Cisco Business 路由器 VLAN 最佳做法和安全提示

目标

本文旨在介绍与在 Cisco Business 设备上配置 VLAN 时执行最佳做法和安全提示相关的概念及操作步骤。

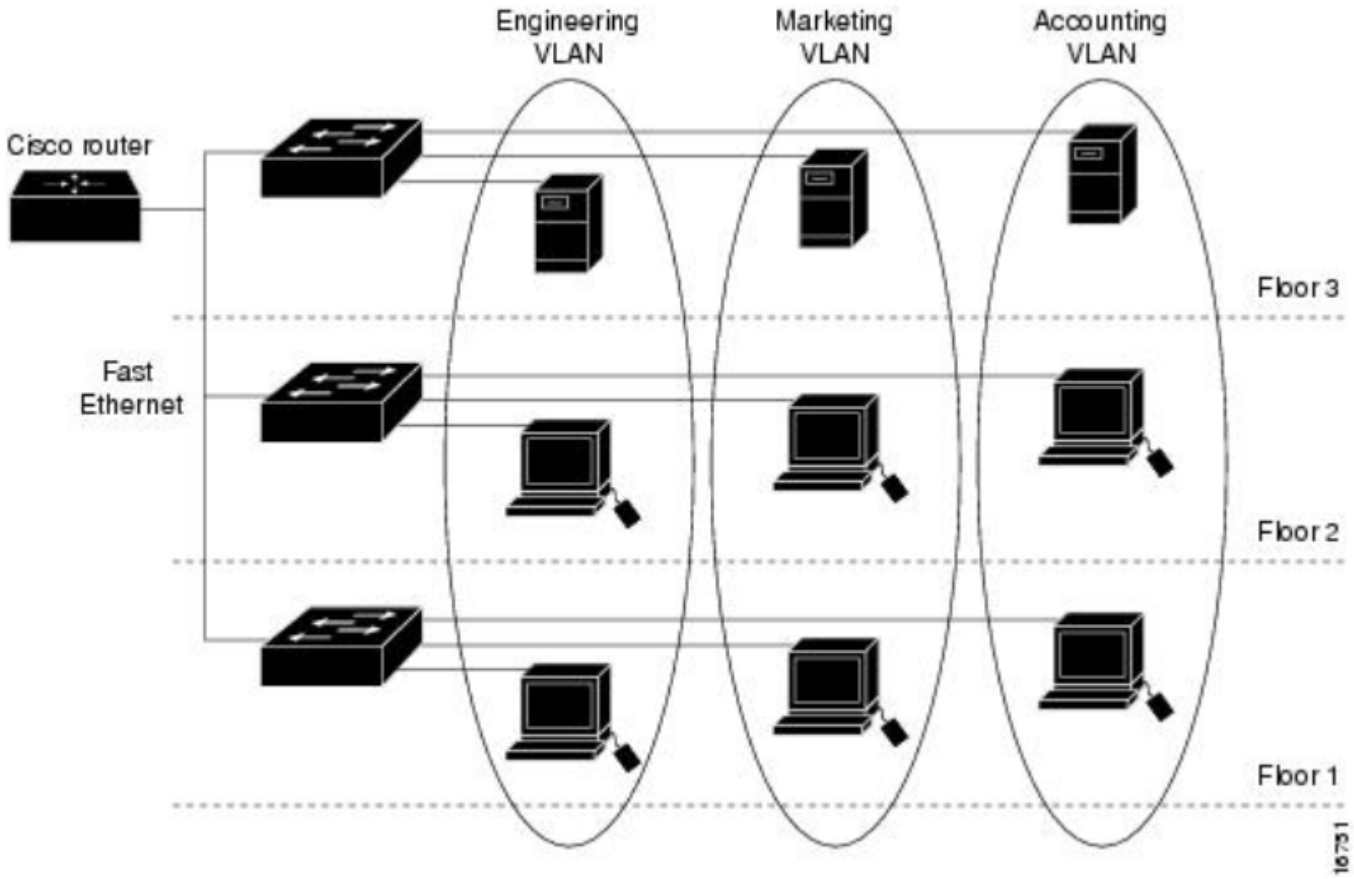
目录

简介

希望提高企业网络的效率，同时保证其安全？其中一种方法是正确设置虚拟局域网(VLAN)。

VLAN是工作站、服务器和网络设备组成的逻辑组，它们看似位于同一个局域网(LAN)中，尽管地理位置分散。简而言之，同一VLAN中的硬件使设备之间的流量得以分离且更加安全。

例如，您可能拥有一个工程、市场营销和会计部门。每个部门都有员工位于大楼的不同楼层，但他们仍需要访问和沟通各自部门内的信息。这对于共享文档和Web服务至关重要。



VLAN需要按照最佳实践进行设置，以确保网络安全。设置VLAN时，请做出以下明智选择。你不会后悔的！

适用设备

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

您可能想知道，RV160或RV260系列路由器最多可容纳16个VLAN，而RV34x系列路由器最多可容纳32个VLAN。RV320最多支持7个VLAN。如果您想了解您的路由器可以承载多少个VLAN，请查看Cisco Website上您的特定型号的 产品手册。选择 **Support**并输入您的型号，或者直接搜索产品手册和型号。

纽伯斯的几个快速词汇

接入端口:接入端口只传输一个VLAN的流量。接入端口通常称为无标记端口，因为该端口上只有一个VLAN，流量可以在无标记的情况下通过。

中继端口:交换机上为多个VLAN传输流量的端口。中继端口通常称为标记端口，因为该端口上有多个VLAN，除一个VLAN外所有流量的标记都需要。

Native VLAN:TRUNK端口中一个未收到标记的VLAN。没有标记的所有流量将发送到本征VLAN。因此，中继的两端都需要确保它们具有相同的本征VLAN，否则流量不会到达正确的位置。

最佳实#1配置 — VLAN端口分配

端口分配基础知识

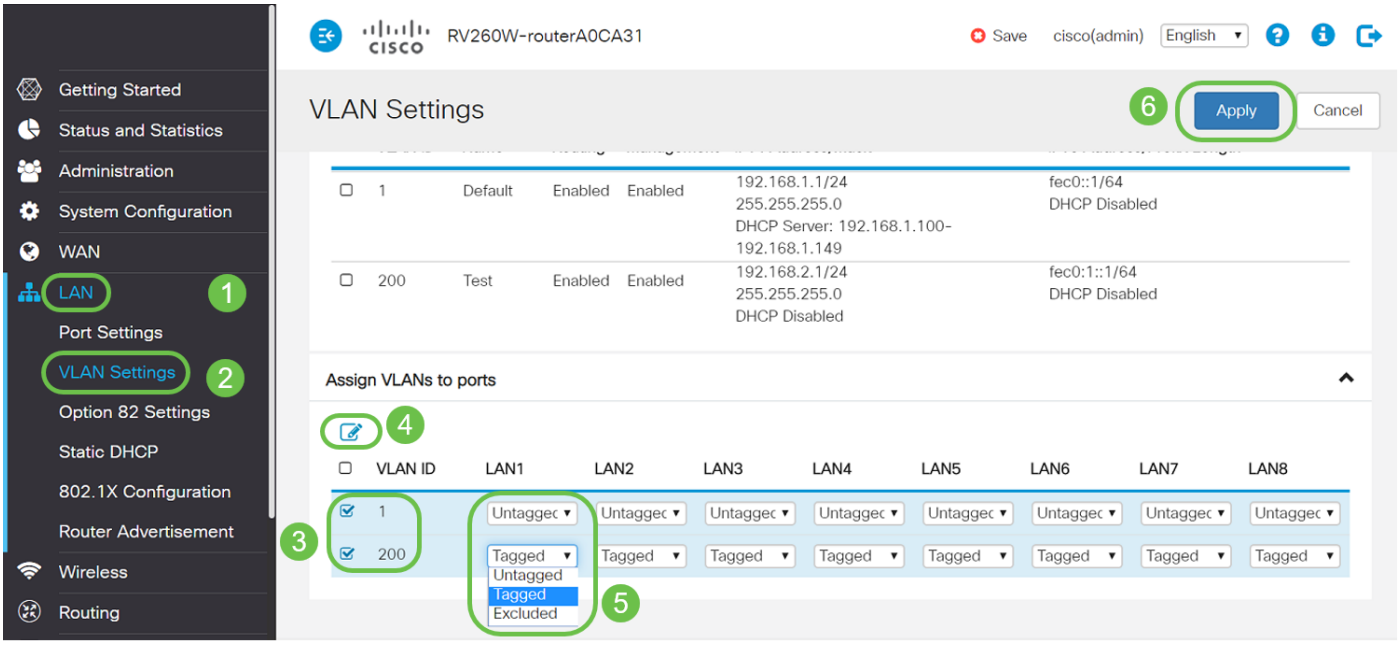
- 每个LAN端口都可以设置为接入端口或中继端口。
- 您不希望在中继上使用的VLAN应该排除。
- 一个VLAN可以置于多个端口中。

配置接入端口

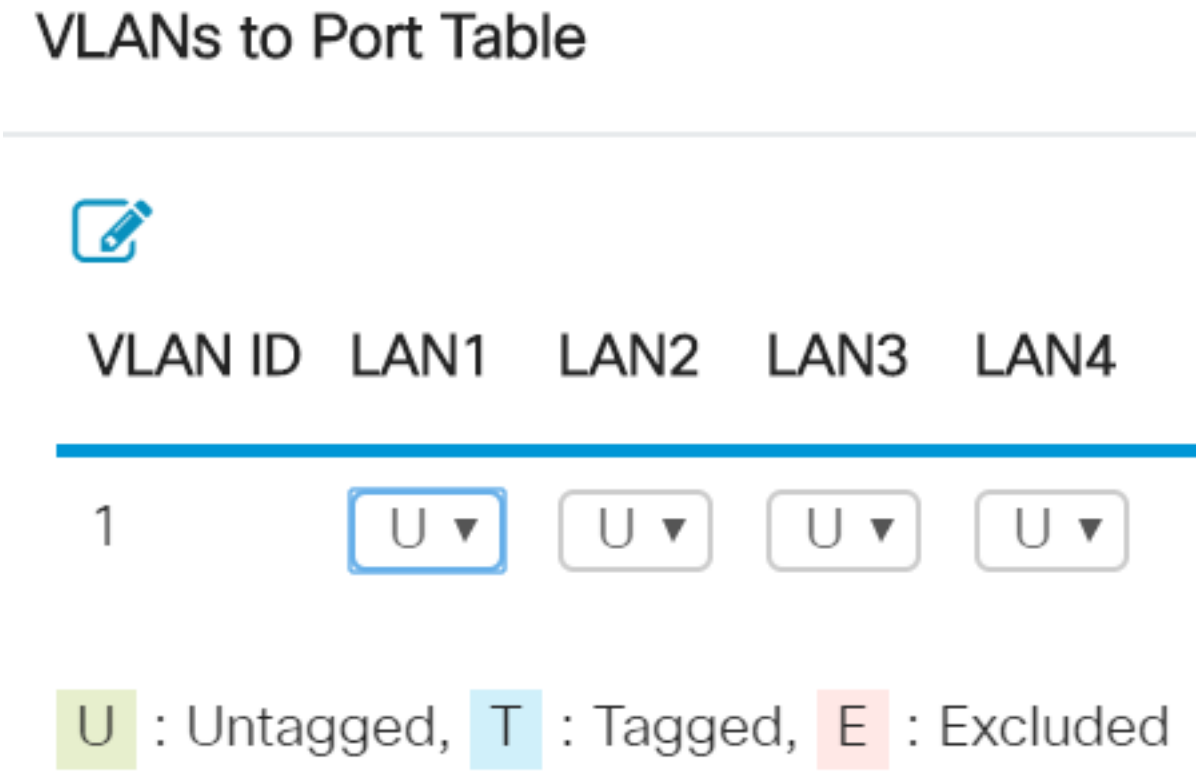
- 在LAN端口上分配一个VLAN
- 分配到此端口的VLAN应标记为*Untagged*
- 对于该端口，所有其他VLAN都应标记为*Excluded*

要正确设置这些设置，请导航到**LAN > VLAN Settings**。选择*VLAN ID*，然后单击**编辑**图标。为列出的任何VLAN的LAN接口选择下拉菜单以编辑VLAN标记。单击 **Apply**。

请看以下为每个VLAN分配了自己的LAN端口的示例：



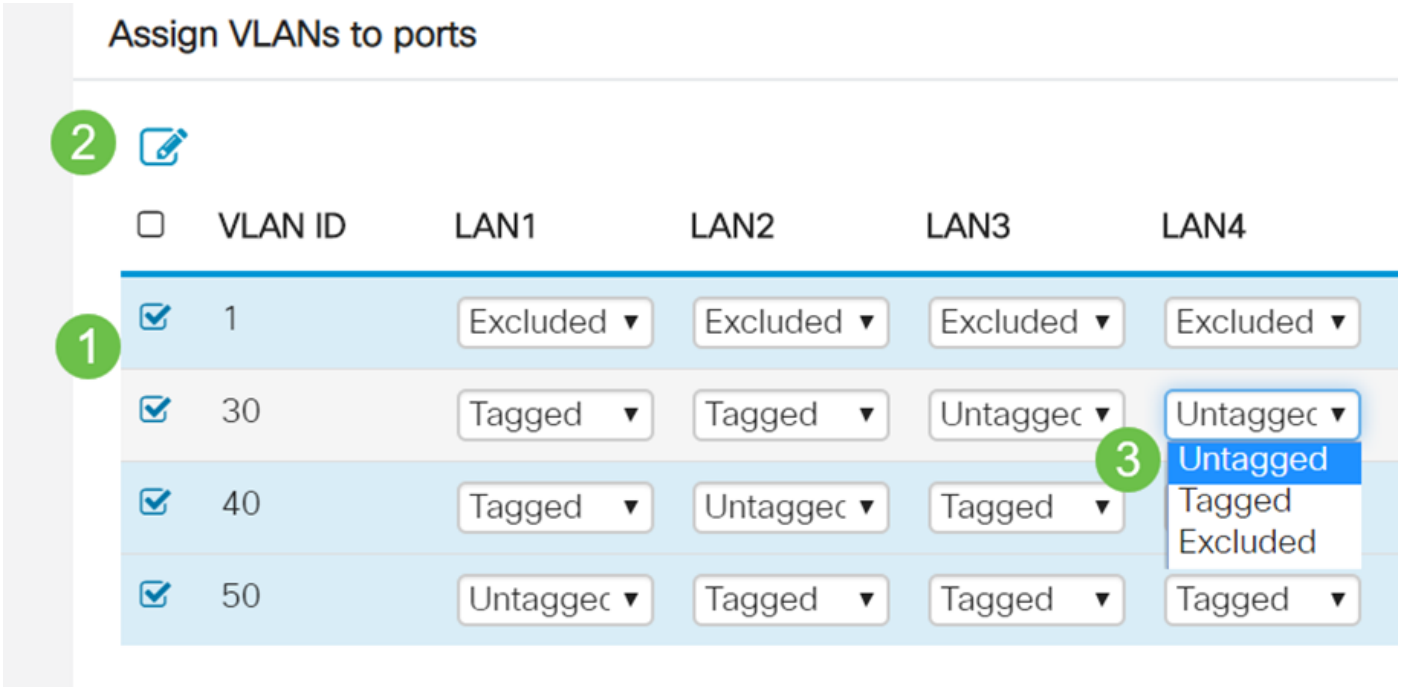
此图形用户界面(GUI)映像来自RV260W路由器。您的选项可能会略有不同。例如，在RV34x系列中，标签 *Untagged*、 *Excluded*和 *Tagged*缩写为第一个字母。过程仍然相同。



配置中继端口

- 两个或多个VLAN共享一个LAN端口
- 其中一个VLAN可以标记为*Untagged*。
- 属于TRUNK端口的其他VLAN应标记为*Tagged*。
- 不属于中继端口的VLAN应为该端口标记为*Excluded*。

请看这个中继端口上的各种VLAN示例。要正确设置这些值，请选择*需要编辑的VLAN ID*。单击编辑*图*标。按照上述建议根据需要进行更改。顺便问一下，您是否注意到VLAN 1从每个LAN端口中排除？[默认VLAN 1的最佳实践]部分将对此进行说明。



常见问题

当VLAN是该端口上唯一的VLAN时，为什么VLAN未标记？

由于接入端口上只分配了一个VLAN，因此来自该端口的传出流量会在帧上不添加任何VLAN标记的情况下发送。当帧到达交换机端口（传入流量）时，交换机将添加VLAN标记。

当VLAN是TRUNK的一部分时，为什么会标记？

这样做是为了确保通过的流量不会发送到该端口上的错误VLAN。VLAN共享该端口。类似于添加到地址中的公寓号，用来确保邮件发送到共享建筑中的正确公寓。

当流量是本征VLAN的一部分时，为什么它保持无标记状态？

本征VLAN是一种通过一台或多台交换机传输无标记流量的方式。交换机将到达标记端口的所有无标记帧分配到本征VLAN。如果本征VLAN上的帧离开中继（已标记）端口，交换机将剥离VLAN标记。

当VLAN不在该端口上时，为什么会将其排除？

这将仅针对用户特别想要的VLAN保留该中继上的流量。这是最佳做法。

最佳实#2指南 — 默认VLAN 1和未使用的端口

所有端口都需要分配给一个或多个VLAN，包括本征VLAN。默认情况下，Cisco Business路由器会将VLAN 1分配给所有端口。

管理VLAN是使用Telnet、SSH、SNMP、系统日志或思科的FindIT来远程管理、控制和监控您网络中的设备的VLAN。默认情况下，这也是VLAN 1。一个好的安全做法是将管理和用户数据流量分开。因此，建议在配置VLAN时，仅将VLAN 1用于管理目的。

要出于管理目的与思科交换机进行远程通信，交换机必须在管理VLAN上配置IP地址。其他VLAN中的用户无法建立到交换机的远程访问会话，除非他们被路由到管理VLAN中，从而提供额外的安全层。此外，交换机应配置为仅接受用于远程管理的加密SSH会话。要阅读有关此主题的一些讨论，请点击思科社区网站上的以下链接：

- 管理VLAN讨论#1
- 管理VLAN讨论#2

常见问题

为什么建议不要使用默认VLAN 1对网络进行虚拟分段？

主要原因是恶意攻击者知道VLAN 1是默认的，并且经常使用。它们可以通过“VLAN跳跃”来访问其他VLAN。顾名思义，恶意攻击者可能会发送伪装为VLAN 1的欺骗流量，从而允许访问中继端口和其他VLAN。

能否将一个未使用的端口分配给默认VLAN 1?

为了确保您的网络安全，您不应这样做。建议将所有这些端口配置为与除默认VLAN 1以外的VLAN关联。

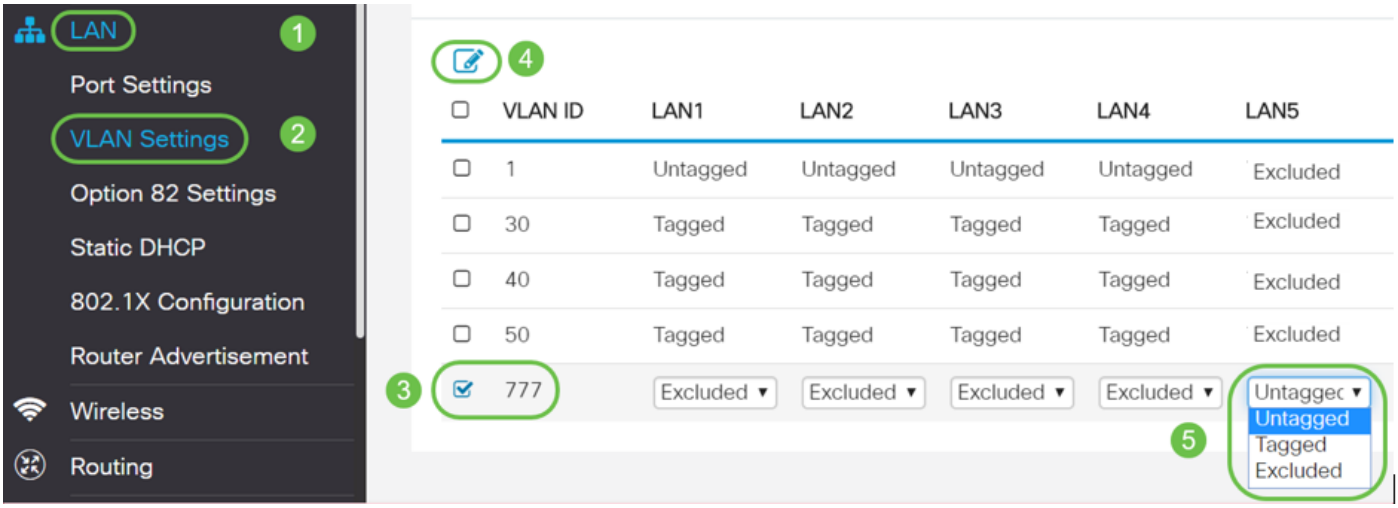
我不想将我的任何生产VLAN分配给未使用的端口。我该怎么办？

建议您按照本文下一节中的说明创建“死端”VLAN。

最佳实#3指南 — 为未使用的端口创建“死端”VLAN

步骤1.导航到**LAN > VLAN Settings**。

为VLAN选择任意随机数。请确保此VLAN未启用DHCP、VLAN间路由或设备管理。这样可以保证其他VLAN更加安全。将任何未使用的LAN端口置于此VLAN中。在下面的示例中，*VLAN 777*已创建并分配给*LAN5*。这应该在所有未使用的LAN端口上完成。



注意，此LAN端口不包括其他VLAN。

步骤2.**点击***Apply*按钮以保存您所做的配置更改。

最佳实#4指南 — VLAN上的IP电话

语音流量具有严格的服务质量(QoS)要求。如果贵公司的计算机和IP电话位于同一个VLAN中，则每个都尝试使用可用带宽，而不考虑其他设备。为避免此冲突，最好为IP电话语音流量和数据流量使用单独的VLAN。要了解有关此配置的更多信息，请查看以下文章和视频：

- 思科技术演讲：使用思科S系列产品设置和配置语音VLAN（视频）
- 在SG500系列交换机上配置带QoS的自动语音VLAN
- 200/300系列管理型交换机上的语音VLAN配置
- 思科技术演讲：在SG350和SG550系列交换机上配置自动语音VLAN（视频）

最佳实#5指南 — VLAN间路由

设置VLAN是为了分隔流量，但有时需要VLAN才能在彼此之间路由。这是VLAN间路由，通常不推荐。如果您的公司需要此功能，请尽可能安全地设置它。使用VLAN间路由时，请确保使用访问控制列表(ACL)限制包含机密信息的服务器的流量。

ACL执行数据包过滤以控制数据包在网络中的移动。数据包过滤通过限制流量访问网络、限制用户和设备访问网络以及防止流量离开网络来提供安全性。IP访问列表可降低欺骗和拒绝服务攻击的可能性，并允许通过防火墙进行动态、临时的用户访问。

- 具有目标ACL限制的RV34x路由器上的VLAN间路由
- 思科技术演讲：在SG250系列交换机上配置VLAN间路由（视频）
- 思科技术演讲：RV180和RV180W上的VLAN间配置(视频)
- RV34x VLAN间访问限制(CSCvo92300漏洞修复)

结论

您已经了解了一些设置安全VLAN的最佳实践。在为网络配置VLAN时，请记住以下提示。下面列出了一些具有分步说明的文章。这些功能将帮助您实现一个高效、高效且适合您企业的网络。

- 在RV160和RV260上配置VLAN设置
- 在RV34x系列路由器上配置虚拟局域网(VLAN)设置
- 在RV320和RV325 VPN路由器上配置VLAN成员资格
- 在RV系列路由器上配置虚拟局域网(VLAN)成员
- 通过CLI在Sx350或SG350X交换机上配置VLAN接口IPv4地址

关于此翻译
思科采用人工翻译与机器翻译相结合的方式将此文档翻译成不同语言，希望全球的用户都能通过各自的语言得到支持性的内容。

请注意：即使是最好的机器翻译，其准确度也不及专业翻译人员的水平。

Cisco Systems, Inc. 对于翻译的准确性不承担任何责任，并建议您总是参考英文原始文档（已提供链接）。