

300系列託管交換器上的位址解析通訊協定(ARP)檢查屬性組態

目標

位址解析通訊協定(ARP)用於將IP位址對應到MAC位址。ARP檢測用於保護網路免受ARP攻擊。ARP檢測通過檢查介面上的資料包來提高流量安全性，這些資料包在 *Interface Settings* (介面設定) 頁面上定義為不可信(untrusted)的介面。當資料包到達不受信任的介面時，ARP檢查會檢視資料包的源IP地址和MAC地址。如果它們與ARP訪問控制規則中的IP地址和MAC地址匹配，則轉發資料包，否則丟棄資料包。

本文介紹如何在300系列託管交換機上配置ARP檢測。

適用裝置

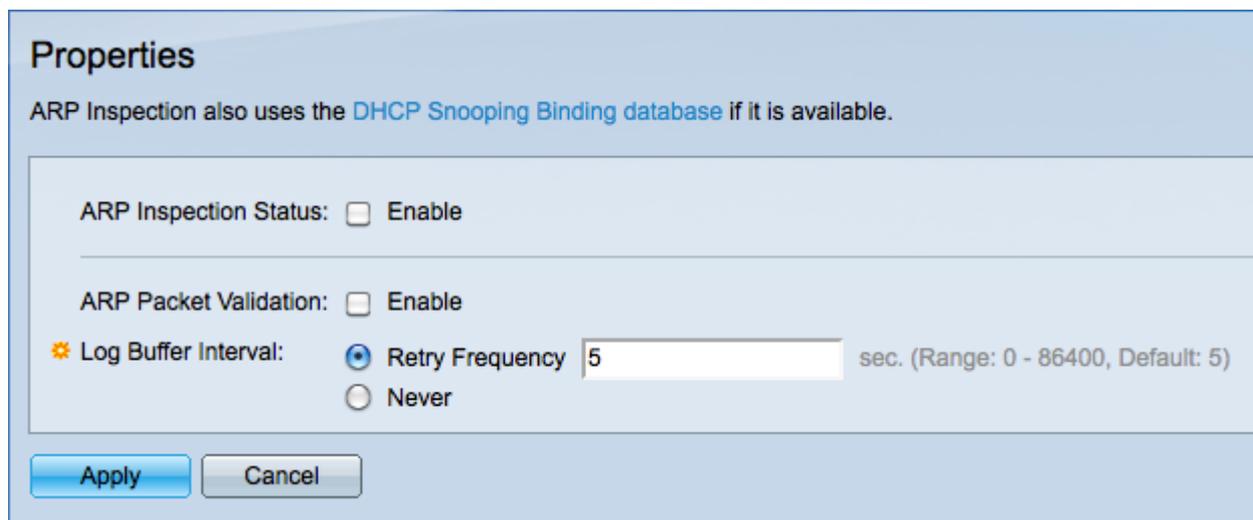
·SF/SG 300系列託管交換器

軟體版本

·1.3.0.62

屬性

步驟1. 登入到Web配置實用程式，然後選擇 **Security > ARP Inspection > Properties**。
Properties 頁面隨即開啟：



Properties

ARP Inspection also uses the [DHCP Snooping Binding database](#) if it is available.

ARP Inspection Status: Enable

ARP Packet Validation: Enable

Log Buffer Interval: Retry Frequency sec. (Range: 0 - 86400, Default: 5)
 Never

Apply Cancel

步驟2. 選中ARP Inspection Status欄位中的**Enable**覈取方塊以啟用ARP檢測。

步驟3. (可選) 選中ARP Packet Validation欄位中的**Enable**覈取方塊以啟用以下驗證。ARP檢查認為無效的資料包將被記錄並丟棄。

·來源MAC — 比較封包的來源MAC位址與ARP要求中傳送者的MAC位址。對於ARP請求和ARP響應均執行此檢查。

·目標MAC — 比較資料包的目的MAC地址與介面的目標MAC地址。此檢查僅針對ARP響應

執行。

- IP地址 — 比較ARP主體中無效IP地址。這些地址包括0.0.0.0、255.255.255.255和所有IP組播地址。

步驟4.點選與Log Buffer Interval欄位中的所需選項對應的單選按鈕。如果ARP檢查詢不到傳入資料包的源IP地址，則會丟棄該資料包，並傳送SYSLOG消息。日誌緩衝區間隔是系統日誌消息之間的時間量。

- 重試頻率 — 輸入定義傳送SYSLOG丟棄資料包消息的頻率（以秒為單位）的值。

- 從不 — 禁用SYSLOG丟棄的資料包消息。

步驟5.按一下**Apply**以儲存變更或按一下**Cancel**以撤消變更。