

300系列託管交換器上基於MAC的存取控制清單(ACL)和存取控制專案(ACE)的組態

目標

訪問控制清單(ACL)是一種安全技術，用於允許或拒絕網路流量。基於MAC的ACL使用第2層資訊來允許或拒絕對流量的訪問。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。300系列託管交換機最多支援512個ACL和512個ACE。

本文說明如何建立基於MAC的ACL，以及如何將ACE套用到300系列託管交換器上的ACL。

適用裝置

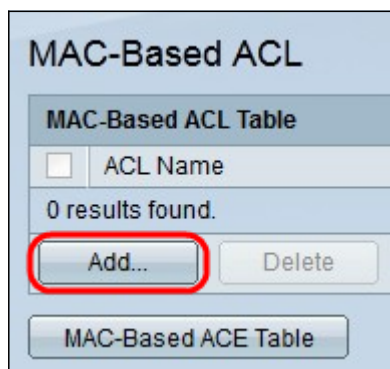
- SG300-10PP
- SG300-10MPP
- SG300-28PP-R
- SG300-28SFP-R
- SF302-08MPP
- SF302-08PP
- SF300-24PP-R
- SF300-48PP-R

軟體版本

- 1.4.0.00p3 [SG300-28SFP-R]
- 6.2.10.18 [所有其他適用裝置]

MAC型ACL

步驟1.登入到Web配置實用程式，然後選擇Access Control > MAC Based ACL。此時會打開基於MAC的ACL頁面：



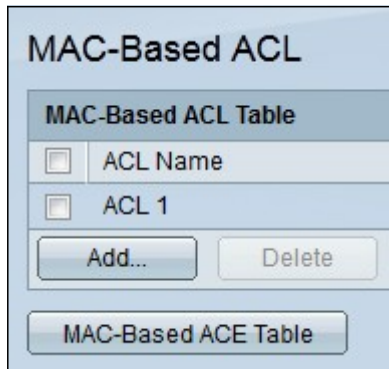
步驟2.按一下Add。系統將顯示Add MAC-Based ACL視窗。



ACL Name: (5/32 Characters Used)

步驟3.在「ACL名稱」欄位中輸入該ACL的名稱。

步驟4.按一下Apply。即會建立ACL。



MAC-Based ACL

MAC-Based ACL Table

<input type="checkbox"/>	ACL Name
<input type="checkbox"/>	ACL 1

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。

注意：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.登入到Web配置實用程式並選擇訪問控制>基於MAC的ACE。將開啟基於MAC的ACE頁：

步驟2.從ACL Name下拉選單中，選擇要應用規則的ACL。

步驟3.按一下Go。將顯示已為ACL配置的ACE。

步驟4.按一下Add將新規則新增到ACL。出現Add MAC-Based ACE視窗。

ACL名稱欄位顯示ACL的名稱。

步驟5.在「優先順序」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。

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。

- Permit — 交換機轉發符合ACE所需標準的資料包。
- deny — 交換機丟棄不符合ACE所需標準的資料包。
- 關閉 — 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。

注意：可以在*Port Settings*頁面上重新啟用禁用的埠。

步驟7.選中Time Range欄位中的**Enable**竅取方塊，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.從Time Range Name下拉選單中，選擇要應用於ACE的時間範圍。

註：單擊編輯可導航到「時間範圍」頁並建立一個時間範圍。

步驟9.在Destination MAC Address欄位中點選與ACE的所需條件對應的單選按鈕。

- Any — 所有目標MAC地址都適用於ACE。

·使用者定義 — 在「目標MAC地址值」和「目標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。

步驟10.在Source MAC Address欄位中點選與ACE的所需條件對應的單選按鈕。

·Any — 所有源MAC地址都適用於ACE。

·使用者定義 — 在「目標MAC地址值」和「目標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。

步驟11.輸入將與幀的VLAN標籤匹配的VLAN ID。

步驟12. (可選) 要在ACE標準中包括802.1p值，請選中802.1p欄位中的Include。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是一種規範，它使第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。

·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.輸入要匹配的幀的Ethertype。Ethertype是乙太網幀中的兩個二進位制八位數欄位，用於指示幀的有效負載使用哪個協定。

步驟15.按一下**Apply**。建立ACE。在本示例中，建立的ACE拒絕從定義的源MAC地址傳送到所有目標地址的流量。