交換機術語表

目標

本文包含用於設定、配置和排除Cisco Small Business交換機故障的術語清單。

適用裝置

- Sx200系列
- Sx250系列
- Sx300系列
- Sx350系列
- SG300X系列
- Sx500 系列
- Sx550X系列

術語清單

- 802.1X Supplicant客戶端 — Supplicant客戶端是802.1X IEEE標準的三個角色之一。802.1X的開發目的是在OSI模型的第2層提供安全保護。它由以下元件組成：Supplicant客戶端、Authenticator和Authentication Server。Supplicant客戶端是連線到網路以便訪問該網路上的資源的客戶端或軟體。它需要提供憑證或憑證以取得IP位址，並成為該特定網路的一部分。請求方在經過身份驗證之前不能訪問網路的資源。
- ACL — 訪問控制清單(ACL)是網路流量過濾器和相關操作的清單，用於提高安全性。它阻止或允許使用者訪問特定資源。ACL包含允許或拒絕訪問網路裝置的主機。路由器或交換器會根據存取清單中的指定條件，檢查每個封包以確定轉送或捨棄封包。訪問清單條件可以是流量的源地址、流量的目的地址、上層協定或其他資訊。
- IGMP窺探 — 網際網路群組管理通訊協定(IGMP)是一種在交換器上執行的通訊協定，允許交換器動態得知多點傳播流量。IGMP偵聽是一種功能，允許網路交換機偵聽主機和路由器之間的IGMP會話。IGMP偵聽執行在路由器中啟用的過濾機制，以便僅將組的多播流量轉發到已加入組的埠。因此，通過IGMP監聽，網路上的流量會減少，並且可以提高路由器後主機的效能。組播可以從不需要組播的鏈路中過濾出來。

- IPv4 - IPv4是用於識別網路中裝置的32位元定址系統。它是大多數電腦網路（包括Internet）中使用的編址系統。

- IPv6 — IPv6是用於識別網路中裝置的128位編址系統。它是IPv4的後繼路由器和電腦網路中使用的最新版本定址系統。IPv6目前正在全球推廣。IPv6地址由八個十六進位制數字欄位表示，每個欄位包含16位。IPv6地址分為兩部分，每部分由64位組成。第一部分是網路地址，第二部分是主機地址。

- 連結翻動 — 連結翻動是指交換器上的實體介面不斷開啟和關閉、每秒三次或以上，持續至少10秒的情況。常見原因通常與電纜故障、不受支援或非標準、小型封裝熱插拔(SFP)或其他鏈路同步問題有關。鏈路抖動的原因可能是間歇性的或永久性的。

- MAC型ACL — 媒體存取控制(MAC)型存取控制清單(ACL)是來源MAC位址的清單。如果封包從無線存取點傳至區域網路(LAN)連線埠，或反之亦然，則此裝置會檢查封包的來源MAC位址是否與清單中的任何專案相符，並檢查ACL規則與框架的內容是否相符。然後，它使用匹配的結果來允許或拒絕此資料包。但是，將不會檢查從LAN到LAN埠的資料包。

- MLD窺探 — 多點傳送是一種網路層技術，用於將資料封包從一台主機傳送到群組中的選定主機。在較低層，交換機在所有埠上廣播組播流量，即使只有一台主機希望接收該流量。組播偵聽程式發現(MLD)監聽用於將IPv6組播流量僅轉發到所需主機。當交換機上啟用MLD監聽時，它會檢測IPv6路由器與介面上連線的組播主機之間交換的MLD消息。然後，它維護一個限制IPv6組播流量的表，並將其動態轉發到要接收該流量的埠。

- MSTP — 多生成樹協定(MSTP)是一種協定，可為單個物理網路上的每個虛擬LAN(VLAN)建立多個生成樹（例項）。這允許每個VLAN具有已配置的根網橋和轉發拓撲。這減少了整個網路中的橋接通訊協定資料單元(BPDU)數量，並減輕了網路裝置中央處理單元(CPU)的壓力。

- 埠/VLAN映象 — 映象是監控網路流量的一種方法。使用埠或VLAN映象時，網路裝置埠（源埠）上的傳入和傳出資料包的副本會被轉發到另一個埠（目標埠），在此會研究資料包。網路管理員將此工具用作診斷工具。

- 埠安全 — 配置埠安全是增強網路安全的一種方式。它可以在特定埠或鏈路聚合組(LAG)上配置。LAG將單個介面合併到單個邏輯鏈路中，可提供最多八個物理鏈路的聚合頻寬。您可以限制或允許對給定埠/LAG上的不同使用者的訪問。連線埠資安也可搭配動態學習及靜態MAC位址使用，以限制連線埠的輸入流量。

- 基於協定的VLAN — 可以定義基於協定的組並將其繫結到埠；因此，源自協定組的每個資料包都會分配到頁面上配置的VLAN。基於協定的VLAN將物理網路劃分為每個所需協定的邏輯VLAN組。在入站資料包中，將檢查幀，並根據協定型別確定VLAN成員資格。基於協定的組到VLAN的對映有助於將協定組對映到單個埠。

- QoS — 服務品質(QoS)允許您為不同的應用程式、使用者或資料流確定流量的優先順序。它還可以用來保證效能達到指定的水準，從而影響客戶的服務品質。QoS通常受以下因素影響：抖動、延遲和丟包。

- RADIUS伺服器 — 遠端驗證撥入使用者服務(RADIUS)是一種用於連線和使用網路服務的裝置的驗證機制。用於集中身份驗證、授權和記帳。RADIUS伺服器透過輸入的登入憑證驗證使用者的身分，以調控網路的存取。例如，在大學校園中安裝了公共Wi-Fi網路。只有那些擁有密

碼的學生才能訪問這些網路。RADIUS伺服器會檢查使用者輸入的密碼，並在適當情況下授權或拒絕存取。

- RSTP — 快速生成樹協定(RSTP)是STP的增強功能。RSTP在拓撲更改後提供更快的生成樹收斂。STP可能需要30到50秒來響應拓撲更改，而RSTP在配置的Hello時間的3倍之內做出響應。RSTP向後相容STP。

- SNMP — 簡單網路管理協定(SNMP)是儲存和共用有關網路裝置資訊的網路標準。SNMP可促進網路管理、疑難排解和維護。

- 生成樹 — 生成樹協定(STP)是在區域網(LAN)上使用的網路協定。STP的目的是確保LAN無環路拓撲。STP通過一種演算法消除環路，該演算法保證兩個網路裝置之間只有一個活動路徑。STP可確保流量在網路中採用儘可能最短路徑。如果活動路徑出現故障，STP還可以自動重新啟用冗餘路徑作為備份路徑。

- SSL伺服器 — 安全套接字層(SSL)是一種協定，主要用於網際網路上的安全管理。它使用位於HTTP層和TCP層之間的程式層。對於身份驗證，SSL使用經過數位簽章並繫結到公鑰的證書來標識私鑰所有者。此身份驗證在連線期間會有所幫助。通過使用SSL，證書在驗證過程中以塊形式交換，其格式在ITU-T標準X.509中描述。然後，由外部的認證機構簽發數位簽章的X.509證書。

- Syslog Aggregation — 系統日誌服務僅接受消息，並將其儲存在檔案中，或根據簡單配置檔案列印這些消息。Syslog Aggregation表示每次發生例項時，螢幕上不會顯示多個相同型別的系統日誌消息。啟用日誌記錄聚合允許您過濾在特定時間段內將接收的系統消息。它會收集一些相同型別的系統日誌消息，因此這些消息在出現時不會顯示，而是以指定時間間隔顯示。

- TACACS+ — 終端存取控制器存取控制系統(TACACS+)是思科專有通訊協定，用於透過使用者名稱和密碼提供驗證和授權來實作增強型資安。要配置TACACS+伺服器，使用者必須具有15個訪問許可權，該訪問許可權允許使用者訪問交換機的所有配置功能。某些交換器可以充當TACACS+使用者端，所有連線的使用者均可以透過正確設定的TACACS+伺服器進行網路中的驗證和授權。TACACS+僅支援IPv4。

- TFTP伺服器 — 簡單式檔案傳輸協定(TFTP)伺服器是用於在LAN上的裝置之間自動傳輸配置和引導檔案的伺服器。協定非常簡單，允許低記憶體使用；但是，這種簡單性也允許協定很容易受到危害。因此，TFTP很少用於Internet。

- VLAN — 虛擬區域網(VLAN)是一種交換網路，它按功能、區域或應用進行邏輯分段，而不考慮使用者的物理位置。VLAN是一組主機或埠，它們可以位於網路中的任何位置，但進行通訊的方式就像它們位於同一個物理網段上一樣。VLAN允許您在不更改任何物理連線的情況下將裝置移動到新的VLAN，從而有助於簡化網路管理。

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）。