200/300系列託管交換機上的802.1X屬性配置

目標

802.1X IEEE標準的*屬性*頁面在200/300系列託管交換機的「安全」部分中提供了不同的身份驗證選項。802.1X IEEE標準支援基於埠的使用者身份驗證。在已啟用802.1X的指定網路中，使用者必須等待完成驗證，才能透過網路傳送資料。您可以啟用802.1X並建立埠的身份驗證方法。本文說明如何在200/300系列託管交換器上設定802.1X屬性。

適用裝置

·SF/SG 200和SF/SG 300系列託管交換器

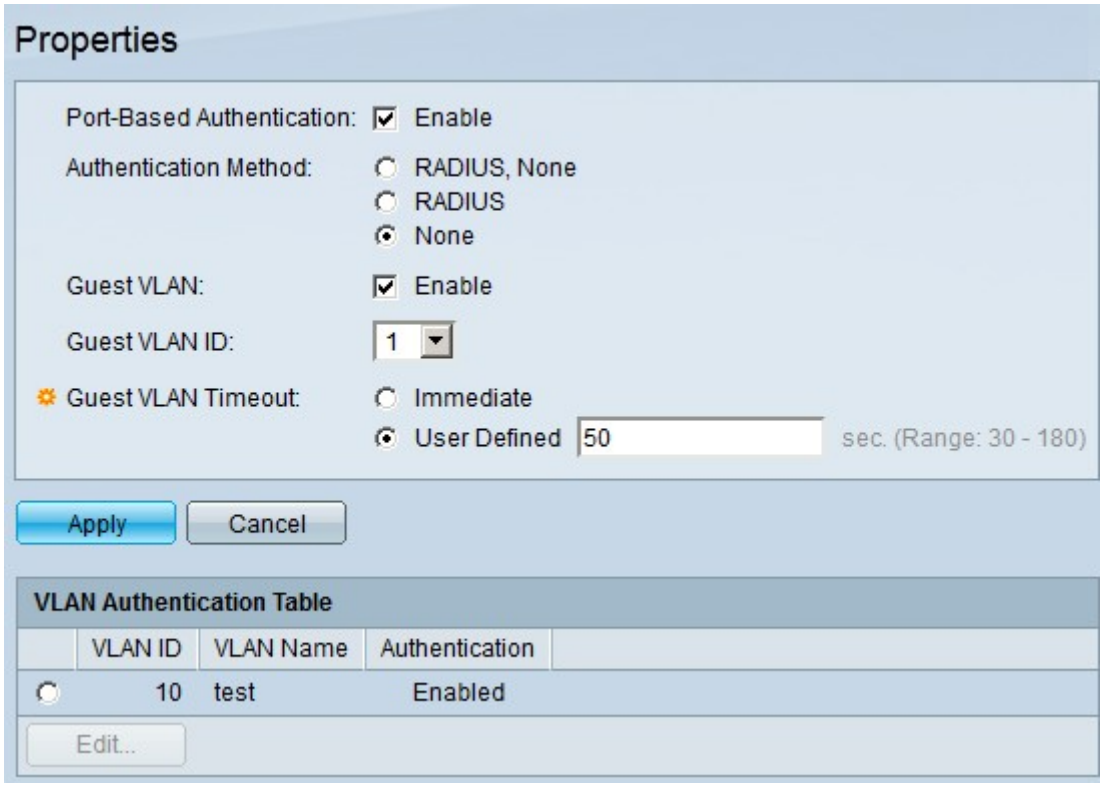
軟體版本

•3.1.0.62

802.1X屬性配置

定義802.1X屬性引數

步驟1.登入到Web配置實用程式，然後選擇**Security > 802.1X > Properties。***Properties*頁面隨即開啟：



步驟2.要啟用基於埠的802.1x身份驗證，請在Port-Based Authentication欄位中選中**Enable**。

步驟3.點選與Authentication Method欄位中所需的身份驗證方法對應的單選按鈕。可用選項包括：

·RADIUS，無 — 首先與RADIUS伺服器進行身份驗證。如果RADIUS伺服器沒有回應，則允許連線的裝置無需驗證。

·RADIUS — 僅通過RADIUS伺服器驗證使用者。如果RADIUS伺服器沒有回應，使用者會拒絕服務。

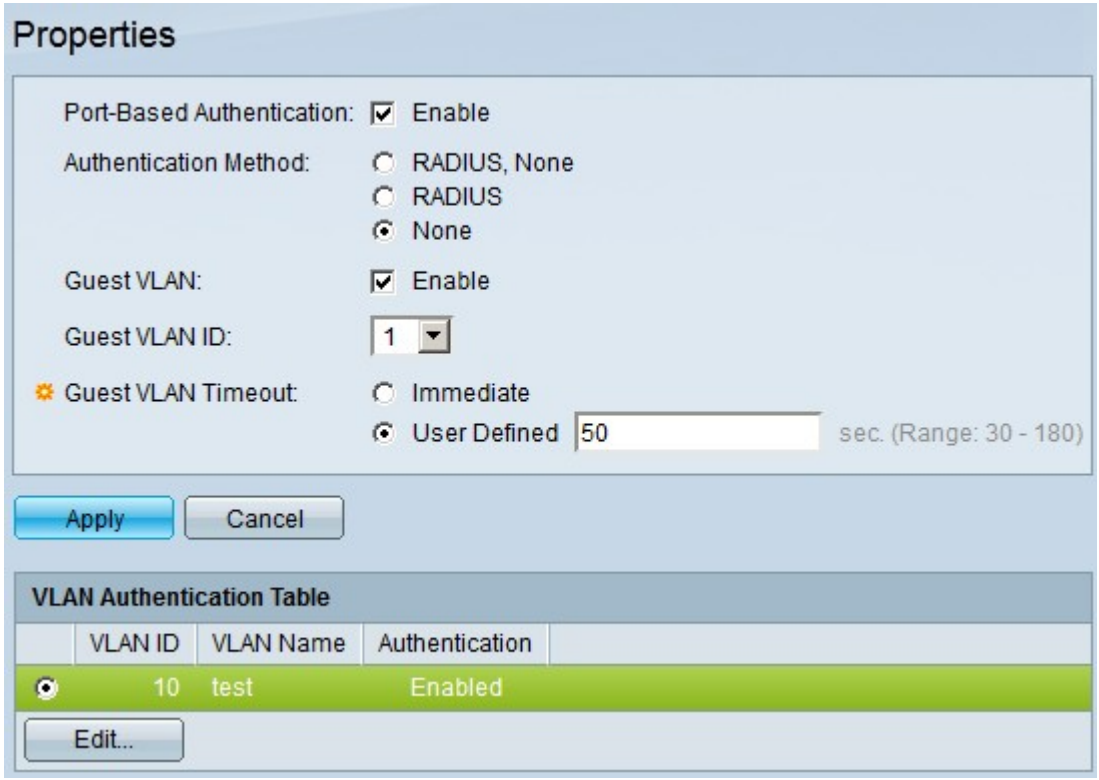
·無 — 使用者不需要身份驗證，允許所有使用者。

步驟3.按一下「**Apply**」以儲存組態。

未經驗證的VLAN配置

未經授權的連線埠不能存取VLAN，除非此VLAN是訪客VLAN。您可以對這些VLAN進行驗證。本節介紹如何在200/300系列託管交換器上驗證VLAN。

步驟1.登入到Web配置實用程式，然後選擇**Security > 802.1X > Properties。***Properties*頁面隨即開啟：



步驟2.在VLAN身份驗證表下，按一下要啟用身份驗證的VLAN的單選按鈕。

步驟3.按一下「**Edit**」。此時會顯示*「編輯」*視窗：

步驟4.在驗證欄位中，勾選**Enable**覈取方塊以在所選VLAN上啟用驗證。

步驟5.按一下「**Apply**」以儲存組態。

關於此翻譯

思科已使用電腦和人工技術翻譯本文件，讓全世界的使用者能夠以自己的語言理解支援內容。請注意，即使是最佳機器翻譯，也不如專業譯者翻譯的內容準確。Cisco Systems, Inc. 對這些翻譯的準確度概不負責，並建議一律查看原始英文文件（提供連結）。