# 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<u>最新版</u>)
- 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<u>最新版</u>)

## 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3.在ACL Name欄位中輸入新ACL的名稱。

ACL Name: ACL1 (4/32 characters used)
Apply Close
Success. To permanently save the configuration, go to the Copy/Save Configuration page or click the Save icon.
ACL Name: (0/32 characters used)
Apply Close
步驟5.(可選)按一下 <b>Save</b> ,將設定儲存到啟動組態檔中。
P 28-Port Gigabit PoE Managed Switch
MAC-Based ACL

配置基於MAC的ACE

MAC-Based ACE Table

Delete

現在,您應該在交換器上設定一個基於MAC的ACL。

MAC-Based ACL Table

ACL Name

Add...

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。

cisco SG350-28M
Getting Started
Dashboard
Configuration Wizards
Search
<ul> <li>Status and Statistics</li> </ul>
<ul> <li>Administration</li> </ul>
<ul> <li>Port Management</li> </ul>
<ul> <li>Smartport</li> </ul>
<ul> <li>VLAN Management</li> </ul>
Spanning Tree
MAC Address Tables
<ul> <li>Multicast</li> </ul>
<ul> <li>IP Configuration</li> </ul>
<ul> <li>Security</li> </ul>
✓ Access Control
MAC-Based ACL
MAC-Based ACE
IPV4-Based ACL
IPv4-Based ACE
IPv6-Based ACL
IPvb-Based ACE
ACL Binding (Port)
Quality of Service

**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。

Display Mode:	Advanced <b>v</b>	Logout	About	Help
and the second second second	Basic			0
	Advanced			

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	
🌣 Priority:	1	(Range: 1 - 2147483647
Action:	<ul> <li>Permit</li> <li>Deny</li> <li>Shutdown</li> </ul>	
Logging:	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。

Priority:	1	(Range: 1 - 2147483647)
Action:	Permit Deny 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。

Time Range:	Enable
Time Range Name:	1 T 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。

Time Range:	1	E	nable
Time Range Name:	1	۲	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	(1/32 characters used)
Absolute Starting Time:	•	Immediate Date 2016 ▼ Jan ▼ 01 ▼ Time 00 ▼ 00 ▼ HH:MM
Absolute Ending Time:	•	Infinite Date 2017 ▼ Dec ▼ 01 ▼ Time 23 ▼ 59 ▼ HH:MM
Apply Close		

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:	1	(Range: 1 - 2147483647)
Action:	<ul><li>Permit</li><li>Deny</li><li>Shutdown</li></ul>	
Logging:	Enable	
Time Range:	Enable	
Time Range Name:	1 ▼ Edit	
Destination MAC Address:	<ul> <li>Any</li> <li>User Defined</li> </ul>	
Destination MAC Address Value:		
Destination MAC Wildcard Mask:		(0s for matching, 1s for no matching
Source MAC Address:	<ul><li>Any</li><li>User Defined</li></ul>	
Source MAC Address Value:	a2:b2:c2:d2:e2:f2	
Source MAC Wildcard Mask:	00000001111	(Os for matching, 1s for no matching
VLAN ID:	2	(Range: 1 - 4094)
802.1p:	Include	
🜣 802.1p Value:	1	(Range: 0 - 7)
🌣 802.1p Mask:	0	(Range: 0 - 7)
Ethertype:	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。

P 28-Port Gigabit PoE Managed Switch										
MAC-Based ACE										
MA	MAC-Based ACE Table									
Filte	r: ACL N	ame equa	als to ACL	.1 🔻 🕻	30					
	Priority	Action	Logging	Time Ra	ange	Destination				
				Name	State	MAC Address				
	1	Deny	Enabled	1	Active	Any				
	2 Permit Enabled 1 Active a1:b1:c1:d1:e1:f1									
Add Edit Delete										
MAC-Based ACL Table										

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
- <u>350X系列交換器產品頁面</u>
- 550系列交換器產品頁面
- <u>550X系列交換器產品頁面</u>

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