在SG350XG和SG550XG上建立基於MAC的ACL

目標

訪問控制清單(ACL)是一組規則，可以建立這些規則以根據資料包是否滿足某些標準來對其進行操作。這些標準可以是資料包的源或目標地址、報頭欄位和其他各種元件。如果封包與ACL的指定條件相符，便會捨棄或允許其繼續。基於MAC的ACL使用分析資料包第2層報頭的規則（例如MAC地址、VLAN ID和Ethertype值），以滿足這些標準。通過實施基於MAC的ACL，您可以在第2層控制資料包在交換機上傳輸。

本文檔的目的是向您展示如何在SG350XG和SG550XG交換機上建立並配置基於MAC的ACL。

適用裝置

- SG350XG
- SG550XG

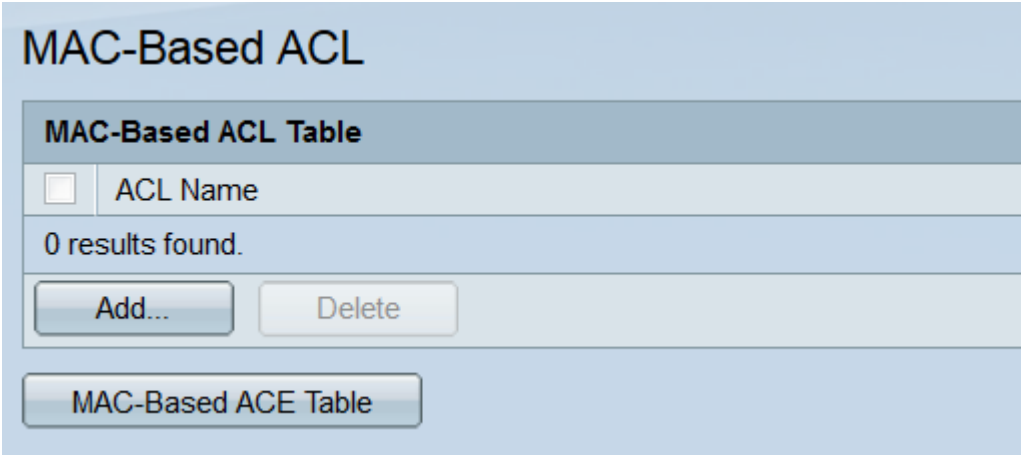
軟體版本

- v2.0.0.73

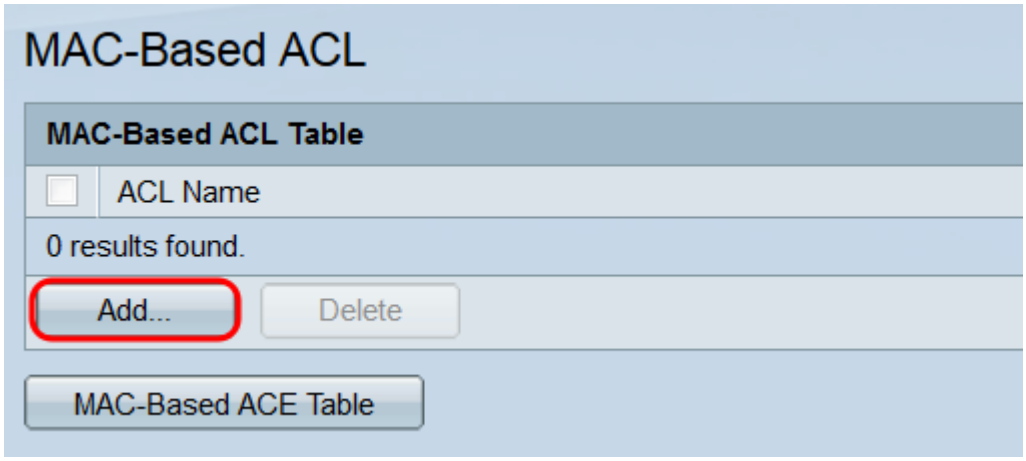
設定 MAC型ACL

建立 acl和規則

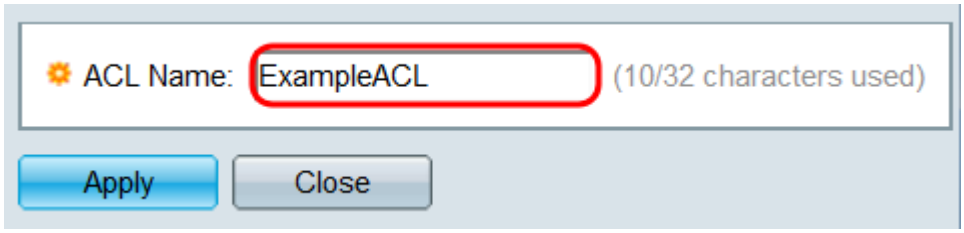
步驟1.登入到Web配置實用程式，然後選擇**Access Control > MAC-Based ACL**。將打*開基於MAC的ACL*頁面。



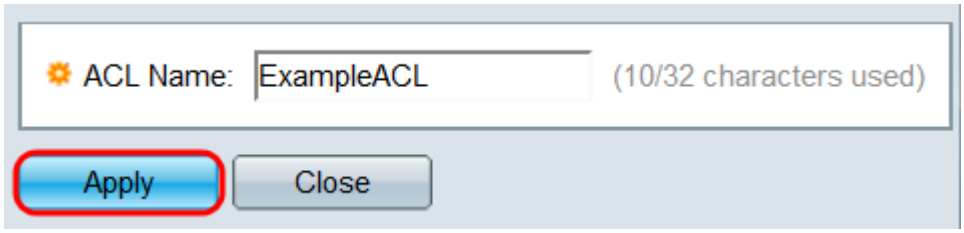
步驟2.*基於MAC的ACL表*將顯示交換機上當前所有基於MAC的ACL。要建立新的ACL，請按一下**Add...**按鈕。將會開啟*Add MAC-Based ACL*視窗。



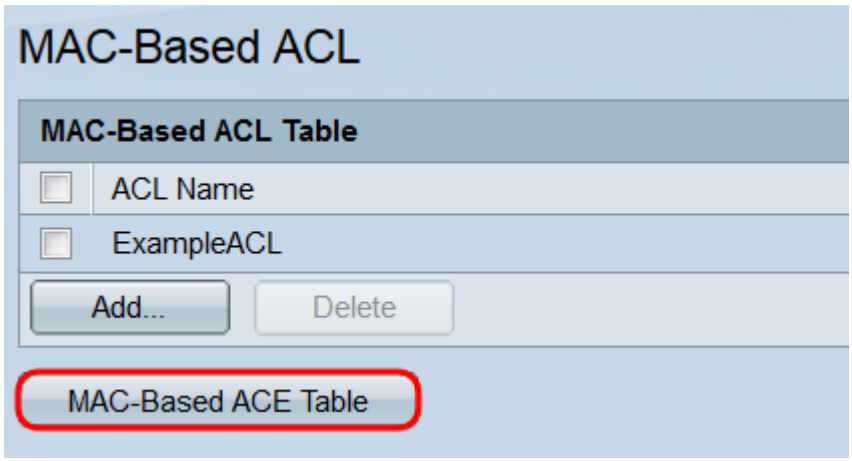
步驟3.在*ACL Name*欄位中，輸入新ACL的名稱。此名稱不會影響ACL的功能，僅供識別。



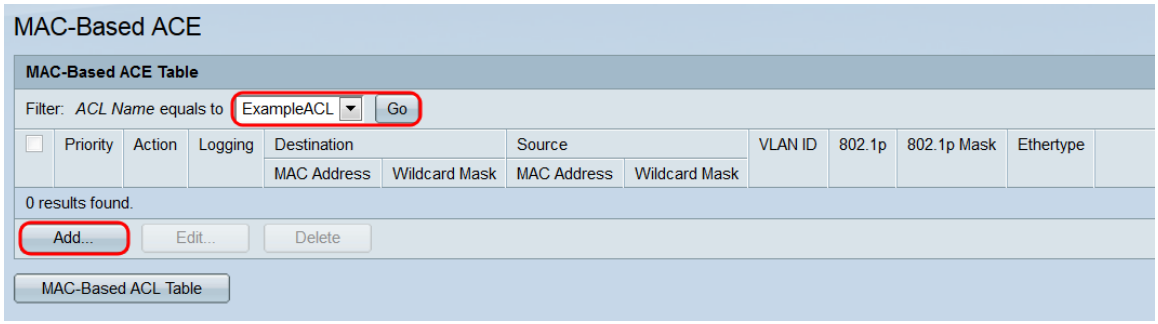
步驟4.按一下**Apply**。新ACL將新增到基*於MAC的ACL表中*。按一下**Close**以返回*MAC-Based ACL*頁面，或重複上一步驟建立另一個ACL。



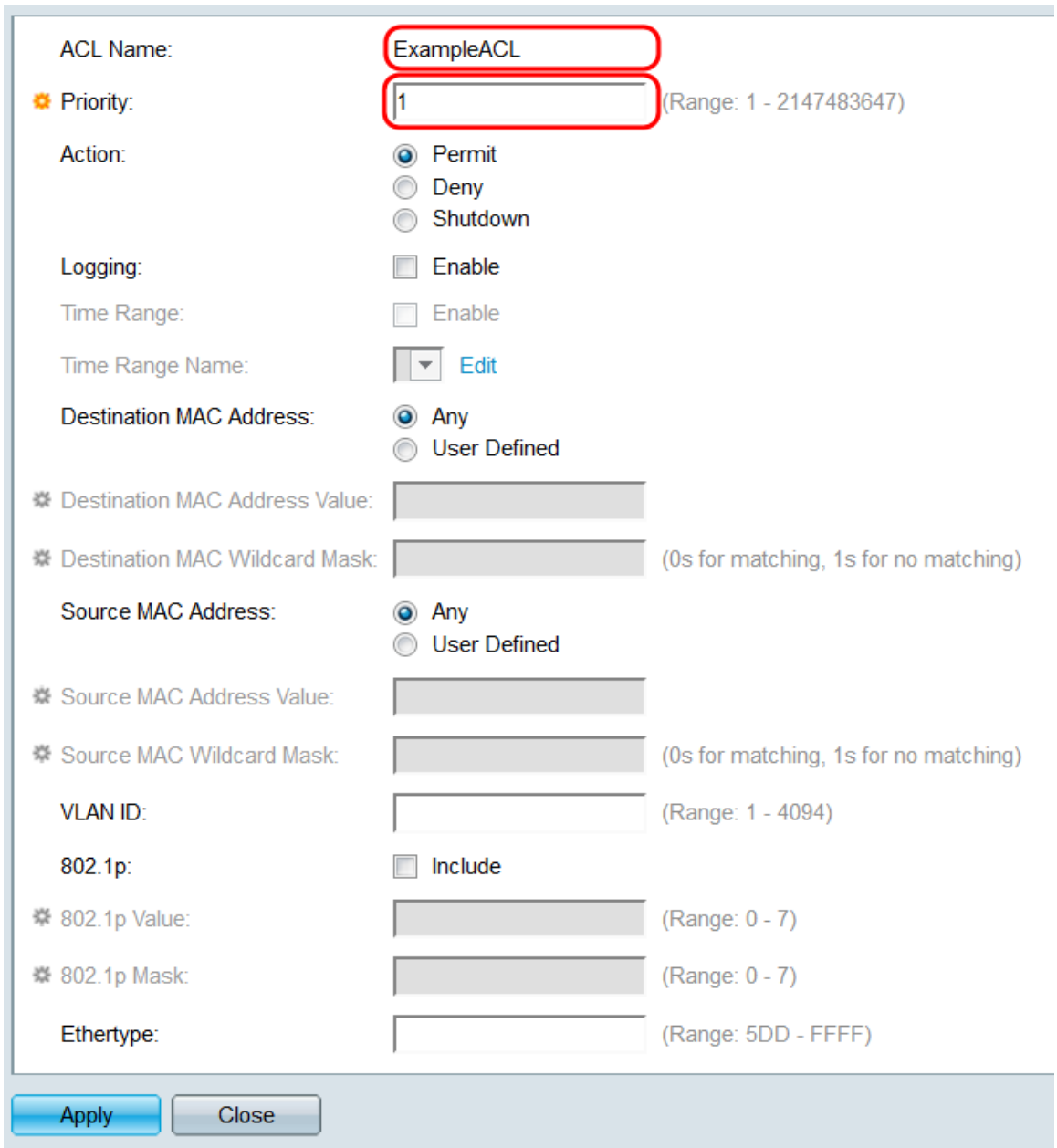
步驟5.所有新建立的ACL都將為空；也就是說，它不包含任何根據MAC地址阻止或允許資料包的規則。要建立這些規則，必須將訪問控制條目(ACE)新增到ACL中。為此，請按一下**MAC-Based ACE Table**按鈕以轉至*MAC-Based ACE*頁。



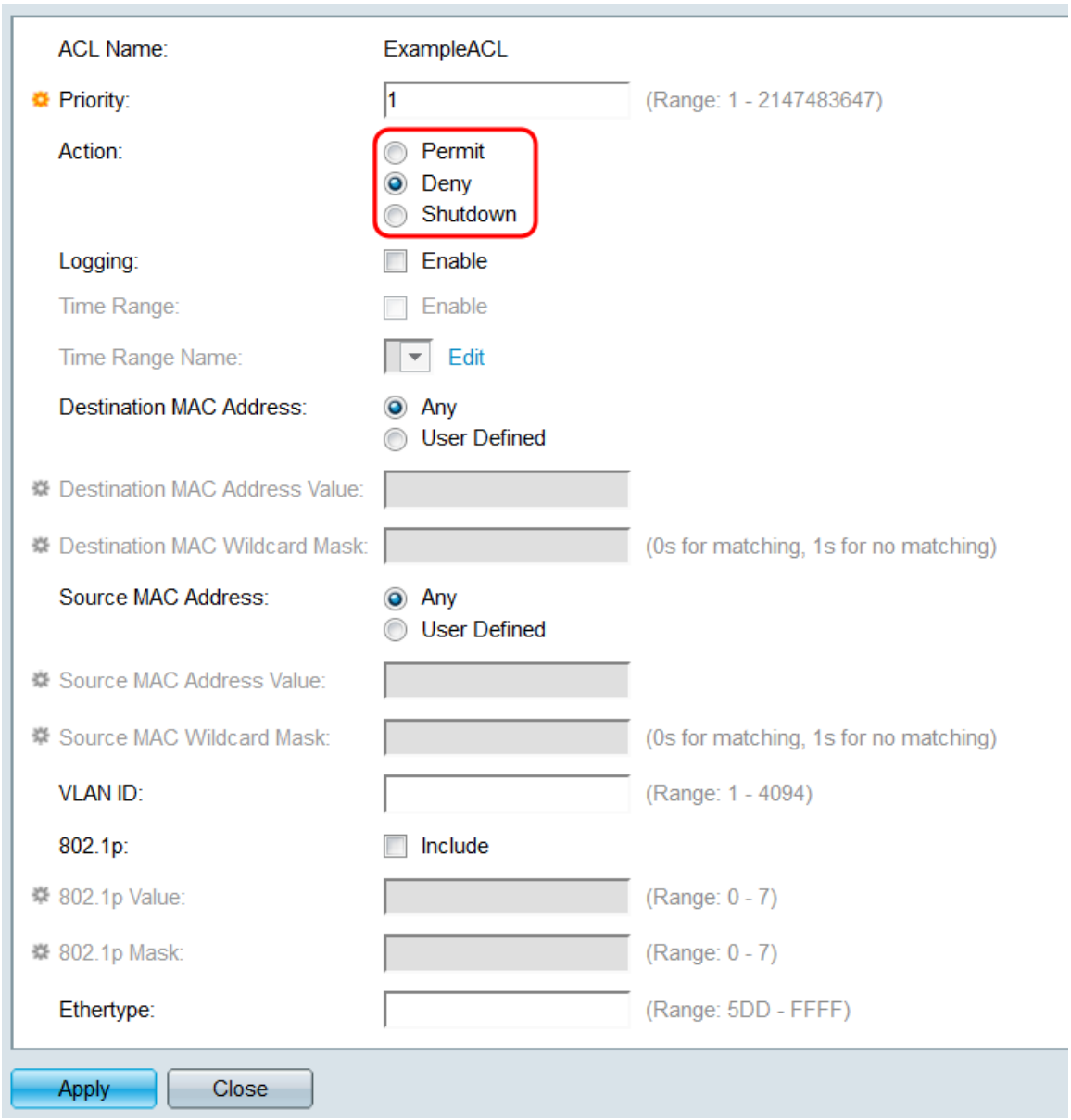
步驟6.在「*MAC-Based ACE*」頁面上，通過基於MAC的ACE表頂部的下拉選單選擇要向其新增ACE的ACL，然後按一下*Go*。該表顯示當前與選定ACL關聯的所有ACE。要新增ACE，請按一下**Add...**按鈕。將會開啟*Add MAC-Based ACE* 視窗。



步驟7. *ACL Name* 欄位會顯示您要將ACE新增到的ACL的名稱。在*Priority*欄位中，輸入ACE的優先順序編號。ACE的優先順序越高，處理它的速度越快。範圍是從1到2147483647,1是最高優先順序。



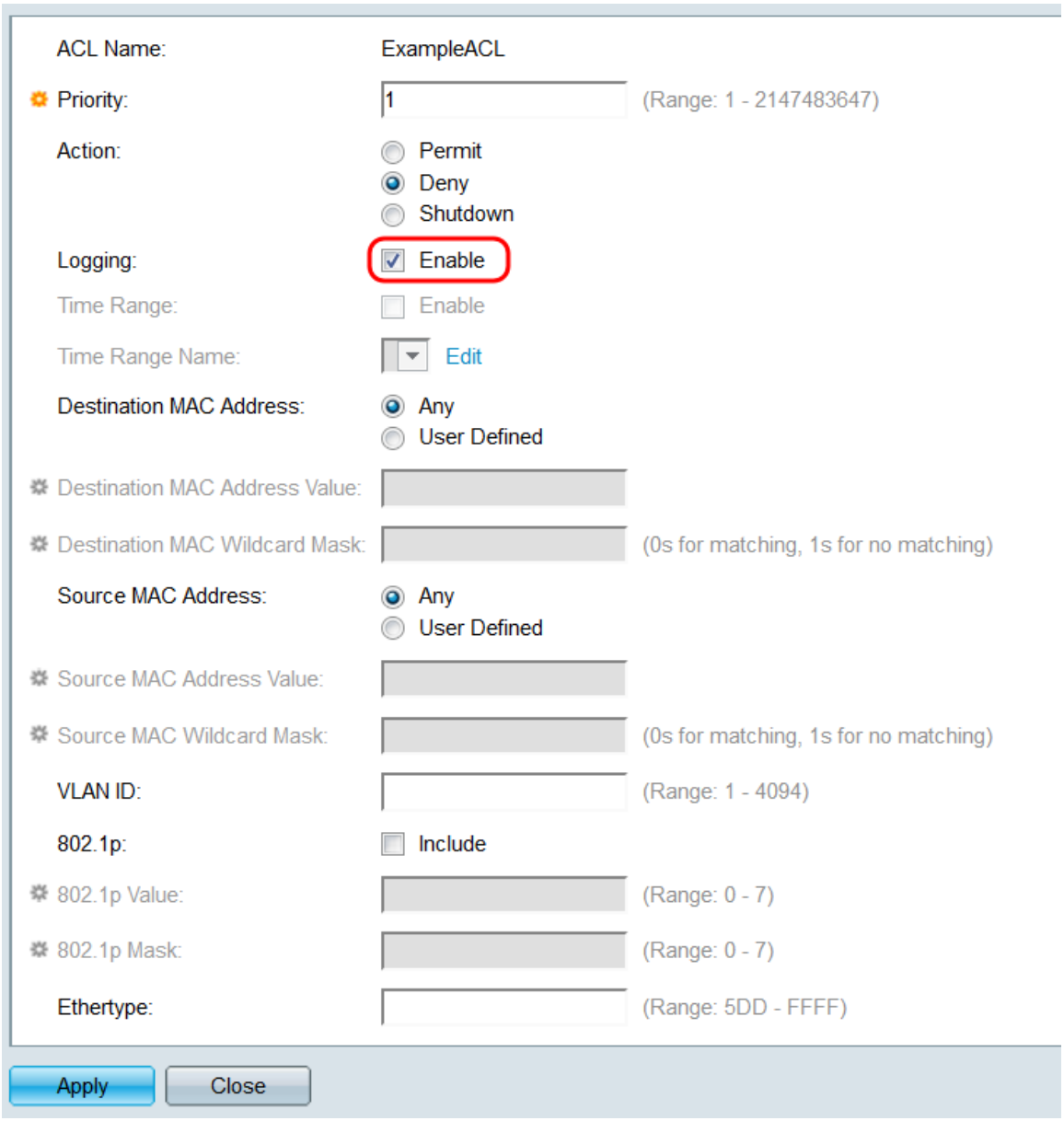
步驟8.在*Action*欄位中，選擇一個單選按鈕，以確定在滿足ACE標準時將發生的情況。



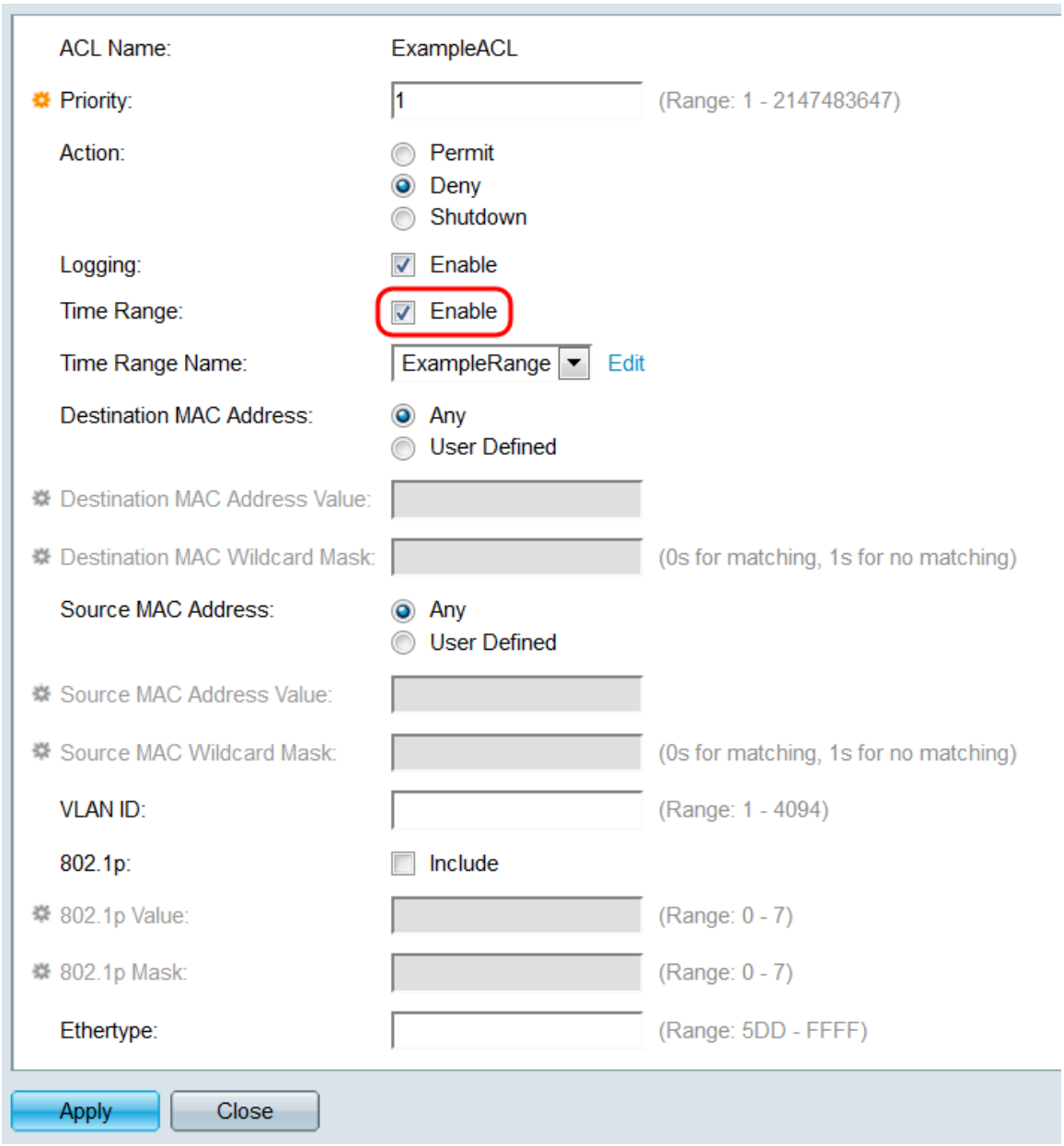
選項包括：

- 允許 — 轉發符合條件的資料包。
- Deny — 丟棄符合條件的資料包。
- Shutdown — 捨棄符合條件的資料包，然後停用連線埠。

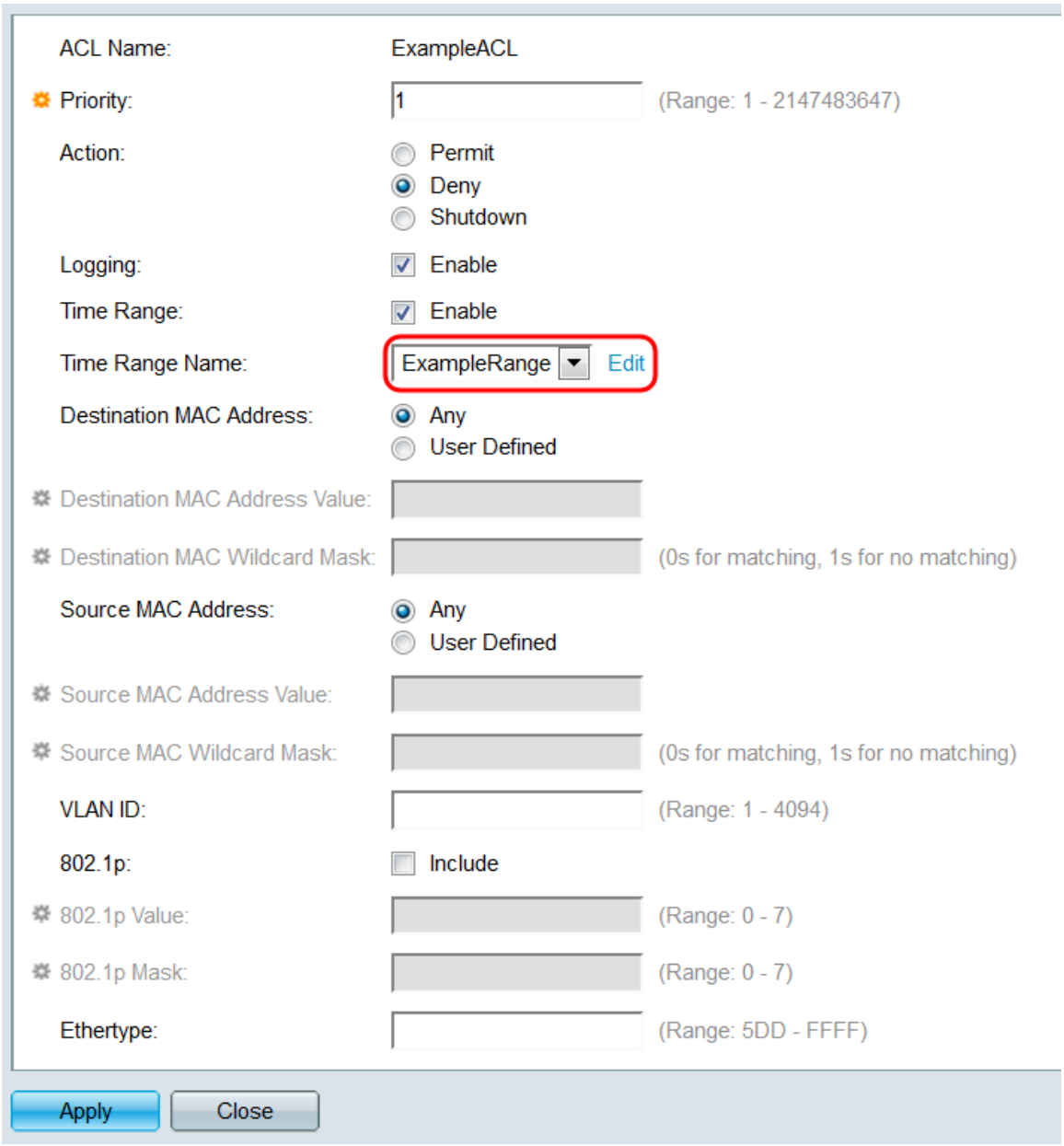
步驟9.在*Logging*欄位中，選中**Enable**覈取方塊以啟用與ACE規則匹配的日誌記錄ACL流。如果使用的是基本顯示模式，請跳至步驟12。可以通過Web實用程式右上角的下拉選單更改顯示模式。



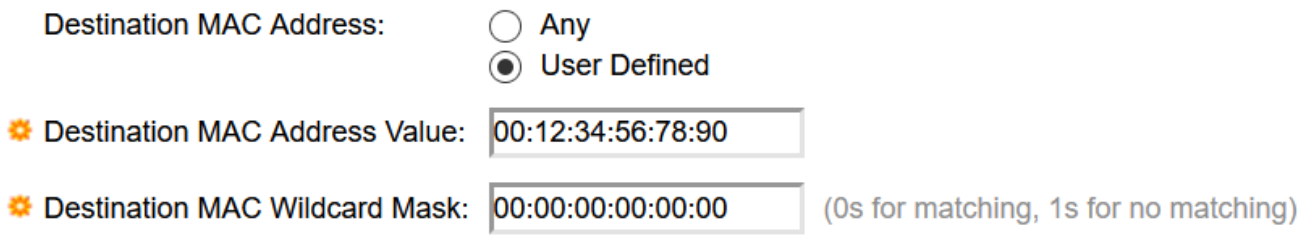
步驟10.在*Time Range*欄位中，選中**Enable**覈取方塊，使ACE僅在指定的時間範圍內處於活動狀態。如果交換機上未配置現有時間範圍，則此欄位不可用。



步驟11.如果已啟用此ACE的時間範圍，則*Time Range Name*欄位將可用。使用下拉選單選擇交換機上已配置的時間範圍以應用於ACE。如果交換器上沒有時間範圍，此欄位將不可用；按一下**Edit**連結可轉到「*Time Range*」頁，以建立或修改時間範圍。有關詳細資訊，請參閱*在SG350XG和SG550XG上設定時間範圍*一文。



步驟12.在*Destination MAC Address*欄位中，選擇單選按鈕以確定哪些目標MAC地址將構成匹配。選擇**Any**使任何目標地址匹配，或選擇**User Defined**指定地址或地址範圍。



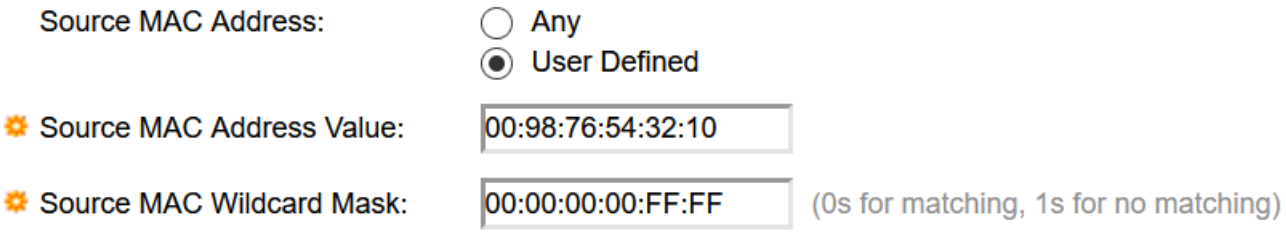
如果選擇了**使用者定義**，請填寫以下欄位：

- 目標MAC地址值 — 輸入目標MAC地址。如果資料包包含此目標地址，ACE會將其視為匹配項。
- 目標MAC萬用字元掩碼 — 輸入掩碼以定義地址範圍。將位設定為1將忽略MAC地址中的對應位，而0將匹配位。

附註：給定掩碼0000 0000 0000 0000 0000 0000 0000 000 0000 111 111（表示您匹配的是0的位，而非1的位）。 您需要將1轉換為十六進位制值，然後對四個0寫入0。在此示例中，由

於1111 111 = FF，因此將寫入掩碼：00:00:00:00:00:FF。

步驟13.在*源MAC地址*欄位中，選擇單選按鈕以確定哪些源MAC地址將構成匹配。選擇**Any**使任何源地址匹配，或選擇**User Defined**指定地址或地址範圍。



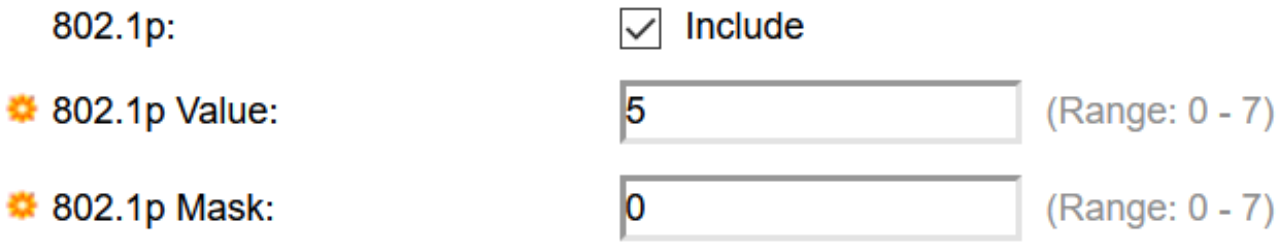
如果選擇了**使用者定義**，請填寫以下欄位：

- 源MAC地址值 — 輸入源MAC地址。如果資料包包含此源地址，ACE會將其視為匹配項。
- 源MAC萬用字元掩碼 — 輸入掩碼以定義地址範圍。將位設定為1將忽略MAC地址中的相應位，而0將匹配位（例如00:00:00:00:00:11）。

附註：給定掩碼0000 0000 0000 0000 0000 0000 0000 000 0000 111 111（表示您匹配的是0的位，而非1的位）。 您需要將1轉換為十六進位制值，然後對四個0寫入0。在此示例中，由於1111 111 = FF，因此將寫入掩碼：00:00:00:00:00:FF。

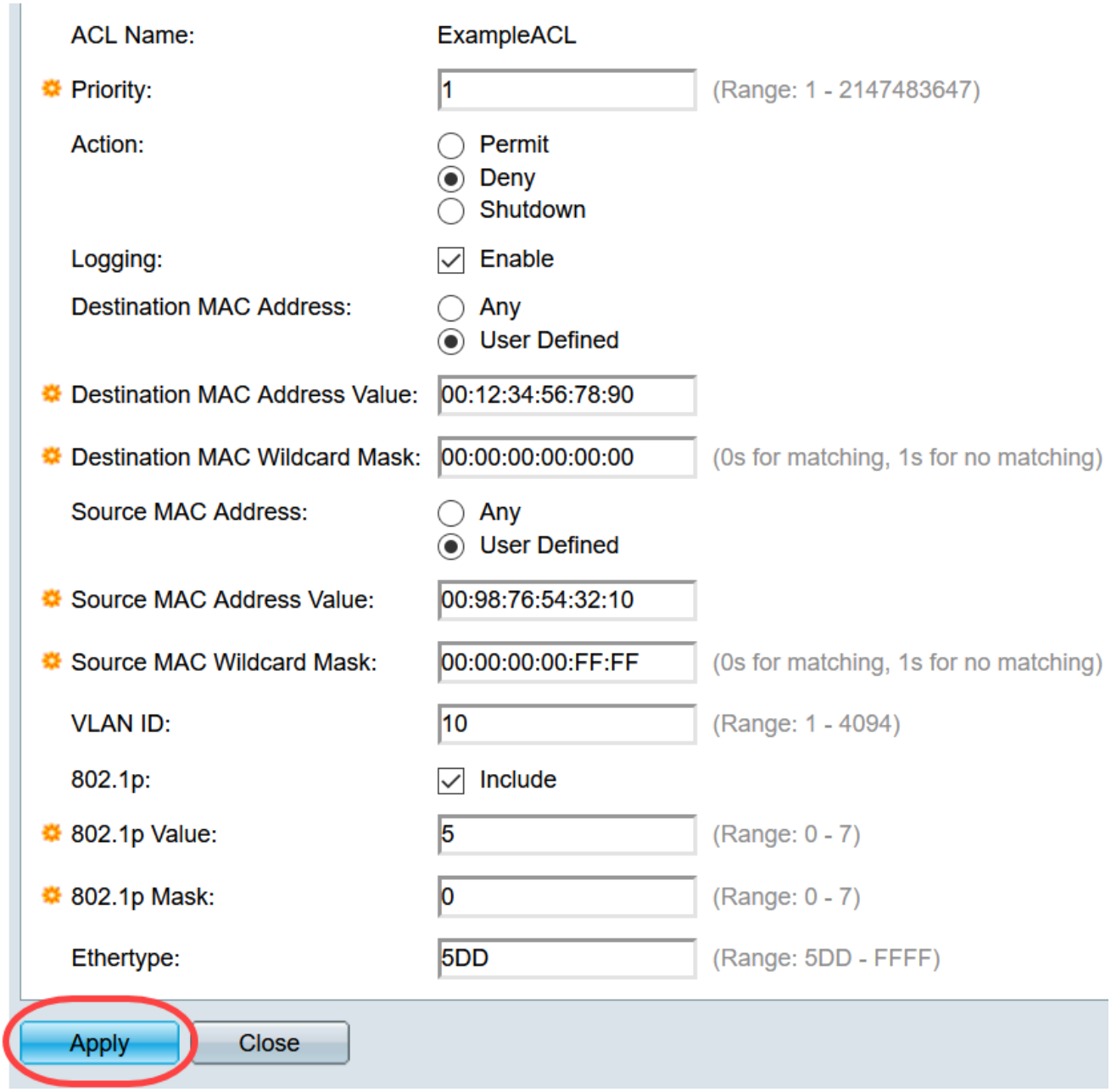
步驟14.在「*VLAN ID*」欄位中，輸入1到4094之間的VLAN ID。如果資料包包含此VLAN ID，ACE會將其視為匹配項。此欄位不是必填欄位；將其保留為空將導致ACE檢查資料包時不考慮VLAN ID。

步驟15.在*802.1p*欄位中，選中**Include**覈取方塊以使ACE包含802.1p標準。如果包括802.1p標準，請分別在*802.1p Value* 和*802.1p Mask* 欄位中輸入802.1p值和掩碼。兩個欄位的範圍都是0到7。如果資料包包含對應的802.1p值並且適合掩碼，則ACE會將其視為匹配項。



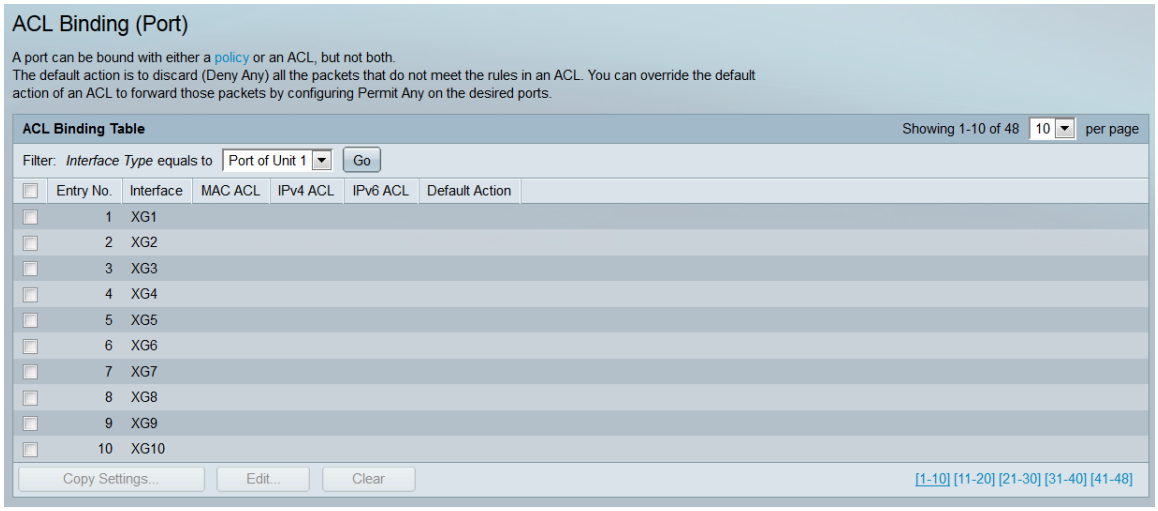
步驟16.在*Ethertype*欄位中，輸入將與傳入封包比較的Ethertype值。Ethertype是幀中兩個二進位制八位數的欄位，表示資料包中封裝了哪個協定。範圍為5DD- FFFF。如果資料包包含指定的Ethertype值，則ACE會將其視為匹配項。在此IEEE標準頁面上可以找到Ethertype值的清單。

步驟17.按一下**Apply**。ACE將新增到指定的ACL。按一下**Close**返回基於*MAC的ACE*頁面。

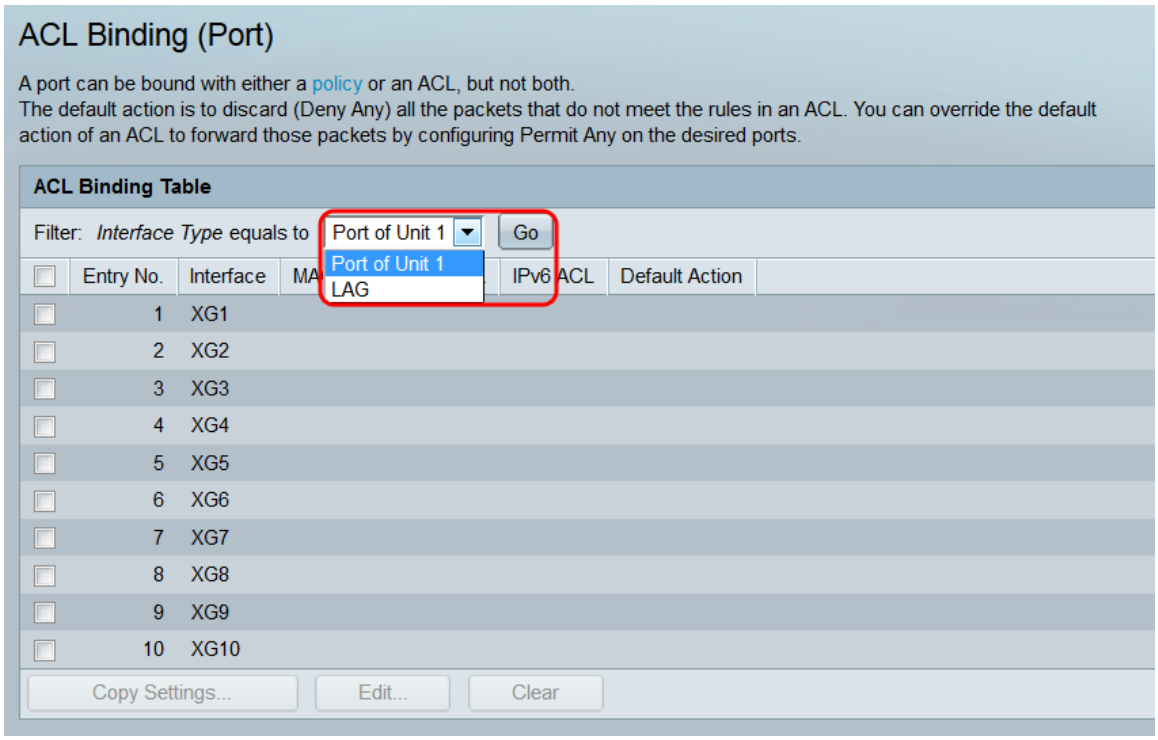


對映基於MAC的ACL 到埠

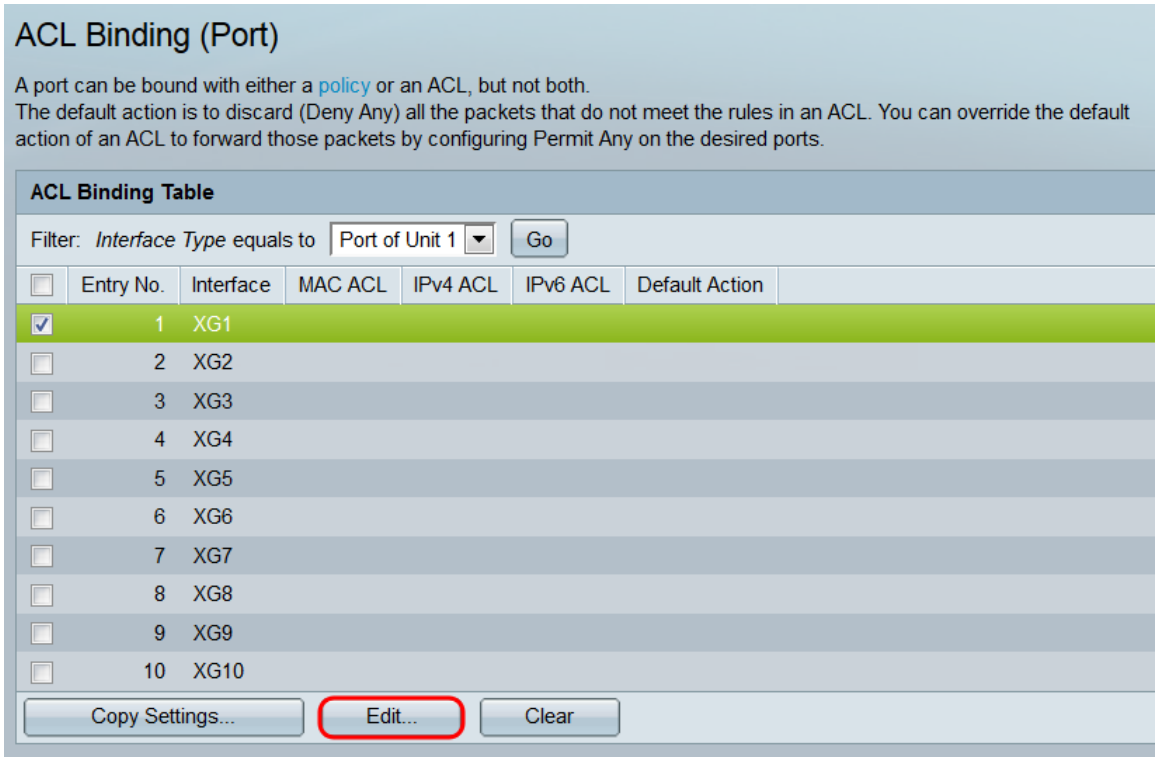
步驟1. ACL可以對映到埠或VLAN。要將基於MAC的ACL對映到埠，請導航至**訪問控制> ACL繫結（埠）**。 此時會開啟「*ACL繫結（埠）*」頁。



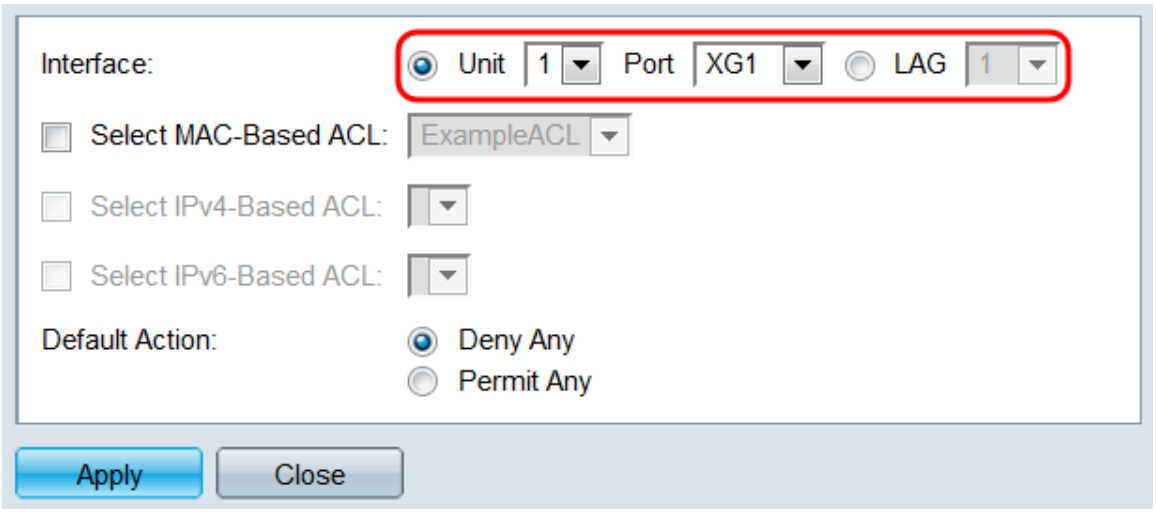
步驟2.在*ACL繫結表*頂部的下拉選單中，選擇埠或LAG（鏈路聚合組）作為介面型別。如果交換器是堆疊的一部分，可以選擇其他裝置的連線埠。按一下**Go**以顯示指定介面型別的清單。



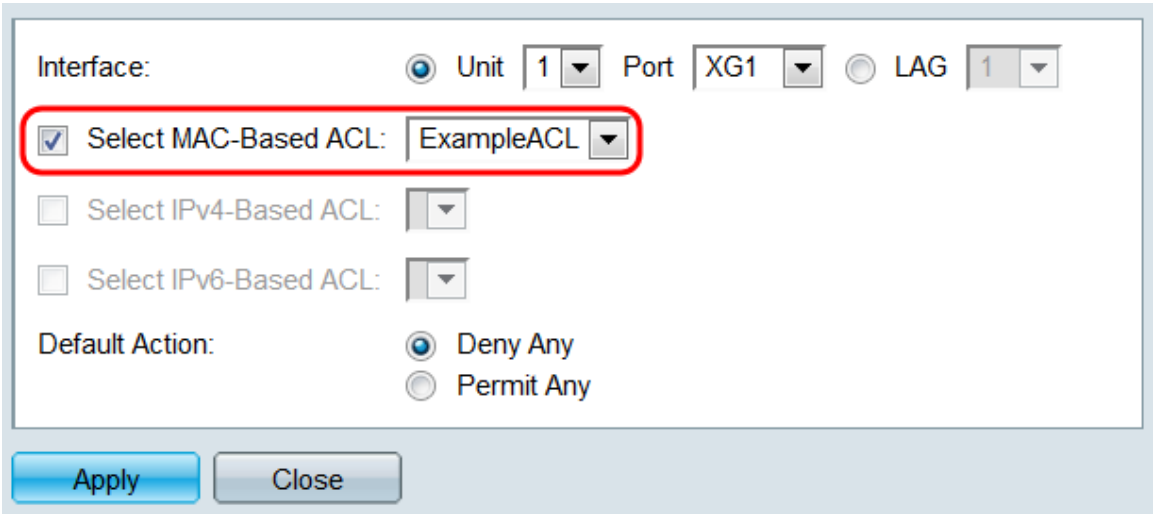
步驟3.選中介面的覈取方塊，然後按一下**Edit...**按鈕。*編輯ACL繫結*視窗開啟。



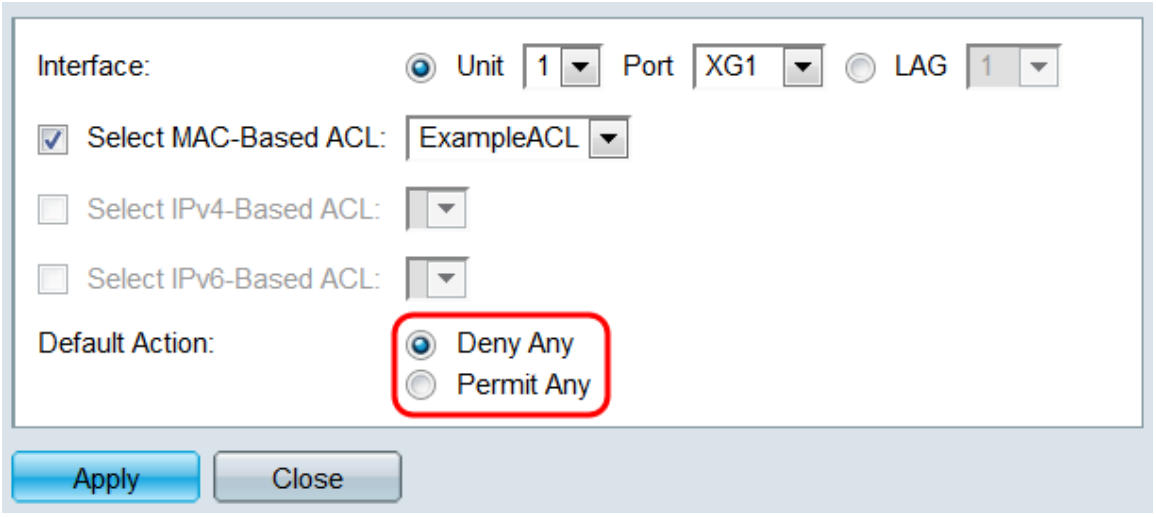
步驟4. *Interface*欄位顯示目前設定的連線埠或LAG。它會自動顯示在ACL繫結表中選*定的介面*。此欄位可用於在不同介面之間快速切換，而無需返回*ACL Binding(Port)*頁。



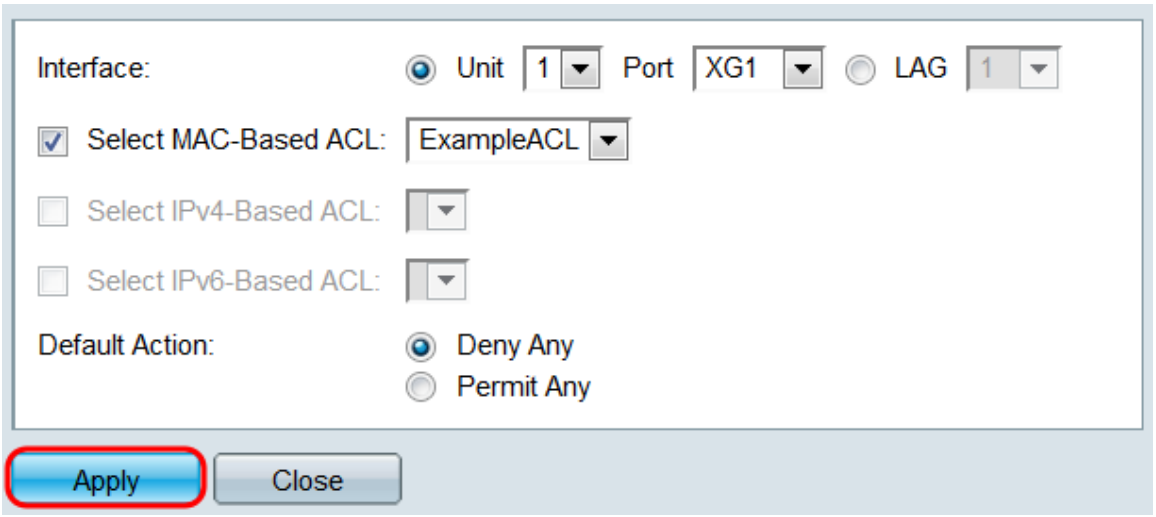
步驟5.選中**選擇基於MAC的ACL**覈取方塊，並使用下拉選單選擇要對映到指定介面的ACL。



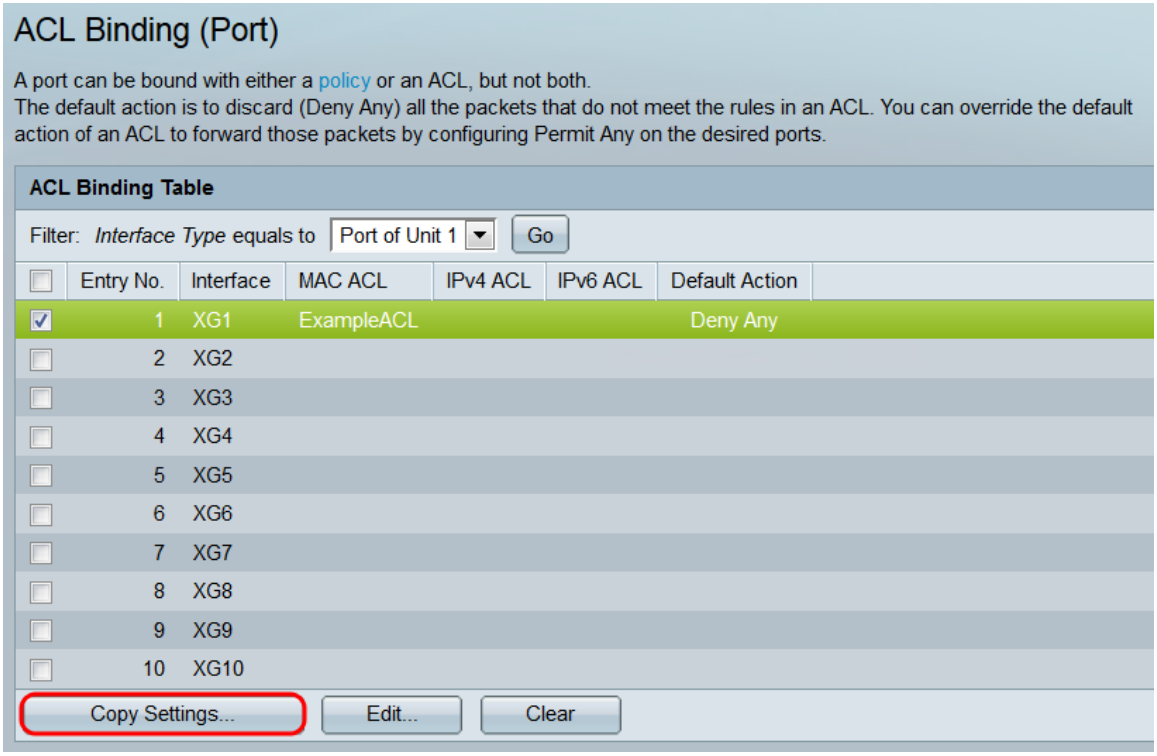
步驟6.在*Default Action*欄位中，選擇單選按鈕以確定如何處理與ACL標準不匹配的資料包。預設值為**Deny Any**，會捨棄與ACL標準不符的任何封包；**Permit Any**將轉發不匹配的資料包。



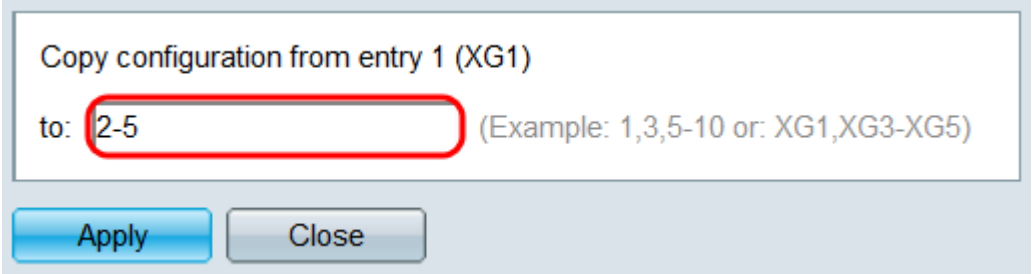
步驟7.按一下**Apply**。該ACL將對映到指定的介面。您可以使用*Interface*欄位選擇要設定的不同介面，或按一下**Close**以返回*ACL Binding(Port)*頁面。



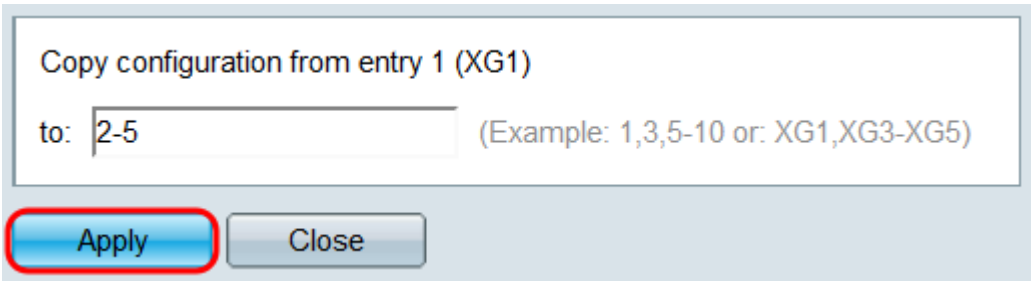
步驟8.要將介面的設定快速複製到其它介面，請選中要複製的介面的覈取方塊，然後按一下**Copy Settings...按鈕**。*複製設定*視窗開啟。



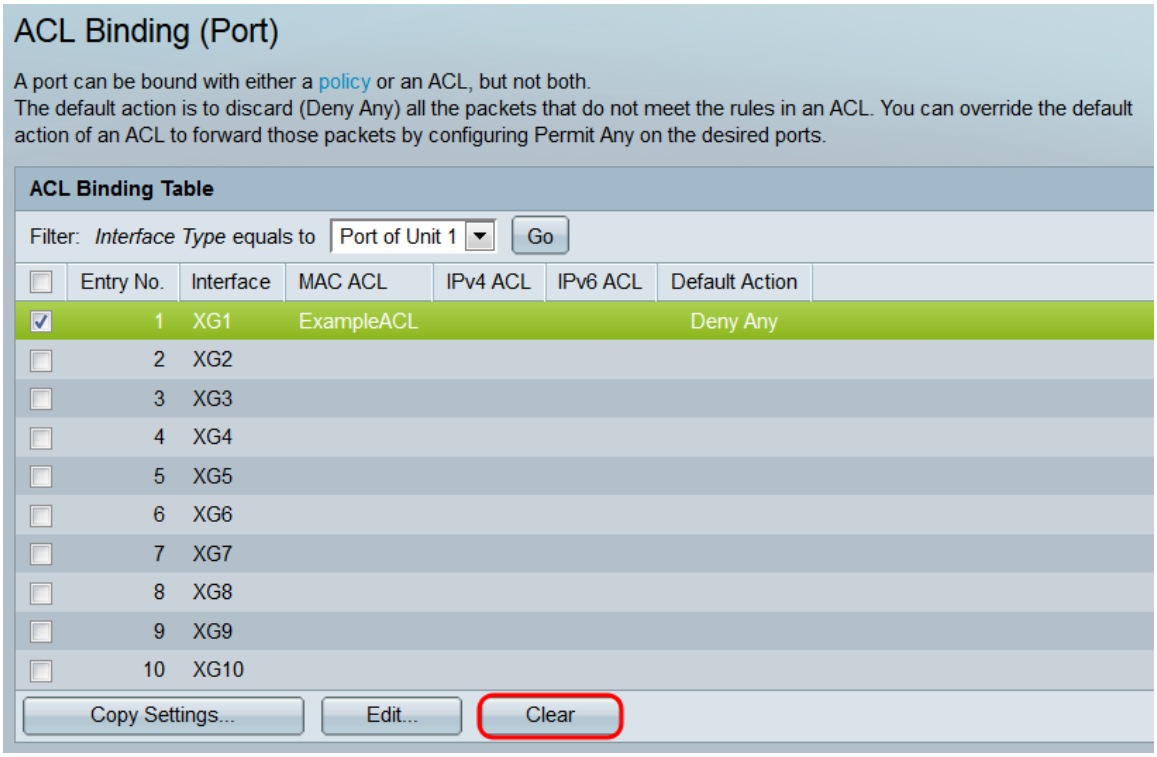
步驟9.在文本欄位中，輸入要複製設定的介面。介面可以用逗號分隔，也可以指定範圍。



步驟10.按一下**Apply**。設定被複製。

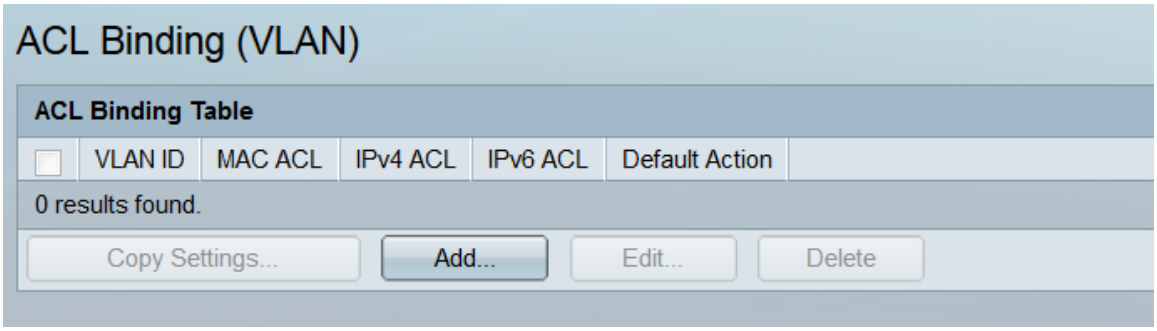


步驟11.如果要清除介面的設定，請選中其覈取方塊，然後按一下**清除**。請注意，可以同時選擇和清除多個介面。

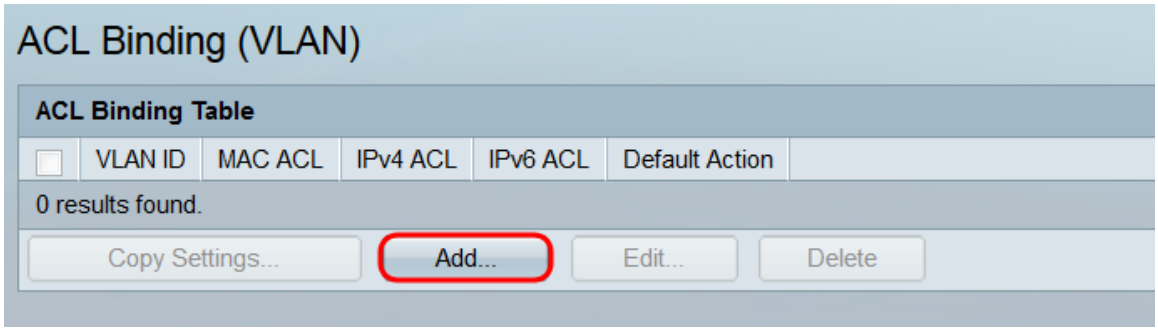


將基於MAC的ACL對映到VLAN

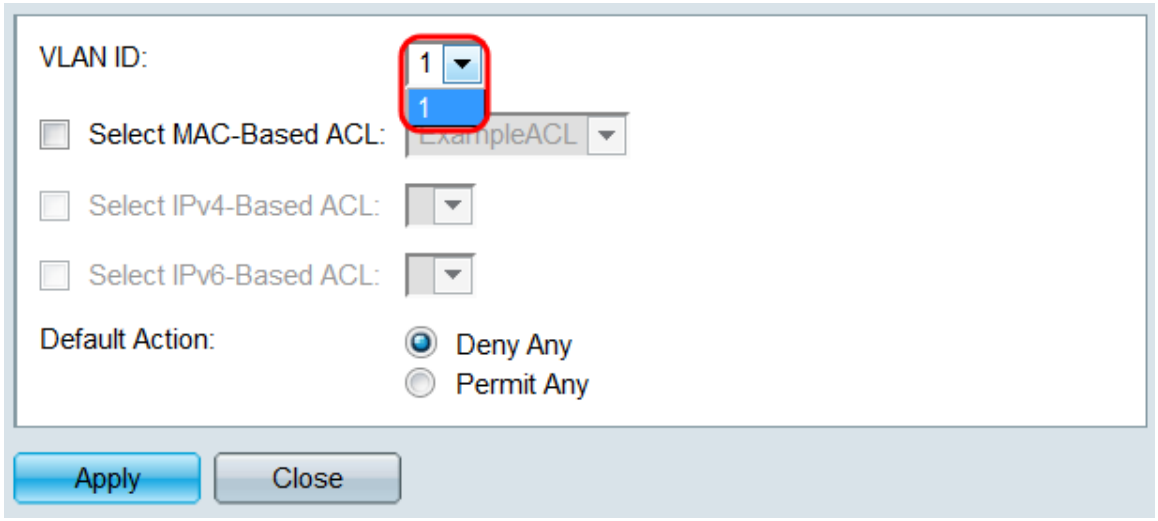
步驟1. ACL可以對映到埠或VLAN。要將基於MAC的ACL對映到VLAN，請導航到**Access Control > ACL Binding(VLAN)**。 此時會開啟「*ACL繫結(VLAN)*」頁面。



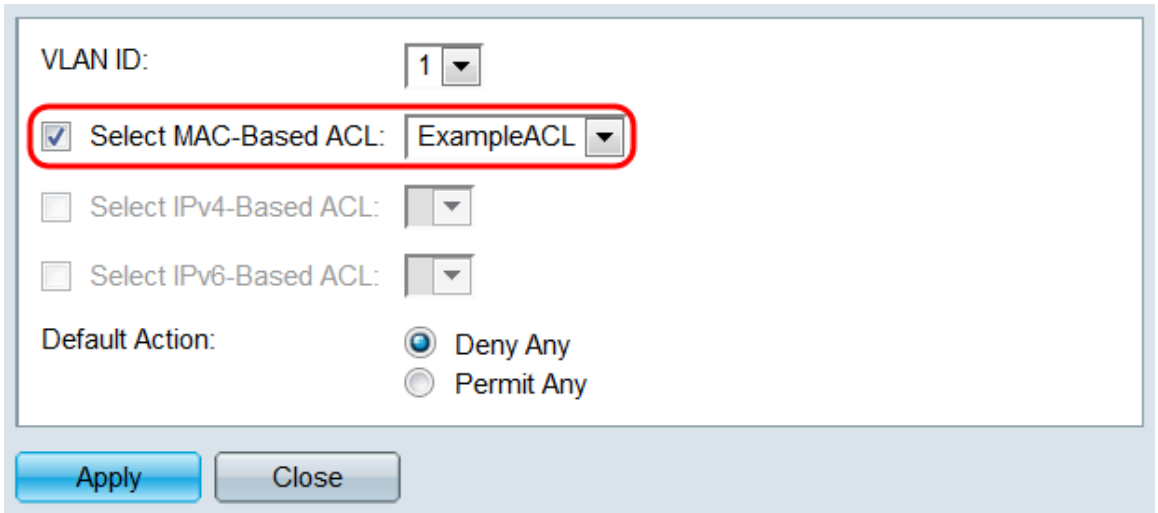
步驟2. *ACL繫結表*顯示當前對映到VLAN的所有ACL。如果未對映ACL，則表為空。要將ACL對映到VLAN，請按一下**Add...**按鈕。*Add ACL Binding* 視窗開啟。



步驟3.使用*VLAN ID*欄位中的下拉式清單選擇要將ACL對應到的VLAN。此欄位還可用於快速在不同的VLAN之間切換，而無需返回*到ACL繫結(VLAN)*頁面。

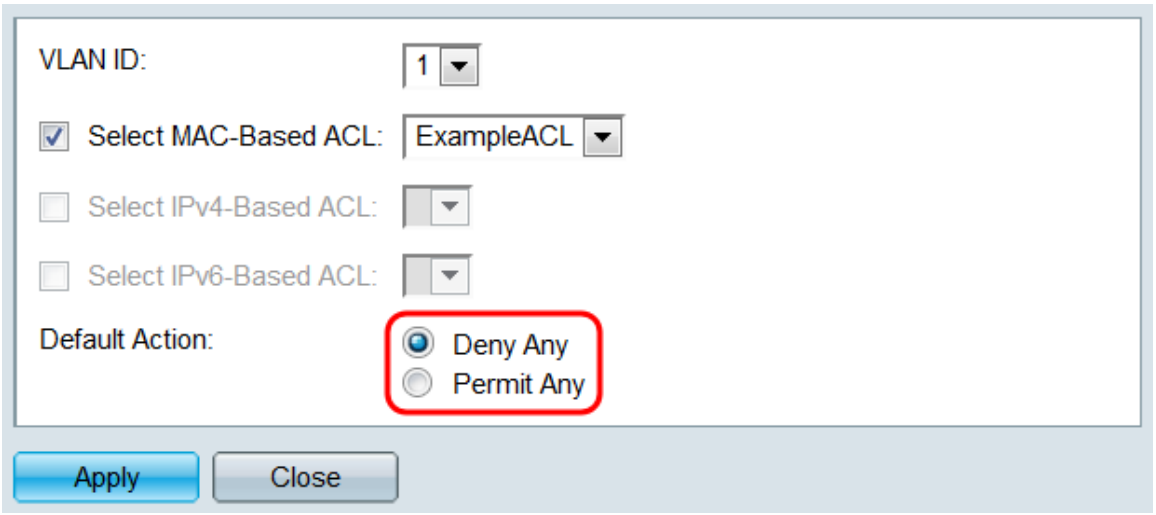


步驟4.選中**選擇基於MAC的ACL**覈取方塊，並使用下拉選單選擇要對映到指定VLAN的ACL。

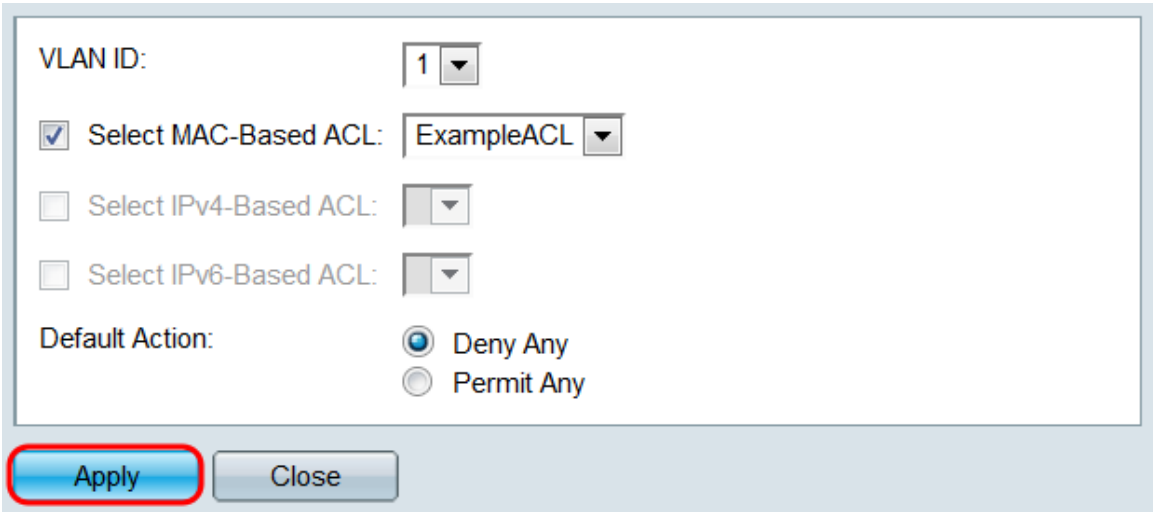


附註：不能將使用VLAN ID作為其標準一部分的基於MAC的ACL繫結到VLAN。此外，不能將時間範圍的ACL繫結到VLAN。

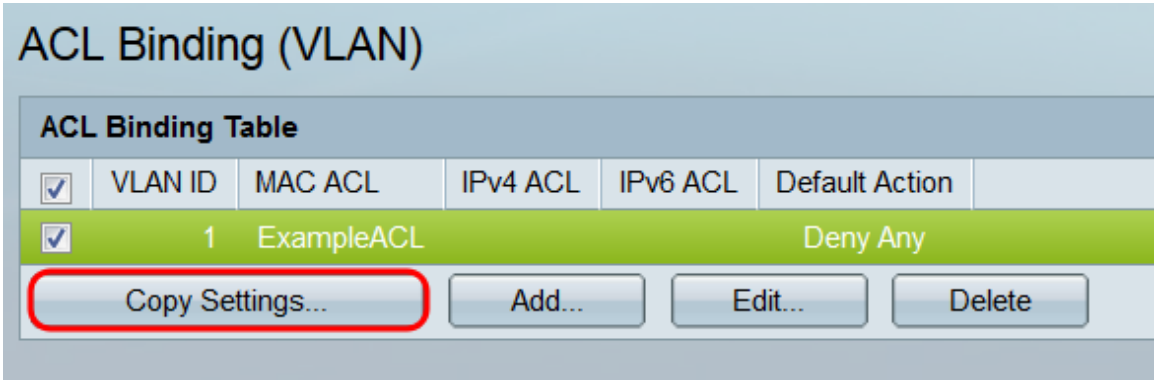
步驟5.在*Default Action*欄位中，選擇單選按鈕以確定如何處理與ACL標準不匹配的資料包。預設值為**Deny Any**，會捨棄與ACL標準不符的任何封包；**Permit Any**將轉發不匹配的資料包。



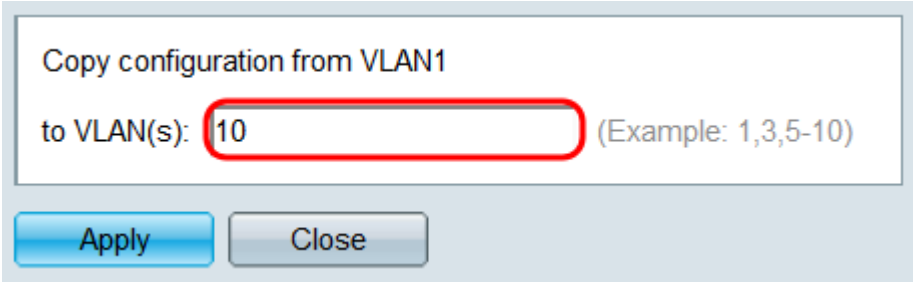
步驟6.按一下**Apply**。ACL會對映到指定的VLAN。您可以使用*VLAN ID*欄位選擇要設定的VLAN，或按一下**Close**以返回*ACL Binding(VLAN)*頁。



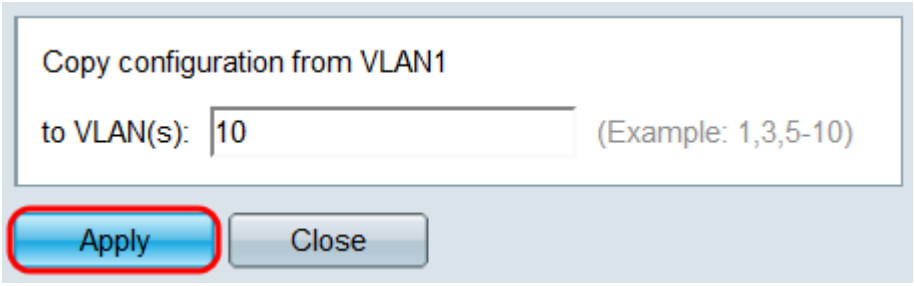
步驟7.要快速將VLAN的設定複製到其他VLAN，請選中要複製的VLAN配置的覈取方塊，然後按一下**複製設定.....**按鈕。*複製設定*視窗開啟。



步驟8.在文本欄位中，輸入要複製設定的VLAN ID或VLAN ID。ID可以用逗號分隔，也可以指定範圍。



步驟9.按一下**Apply**。設定被複製。



步驟10.如果要清除VLAN的設定，請選中其覈取方塊，然後按一下**刪除**。請注意，可以同時選擇和清除多個VLAN。