

在受管交換機上配置基於MAC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。基於媒體訪問控制(MAC)的訪問控制清單(ACL)是使用第2層資訊允許或拒絕流量訪問的源MAC地址清單。如果封包從無線存取點傳至區域網路(LAN)連線埠，或反之亦然，則此裝置會檢查封包的來源MAC位址是否與清單中的任何專案相符，並檢查ACL規則與框架的內容是否相符。然後使用匹配的結果來允許或拒絕此資料包。但是，將不會檢查從LAN到LAN埠的資料包。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。

本文提供如何在託管交換機上配置基於MAC的ACL和ACE的說明。

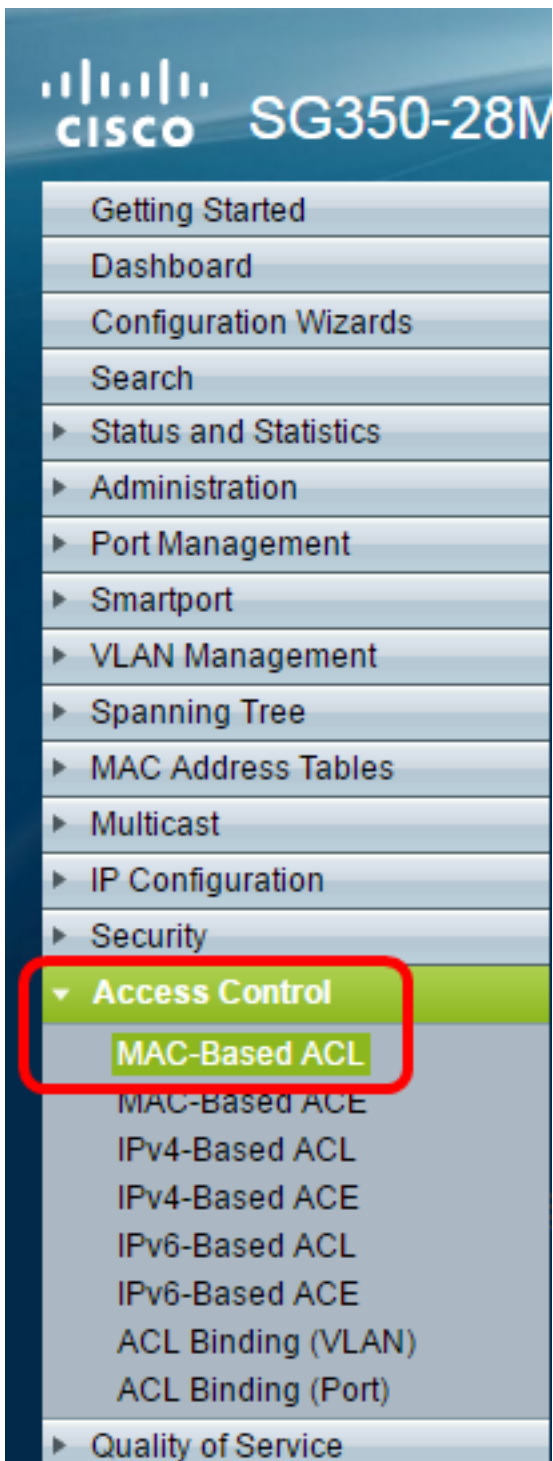
適用裝置 | 軟體版本

- Sx350系列 | 2.2.0.66(下載[最新版](#))
- SG350X系列 | 2.2.0.66(下載[最新版](#))
- Sx500系列 | 1.4.5.02(下載[最新版本](#))
- Sx550X系列 | 2.2.0.66(下載[最新版](#))

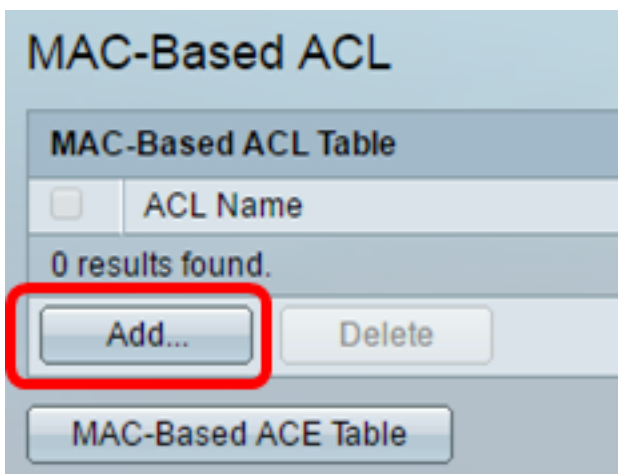
配置基於MAC的ACL和ACE

配置基於MAC的ACL

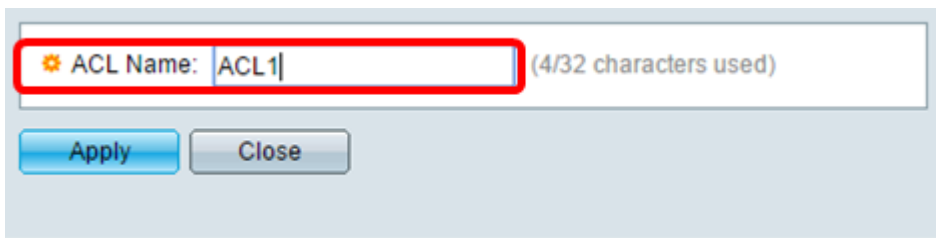
步驟1. 登入到基於Web的實用程式，然後轉到訪問控制>基於MAC的ACL。



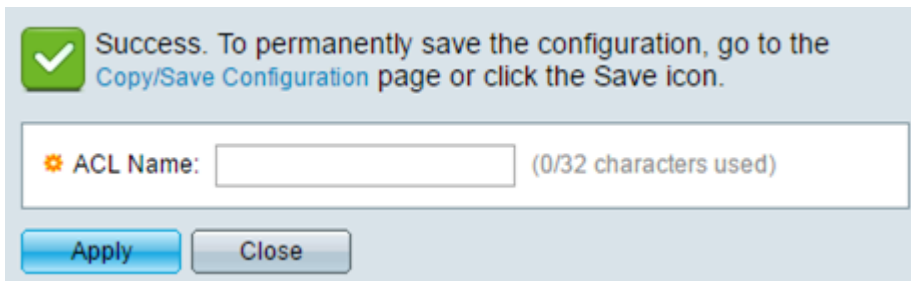
步驟2. 按一下Add按鈕。



步驟3. 在ACL Name欄位中輸入新ACL的名稱。



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一個基於MAC的ACL。

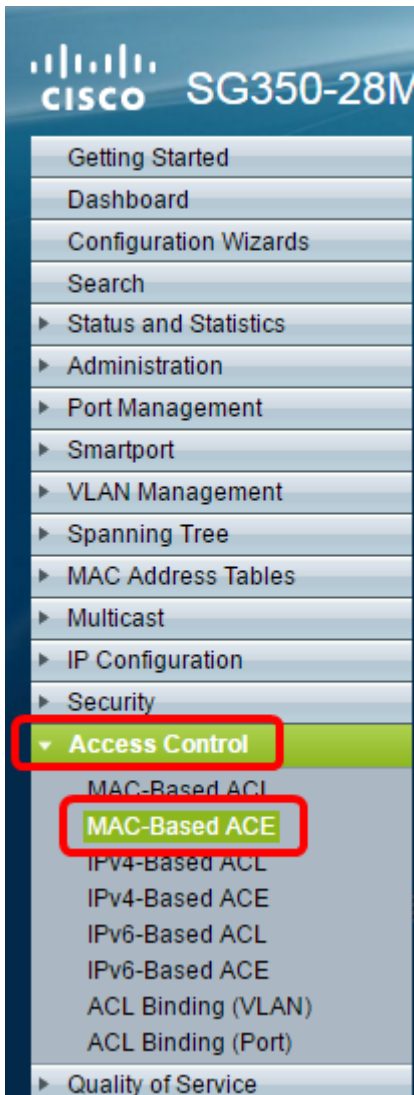
配置基於MAC的ACE

當埠收到幀時，交換機通過第一個ACL處理該幀。如果幀匹配第一個ACL的ACE過濾器，則會執行ACE操作。如果幀與任何ACE過濾器都不匹配，則處理下一個ACL。如果在所有相關ACL中未找到與任何ACE相匹配的，則預設丟棄該幀。

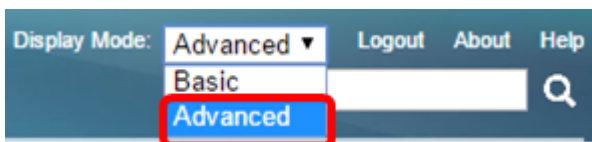
在此方案中，將建立ACE以拒絕從特定使用者定義的源MAC地址傳送到任何目標地址的流量。

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。

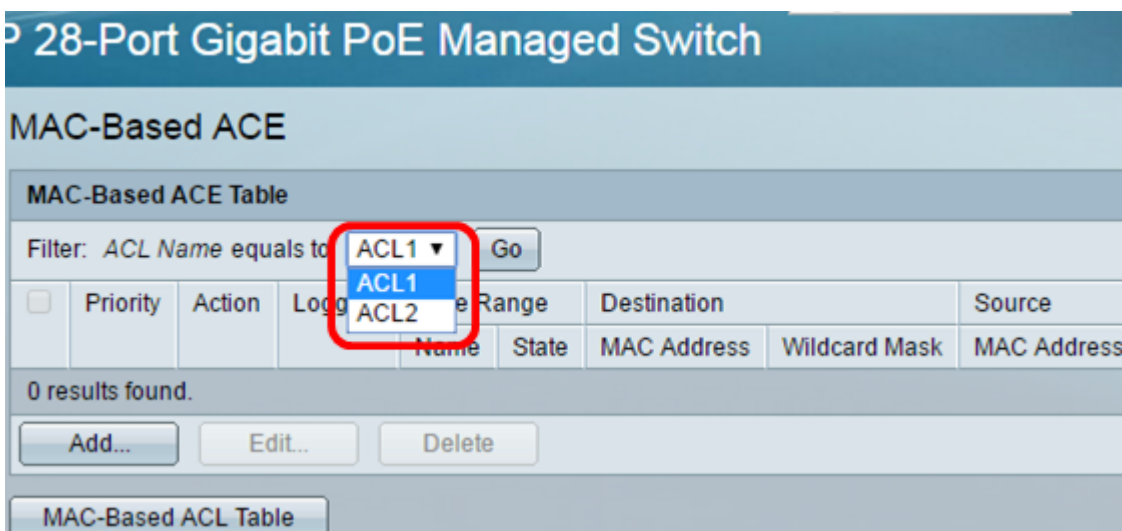
步驟1. 在基於Web的實用程式上，轉至 **訪問控制 > 基於MAC的ACE**。



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。

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

步驟5. (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。

步驟6.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Deny。

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

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。

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

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。

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

附註： 可以按一下編輯以導航到「時間範圍」頁並在該頁上建立時間範圍。

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

Absolute Starting Time: Immediate
 Date Time HH:MM

Absolute Ending Time: Infinite
 Date Time HH:MM

步驟9.在Destination MAC Address區域中，點選與ACE的所需條件對應的單選按鈕。

Destination MAC Address: Any
 User Defined

✱ Destination MAC Address Value:

✱ Destination MAC Wildcard Mask: (0s for matching, 1s for no matching)

選項包括：

Any — 所有目標MAC地址都適用於ACE。

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

步驟10.在Source MAC Address區域中按一下與ACE的所需標準對應的單選按鈕。

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)

Apply Close

選項包括：

Any — 所有源MAC地址都適用於ACE。

使用者定義 — 在源MAC地址值和源MAC萬用字元掩碼欄位中輸入要應用於ACE的MAC地址和MAC萬用字元掩碼。萬用字元掩碼用於定義MAC地址範圍。

附註：在此示例中，選擇了User Defined。

步驟11。(可選) 在VLAN ID欄位中，輸入與訊框的VLAN標籤相符的VLAN ID。

步驟12。(可選) 要在ACE條件中包括802.1p值，請選中**Include** in the 802.1p覈取方塊。802.1p涉及技術服務類別(CoS)。CoS是乙太網幀中的3位欄位，用於區分流量。

步驟13.如果包括802.1p值，請輸入以下欄位：

802.1p值 — 輸入要匹配的802.1p值。802.1p規範使第2層交換機能夠區分流量的優先順序並執行動態組播過濾。這些值如下：

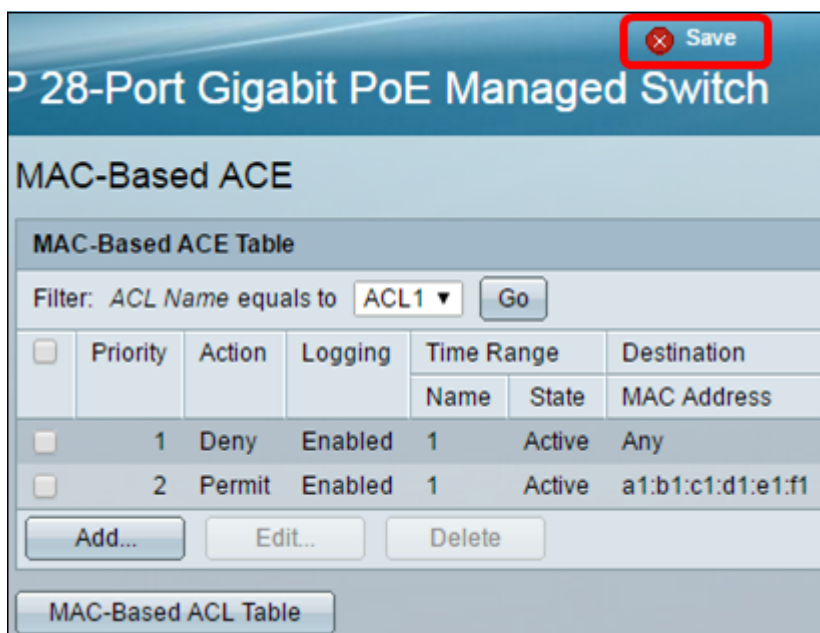
- 0 — 背景。最不優先的資料，如批次傳輸、遊戲等。
- 1 — 盡最大努力。在普通LAN優先順序上需要盡力傳送的資料。網路不提供任何傳送保證，但資料根據流量獲得未指定的位元率和傳送時間。
- 2 — 出色的努力。需要重要使用者盡力交付的資料。
- 3 — 關鍵應用，如Linux虛擬伺服器(LVS)電話會話初始協定(SIP)。
- 4 — 影片。延遲和抖動小於100毫秒。
- 5 — 語音Cisco IP電話預設值。延遲和抖動小於10毫秒。
- 6 — 網際控制LVS電話即時傳輸協定(RTP)。
- 7 — 網路控制。維護和支援網路基礎設施要求很高。

802.1p掩碼 — 輸入802.1p值的萬用字元掩碼。此萬用字元掩碼用於定義802.1p值的範圍。

步驟14。(可選)輸入要匹配的幀的Ethertype。Ethertype是乙太網幀中的2個二進位制八位數的欄位，用於指示幀的有效負載使用哪個協定。

步驟14.按一下**Apply**，然後按一下**Close**。建立ACE並將其與ACL名稱關聯。

步驟15.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MAC的ACE。

您可能會發現其他有價值的連結：

- [350系列交換器產品頁面](#)
- [350X系列交換器產品頁面](#)
- [550系列交換器產品頁面](#)
- [550X系列交換器產品頁面](#)

檢視與本文相關的影片.....

[按一下此處檢視思科的其他技術對話](#)