在交換器上設定基於IPv4的存取控制清單(ACL)和存取控制專案(ACE)

目標

訪問控制清單(ACL)是一個網路流量過濾器清單和相關操作清單，用於提高安全性。它阻止或允許使用者訪問特定資源。ACL包含允許或拒絕訪問網路裝置的主機。

基於IPv4的ACL是使用第3層資訊允許或拒絕流量訪問的源IPv4地址清單。IPv4 ACL會根據設定的IP過濾器來限制IP相關流量。過濾器包含與IP資料包匹配的規則，如果資料包匹配，規則還會規定應允許還是拒絕該資料包。

訪問控制條目(ACE)包含實際訪問規則條件。建立ACE後，ACE將應用於ACL。

您應該使用訪問清單來提供訪問網路的基本安全級別。如果沒有在網路裝置上配置訪問清單，則允許通過交換機或路由器的所有資料包到達網路的所有部分。

本文提供如何在受管交換機上配置基於IPv4的ACL和ACE的說明。

適用裝置

- Sx350系列
- SG350X系列
- Sx500系列
- Sx550X系列

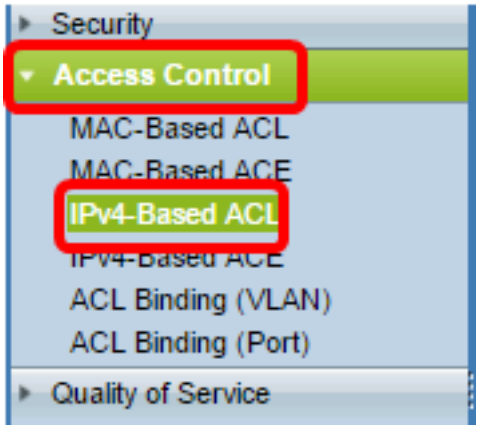
軟體版本

- 1.4.5.02 - Sx500系列
- 2.2.5.68 - Sx350系列、SG350X系列、Sx550X系列

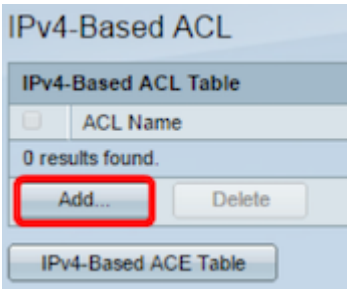
配置基於IPv4的ACL和ACE

配置基於IPv4的ACL

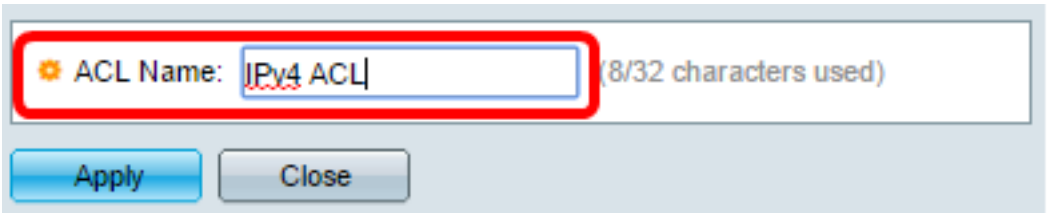
步驟1.登入到基於Web的實用程式，然後轉到**訪問控制>基於IPv4的ACL**。



步驟2.按一下**Add**按鈕。

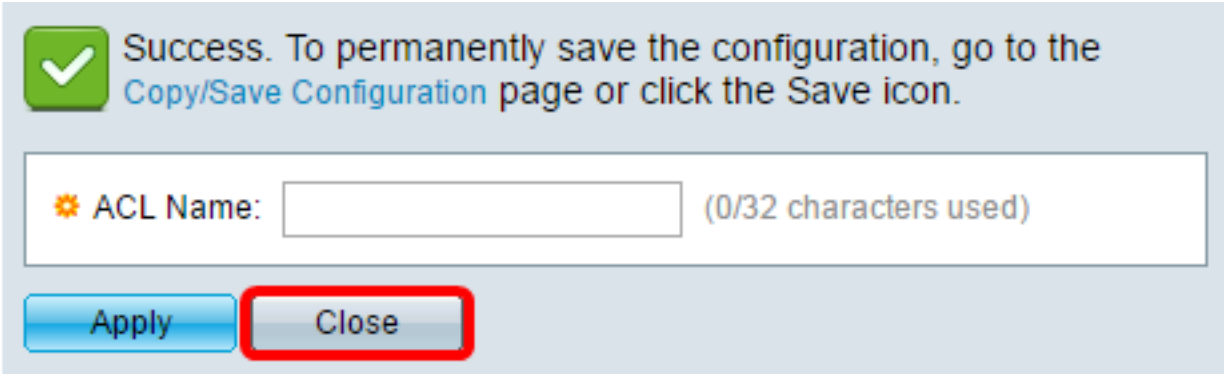


步驟3.在*ACL Name*欄位中輸入新ACL的名稱。



附註：本範例中使用的是IPv4 ACL。

步驟4.按一下**Apply** ，然後按一下**Close**。



步驟5.（可選）按一下**Save**，將設定儲存到啟動組態檔中。

現在，您應該在交換器上設定了一個基於IPv4的ACL。

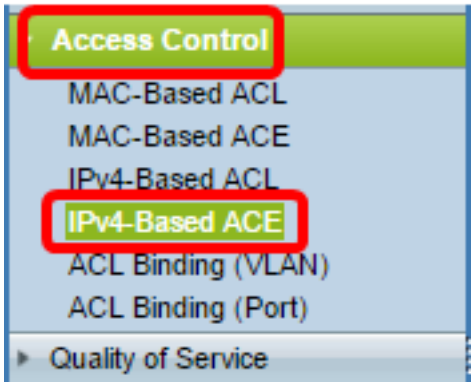
配置基於IPv4的ACE

當連線埠上收到封包時，交換器會透過第一個ACL處理封包。如果資料包匹配第一個ACL的ACE過濾器，則會執行ACE操作。如果資料包與任一ACE過濾器都不匹配，則處理下一個ACL。如果在所有相關ACL中找不到與任何ACE相符的ACE，則預設丟棄資料包。

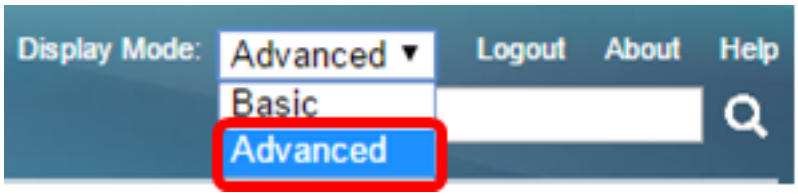
在此方案中，將建立ACE以拒絕從特定使用者定義的源IPv4地址傳送到任何目標地址的流量。

附註：可通過建立允許所有流量的低優先順序ACE來避免此預設操作。

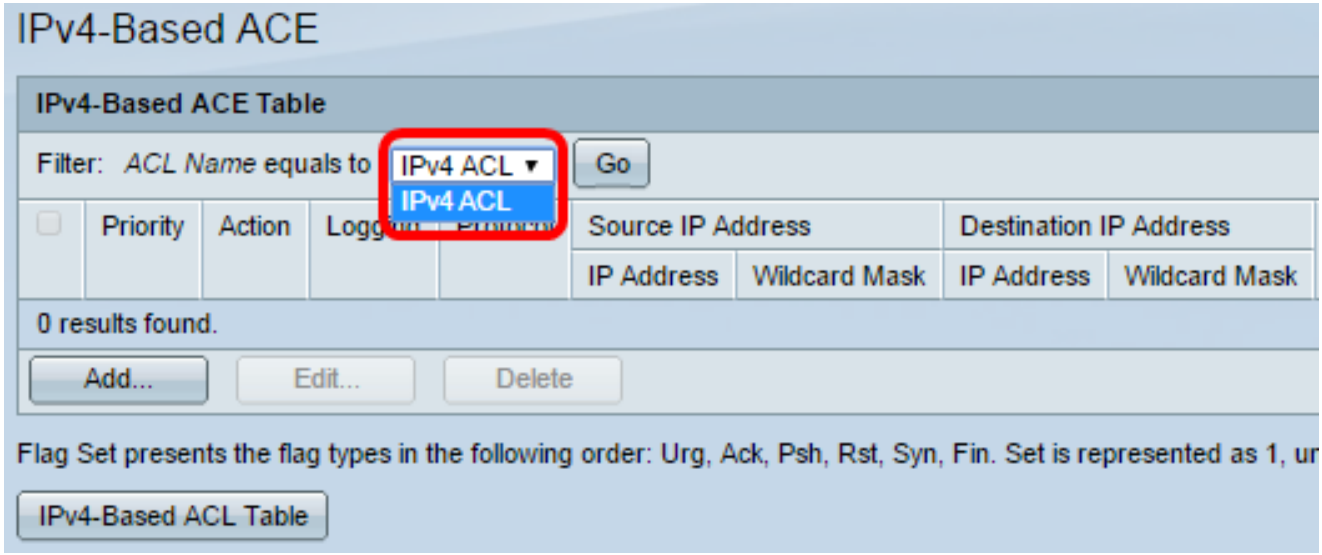
步驟1.在基於Web的實用程式上，轉至**訪問控制>基於IPv4的ACE**。



重要事項：若要充分利用交換器的可用特性及功能，請透過從頁面右上角的「Display Mode」下拉式清單選擇**Advanced**，以變更為「Advanced」模式。



步驟2.從ACL Name下拉選單中選擇ACL，然後按一下**Go**。

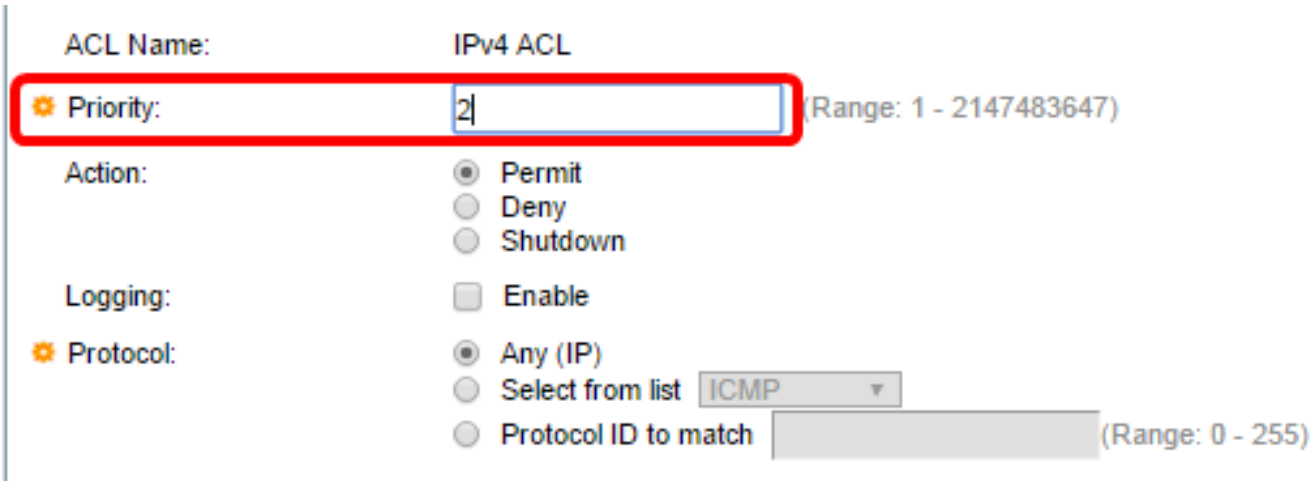


附註：表中將顯示已為ACL配置的ACE。

步驟3.按一下**Add**按鈕將新規則新增到ACL。

附註：*ACL Name*欄位顯示ACL的名稱。

步驟4.在*Priority*欄位中輸入ACE的優先順序值。首先處理優先順序值較高的ACE。值1是最高優先順序。範圍為1到2147483647。



附註：在本示例中，使用2。

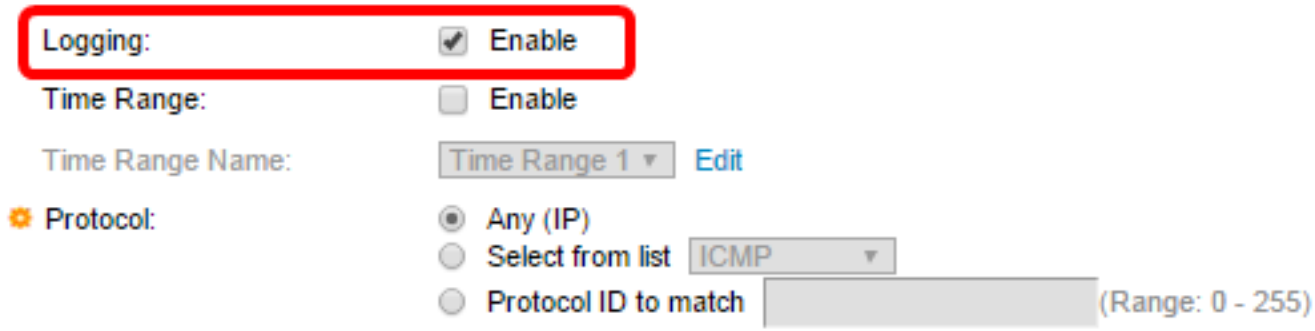
步驟5.點選與滿足所需ACE標準時所需執行的操作對應的單選按鈕。

附註：在此示例中，選擇Permit。

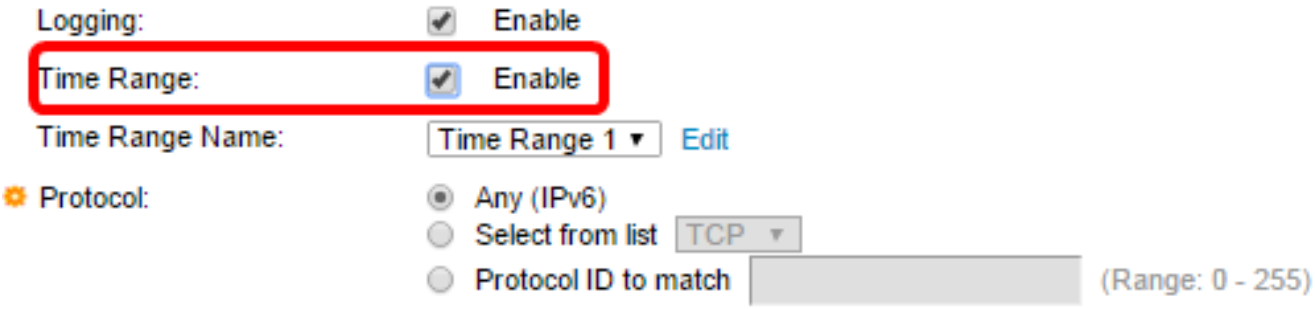
- 允許 — 交換機轉發符合ACE所需標準的資料包。
- 拒絕 — 交換機丟棄符合ACE必需標準的資料包。
- Shutdown — 交換機丟棄不符合ACE必需標準的資料包，並禁用接收資料包的埠。

附註：可以在Port Settings頁面上重新啟用禁用的埠。

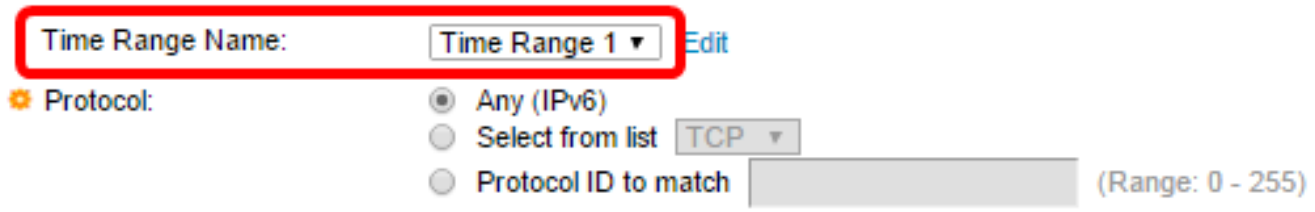
步驟6.（可選）選中**Enable** Logging覈取方塊以啟用與ACL規則匹配的ACL流的日誌記錄。



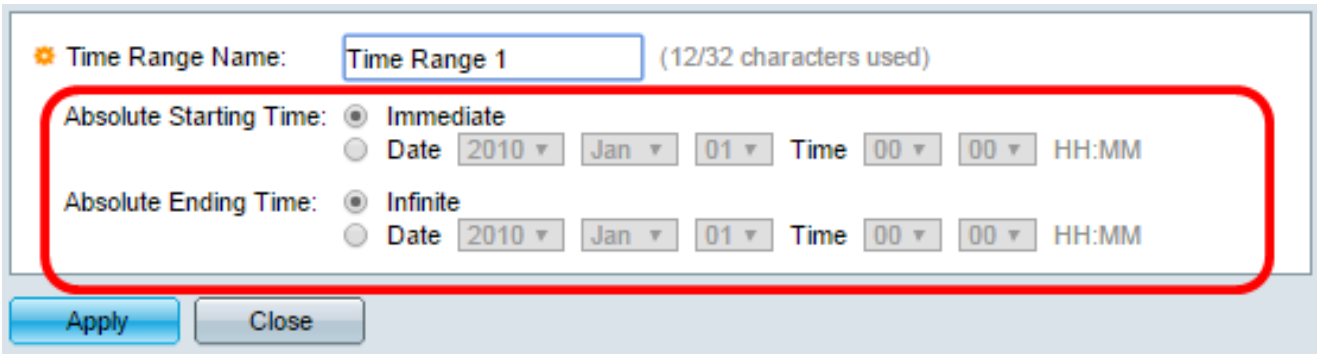
步驟7.（可選）選中**Enable** Time Range覈取方塊，允許為ACE配置時間範圍。時間範圍用於限制ACE的有效時間。



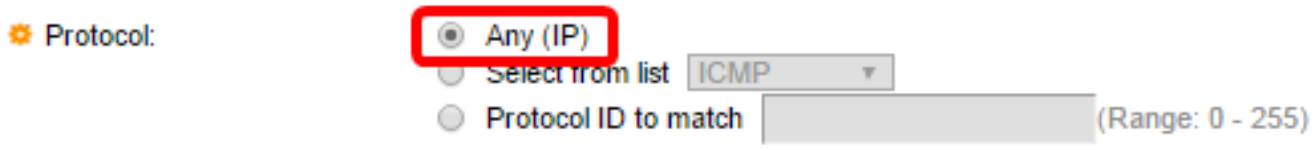
步驟8.（可選）從Time Range Name下拉選單中，選擇要應用於ACE的時間範圍。



附註：可以按一下**編輯**在「時間範圍」頁上導航並建立時間範圍。



步驟9.在「協定」區域選擇協定型別。將根據特定協定或協定ID建立ACE。

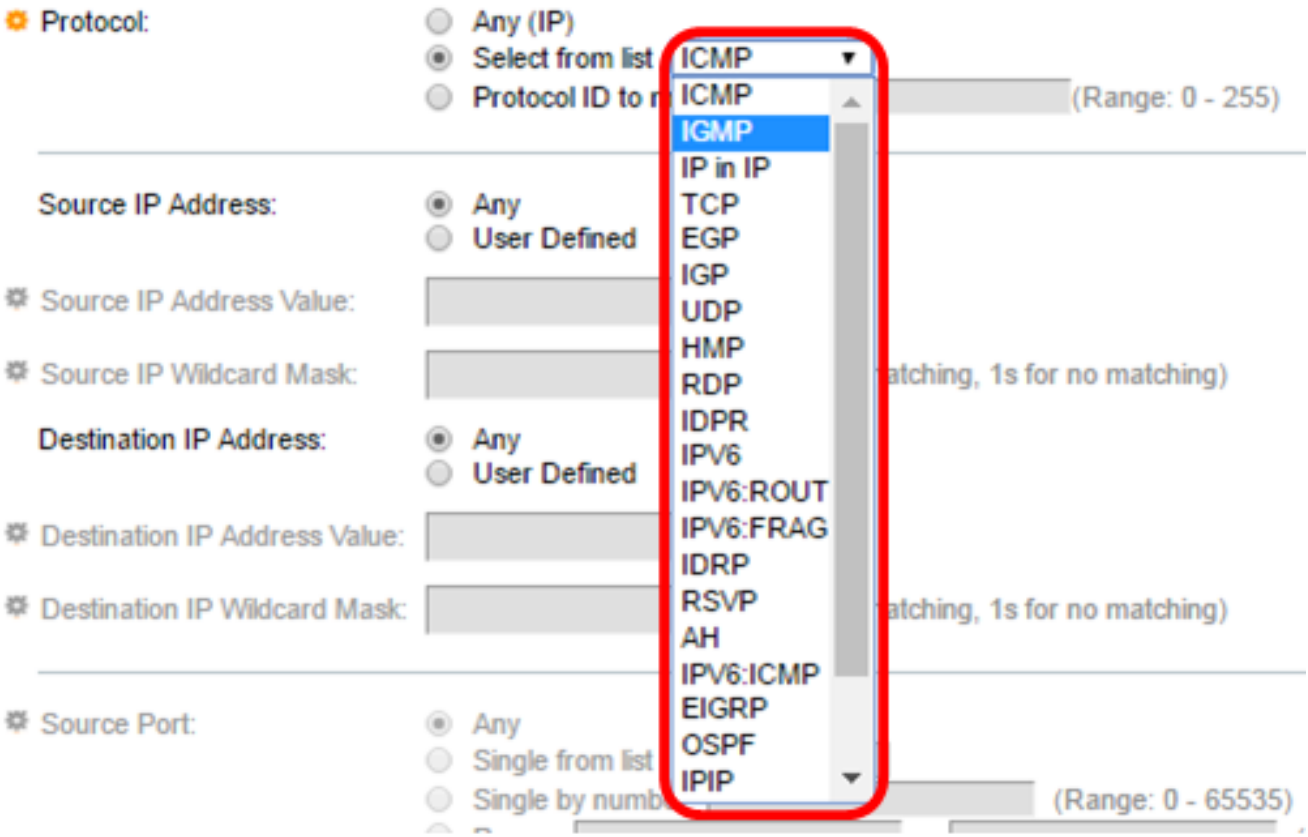


選項包括：

- Any(IP) — 此選項將ACE配置為接受所有IP協定。
- Select from list — 此選項可讓您從下拉選單中選擇一個通訊協定。如果您更喜歡此選項，請跳至步驟10。
- 要匹配的協定ID — 此選項將允許您輸入協定ID。如果您更喜歡此選項，請跳至步驟11。

附註：在此範例中，選擇Any(IP)。

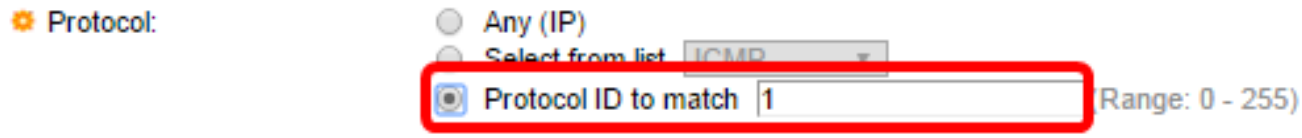
步驟10。（可選）如果您在步驟9中選擇了從清單中選擇，請從下拉選單中選擇一個協定。



選項包括：

- ICMP — 網際網路控制訊息通訊協定
- IP內IP - IP內封裝
- TCP — 傳輸控制通訊協定
- EGP — 外部閘道通訊協定
- IGP — 內部閘道通訊協定
- UDP — 使用者資料包協定
- HMP — 主機對映協定
- RDP — 可靠資料包通訊協定
- IDPR — 域間策略路由
- IPV6 - IPv6 over IPv4隧道
- IPV6:ROUT — 通過網關匹配屬於IPv6 over IPv4路由的資料包
- IPV6:FRAG — 匹配屬於IPv6 over IPv4片段報頭的資料包
- IDRP — IS-IS域間路由協定
- RSVP — 更新通訊協定
- AH — 身份驗證報頭
- IPV6:ICMP - IPv6的ICMP
- EIGRP — 增強型內部網關路由協定
- OSPF — 開放最短路徑優先
- IPIP - IP內IP
- PIM — 通訊協定無關多點傳送
- L2TP — 第2層通道通訊協定

步驟11。（可選）如果您在步驟9中選擇了要匹配的協定ID，請在「要匹配的協定ID」*欄位中輸入協定*ID。



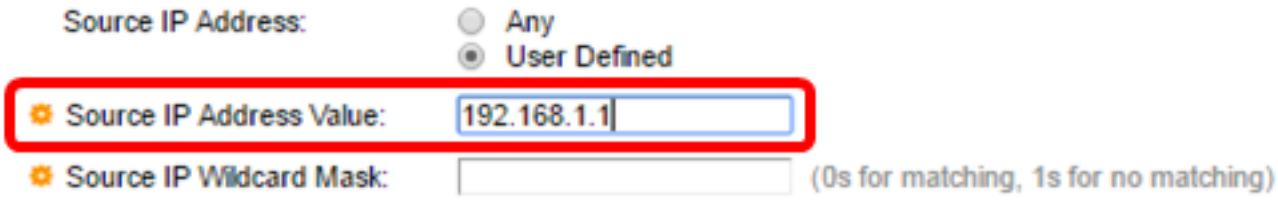
步驟12.在Source IP Address區域中按一下與ACE的所需標準對應的單選按鈕。

選項包括：

- Any — 所有源IPv4地址都適用於ACE。
- 使用者定義 — 在*源IP地址值*和*源IP萬用字元掩碼*欄位中輸入要應用於ACE的IP地址和IP萬用字元掩碼。萬用字元掩碼用於定義IP地址範圍。

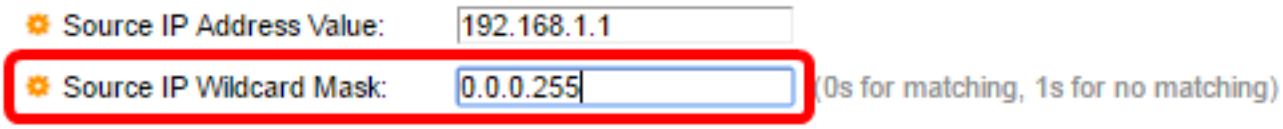
附註：在此示例中，選擇了User Defined。如果您選擇Any，請跳至步驟15。

步驟13.在*Source IP Address* Value欄位中*輸入源IP地*址。



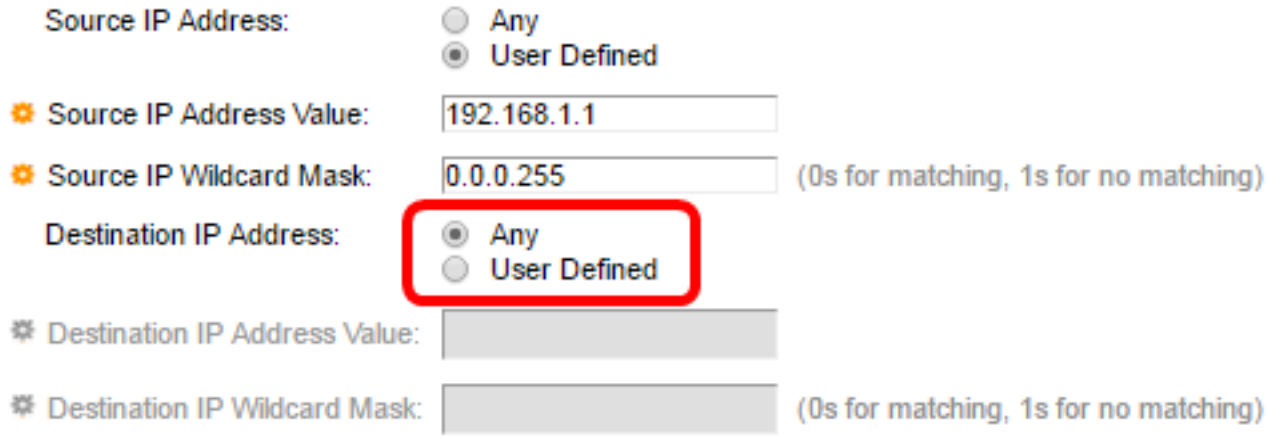
附註：本示例使用192.168.1.1。

步驟14.在*Source IP Wildcard* Mask欄位中輸入源*萬用字元掩*碼。



附註：本示例使用0.0.0.255。

步驟15.在Destination IP Address區域中按一下與ACE的所需條件對應的單選按鈕。



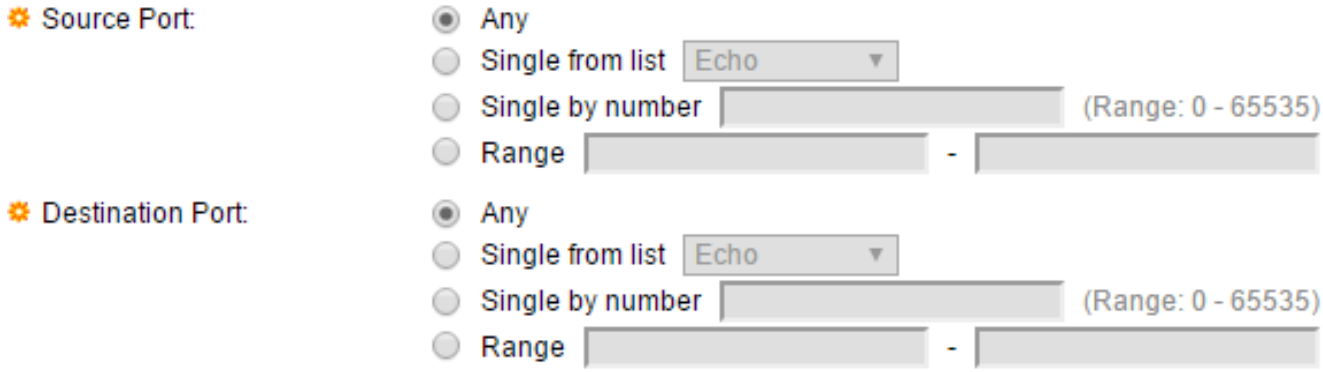
選項包括：

- Any — 所有目標IPv4地址都適用於ACE。

- 使用者定義 — 在*Destination IP Address Value*和*Destination IP Wildcard Mask*欄位中輸入要應用於ACE的IP地址和IP萬用字元掩碼。萬用字元掩碼用於定義IP地址範圍。

附註：在此示例中，選擇了Any。選擇此選項意味著要建立的ACE將允許從指定IPv4地址到任何目標的ACE流量。

步驟16。（可選）按一下Source Port區域中的單選按鈕。預設值為Any。



- Any — 與所有源埠匹配。
- Single from清單 — 可以選擇與資料包匹配的單個TCP/UDP源埠。只有在「Select from List」下拉選單中選擇800/6-TCP或800/17-UDP時，此欄位才會處於作用中狀態。
- Single by number — 可以選擇與資料包匹配的單個TCP/UDP源埠。只有在「Select from List」下拉選單中選擇800/6-TCP或800/17-UDP時，此欄位才會處於作用中狀態。
- 範圍 — 可以選擇與資料包匹配的TCP/UDP源埠範圍。可以配置八個不同的埠範圍（在源埠和目的埠之間共用）。TCP和UDP協定各有八個埠範圍。

步驟17。（可選）按一下Destination Port區域中的單選按鈕。預設值為Any。

- Any — 與所有源埠匹配
- Single from清單 — 可以選擇與資料包匹配的單個TCP/UDP源埠。只有在「Select from List」下拉選單中選擇800/6-TCP或800/17-UDP時，此欄位才會處於作用中狀態。
- Single by number — 可以選擇與資料包匹配的單個TCP/UDP源埠。只有在「Select from List」下拉選單中選擇800/6-TCP或800/17-UDP時，此欄位才會處於作用中狀態。
- 範圍 — 可以選擇與資料包匹配的TCP/UDP源埠範圍。可以配置八個不同的埠範圍（在源埠和目的埠之間共用）。TCP和UDP協定各有八個埠範圍。

步驟18。（可選）在TCP標誌區域中，選擇用於過濾資料包的一個或多個TCP標誌。過濾的資料包將被轉發或丟棄。通過TCP標籤過濾資料包可增強資料包控制，從而提高網路安全性。

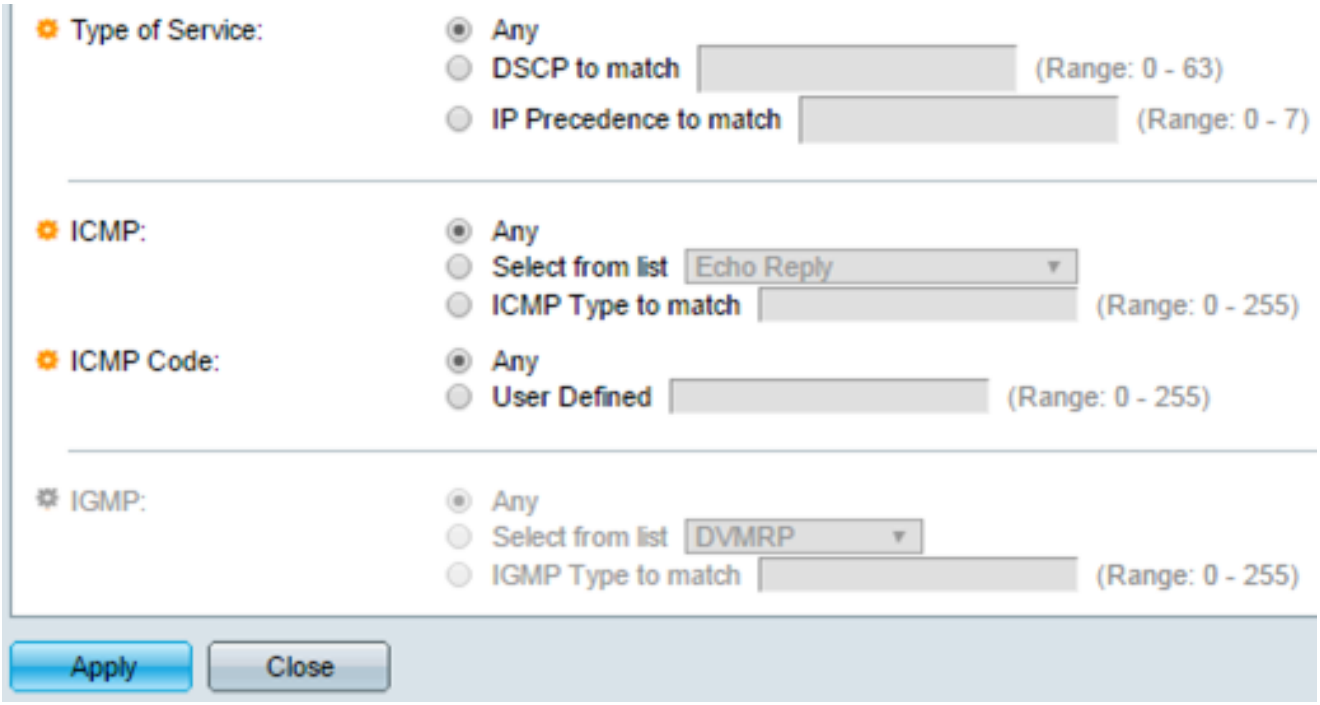
- Set — 如果設定了標誌，則匹配。
- Unset — 如果未設定標誌，則匹配。
- 不介意 — 忽略TCP標誌。

TCP標誌是：

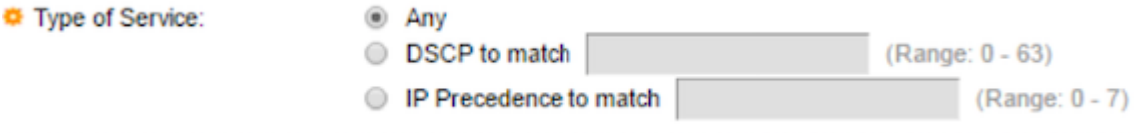
- Urg — 此標誌用於將傳入資料標識為Urgent。
- Ack — 此標誌用於確認資料包的成功接收。

- Psh — 此標誌用於確保資料被賦予優先順序（應賦予優先順序），並在傳送端或接收端進行處理。
- Rst — 當不用於當前連線的段到達時，使用此標誌。
- Syn — 此標誌用於TCP通訊。
- Fin — 當通訊或資料傳輸完成時使用此標誌。

步驟19。（可選）從「服務型別」區域按一下IP資料包的服務型別。



選項包括：



- Any — 可以是任何型別的服務來應對流量擁塞。
- DSCP to Match — DSCP是一種用於分類和管理網路流量的機制。6位(0-63)用於選擇資料包在每個節點上經歷的每跳行為。
- 要匹配的IP優先順序 — IP優先順序是一種服務型別(TOS)模型，網路使用該模型幫助提供相應的服務品質(QoS)承諾。此模式使用IP標頭中服務型別位元組的三個最高有效位，如RFC 791和RFC 1349中所述。帶有IP Preference值的關鍵字如下：

  - 0 — 常式

  - 1 — 表示優先順序

  - 2 — 立即

  - 3 — 用於快閃記憶體

  - 4 — 用於快閃記憶體覆蓋

  - 5 — 對於關鍵

  - 6 — 用於網際網路

- 7 — 用於網路

步驟20。（可選）如果ACL的IP協定為ICMP，請按一下用於過濾的ICMP消息型別。按名稱選擇消息型別或輸入消息型別編號：

- Any — 接受所有消息型別。
- 從清單中選擇 — 您可以按名稱選擇消息型別。
- 要匹配的ICMP型別 — 用於過濾目的的消息型別數量。範圍為0到255。

步驟21.（可選）ICMP消息可以有一個指示如何處理消息的代碼欄位。按一下以下選項之一以配置是否過濾此代碼：

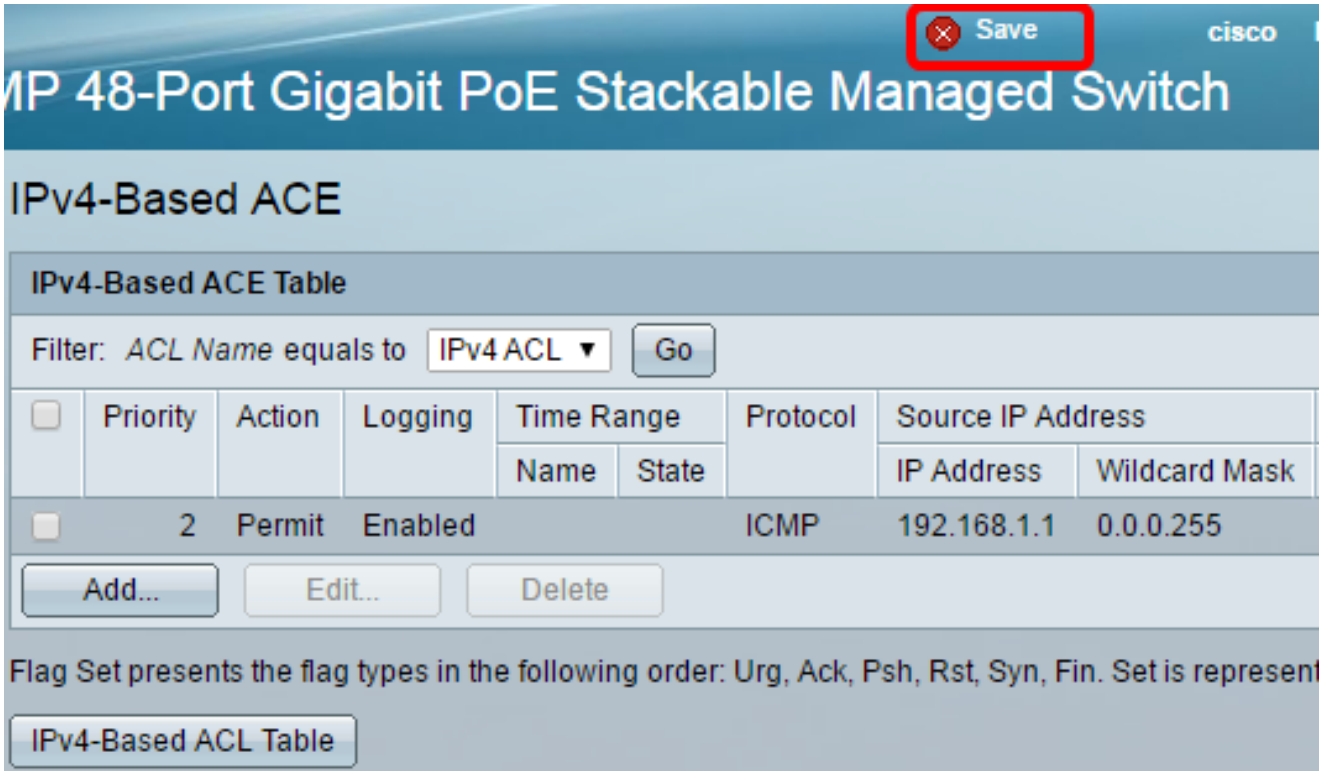
- Any — 接受所有代碼。
- 使用者定義 — 您可以輸入ICMP代碼以進行過濾。範圍為0到255。

步驟22。（可選）如果ACL基於IGMP，請按一下用於過濾的IGMP消息型別。按名稱選擇消息型別或輸入消息型別編號：

- Any — 接受所有消息型別。
- Select from list — 您可以從下拉式清單中選擇任何選項：
- DVMRP — 使用反向路徑泛洪技術，通過除資料包到達的介面以外的每個介面傳送接收資料包的副本。
- Host-Query — 定期在每個連線的網路上傳送常規主機查詢消息以獲取資訊。
- Host-Reply — 對查詢進行回覆。
- PIM — 本地和遠端組播路由器之間使用協定無關組播(PIM)將組播流量從組播伺服器定向到許多組播客戶端。
- Trace — 提供有關加入和退出IGMP組播組的資訊。
- 要匹配的IGMP型別 — 用於過濾目的的消息型別的數量。範圍為0到255。

步驟23.按一下**Apply**，然後按一下**Close**。建立ACE並將其與ACL名稱關聯。

步驟24.按一下**Save**，將設定儲存到啟動組態檔中。



現在，您應該在交換機上配置基於IPv4的ACE。