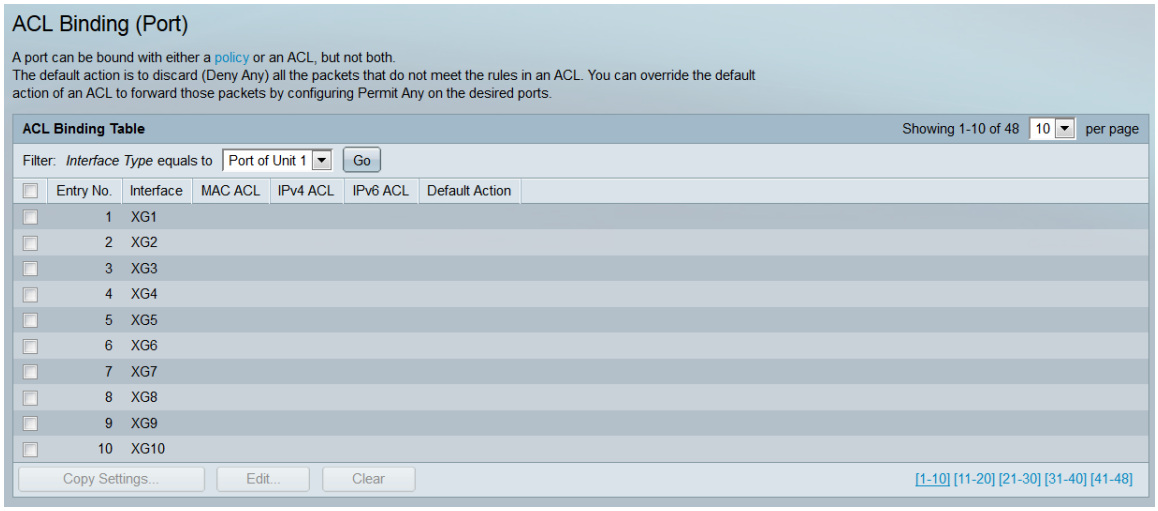
Ethertypeは、パケットにカプセル化されるプロトコルを示す、フレーム内の2オクテットフィールドです。範囲は5DD - FFFFです。パケットに指定されたEthertype値が含まれている場合、ACEはそれを一致と見なします。Ethertype値のリストは、このIEEE標準ページで確認できます。

ステップ17:[Apply]をクリックします。ACEが指定されたACLに追加されます。[閉じる]をクリックして、[*MAC-Based ACE]ページに戻ります。*

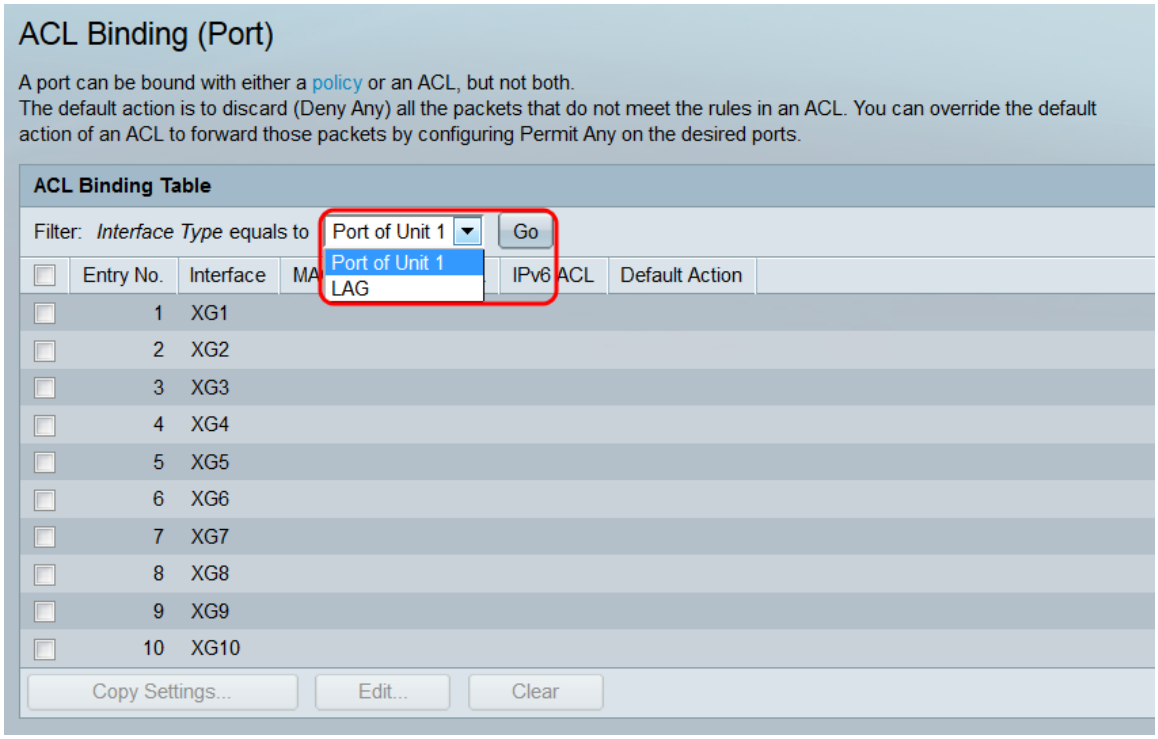


MACベースのACLのマッピング ポートへ

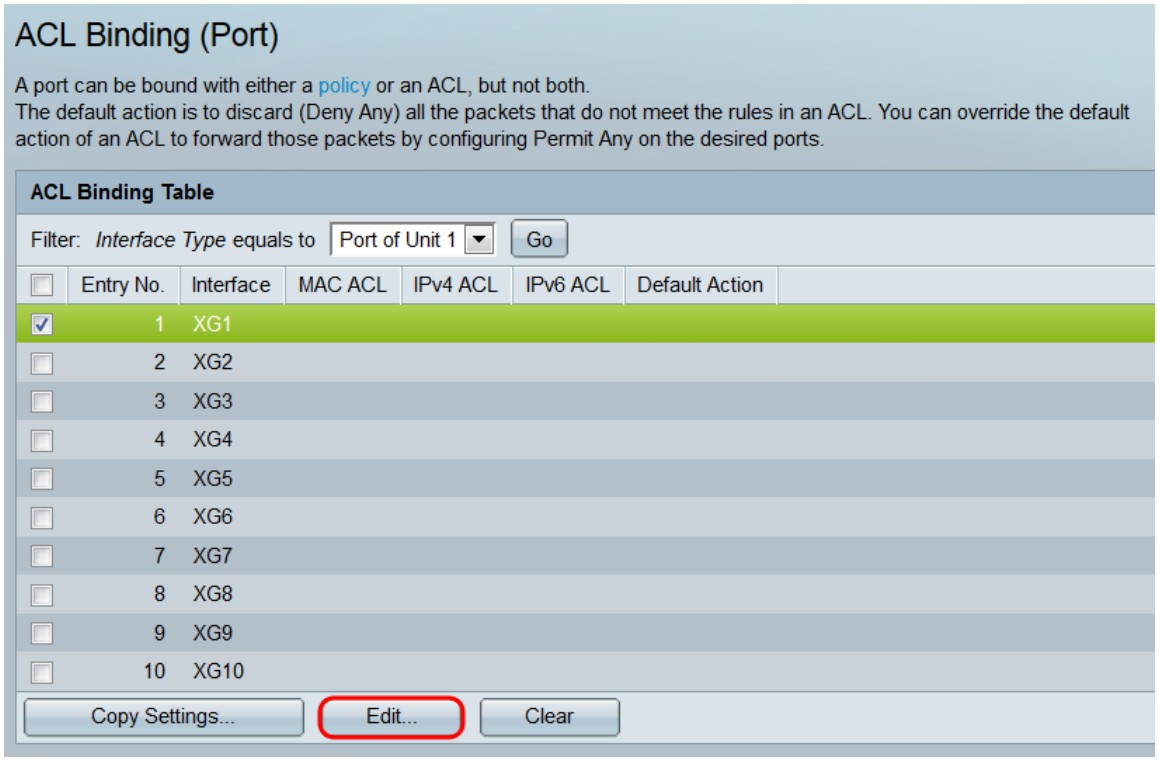
ステップ1:ACLはポートまたはVLANのいずれかにマッピングできます。MACベースのACLをポートにマップするには、[**Access Control**] > [**ACL Binding (Port)**]に移動します。 [*ACL Binding (Port)]ページが*開きます。



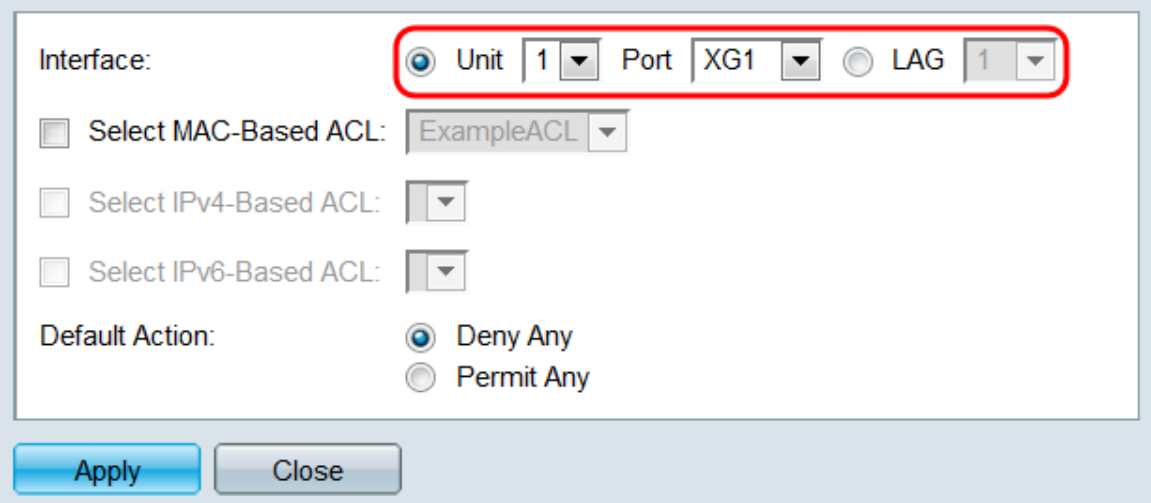
ステップ2:[*ACL Binding Table*]の上部にあるドロップダウンリストで、インターフェイスタイプとしてポートまたはLAG（リンク集約グループ）を選択します。スイッチがスタックの一部である場合は、他のユニットのポートを選択できます。[**Go**]をクリックすると、指定したインターフェイスタイプのリストが表示されます。



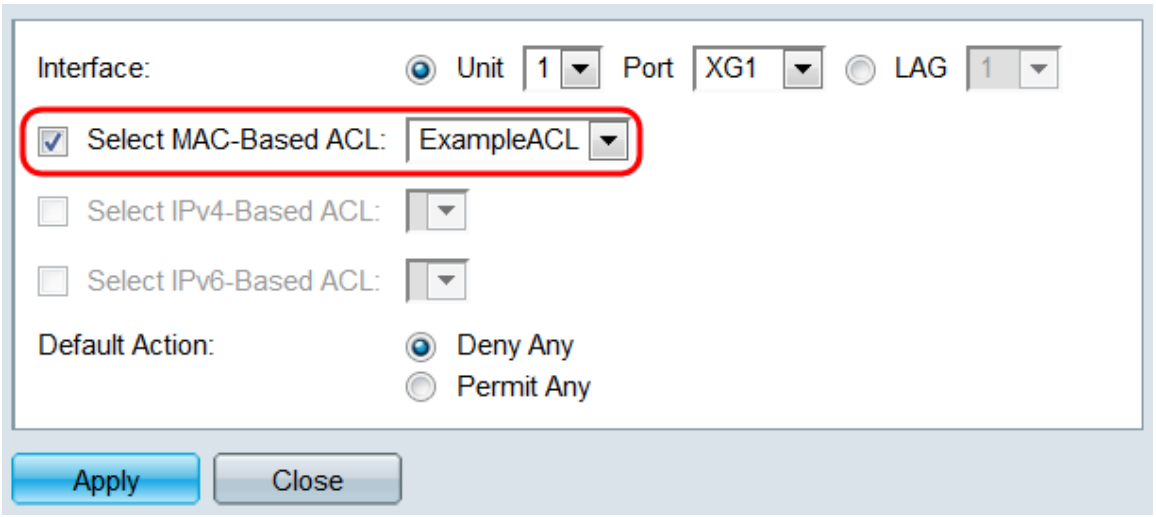
ステップ3：インターフェイスのチェックボックスを選択し、[**Edit...**]**ボタンをクリック**します。[*Edit ACL Binding*]ウィンドウが開きます。



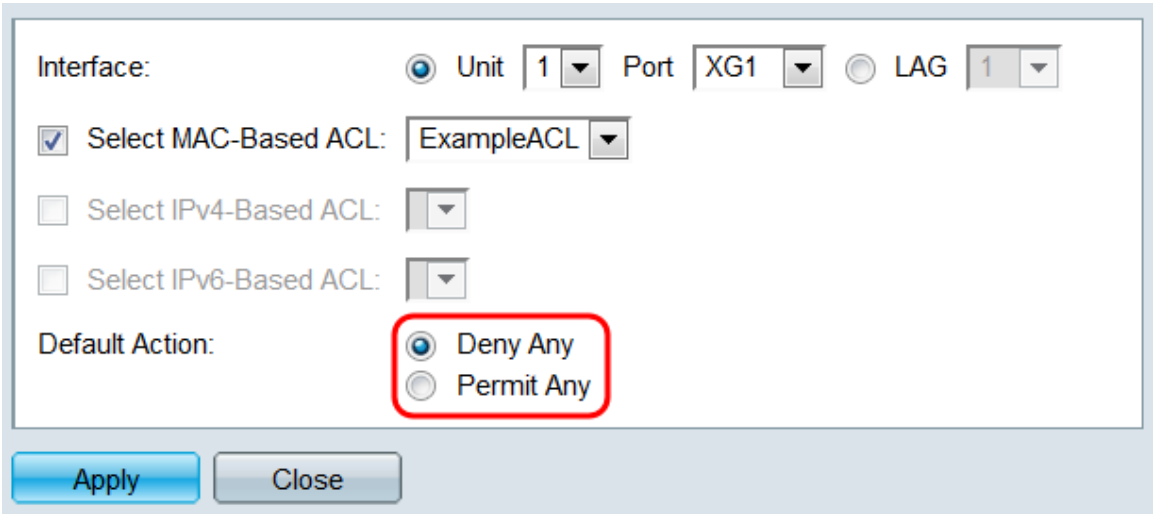
ステップ4:[*Interface*]フィールドには、現在設定されているポートまたはLAGが表示されます。ACLバインディングテーブルで選択されたインターフェイスが*自動的に表示されます。*このフィールドを使用すると、*ACL* Binding (*Port*)ページに戻ることなく、異なるインターフェイス間を迅速に切り替えることができます。



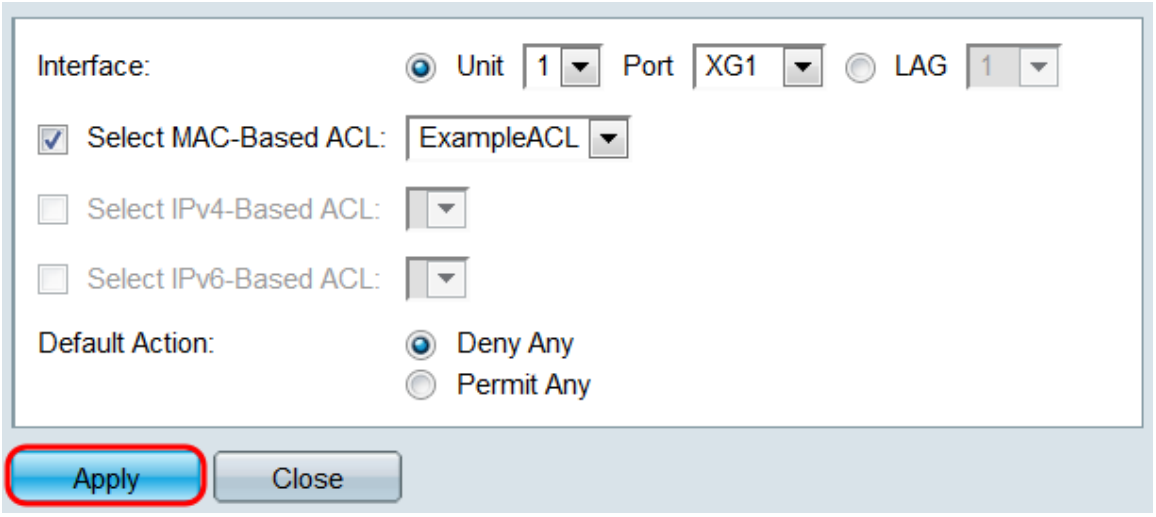
ステップ5:[**Select MAC-Based ACL**]チェックボックスをオンにして、ドロップダウンリストを使用して、指定したインターフェイスにマッピングするACLを選択します。



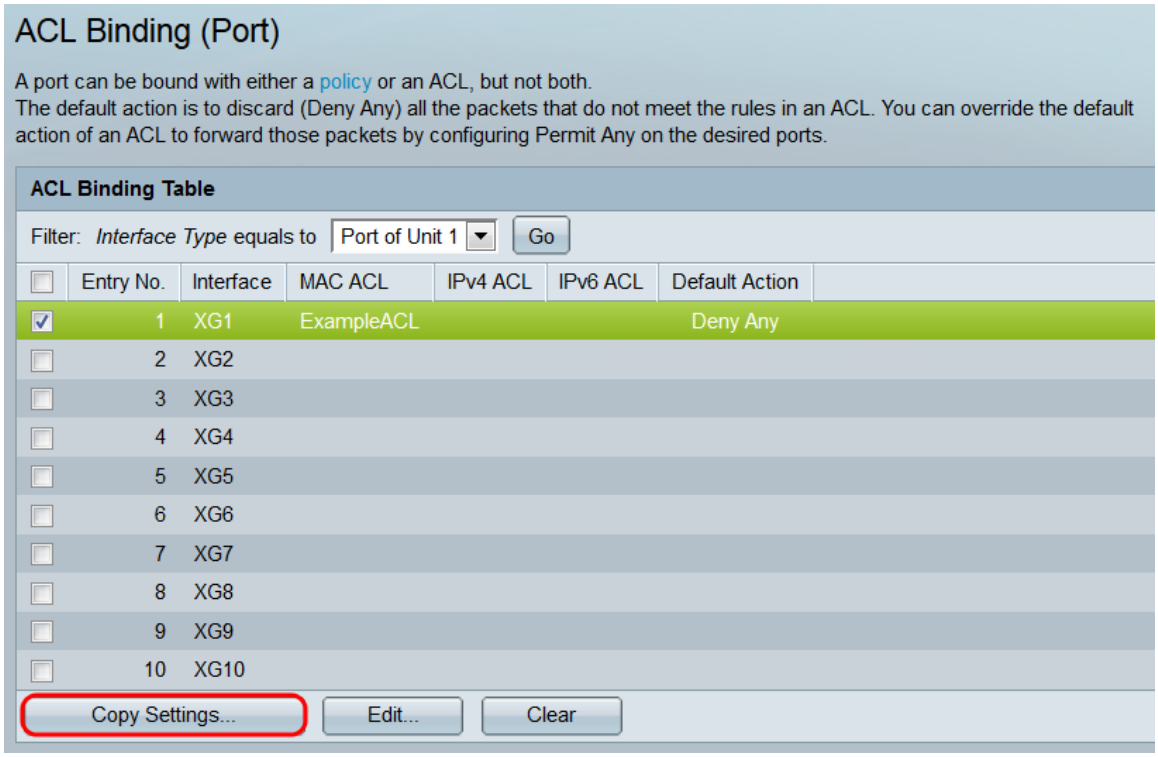
ステップ6:[*Default Action*]フィールドで、ACLの基準に一致しないパケットの処理方法を決定するラジオ・ボタンを選択します。デフォルトは**Deny Any**で、ACLの基準に一致しないパケットはすべてドロップされます。**Permit Any**は、一致しないパケットを転送します。



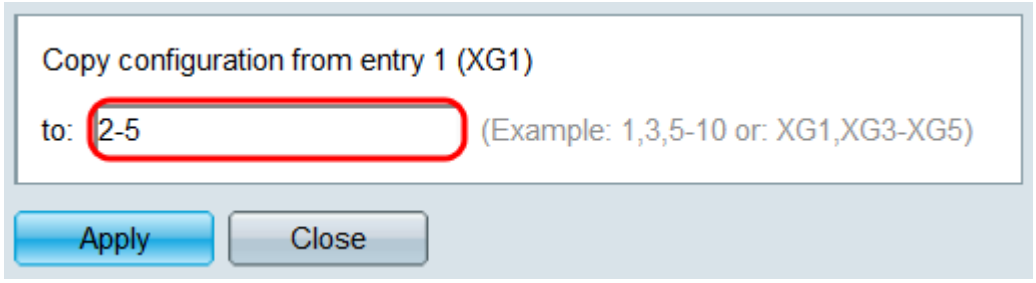
ステップ7:[Apply]をクリ**ックします**。ACLは指定されたインターフェイスにマッピングされます。[インターフェース*]*フィールドを使用して設定する別のインターフェイスを選択するか、[閉じる]をクリックして[*ACLバインド（ポート）]ページに戻ります。*



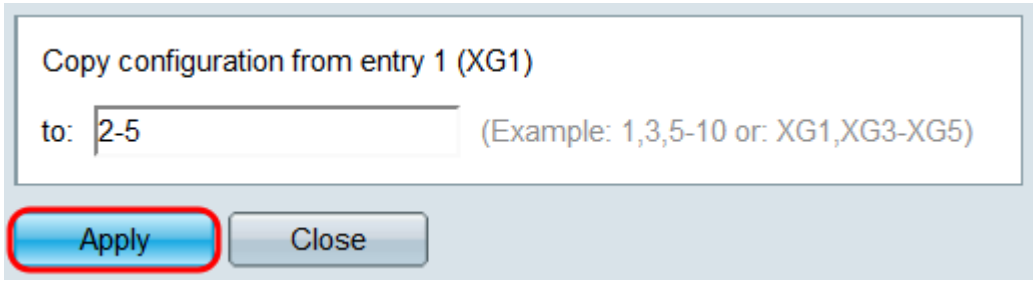
ステップ8：インターフェイスの設定を他のインターフェイスにすばやくコピーするには、コピーするインターフェイスのチェックボックスをオンにし、[設定のコピー...]**ボタンをクリック**します。「設定のコピー」ウィンドウが開きます。



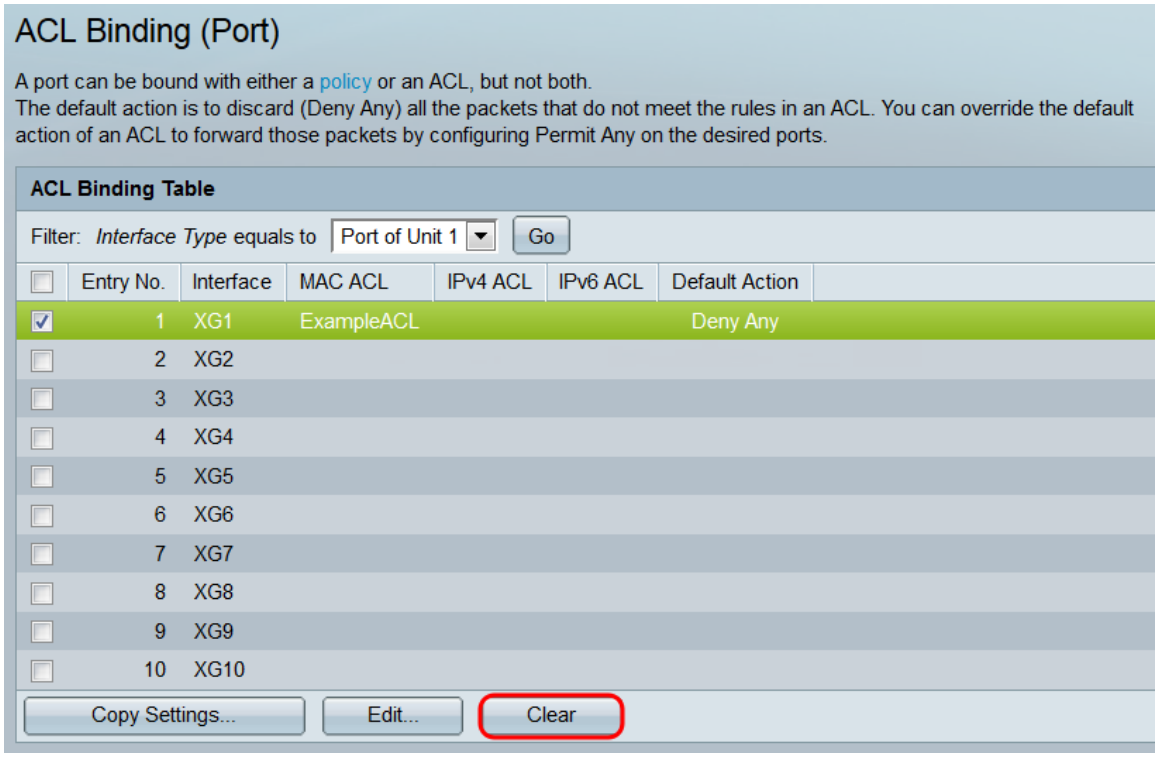
ステップ9：テキストフィールドに、設定をコピーするインターフェイスを1つ以上選択します。インターフェイスはカンマで区切るか、範囲を指定できます。



ステップ10:[Apply]をクリックします。設定がコピーされます。

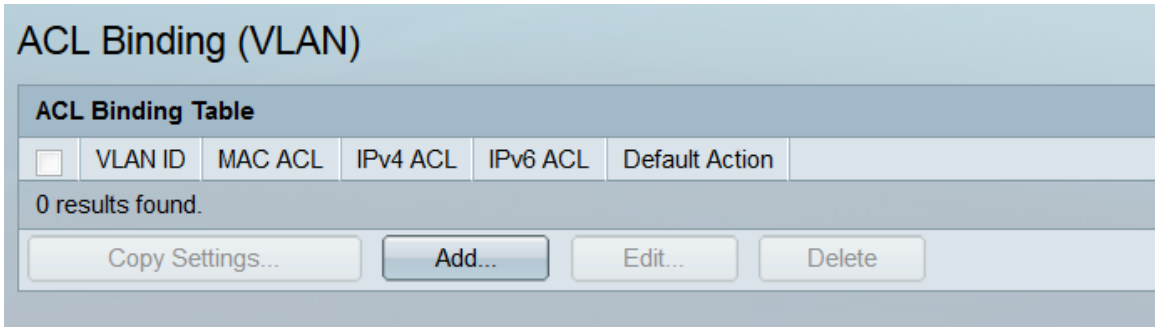


ステップ11：インターフェイスの設定をクリアする場合は、そのチェックボックスをオンにして[クリア]をクリックします。複数のインターフェイスを同時に選択およびクリアできることに注意してください。

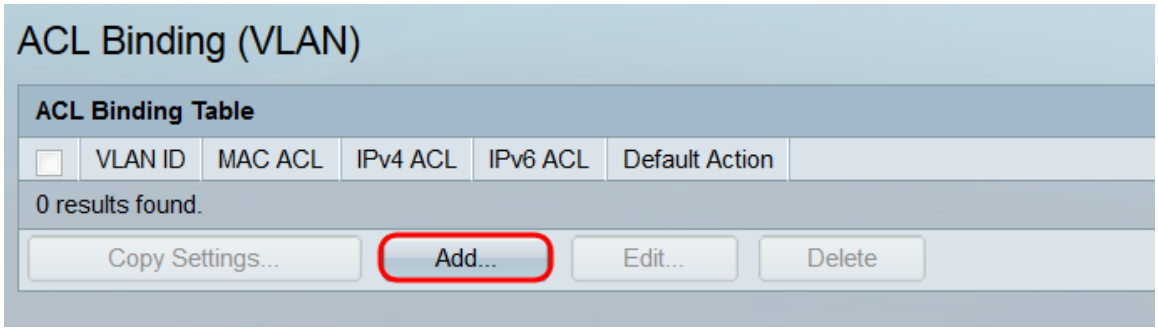


MACベースのACLのVLANへのマッピング

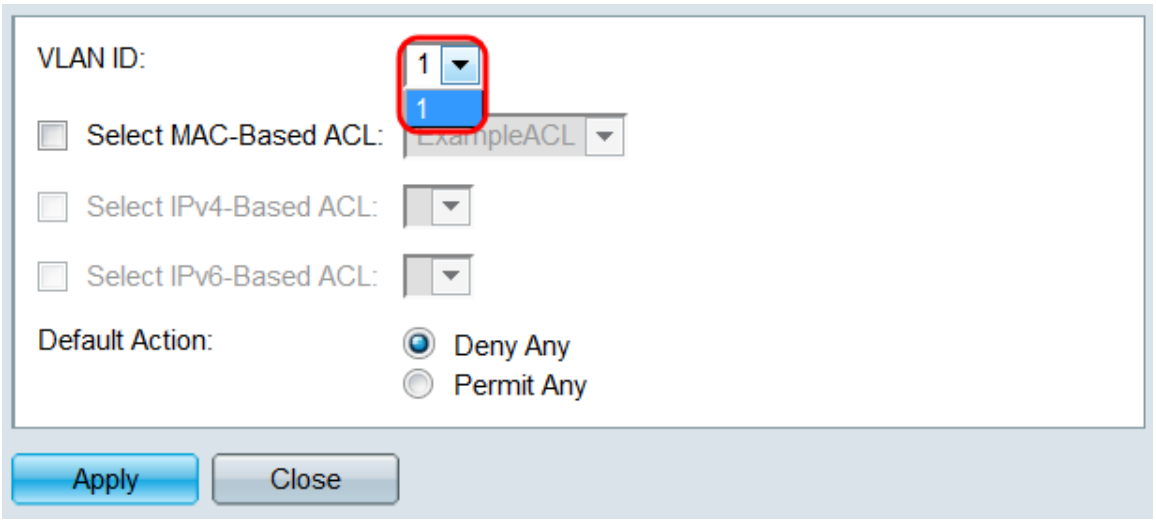
ステップ1:ACLはポートまたはVLANのいずれかにマッピングできます。MACベースのACLをVLANにマッピングするには、**[Access Control] > [ACL Binding (VLAN)]に移動します**。 *[ACL Binding (VLAN)]ページが開きます。*



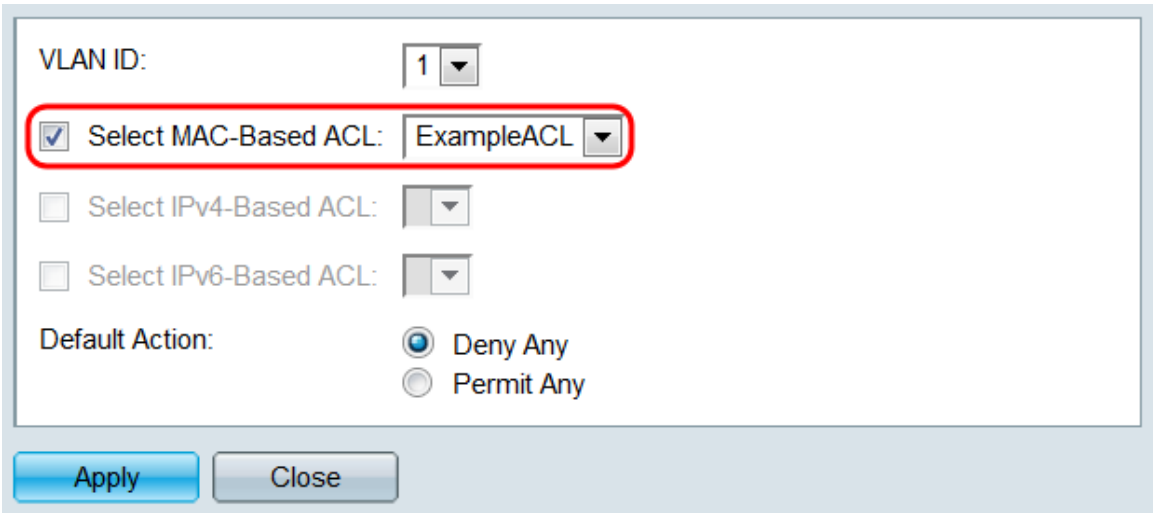
ステップ2:ACLバインディングテーブルに、現在VLANにマッピングされているすべてのACLが表示されます。ACLがマッピングされていない場合、テーブルは空です。ACLをVLANにマッピングするには、**[Add...]ボタンをクリック**します。[Add ACL *Binding]ウィンドウが開きます。*



ステップ3:VLAN IDフィールドのドロップダウンリストを使用して、ACLをマッピングするVLANを*選択します。このフィールドは、[ACL Binding (VLAN)]ページに戻ることなく、異なるVLAN間を迅速に切り替えるために使用することもできます。*

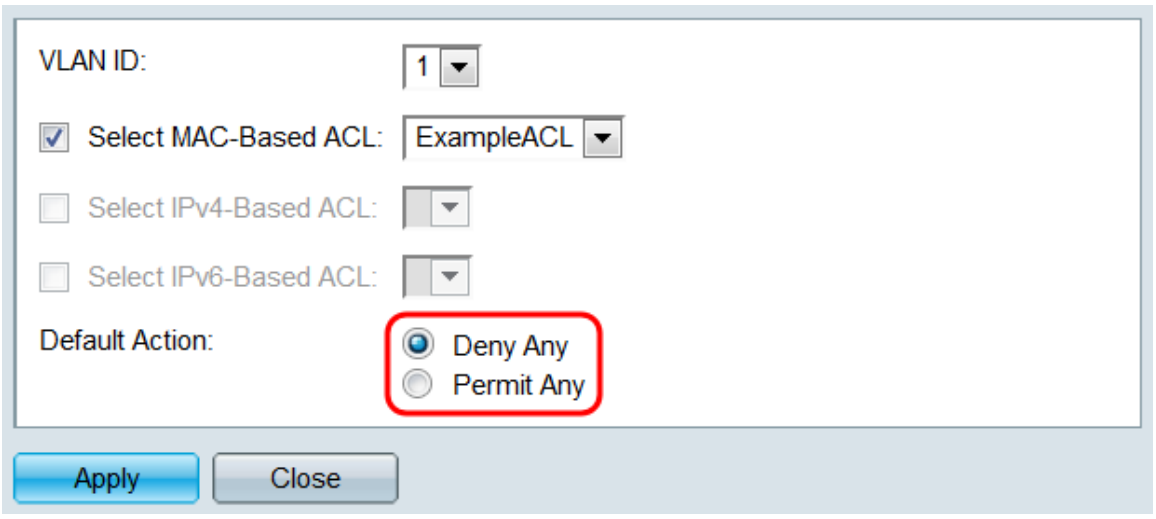


ステップ4:[**Select MAC-Based ACL**]チェックボックスをオンにして、ドロップダウンリストを使用して、指定したVLANにマッピングするACLを選択します。



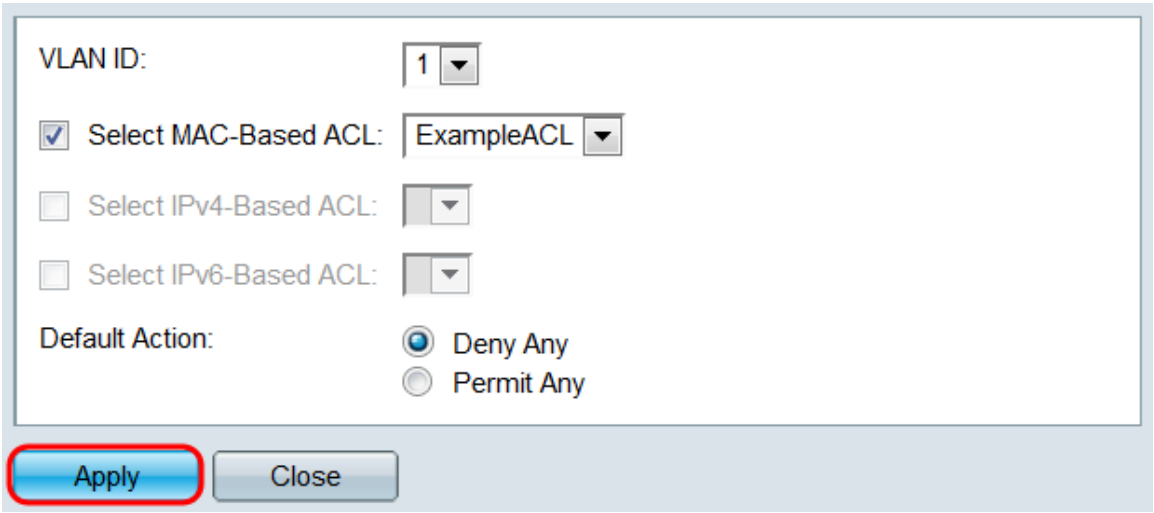
注：VLAN IDを基準の一部として使用するMACベースのACLをVLANにバインドすることはできません。また、時間範囲を持つACLはVLANにバインドできません。

ステップ5:[*Default Action*]フィールドで、ACLの基準に一致しないパケットの処理方法を決定するラジオ・ボタンを選択します。デフォルトは**Deny Any**で、ACLの基準に一致しないパケットはすべてドロップされます。**Permit Any**は、一致しないパケットを転送します。

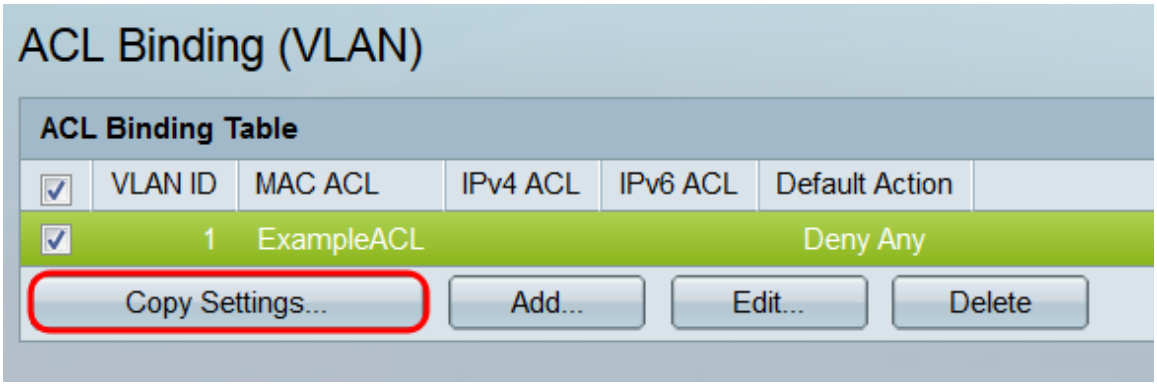


ステップ6:[Apply]をクリ**ックします**。ACLは指定されたVLANにマッピングされます。

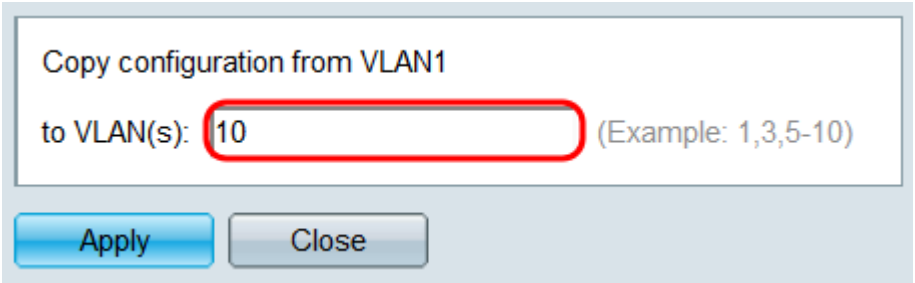
[VLAN ID]フィールドを使用して、設定する別のVLANを選択するか、[閉じる]をクリックして[*ACLバインド(VLAN)]ページに戻ります。*



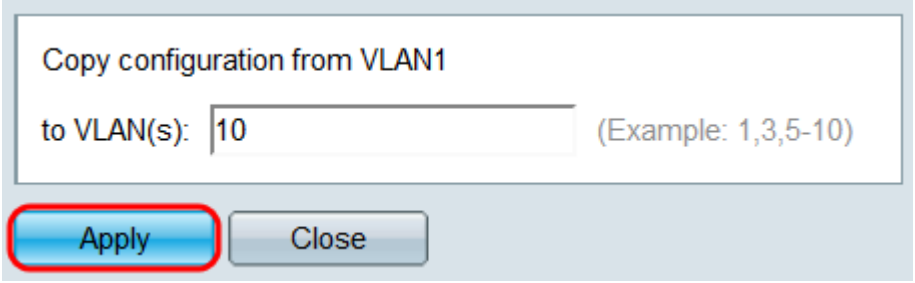
ステップ7:VLANの設定を他のVLANにすばやくコピーするには、コピーするVLAN設定のチェックボックスをオンにし、**[Copy Settings...]ボタンをクリックします。**「設定のコピー」ウィンドウが開きます。



ステップ8：テキストフィールドに、設定をコピーするVLAN IDまたはVLAN IDを入力します。IDはカンマで区切るか、範囲を指定できます。



ステップ9:[Apply]をクリ**ックします。**設定がコピーされます。



ステップ10:VLANの設定をクリアする場合は、そのチェックボックスをオンにして[**Delete**

]をクリックします。複数のVLANを同時に選択してクリアできることに注意してください。