在Sx500系列堆疊式交換機上配置IP源保護繫結資料庫

目標

IP源防護是一項安全功能，可用於防止主機嘗試使用相鄰主機的IP地址時引起的流量攻擊。啟用IP Source Guard時，交換機僅將客戶端IP流量傳輸到DHCP監聽繫結資料庫中包含的IP地址。如果主機傳送的封包與資料庫中的專案相符，交換器會轉送封包。如果資料包與資料庫中的某個條目不匹配，則會丟棄該資料包。

在即時方案中，使用IP源保護的一種方式是幫助防止不受信任的第三方試圖偽裝成真正使用者的「中間人」攻擊。根據IP源保護繫結資料庫中配置的地址，僅允許來自具有該IP地址的客戶端的流量，並且丟棄其餘的資料包。

注意：應啟用DHCP監聽，IP源保護才能正常工作。有關如何啟用DHCP監聽的更多詳細資訊，請參閱*Sx500系列堆疊式交換機上的DHCP監聽繫結資料庫配置*一文。還需要配置繫結資料庫以指定允許的IP地址。

本文說明如何在Sx500系列堆疊式交換機上為IP源保護配置繫結資料庫。

適用裝置

·Sx500系列堆疊式交換器

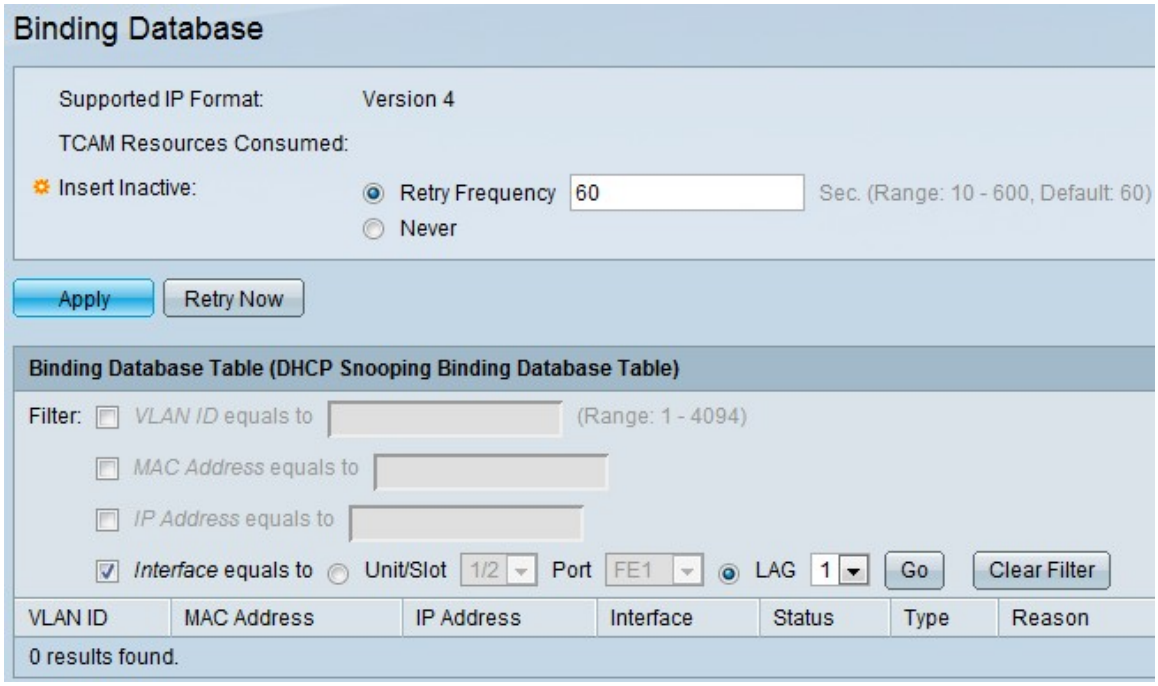
軟體版本

·v1.2.7.76

IP源保護繫結資料庫的配置

繫結資料庫

步驟1.登入到Web配置實用程式，然後選擇**Security > IP Source Guard > Binding Database**。此時將開啟「*繫結數*據庫」頁：



步驟2.從Insert Inactive欄位的以下選項中按一下相應的條目，以選擇交換機應使非活動條目處於活動狀態的頻率。DHCP監聽繫結資料庫使用三重內容可定址儲存器(TCAM)來維護資料庫。

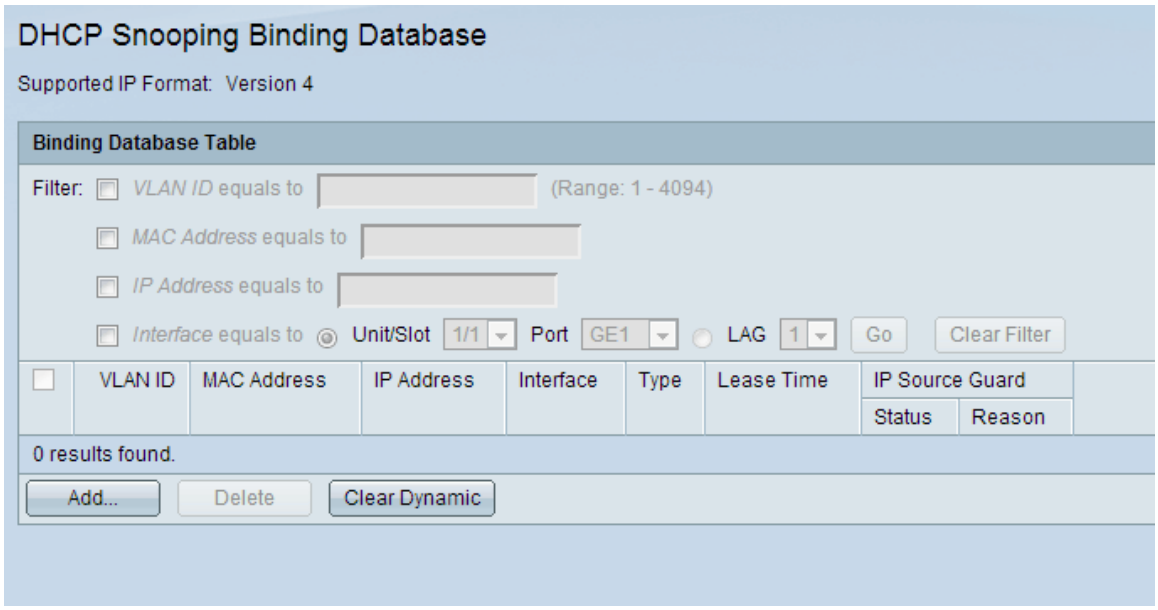
·重試頻率 — 提供檢查TCAM資源的頻率。預設值為 60。

·從不 — 從不嘗試啟用非活動地址。

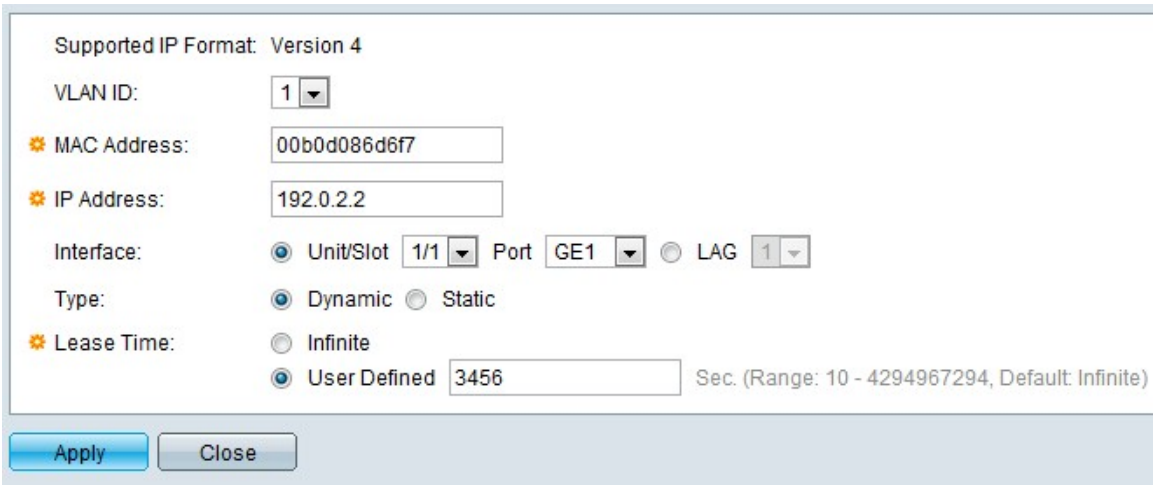
步驟3.按一下**Apply**以更新執行中的組態檔。

新增繫結資料庫條目

步驟1.登入到Web配置實用程式，然後選擇**IP Configuration > DHCP > DHCP Snooping Binding Database**，開啟「*DHCP Snooping Binding Database*」頁。



步驟2.按一下**Add**在*Add DHCP Snooping Entry*頁中輸入條目。

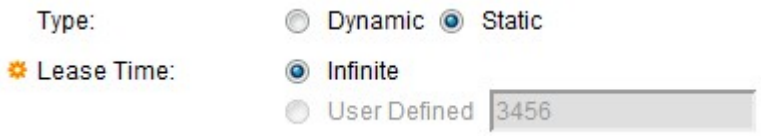


步驟3.從VLAN ID欄位中的資料包預期所在的下拉選單中選擇VLAN ID。

步驟4.在MAC Address欄位中輸入要匹配的MAC地址。

步驟5.在IP Address欄位中輸入要匹配的IP地址。

步驟6.從Interface下拉選單選擇介面，以顯示資料包預期所在的埠或LAG。

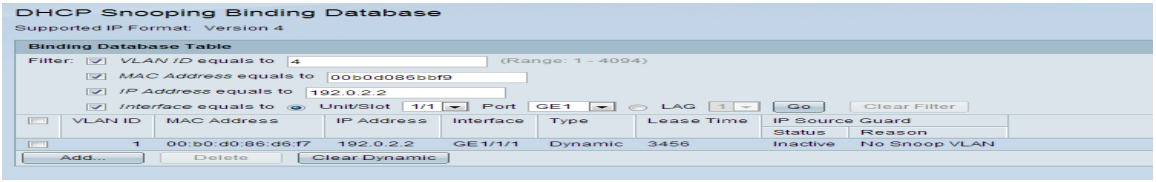


步驟7.在「型別」欄位中按一下型別以顯示條目是「動態」還是「靜態」。

·動態 — Entry的租用時間有限。

·靜態 — 靜態配置條目。

步驟8.在「租用時間」欄位中輸入租用時間。如果條目是動態的，請輸入條目保持活動狀態的持續時間。如果沒有租用時間，則按一下**Infinite**。



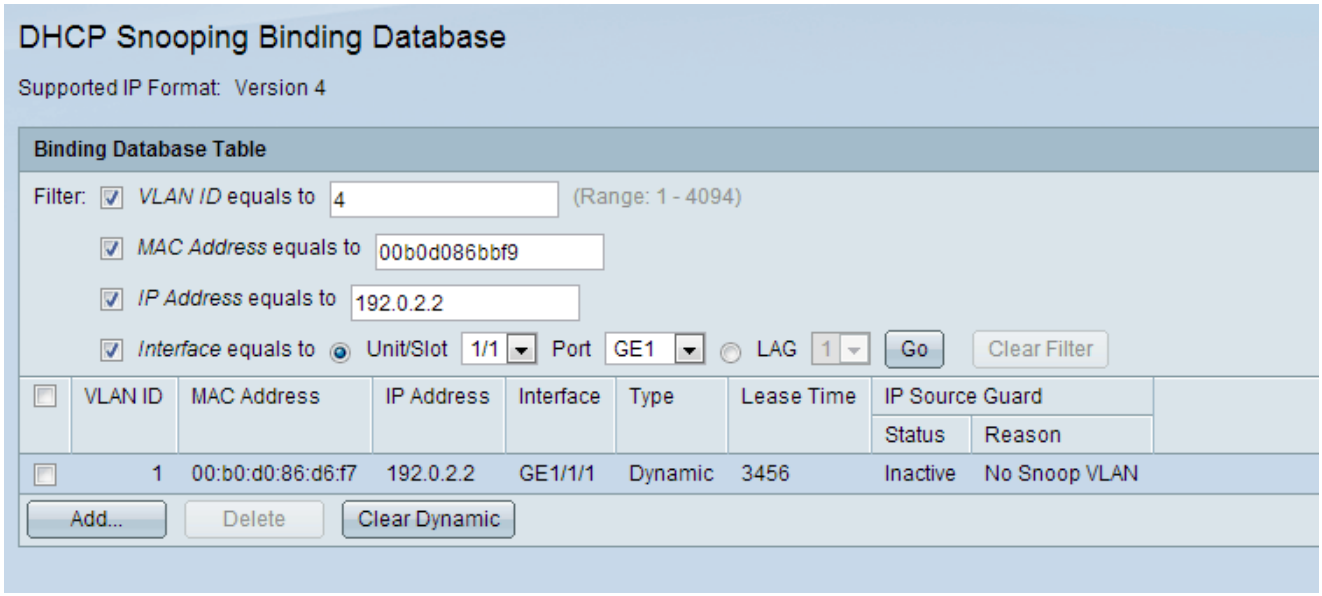
如果介面處於非活動狀態，則其原因將顯示在「原因」欄位中。原因如下：

·沒有問題 — 介面處於活動狀態。

·無監聽VLAN — VLAN上未啟用DHCP監聽。

·可信埠 — 埠是可信的。

·資源問題 — 使用TCAM資源。



步驟9.要檢視條目的子集，請在繫結資料庫表中輸入相應的搜尋條件，然後按一下**Go**。過濾器覈取方塊用於從DHCP繫結資料庫表中過濾出特定條目。

步驟10。（可選）若要移除已輸入的值並輸入新值，請按一下**清除動態**。

步驟11.按一下**Apply**以更新執行中的組態檔。