

在Sx500系列堆疊式交換機上配置802.1x屬性

目標

IEEE 802.1x標準便於客戶端和伺服器之間的訪問控制。在LAN或交換器可以向使用者端提供服務之前，連線到交換器連線埠的使用者端必須透過執行遠端驗證撥入使用者服務 (RADIUS)的驗證伺服器進行驗證。要啟用802.1x基於埠的身份驗證，應在交換機上全域性啟用802.1x。

要完全配置802.1x，必須完成以下配置：

1. 建立VLAN，按一下[此處](#)。
2. 將埠分配給VLAN，繼續上文提到的文章。要在CLI中進行配置，請按一下[此處](#)。
3. 配置埠身份驗證，按一下[此處](#)。

本文說明如何設定802.1x屬性，包括驗證和訪客VLAN屬性。請參閱上述文章瞭解其他配置。訪客VLAN提供對服務的訪問，這些服務不要求訂閱裝置或埠通過802.1x或基於MAC的身份驗證進行身份驗證和授權。

適用裝置

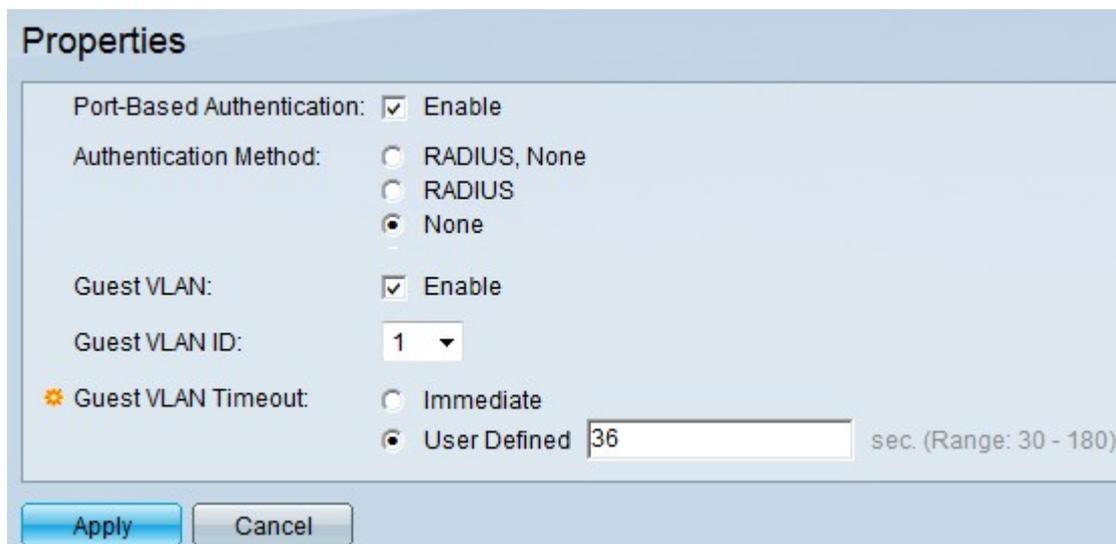
·Sx500系列堆疊式交換器

軟體版本

•1.3.0.62

在802.1x屬性中啟用基於埠的身份驗證和訪客VLAN

步驟1. 登入到Web配置實用程式以選擇Security > 802.1X > Properties。此時將開啟Properties頁：



The screenshot shows the 'Properties' configuration window for 802.1X authentication. The settings are as follows:

- Port-Based Authentication: Enable
- Authentication Method: RADIUS, None; RADIUS; None
- Guest VLAN: Enable
- Guest VLAN ID: 1 (dropdown menu)
- Guest VLAN Timeout: Immediate; User Defined 36 sec. (Range: 30 - 180)

Buttons: Apply, Cancel

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

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1

Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

步驟3.從Authentication Method欄位按一下所需的單選按鈕。RADIUS伺服器執行使用者端的驗證。此伺服器會驗證使用者是否經過驗證，並通知交換器是否允許使用者端存取LAN和其他交換器服務。交換器充當Proxy，且伺服器對使用者端是透明的。

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1

Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

- RADIUS， None — 這首先在RADIUS伺服器的幫助下執行埠身份驗證。如果沒有來自伺服器的響應（例如同伺服器關閉時），則不執行身份驗證，並且允許會話。如果伺服器可用且使用者憑據不正確，則訪問將被拒絕，會話將結束。
- RADIUS — 基於RADIUS伺服器執行埠身份驗證。如果未執行身份驗證，則會話將終止。
- 無 — 不對使用者進行身份驗證並允許會話。

步驟4. (可選) 勾選「Enable」，在「Guest VLAN」欄位中，為未經授權的連線埠啟用訪客VLAN。如果啟用了訪客VLAN，所有未授權的埠將自動加入在訪客VLAN ID欄位中選擇的VLAN。如果連線埠稍後獲得授權，則會將其從訪客VLAN中移除。

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1

☀ Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

必須先配置訪客VLAN模式，然後才能使用MAC身份驗證模式。802.1x框架使裝置（請求方）能夠向其連線的遠端裝置（驗證方）請求埠訪問。只有在請求埠訪問的請求方經過身份驗證和授權後，才允許向埠傳送資料。否則，除非將資料傳送到訪客VLAN和/或未經身份驗證的VLAN，否則身份驗證器丟棄請求方資料。

附註：訪客VLAN（如果已設定）是具有以下特性的靜態VLAN：

- 必須從現有的靜態VLAN手動定義。
- 自動僅對已連線且已啟用訪客VLAN的未授權裝置或裝置埠可用。
- 如果連線埠啟用訪客VLAN，則交換器會在連線埠未獲授權時自動將連線埠新增為訪客VLAN的無標籤成員，並在連線埠的第一個請求者獲授權時從訪客VLAN移除連線埠。
- 訪客VLAN不能同時用作語音VLAN和未經身份驗證的VLAN。

Timesaver：如果訪客VLAN已禁用，請跳至步驟7。

步驟5.從Guest VLAN ID下拉選單的VLAN清單中選擇訪客VLAN ID。

Properties

Port-Based Authentication: Enable

Authentication Method: RADIUS, None
 RADIUS
 None

Guest VLAN: Enable

Guest VLAN ID: 1

☀ Guest VLAN Timeout: Immediate
 User Defined 36 sec. (Range: 30 - 180)

Apply Cancel

步驟6.在Guest VLAN Timeout欄位中按一下所需的單選按鈕。可用的選項包括：

- 立即 — 訪客VLAN在10秒的時間段後過期。
- 使用者定義 — 在「使用者定義」欄位中輸入手動時間段。

附註：連結後，如果軟體沒有偵測802.1x要求者或連線埠驗證失敗，則只有在訪客VLAN逾時期間到期後，才會將連線埠新增到訪客VLAN。如果連線埠從「已授權」變更為「未授權」

，則只有在訪客VLAN逾時期間到期後，才會將連線埠新增到訪客VLAN。VLAN身份驗證表顯示所有VLAN並顯示是否在它們上啟用身份驗證。

步驟7. 按一下**Apply**以儲存設定。

未經驗證的VLAN配置

啟用802.1x時，除非未經授權的埠或裝置是訪客VLAN或未經身份驗證VLAN的一部分，否則不允許這些埠或裝置訪問VLAN。需要使用「埠到VLAN」頁面將埠**手動新增到VLAN**。

步驟1. 登入到Web配置實用程式以選擇**Security > 802.1X > Properties**。此時將打開「*Properties*」頁。

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
<input checked="" type="radio"/>	2	VLAN 2	Enabled
<input type="radio"/>	3	VLAN 3	Enabled

Edit..

步驟2. 向下滾動頁面到VLAN身份驗證表，按一下要禁用身份驗證的VLAN的單選按鈕，然後按一下**編輯**。**編輯VLAN驗證**頁面隨即開啟。

VLAN ID: ▼

VLAN Name: VLAN 2

Authentication: Enable

Apply **Close**

步驟3. (可選) 從VLAN ID下拉式清單中選擇VLAN ID。

VLAN ID: ▼

VLAN Name: VLAN 2

Authentication: Enable

Apply **Close**

步驟4. 取消選中**Enable**以停用驗證，並使VLAN成為未驗證的VLAN。

步驟5. 按一下**Apply**以應用設定。對VLAN身份驗證表進行更改：

VLAN Authentication Table			
	VLAN ID	VLAN Name	Authentication
<input type="radio"/>	2	VLAN 2	Disabled
<input type="radio"/>	3	VLAN 3	Enabled

Edit..