在Cisco Sx220系列智慧交換機上配置802.1X埠身 份驗證

目標

本文的目的是向您展示如何在Sx220系列智慧交換機上配置埠身份驗證。

802.1X埠身份驗證支援為裝置上的每個埠配置802.1X引數。請求身份驗證的連線埠稱為請求 方。身份驗證器是交換機或接入點,充當請求者的網路防護。驗證器將驗證訊息轉送到 RADIUS伺服器,以便連線埠可以驗證且可以傳送和接收資訊。

適用裝置

• Sx220系列

軟體版本

• 1.1.0.14

配置埠身份驗證

步驟1.登入到交換機基於Web的實用程式,然後選擇Security > 802.1X > Port Authentication。

IP Configuration		
• S	ecurity	
	TACACS+	
	RADIUS	
•	Management Access Method	
	Password Strength	
	Management Access Authentic	
	TCP/UDP Services	
	Storm Control	
	Port Security	
	802.1X	
	Properties	
	Port Authentication	
	Host and Session Authentica	
	Authenticated Hosts	
•	Denial of Service	

步驟2.點選要配置的埠的單選按鈕,然後點選Edit。

2	3	GE3	N/A	Disabled	Disabled	Disabled	Enabled
\odot		GE4	N/A	Disabled	Disabled	Disabled	Enabled
0	5	GE5	N/A	Disabled	Disabled	Disabled	Enabled
0	6	GE6	N/A	Disabled	Disabled	Disabled	Enabled
0	7	GE7	N/A	Disabled	Disabled	Disabled	Enabled
0	8	GE8	N/A	Auto	Disabled	Enabled	Enabled
0	9	GE9	N/A	Disabled	Disabled	Disabled	Enabled
0	10	GE10	N/A	Disabled	Disabled	Disabled	Enabled
0	11	GE11	N/A	Disabled	Disabled	Disabled	Enabled
\circ	12	GE12	N/A	Disabled	Disabled	Disabled	Enabled
0	13	GE13	N/A	Disabled	Disabled	Disabled	Enabled
0	14	GE14	N/A	Disabled	Disabled	Disabled	Enabled
0	15	GE15	N/A	Disabled	Disabled	Disabled	Enabled
0	16	GE16	N/A	Disabled	Disabled	Disabled	Enabled
0	17	GE17	N/A	Disabled	Disabled	Disabled	Enabled
0	18	GE18	N/A	Disabled	Disabled	Disabled	Enabled
0	19	GE19	N/A	Disabled	Disabled	Disabled	Enabled
0	20	GE20	N/A	Disabled	Disabled	Disabled	Enabled
0	21	GE21	N/A	Disabled	Disabled	Disabled	Enabled
0	22	GE22	N/A	Disabled	Disabled	Disabled	Enabled
0	23	GE23	N/A	Disabled	Disabled	Disabled	Enabled
0	24	GE24	N/A	Disabled	Disabled	Disabled	Enabled
0	25	GE25	N/A	Disabled	Disabled	Disabled	Enabled
\bigcirc	26	GE26	N/A	Disabled	Disabled	Disabled	Enabled
	Copy Set	tings	Edi	t			

附註:在本例中,選擇了埠GE4。

步驟3. Edit Port Authentication視窗隨後將彈出。從Interface下拉選單中,確保指定的埠是您 在第2步中選擇的埠。否則,按一下下拉箭頭並選擇正確的埠。

Interface:	Port GE4 🔻
Administrative Port Control:	 Disabled Force Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	 Disabled Reject Static
Guest VLAN:	Enable

步驟4.選擇管理埠控制的單選按鈕。這將確定埠授權狀態。選項包括:

- •已禁用 禁用802.1X。這是預設狀態。
- ・強制未授權 通過將介面移至未授權狀態來拒絕介面訪問。交換機不通過介面向客戶端 提供身份驗證服務。
- 自動 在交換機上啟用基於埠的身份驗證和授權。根據交換機和客戶端之間的身份驗證 交換,該介面在已授權或未授權狀態之間移動。
- 強制授權 未經驗證即授權介面。

Interface:	Port GE4 V
Administrative Port Control:	Disabled Eorce Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	 Disabled Reject Static
Guest VLAN:	Enable

附註:在本示例中,選擇了Auto。

步驟5.(可選)選擇RADIUS VLAN分配的單選按鈕。這將啟用指定埠上的動態VLAN分配。 選項包括:

- •已禁用 忽略VLAN授權結果並保留主機的原始VLAN。這是預設操作。
- 拒絕 如果指定的埠收到VLAN授權資訊,它將使用該資訊。但是,如果沒有VLAN授權 資訊,則會拒絕主機並使其未授權。
- •靜態 如果指定的埠收到VLAN授權資訊,它將使用該資訊。但是,如果沒有VLAN授權 資訊,它將保留主機的原始VLAN。

附註:如果存在來自RADIUS的VLAN授權資訊,但是未在測試裝置(DUT)上管理性建立 VLAN,則會自動建立VLAN。在此示例中,選擇了Static。

Interface:	Port GE4 🔻
Administrative Port Control:	 Disabled Force Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	Disabled Reject Static
Guest VLAN:	Enable

快速提示:要使動態VLAN分配功能正常工作,交換機需要由RADIUS伺服器傳送以下VLAN屬 性:

- [64] Tunnel-Type = VLAN(型別13)
- [65] Tunnel-Medium-Type = 802(型別6)
- [81] Tunnel-Private-Group-Id = VLAN ID

步驟6.(可選)勾選Enable覈取方塊,使訪客VLAN將訪客VLAN用於未授權的埠。

Interface:	Port GE4 🔻
Administrative Port Control:	 Disabled Force Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	 Disabled Reject Static
Guest VLAN:	💌 Enable

步驟7.選中Enable覈取方塊以定期重新驗證。這將啟用在指定的重新身份驗證時間段後埠重新 身份驗證嘗試。



附註:此功能預設啟用。

步驟8.在*Reauthentication Period*欄位中輸入值。這是重新驗證連線埠的時間(以秒為單位)。

Interface:	Port GE4 🔻
Administrative Port Control:	 Disabled Force Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	 Disabled Reject Static
Guest VLAN:	Enable
Periodic Reauthentication:	Enable
Reauthentication Period:	3600
Reauthenticate Now:	

附註:在此範例中,使用預設值3600。

步驟9.(可選)選中Reauthenticate Now覈取方塊以啟用立即埠重新身份驗證。

附註:Authenticator State欄位顯示身份驗證的當前狀態。

Interface:	Port GE4 V
Administrative Port Control:	 Disabled Force Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	 Disabled Reject Static
Guest VLAN:	Enable
Periodic Reauthentication:	Enable
Reauthentication Period:	3600
Reauthenticate Now:	
Authenticator State:	N/A

附註:如果埠未處於Force Authorized或Force Unauthorized狀態,則該埠處於Auto Mode並 且驗證器顯示正在進行的驗證狀態。連線埠通過驗證後,狀態顯示為「Authenticated」。

步驟10.在*Max Hosts*欄位中,輸入特定連線埠上允許的最大驗證主機數量。該值僅在多會話 模式下生效。

Interface:	Port GE4 V
Administrative Port Control:	 Disabled Force Unauthorized Auto Force Authorized
RADIUS VLAN Assignment:	 Disabled Reject Static
Guest VLAN:	Enable
Periodic Reauthentication:	Enable
Reauthentication Period:	3600
Reauthenticate Now:	•
Authenticator State:	N/A
Max Hosts:	256

附註:在此範例中,使用預設值256。

步驟11.在Quiet Period欄位中,輸入交換器在驗證交換失敗後保持安靜狀態的秒數。當交換機處於安靜狀態時,這意味著交換機沒有偵聽來自客戶端的新身份驗證請求。

Reauthentication Period:	3600
Reauthenticate Now:	
Authenticator State:	N/A
Max Hosts:	256
Quiet Period:	60

附註:在本示例中,使用預設值60。

步驟12.在*重發EAP*欄位中,輸入交換機在重新傳送請求之前等待請求方(客戶端)對可擴展 身份驗證協定(EAP)請求或身份幀的響應的秒數。

Reauthentication Period:	3600
Reauthenticate Now:	
Authenticator State:	N/A
Max Hosts:	256
Quiet Period:	60
Resending EAP:	30

附註:在此範例中,使用預設值30。

步驟13.在*Max EAP Requests*欄位中,輸入可以傳送的最大EAP請求數。如果在定義的時間段 (請求方超時)之後未收到響應,身份驗證過程將重新啟動。

Reauthentication Period:	3600
Reauthenticate Now:	v
Authenticator State:	N/A
Max Hosts:	256
Quiet Period:	60
Resending EAP:	30
Max EAP Requests:	2

附註:在此範例中,使用預設值2。

步驟14.在Supplicant Timeout欄位中,輸入將EAP請求重新傳送到請求方之前的秒數。

Max Hosts:	256
Quiet Period:	60
Resending EAP:	30
Max EAP Requests:	2
Supplicant Timeout:	30

附註:在此範例中,使用預設值30。

步驟15.在Server Timeout欄位中,輸入交換器將要求重新傳送到驗證伺服器之前經過的秒數

Max Hosts:	256
Quiet Period:	60
Resending EAP:	30
Max EAP Requests:	2
Supplicant Timeout:	30
Server Timeout:	30
Apply Close	

附註:在此範例中,使用預設值30。

步驟16.按一下Apply。

o

現在,您應該在交換機上成功配置埠身份驗證。