

300系列託管交換機上的埠安全配置

目標

網路的安全非常重要。安全網路可防止入侵者入侵您的網路。增強網路中安全性的一種方法是配置埠安全。連線埠資安允許您在特定連線埠或連結彙總群組(LAG)上設定資安。LAG將單個介面合併到單個邏輯鏈路中，可提供最多八個物理鏈路的聚合頻寬。您可以限制或允許特定埠/LAG上的不同使用者訪問。

本文說明如何在300系列託管交換器上設定連線埠安全性。

適用裝置

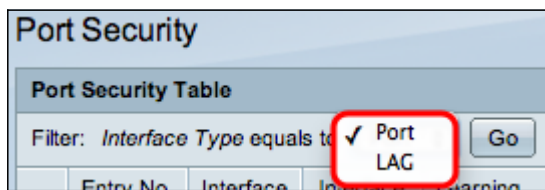
- SG300-10PP
- SG300-10MPP
- SG300-28PP-R
- SG300-28SFP-R
- SF302-08MPP
- SF302-08PP
- SF300-24PP-R
- SF300-48PP-R

軟體版本

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

連線埠安全組態

步驟1.登入到Web配置實用程式並選擇**Security > Port Security**。*Port Security*頁面隨即開啟：



步驟2.從Interface Type Equals下拉選單中選擇Port或LAG，然後點選Go。

步驟3.按一下要編輯其安全設定的介面的單選按鈕。

步驟4.按一下「Edit」。出現*Edit Port Security Interface Settings*視窗：

Interface:	<input checked="" type="radio"/> Port <input type="text" value="FE1"/>	<input type="radio"/> LAG <input type="text" value="1"/>
Interface Status:	<input type="checkbox"/> Lock	
Learning Mode:	<input checked="" type="radio"/> Classic Lock <input type="radio"/> Limited Dynamic Lock <input type="radio"/> Secure Permanent <input type="radio"/> Secure Delete on Reset	
* Max No. of Address Allowed:	<input type="text" value="1"/>	(Range: 0 - 256, Default: 1)
Action on Violation:	<input checked="" type="radio"/> Discard <input type="radio"/> Forward <input type="radio"/> Shutdown	
Trap:	<input type="checkbox"/> Enable	
* Trap Frequency:	<input type="text" value="10"/>	sec (Range: 1 - 1000000, Default: 10)

Interface:	<input type="radio"/> Port <input type="text" value="FE1"/>	<input type="radio"/> LAG <input type="text" value="1"/>
Interface Status:	<input type="checkbox"/> Lock	
Learning Mode:	<input checked="" type="radio"/> Classic Lock <input type="radio"/> Limited Dynamic Lock <input type="radio"/> Secure Permanent <input type="radio"/> Secure Delete on Reset	
✱ Max No. of Address Allowed:	<input type="text" value="1"/>	(Range: 0 - 256, Default: 1)
Action on Violation:	<input type="radio"/> Discard <input type="radio"/> Forward <input type="radio"/> Shutdown	
Trap:	<input type="checkbox"/> Enable	
✱ Trap Frequency:	<input type="text" value="10"/>	sec (Range: 1 - 1000000, Default: 10)
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

步驟5. (可選) 若要鎖定介面，使其無法傳送和接收資料流量，請在介面狀態列位中勾選Lock核取方塊。

Interface Status:	<input checked="" type="checkbox"/> Lock	
Learning Mode:	<input checked="" type="radio"/> Classic Lock <input type="radio"/> Limited Dynamic Lock <input type="radio"/> Secure Permanent <input type="radio"/> Secure Delete on Reset	
✱ Max No. of Address Allowed:	<input type="text" value="5"/>	(Range: 0 - 256, Default: 1)
Action on Violation:	<input type="radio"/> Discard <input type="radio"/> Forward <input checked="" type="radio"/> Shutdown	
Trap:	<input type="checkbox"/> Enable	
✱ Trap Frequency:	<input type="text" value="10"/>	sec (Range: 1 - 1000000, Default: 10)
<input type="button" value="Apply"/> <input type="button" value="Close"/>		

步驟6. 在Learning Mode欄位中，按一下所需學習模式的單選按鈕。可用選項包括：

- 經典鎖定 — 無論已獲知的裝置數量如何，立即鎖定埠。
- 受限動態鎖定 — 刪除與要鎖定它的埠相關的當前MAC地址。埠可以學習特定數量的裝置。
- 安全永久 — 保留與埠相關的當前MAC地址，並可獲知特定數量的裝置。
- 重置時安全刪除 — 重置後刪除與埠相關的當前MAC地址。交換器重設後，連線埠可以得知特定數量的裝置。

步驟7. 在允許的最大地址數欄位中，輸入允許埠學習的最大MAC地址數。如果輸入0，則連線埠僅支援靜態位址。

步驟8. 如果在步驟5中鎖定埠，則在Action on Violation欄位中，按一下發生違規時要執行的操作的單選按鈕。可用選項包括：

- 丟棄 — 如果源未知，則丟棄資料包。
- 轉發 — 如果源未知，則轉發資料包。
- 關機 — 資料包被丟棄，埠關閉。

步驟9. (可選) 每次在鎖定的埠上收到資料包時，都會觸發陷阱，確保資料包不會與鎖定的埠衝突。要啟用陷阱，請選中Trap欄位中的**Enable**覈取方塊。陷阱是從代理到管理器的同步通知，包括當前的sysUpTime值，它們是在簡單網路管理協定(SNMP)代理滿足條件時生成的。這些條件在管理資訊庫(MIB)中定義

步驟10.如果在步驟9中啟用陷阱，請在「陷阱頻率」欄位中輸入每個陷阱之間的最短時間（以秒為單位）。

步驟11.按一下**Apply**。

下圖顯示已配置埠的變化。

附註：要將一個埠的埠安全配置應用到多個埠，請參閱**將埠安全配置應用到多個埠**部分。

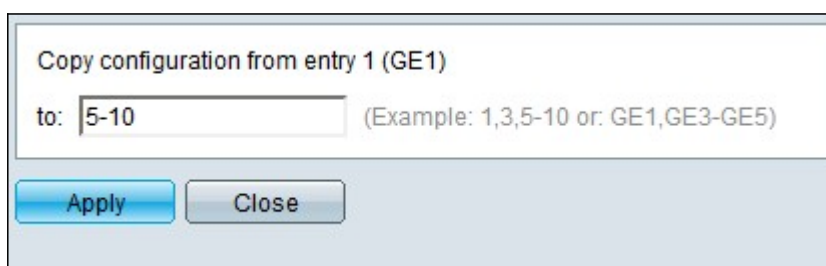
將連線埠安全組態套用到多個連線埠

本節介紹如何將單個埠的安全埠配置應用到多個埠。

步驟1.登入到Web配置實用程式並選擇**Security > Port Security**。*Port Security*頁面隨即開啟：

步驟2.按一下要將其配置應用到多個埠的埠的單選按鈕。

步驟3.按一下「Copy Settings」。出現「Copy Settings」視窗。



Copy configuration from entry 1 (GE1)

to: (Example: 1,3,5-10 or: GE1,GE3-GE5)

Apply Close

步驟4.在「至」欄位中，輸入埠範圍，此範圍與您在步驟2中選擇的埠具有相同埠安全配置。您可以使用埠號或埠名稱作為輸入。可以輸入以逗號分隔的每個埠，如1、3、5或GE1、GE3、GE5，也可以輸入埠範圍，如1-5或GE1-GE5。

步驟5.按一下Apply以儲存組態。

下圖顯示了將單埠安全配置應用到多個埠的情況。

