Cisco Business 路由器的 VLAN 最佳作法和安全秘訣

目標

本文的宗旨在於說明在 Cisco Business 設備上設定 VLAN 時，執行最佳作法和安全秘訣的概念和步驟。

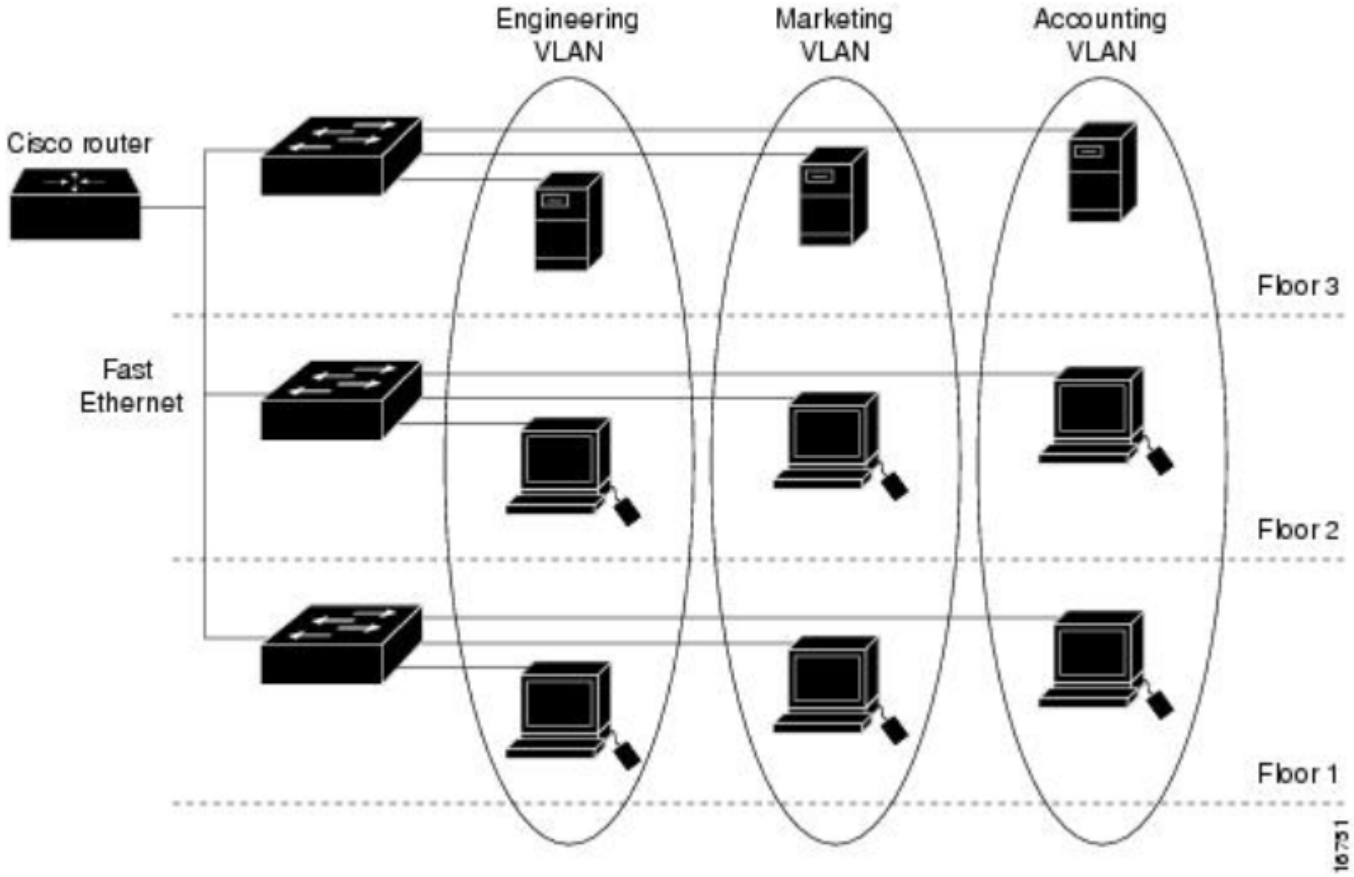
目錄

簡介

希望提高企業網路的效率，同時保證其安全？正確設定虛擬區域網路(VLAN)是其中一種方式。

VLAN是一組工作站、伺服器和網路裝置組成的邏輯組，它們看似位於同一個區域網(LAN)上，儘管它們處於地理分佈狀態。簡而言之，同一VLAN上的硬體可使裝置之間的流量保持獨立，並且更加安全。

例如，您可能有一個工程、市場行銷和會計部門。每個部門都有員工在建築的不同樓層，但他們仍然需要訪問和交流各自部門內的資訊。這對於共用文檔和Web服務至關重要。



VLAN需要設定最佳實踐，以確保網路安全。設定VLAN時做出以下明智選擇。你不會後悔的！

適用裝置

- RV042
- RV110W
- RV130
- RV132
- RV134W
- RV160W
- RV215W
- RV260
- RV260P
- RV260W
- RV320
- RV325
- RV340
- RV340W
- RV345
- RV345P

您可能感興趣的是，RV160或RV260系列路由器最多可以承載16個VLAN，而RV34x系列路由器最多可以承載32個VLAN。RV320最多支援7個VLAN。如果您想瞭解路由器可承載的VLAN數量，請檢視 Cisco Website上您特定型號的資料表。選擇 **支援**並輸入您的型號，或者只搜尋資料表和型號。

紐伯斯的幾個快速辭彙

接入埠：接入埠只傳輸一個VLAN的流量。存取連線埠通常稱為無標籤連線埠，因為此連線埠上只

有一個VLAN，且流量可以無標籤通過。

中繼埠：交換機上承載多個VLAN流量的埠。主干連線埠通常稱為標籤連線埠，因為此連線埠上有多個VLAN，且除一個VLAN外，所有流量的連線埠都需要標籤。

本徵VLAN:中繼埠中一個沒有接收標籤的VLAN。所有沒有標籤的流量都將傳送到本徵VLAN。因此，中繼的兩端都需要確保它們具有相同的本徵VLAN，否則流量將不會到達正確位置。

最佳實踐#1法 — VLAN埠分配

埠分配基礎知識

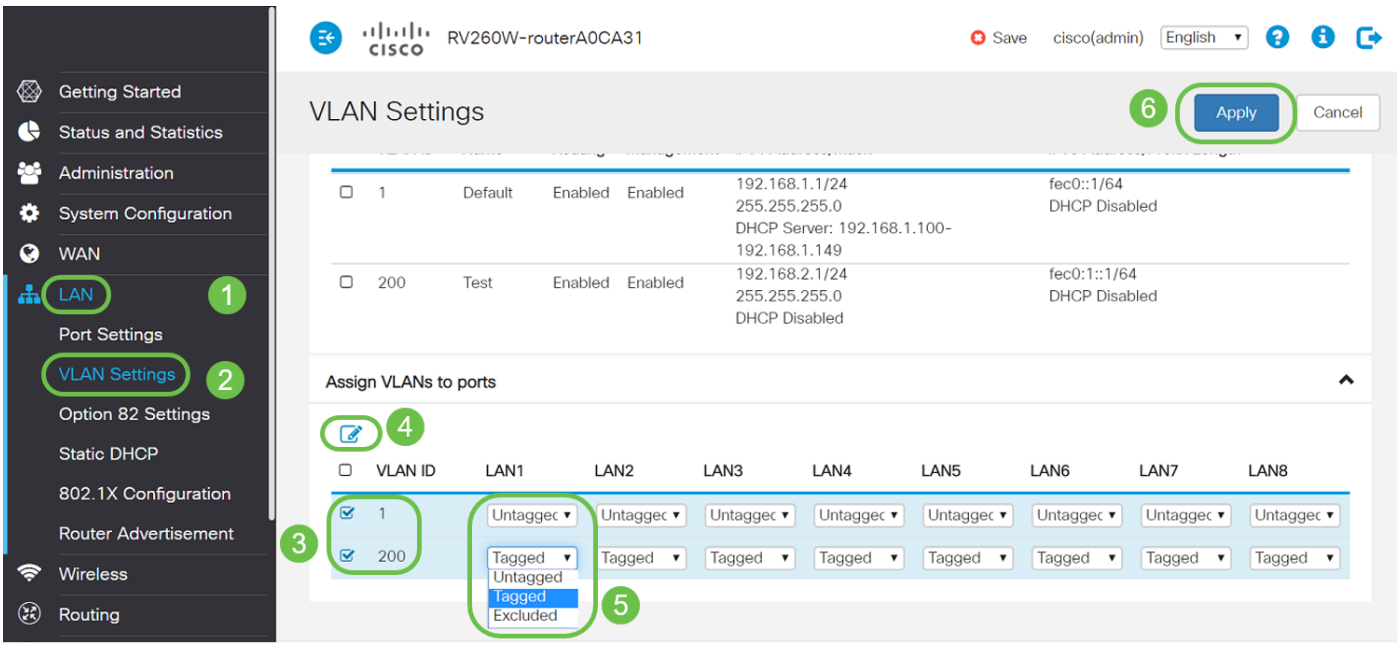
- 每個LAN埠都可以設定為接入埠或中繼埠。
- 不應包含在中繼上的VLAN。
- VLAN可以置於多個埠中。

配置接入埠

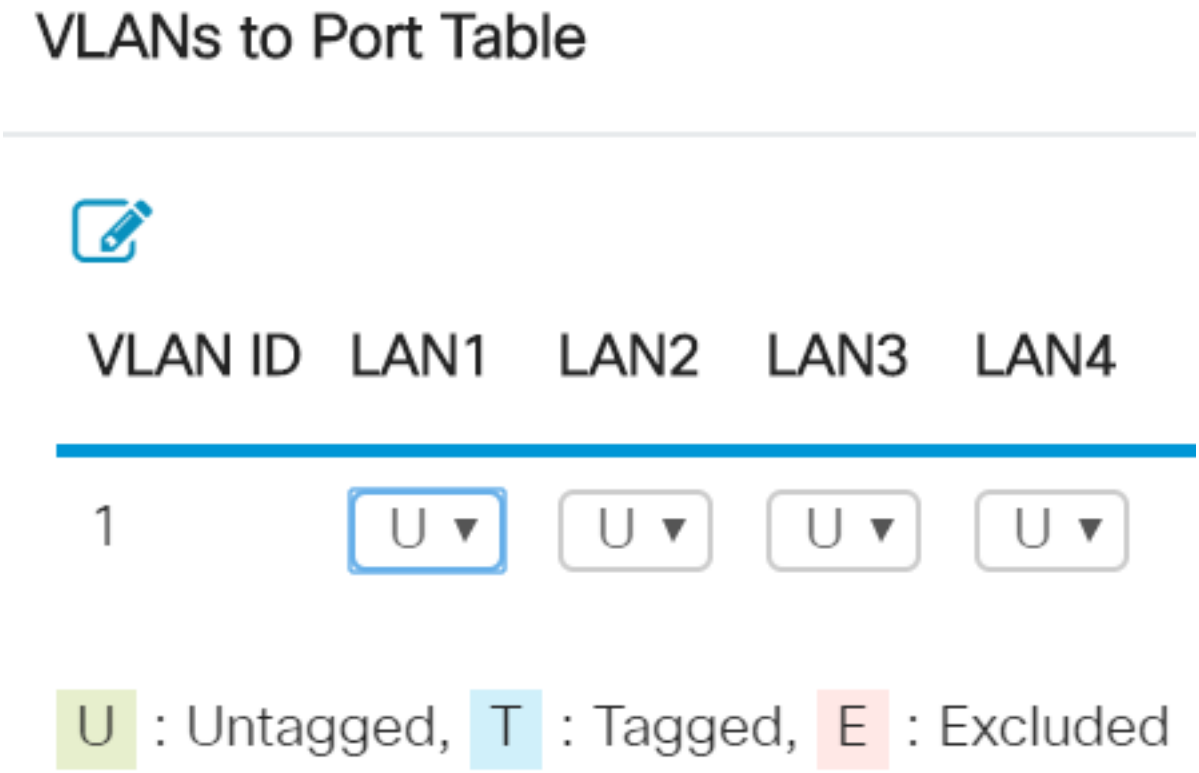
- 在LAN埠上分配一個VLAN
- 分配到此埠的VLAN應標籤為*Untagged*
- 該埠的所有其他VLAN都應標籤為*Excluded*

若要正確設定這些設定，請導覽至**LAN > VLAN Settings**。選擇*VLAN ID*，然後按一下**edit**圖示。選擇列出的VLAN的任何LAN介面的下拉選單，以編輯VLAN標籤。按一下「**Apply**」。

檢視每個指派了自己的LAN連線埠的VLAN的以下範例：



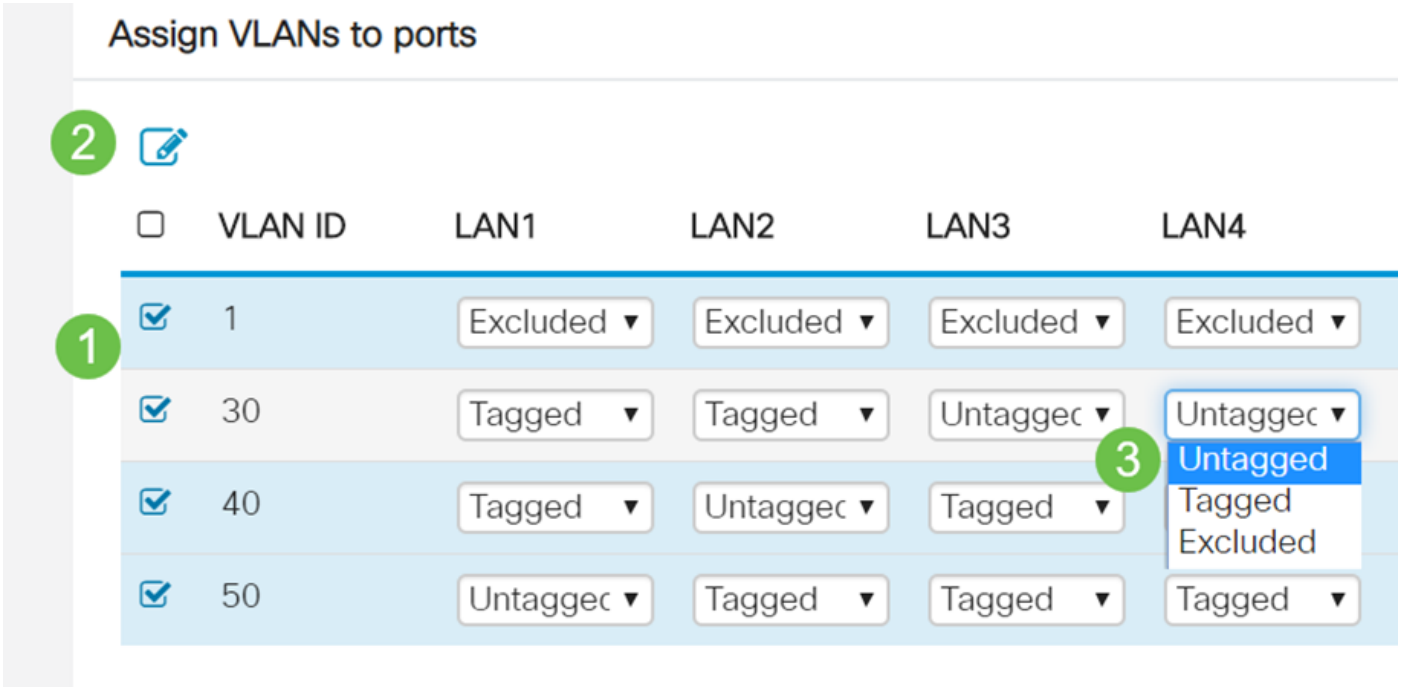
此圖形使用者介面(GUI)映像來自RV260W路由器。您的選項可能會略有不同。例如，在RV34x系列中，標籤 *Untagged*、 *Excluded*和 *Tagged*縮寫為第一個字母。這個過程還是一樣。



配置中繼埠

- 兩個或多個VLAN共用一個LAN連線埠
- 其中一個VLAN可以標籤為*Untagged*。
- 中繼埠中的其餘VLAN應標籤為*Tagged*。
- 不屬於中繼埠的VLAN應為該埠標籤為*Excluded*。

請看一下中繼埠上所有各種VLAN的示例。要正確設定這些值，請*選擇需*要編輯的*VLAN ID*。單擊*edit*圖示。按照上述建議並根據您的需求進行更改。另外，您是否注意到VLAN 1從每個LAN埠中排除？這將在預設VLAN 1的最佳實踐一節中說明。



常見問題

如果VLAN是該埠上唯一的VLAN，為什麼它保持未標籤狀態？

由於一個接入埠上只分配了一個VLAN，因此來自該埠的傳出流量會在幀上不帶有任何VLAN標籤的情況下傳送。當幀到達交換機埠（傳入流量）時，交換機將新增VLAN標籤。

當VLAN作為TRUNK的一部分時，為什麼會對其進行標籤？

這樣做是為了使通過的流量不會傳送到該連線埠上的錯誤VLAN。VLAN共用該埠。類似於新增到地址中的公寓號，目的是確保郵件傳送到共用建築中的正確公寓。

當流量是本徵VLAN的一部分時，為什麼它保持未標籤狀態？

本徵VLAN是一種通過一台或多台交換機傳輸未標籤流量的方式。交換機將到達帶標籤埠的任何未標籤幀分配給本徵VLAN。如果本徵VLAN上的幀離開中繼（已標籤）埠，交換機將剝離VLAN標籤。

為什麼VLAN不在此連線埠上時被排除？

這會保留該主幹上的流量僅針對使用者特別想要的VLAN。這被認為是一種最佳做法。

最佳實踐#2法 — 預設VLAN 1和未使用的埠

所有埠都需要分配給一個或多個VLAN，包括本徵VLAN。預設情況下，思科企業路由器會將VLAN 1分配給所有埠。

管理VLAN是使用Telnet、SSH、SNMP、系統日誌或思科的FindIT來遠端管理、控制和監控您網路中的裝置的VLAN。預設情況下，這也是VLAN 1。良好的安全做法是將管理和使用者資料流量分開。因此，建議在配置VLAN時，僅將VLAN 1用於管理目的。

要出於管理目的與Cisco交換機進行遠端通訊，交換機必須在管理VLAN上配置IP地址。其他VLAN中的使用者無法建立到交換機的遠端訪問會話，除非他們被路由到管理VLAN中，這提供了額外的安全層。此外，交換機應配置為僅接受加密的SSH會話以進行遠端管理。要閱讀有關此主題的一些討論，請點選思科社群網站上的以下連結：

- 管理VLAN討論#1
- 管理VLAN討論#2

常見問題

為什麼不建議使用預設VLAN 1對網路進行虛擬分段？

主要原因是敵對各方知道VLAN 1是預設的，並且經常使用。它們可以通過「VLAN跳躍」來訪問其他VLAN。顧名思義，惡意攻擊者可能會傳送偽裝為VLAN 1的欺騙流量，從而允許訪問中繼埠和其他VLAN。

是否可以將未使用的埠分配給預設VLAN 1?

為了保證網路安全，您不應該這樣做。建議將所有這些埠配置為與預設VLAN 1以外的VLAN關聯。

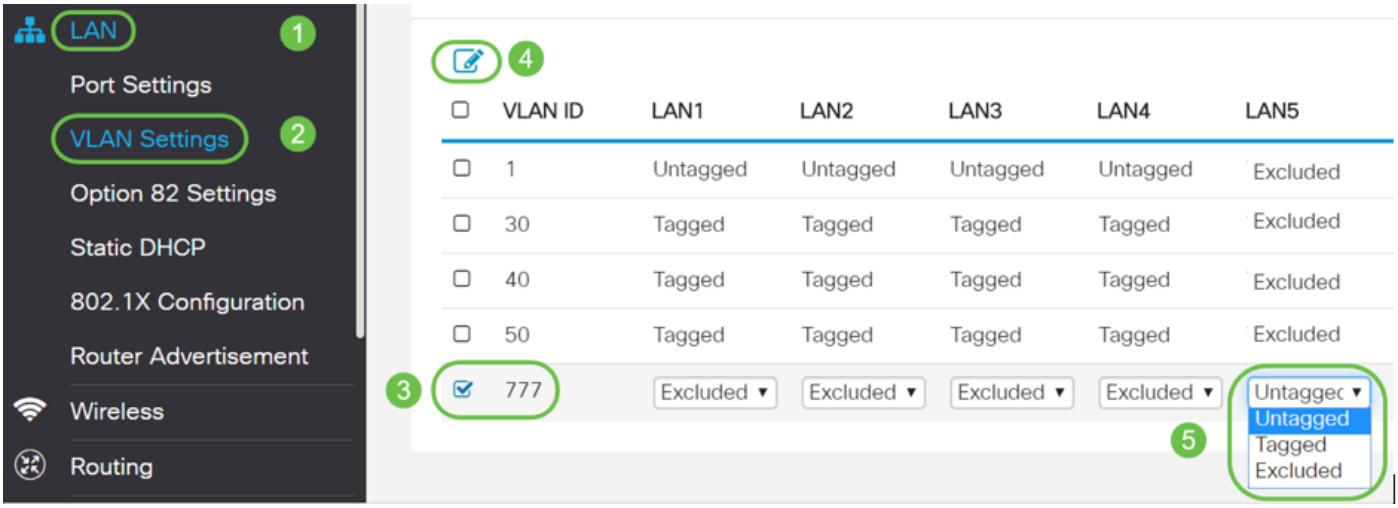
我不想將我的任何生產VLAN分配給未使用的埠。我能做什麼？

建議您按照本文下一節中的說明建立「死端」VLAN。

最佳實#3指南 — 為未使用的埠建立「死端」VLAN

步驟1.導覽至**LAN > VLAN Settings**。

為VLAN選擇任意隨機數。請確保此VLAN未啟用DHCP、VLAN間路由或裝置管理。這樣可讓其他VLAN更加安全。將所有未使用的LAN埠放到此VLAN上。在以下示例中，建立了*VLAN 777*並將其分配給*LAN5*。這應該在所有未使用的LAN埠上完成。



請注意，此LAN連線埠不包含其他VLAN。

步驟2. **按一下***Apply*按鈕以儲存變更的組態。

最佳實#4指南 — VLAN上的IP電話

語音流量具有嚴格的服務品質(QoS)要求。如果您的公司在同一個VLAN中有電腦和IP電話，則每個都嘗試使用可用頻寬，而不考慮其他裝置。為避免此衝突，最好為IP電話語音流量和資料流量使用單獨的VLAN。要瞭解有關此配置的詳細資訊，請查閱以下文章和影片：

- 思科技術演講：使用思科S系列產品設定和配置語音VLAN（影片）
- 在SG500系列交換機上配置具有QoS的自動語音VLAN
- 200/300系列託管交換器上的語音VLAN組態
- 思科技術演講：在SG350和SG550系列交換機上配置自動語音VLAN（影片）

最佳實#5指南 — VLAN間路由

設定VLAN是為了使流量可以分開，但有時您需要VLAN才能在彼此之間路由。這是VLAN間路由，通常不推薦。如果貴公司需要這種設定，請儘可能安全地設定它。使用VLAN間路由時，請確保使用存取控制清單(ACL)將流量限制到包含機密資訊的伺服器。

ACL會執行封包過濾，以控制封包在網路中的移動。資料包過濾通過限制流量訪問網路、限制使用者和裝置訪問網路以及防止流量離開網路來提供安全性。IP訪問清單可降低欺騙和拒絕服務攻擊的可能性，並允許通過防火牆進行動態、臨時的使用者訪問。

- 帶有目標ACL限制的RV34x路由器上的VLAN間路由
- 思科技術演講：在SG250系列交換機上配置VLAN間路由（影片）
- 思科技術演講：RV180和RV180W上的VLAN間配置(影片)
- RV34x VLAN間存取限制(CSCvo92300錯誤修正)

結論

現在您已經瞭解了一些設定安全VLAN的最佳實踐。為網路配置VLAN時，請記住這些提示。下面列出了一些具有逐步說明的專案。這些功能將助您實現高效且適合您企業的網路。

- 在RV160和RV260上配置VLAN設定
- 在RV34x系列路由器上配置虛擬區域網(VLAN)設定
- 在RV320和RV325 VPN路由器上配置VLAN成員身份
- 在RV系列路由器上配置虛擬區域網(VLAN)成員身份
- 通過CLI在Sx350或SG350X交換機上配置VLAN介面IPv4地址

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）。