

在交換機上配置基於IPv6的訪問控制清單(ACL)和訪問控制條目(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。

IPv6中的典型ACL功能與IPv4中的ACL類似。ACL確定要阻止的流量以及要在交換機介面轉發哪些流量。ACL允許根據源地址和目的地址、入站和出站到特定介面進行過濾。每個ACL的結尾都有一個隱含的deny語句。ACL的規則在訪問控制條目(ACE)中配置。

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。

本文提供有關如何在交換機上配置基於IPv6的ACL和ACE的說明。

適用裝置

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

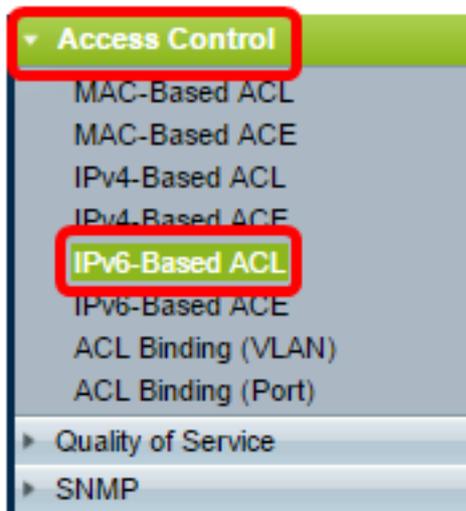
軟體版本

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

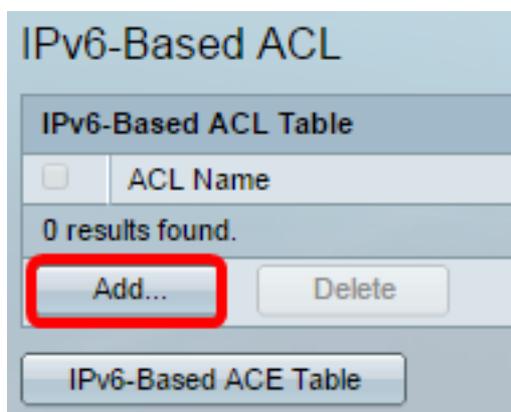
配置基於IPv6的ACL和ACE

配置基於IPv6的ACL

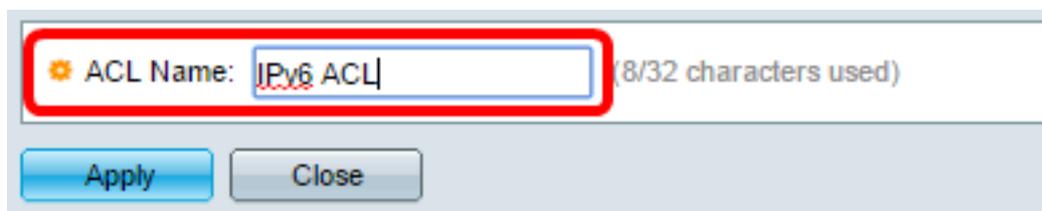
步驟1. 登入到基於Web的實用程式，然後轉到訪問控制>IPv6型ACL。



步驟2. 按一下**Add**按鈕。

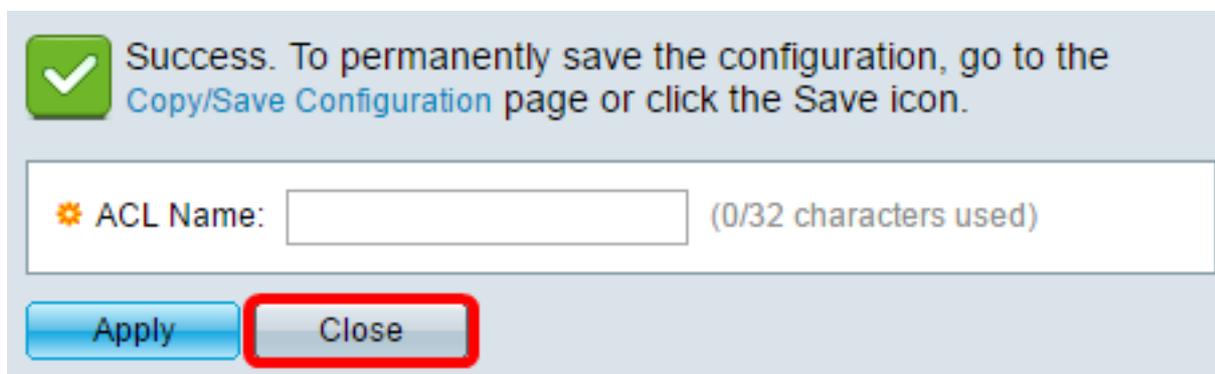


步驟3. 在 *ACL Name* 欄位中輸入新ACL的名稱。



附註：在此示例中，使用IPv6 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，您應該在交換機上配置了一個基於IPv6的ACL。

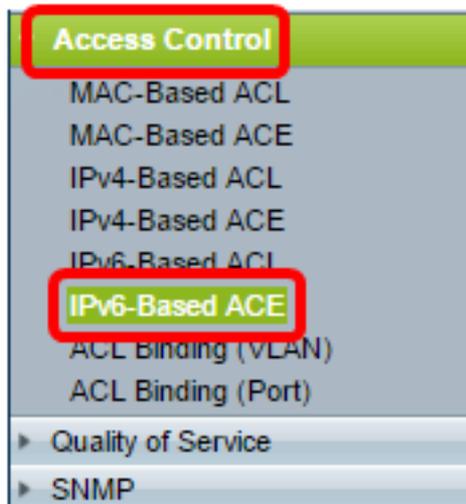
配置基於IPv6的ACE

當埠收到資料包時，交換機通過第一個ACL處理幀。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。

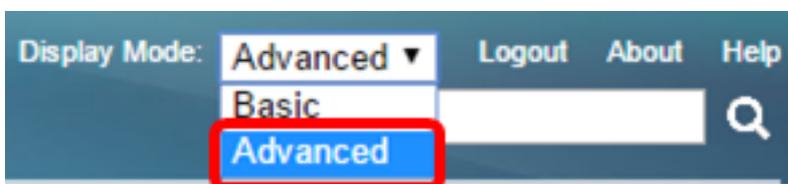
在此方案中，將建立ACE以拒絕從特定使用者定義的源IPv6地址傳送到任何目標地址的流量。

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IPv6的ACE。



重要事項：如果您有Sx350、SG350X、Sx550X交換機，請通過從頁面右上角的Display Mode下拉選單中選擇Advanced來切換到Advanced模式。



步驟2.從ACL Name下拉選單中選擇ACL，然後按一下Go。

IPv6-Based ACE

IPv6-Based ACE Table

Filter: *ACL Name equals to* **IPv6 ACL**

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Protocol	Source		Destination
				Name	State		IP Address	Prefix Length	IP Address
0 results found.									

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, Fin. Set is represented as 1, 0

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。

IPv6-Based ACE

IPv6-Based ACE Table

Filter: *ACL Name equals to* **IPv6 ACL**

<input type="checkbox"/>	Priority	Action	Logging	Time Range		Protocol	Source		
				Name	State		IP Address	P	
0 results found.									

Flag Set presents the flag types in the following order: Urg, Ack, Psh, Rst, Syn, F

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。

ACL Name: IPv6 ACL

Priority: 3 (Range: 1 - 2147483647)

Action: Permit
 Deny
 Shutdown

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)

附註：在此示例中，使用3。

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。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規則匹配的日誌記錄ACL流。

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)

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。如果此選項處於禁用狀態，則ACE可隨時工作。

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)

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：在此示例中，選擇Select from list。

[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協定。

選項包括：

- TCP — 傳輸控制協定(TCP)使兩台主機能夠通訊和交換資料流。TCP可保證資料包的傳輸，並保證資料包按傳送順序傳送和接收。
- UDP — 使用者資料包通訊協定(UDP)會傳輸封包，但並不保證傳送封包。
- ICMP — 將封包與網際網路控制訊息通訊協定(ICMP)配對。

附註：本範例中使用的是TCP。

[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。

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

附註：在此示例中，使用1。

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。

Source IP Address: Any User Defined

選項包括：

- Any — 所有源IPv6地址都適用於ACE。
- 使用者定義 — 在源IP地址值和源IP字首長度欄位中輸入要應用於ACE的IP地址和IP萬用字元掩碼。

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。

Source IP Address: Any User Defined
Source IP Address Value: fe80::d0ba:7021:37f7:d68d

附註：在本示例中，使用了fe80::d0ba:7021:37f7:d68d。

步驟14.在Source IP Prefix Length欄位中輸入源IP字首長度。

Source IP Address: Any User Defined
Source IP Address Value: fe80::d0ba:7021:37f7:d68d
Source IP Prefix Length: 128 (Range: 0 - 128)

附註：在此示例中，使用128。

[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。

Source IP Address: Any User Defined

Source IP Address Value:

Source IP Prefix Length: (Range: 0 - 128)

Destination IP Address: Any User Defined

Destination IP Address Value:

Destination IP Prefix Length: (Range: 0 - 128)

選項包括：

- Any — 所有目標IPv6地址都適用於ACE。
- 使用者定義 — 在 *Destination IP Address Value* 和 *Destination IP Prefix Length* 欄位中輸入要應用於ACE的IP地址和IP萬用字元掩碼。

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IPv6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。

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 — 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。

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。

Type of Service:

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

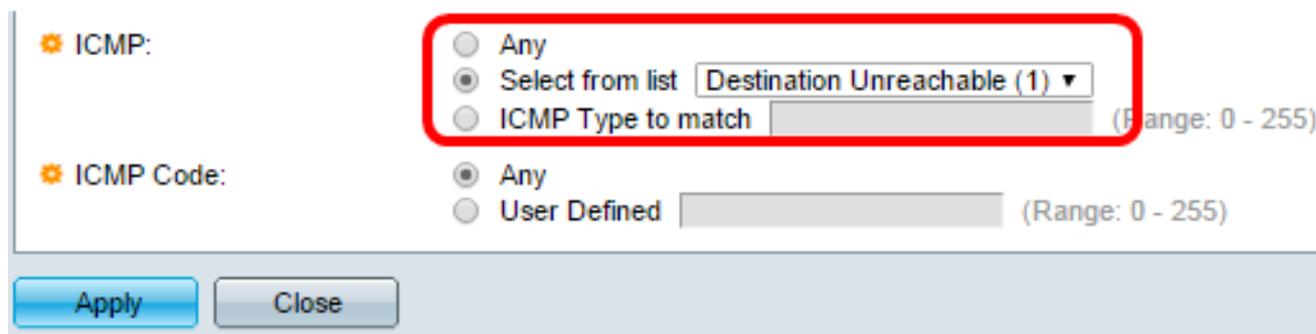
選項包括：

- Any — 可以是任何型別的服務來應對流量擁塞。
- 要匹配的DSCP — 差分服務代碼點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。具有IP首選項值的關鍵字如下：

- 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 — 網際網路
- 7 — 用於網路

附註：在此示例中，選擇了Any。

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：

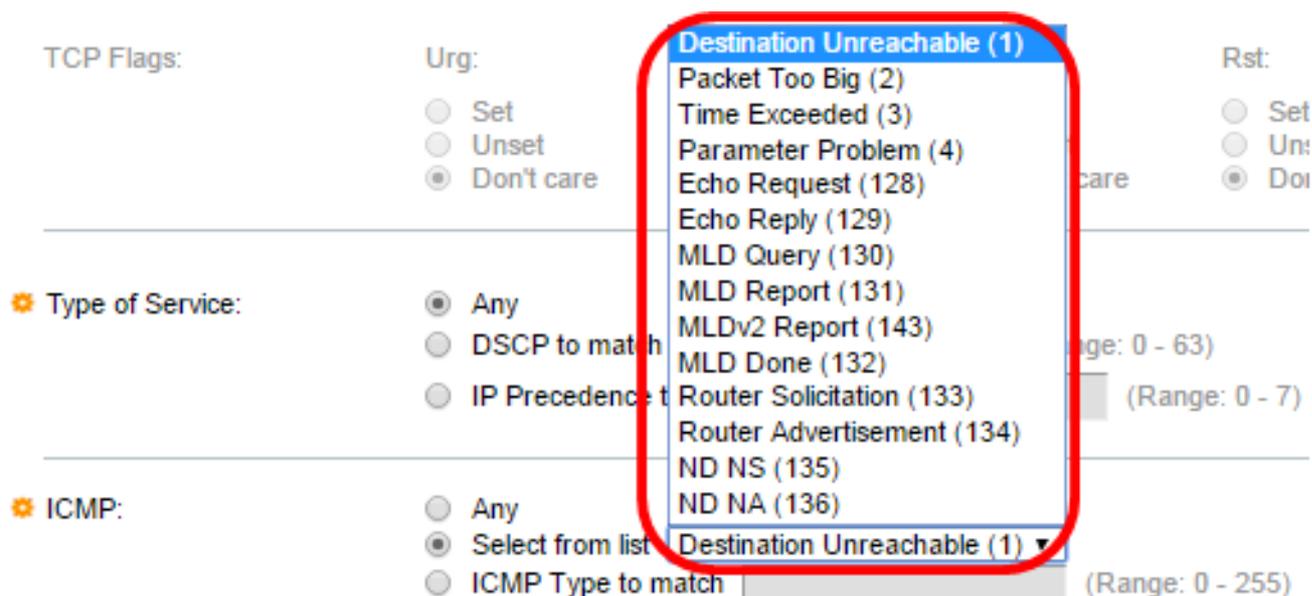


The screenshot shows a configuration window for an ACL. Under the 'ICMP:' section, there are three radio button options: 'Any', 'Select from list', and 'ICMP Type to match'. The 'Select from list' option is selected, and a dropdown menu is open showing 'Destination Unreachable (1)'. Below this, there is a text input field for 'ICMP Type to match' with '(Range: 0 - 255)' next to it. Under the 'ICMP Code:' section, there are two radio button options: 'Any' and 'User Defined'. The 'Any' option is selected. There is also a text input field for 'User Defined' with '(Range: 0 - 255)' next to it. At the bottom of the window are 'Apply' and 'Close' buttons.

- 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。

附註：在此示例中，選擇Select from list。

步驟21。(可選)如果在步驟20中選擇了「從清單中選擇」，請從下拉選單中的可能選項中選擇要過濾的控制消息：



The screenshot shows the same configuration window as in step 20, but with the dropdown menu for 'Select from list' expanded. The menu lists various ICMP message types with their corresponding numbers in parentheses: Destination Unreachable (1), Packet Too Big (2), Time Exceeded (3), Parameter Problem (4), Echo Request (128), Echo Reply (129), MLD Query (130), MLD Report (131), MLDv2 Report (143), MLD Done (132), Router Solicitation (133), Router Advertisement (134), ND NS (135), and ND NA (136). The 'Destination Unreachable (1)' option is highlighted in blue. The background shows other configuration options like 'TCP Flags', 'Urg', 'Type of Service', and 'ICMP Code'.

- 目的地無法連線(1) — 主機或其閘道產生此命令，以通知使用者端由於某些原因而無法連線(例如：網路或主機無法連線錯誤)。
- 封包過大(2) — 資料包大小超過給定MTU。
- 超出時間(3) — 由網關生成，用於通知由於生存時間欄位達到零而丟棄的資料包的來源。
- 引數問題(4) — 對另一個ICMP消息未明確涵蓋的任何錯誤都會生成該引數。
- Echo Request(128) — 這是一個ping，預期在回應回覆中收到其資料。
- 回應回覆(129) — 其是響應回應請求而生成的。
- MLD查詢(130) — 用於瞭解哪些組播地址在連線的鏈路上具有偵聽器。以十進位制形式鍵入130。
- MLD報告(131) — 當消息傳送方偵聽的IPv6組播地址時生成此報告。
- MLD v2報告(143) — 它與版本2的MLD報告相同。
- MLD完成(132) — 當主機離開組時，它會向網路中的組播路由器傳送組播偵聽器完成消息。

- 路由器請求(133) — 這是路由器發現消息。主機只要在偵聽通告時就能發現其相鄰路由器的地址。組播的預設值為224.0.0.2，否則為255.255.255.255。
- 路由器通告(134) — 路由器定期從其每個組播介面組播路由器通告，並通告該介面的IP地址。
- ND NS(135) — 消息由節點發起，用於請求另一個節點的鏈路層地址，也用於重複地址檢測和鄰居不可達性檢測等功能。
- ND NA(136) — 傳送消息以響應NS消息。如果某個節點更改其鏈路層地址，它可以傳送未經請求的NA來通告新地址。

步驟22. (可選) ICMP消息可以有一個指示如何處理消息的代碼欄位。如果在步驟10中選擇ICMP協定，則會啟用此選項。按一下以下選項之一以配置是否按此代碼過濾：

ICMP:
 Any
 Select from list Destination Unreachable (1) ▼
 ICMP Type to match (Range: 0 - 255)

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

- 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。

附註：在此示例中，選擇了Any。

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。

MP 48-Port Gigabit PoE Stackable Managed Switch

IPv6-Based ACE

IPv6-Based ACE Table

Filter: ACL Name equals to IPv6 ACL ▼ Go

	Priority	Action	Logging	Time Range		Protocol	Source
				Name	State		IP Address
<input type="checkbox"/>	3	Deny	Enabled			ICMP	fe80::d0ba:7021:37f7:d68d

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

IPv6-Based ACL Table

現在，您應該在交換機上配置基於IPv6的ACE。