计算机网络实用技术人才培养丛书
锐 捷 职 业 认 证 系 列

设备调试与网络优化

Debugging and Optimizing Networking Devices (DOND)

学习指南

◎ 张选波　吴丽征　周金玲　编著

科学出版社
www.sciencep.com

计算机网络实用技术人才培养丛书
锐 捷 职 业 认 证 系 列

设备调试与网络优化

Debugging and Optimizing Networking Devices (DOND)

学习指南

◎ 张选波 吴丽征 周金玲 编著

科学出版社
www.sciencep.com

内 容 简 介

本书内容涉及最新的主流网络技术，包括路由技术、交换技术、远程接入技术和网络安全技术等，全书以实际的网络环境为依托，结合工程项目中的实践经验，对现在最流行的网络技术进行了系统、全面的阐述。书中提供的真实案例和项目解决方案，可以使学习者更好地掌握网络专业技术，增强实际操作能力。

本书既可以作为本科类院校、高职类院校教学的教材，也可以作为网络设计师、网络工程师、系统集成工程师以及相关技术人员在实际构建园区网络中的技术参考用书。由于具备很强的专业性、实用性和易读性，本书现已被选为锐捷网络有限公司RCCP（锐捷认证资深网络调试工程师）认证的指定教材。

本书配套电子课件、各章的复习题答案可以通过访问 http://labclub.ruijie.com.cn、http://university.ruijie.com.cn 获得。

需要本书或技术支持的读者，请与北京清河 6 号信箱（邮编：100085）发行部联系，电话：010-62978181（总机）、010-82702660，传真：010-82702698，E-mail：tbd@bhp.com.cn。

图书在版编目（CIP）数据

设备调试与网络优化学习指南 / 张选波，吴丽征，周金玲编著. —北京：科学出版社，2009.4

（计算机网络实用技术人才培养丛书）

ISBN 978-7-03-024169-6

Ⅰ. 设… Ⅱ. ①张… ②吴…③周… Ⅲ. 计算机网络—指南 Ⅳ. TP393-62

中国版本图书馆 CIP 数据核字（2009）第 026922 号

责任编辑：刘 芯 / 责任校对：周 玉

责任印刷：密 东 / 封面设计：青青果园

科学出版社 出版

北京东黄城根北街 16 号

邮政编码：100717

http://www.sciencep.com

北京市密东印刷有限公司印刷

科学出版社发行 各地新华书店经销

*

2009 年 4 月第 一 版 开本：787×1092 1/16

2009 年 4 月第一次印刷 印张：22

印数：1-1000 册 字数：523 000

定价：39.00 元

《设备调试与网络优化学习指南》编委会

Debugging and Optimizing Networking Devices (DOND)

主　编：张选波　王　东　张国清

策　划：安淑梅

编　委：方　洋　周　超　高　峡　石　林

“计算机网络实用技术人才培养丛书”
编审委员会

前　言

随着信息化的高速发展，人们已经把更多的生活、娱乐和学习等事务转移到网络这个平台上去开展。小到一个家庭，大到一个企业，甚至是一所高校，为了提高工作效率，并进行更多的信息交流，都需要构建一个园区网，从而实现内部的高效沟通。如果希望能进一步地能够和互联网中的其他地区甚至国家的人群、组织进行信息交流，则需要将内部的园区网接入到互联网中。

本书详细介绍了构建园区网所涉及的各项交换、路由、安全等方面的知识，以及如何将园区网接入到互联网的相关技术，包括 VLAN、STP/RSTP/MSTP、VRRP、RIP、OSPF、局域网安全设计、网络出口设计、远程接入、VPN 等。另外，在最后一章还介绍了在网络故障维护中常用的思路、工具与命令，使读者在对网络进行维护与故障排除中进行借鉴。在本书的各个章中，不仅对相关技术进行了详细的介绍，而且还介绍了为了实现和部署这些技术在网络设备上的配置方式，并且章节的末尾提供了复习题目，以帮助读者巩固所学的内容和达到自我测试的目的。

本书的规划思想是使所需知识具有专业化、体系化、全面化的特征，能够体现和代表当前最新的网络技术发展方向。因此，在课程规划和内容选择上与传统的网络专业教材有很大的区别，本书从各个方面都能满足各级、各类不同专业院校教学与实践的要求。

本书由资深网络技术专家张选波和具有多年教学经验的吴丽征、周金玲在基于多年的网络工程经验、教学经验以及对网络技术的深刻理解上联合编写而成。

本书目标

本书在介绍理论知识和技术原理的同时，还提供了大量的配置案例和示例，以达到理论和实践相结合的目的。在每章的末尾所提供的复习题目中包括了相应章节中的重点内容和主要知识点，能够帮助读者对自己的学习情况和知识的掌握程度进行评估。

本书读者

本书的读者对象可以是本科类院校、高职类院校的学生、教师，也可以为准备参加 RCCP 考试的专业人士，以及希望学习更多园区网构建知识的技术人员。

我们推荐阅读本书的读者有基本的网络技术知识，或者具备 RCNA 认证或者具有与 RCNA 同等水平的网络知识，以便更好地理解本书中所涉及的内容。

阅读方法

本书内容其分为 12 章，每章都对一项或几项协议及技术进行了详细的阐述。因为在理解后续章节内容时需要具备以前章节的知识，所以推荐读者根据章节顺序依次阅读本书。对于具有一定基础的读者也可以灵活地、有选择地对某些章节进行阅读。

本书资源

为了保证课程在学校的有效实施，及课程教学资源的长期提供，还建设了专门的课程实施教学俱乐部的网络资源共享基地，用来支持在课程实施过程中的项目资源更新。读者可以访问 http://labclub.ruijie.com.cn、http://university.ruijie.com.cn，免费获得配套电子课件、各章节的复习题答案以及更多的教学资源。

本书结构

本书共用 12 个章节对园区网相关技术进行了介绍，其中第 10 章、第 11 章为本书的扩展部分，不列为此认证的考试范围，具体结构如下。

第1章　VLAN 技术。

本章首先介绍了 VLAN 技术的原理，然后介绍了利用 SVI 和单臂路由实现 VLAN 间路由的两种方法，最后介绍了 Private VLAN 和 Super VLAN 这两种特殊的 VLAN，此外还介绍了相关技术的配置和使用方法。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 1　单臂路由”、“实验 2　使用 SVI 实现 VLAN 间路由”、“实验 3　跨交换机实现 VLAN 间路由”。

第2章　生成树协议。

本章首先介绍了 STP 中的基本概念与 BPDU 报文格式与内容，然后详细介绍了 STP 选举以及拓扑变更的详细过程，RSTP 的过渡机制和拓扑变更技术和 MSTP 的相关术语，最后介绍了相关技术的配置方法。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 4　配置 RSTP”、“实验 5　配置 MSTP”。

第3章　虚拟路由器冗余协议（VRRP）。

本章首先介绍了 VRRP 技术的应用背景，然后介绍了 VRRP 的各项机制与报文格式，最后介绍了 VRRP 的基本配置与优化调整的相关配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 6　配置 VRRP 单备份组”、“实验 7　配置 VRRP 多备份组”、“实验 8　配置基于 SVI 的 VRRP 备份组”。

第4章　路由信息协议（RIP）。

本章介绍了 RIP 路由协议几个版本的区别以及路由汇总、定时器等特性的配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 9　配置 RIP 版本、汇总、定时器”。

第5章　开放式最短路径优先协议（OSPF）。

本章首先介绍了 OSPF 的工作原理，然后介绍了 OSPF 的报文类型、单区域、多区域等相关概念，最后介绍了 OSPF 路由协议的各项相关配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 10　OSPF 单区域配置”、“实验 11　OSPF 多区域配置”。

第6章　路由重发布与路由控制。

本章详细介绍了路由重发布的作用、原则等以及其相关配置，然后介绍了被动接口、分发列表等路由控制技术与配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 12　配置 RIP 被动接口”、“实验 13　配置 OSPF 被动接口”、“实验 14　调整路由的 AD 值”、“实验 15　配置 RIP 与 OSPF 路由重发布”。

第7章　网络安全控制。

本章介绍了 ARP 检查、DHCP 监听、DAI、ACL 等局域网中常用的相关安全技术及其配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 16　配置 ARP 检查”、“实验 17　配置 DHCP 监听”、“实验 18　配置动态 ARP 检测”、“实验 19　配置标准 IP ACL”、“实验 20　配置扩展 IP ACL”、“实验 21　配置基于 MAC 的 ACL”、“实验 22　配置专家 ACL”、“实验 23　配置基于时间的 ACL”。

第8章　AAA 和 802.1x。

本章详细介绍了 AAA、RADIUS 和 802.1x 技术的相关概念及其配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 24　配置远程登录的 AAA 认证”、“实验 25　配置 PPP 链路的 AAA 认证”、“实验 26　接入层 802.1x”。

第9章　网络出口设计。

本章详细介绍了 NAT 和策略路由这两种网络出口常用技术以及其相关配置。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 27　配置静态 NAT”、“实验 28　配置动态 NAT”、“实验 29　配置 NAT 地址复用（NAPT）”、“实验 30　配置 TCP 负载分配”、“实验 31　配置策略路由”。

第10章　远程接入技术。

本章详细介绍了 WAN 远程接入技术，内容包括 ISDN、帧中继、PPP 等相关技术。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 32　广域网协议的封装”、“实验 33 PPP PAP 认证”、“实验 34　PPP CHAP 认证”、“实验 35　帧中继基本配置”、“实验 36　帧中继交换机配置”。

第11章　虚拟专用网（VPN）。

本章详细介绍了 VPN 技术，内容包括加密、隧道、密钥交换技术以及 VPN 配置实例。实验部分可参照《设备调试与网络优化实验指南》一书中的“实验 37　IPSec VPN 简单配置”、“实验 38 Site To Site IPSec VPN 多站点配置”。

第12章　网络故障处理排除。

本章首先详细介绍了网络故障排除的相关思路、工具、命令等，然后通过实际的故障排除案例向读者展示常见的故障排除方法。

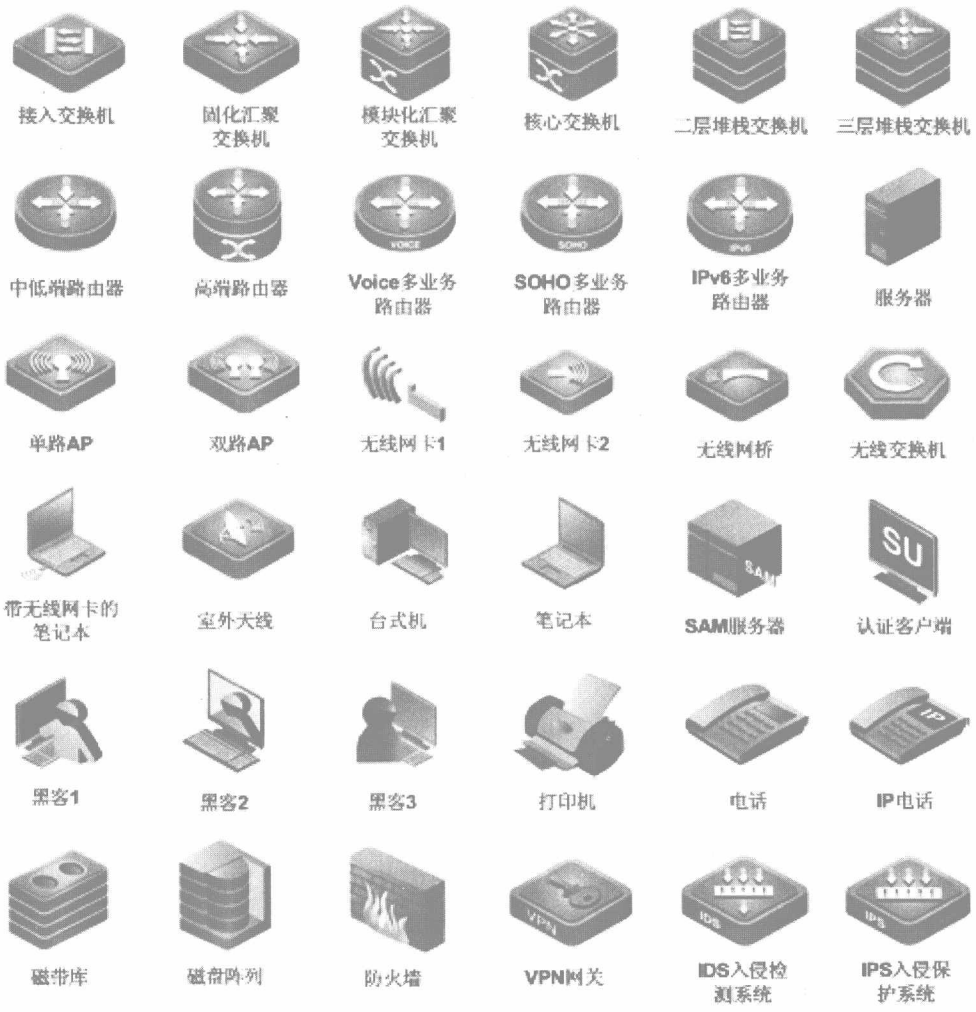
命令语法规范

本书中使用的命令语法规范与产品命令参考手册中的命令语法相同。

- 竖线“|”表示分隔符，用于分开可选择的选项。
- 星号“*”表示可以同时选择多个选项。
- 方括号“[ ]”表示可选项。
- 大括号“{ }”表示必选项。
- **粗体字**表示按照显示的文字输入的命令和关键字。在配置的示例和输出中，粗体字表示需要用户手工输入的命令（例如 **show** 命令）。
- *斜体字*表示需要用户输入的具体值。

本书使用的图标

本书中所使用的图标示例如下所示。



目　录

第 1 章　VLAN 技术

本章重点

- 配置 VLAN
- 使用 SVI 实现 VLAN 间通信
- 使用单臂路由实现 VLAN 间通信
- Private VLAN
- Super VLAN

交换网络拥有传输速度快、误码率低等优点。但另一方面，由于交换机不隔离广播，因此整个交换网络是个广播域，并且网络越大广播域的范围也越大，如图 1-1 所示。当广播域的范围足够大的时候，会使得网络中的广播包过多，导致网络拥塞。同时，交换网络也不利于故障隔离和防止病毒扩散等。为了保留交换网络的优点并同时解决广播域过大的问题，可以应用 VLAN（Virtual Local Area Network，虚拟局域网）技术。在网络中应用 VLAN 技术后，一个 VLAN 所在的范围就是一个广播域。

在二层网络中，不同 VLAN 中的主机无法互相通信，除非使用三层设备。

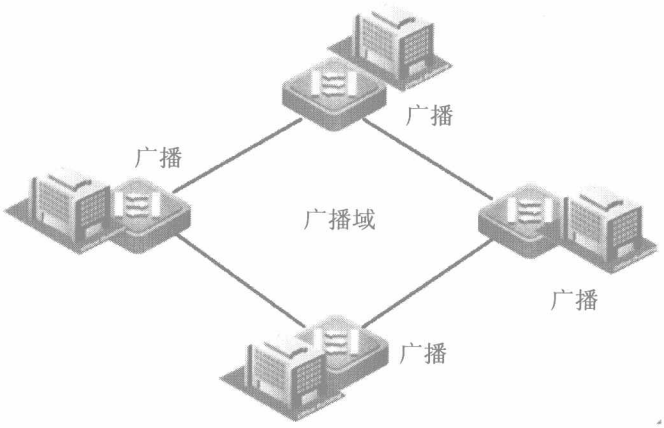


图 1-1　交换网络中的广播域

1.1　配置 VLAN

在交换网络中，由于整个网络处在一个广播域中，所以广播和未知单播帧会扩散到网络中的全部端口。

应用 VLAN 技术后不同的 VLAN 之间，不但广播包无法发送，而且正常的单播通信也被隔离。在实际网络构建中，通常需要实现的是网络之间的互通性，本章将重点讲解如何实现不同 VLAN 间的互相通信，以及在网络中使用的一些特殊的 VLAN 技术，如 Private VLAN 和 Super VLAN。

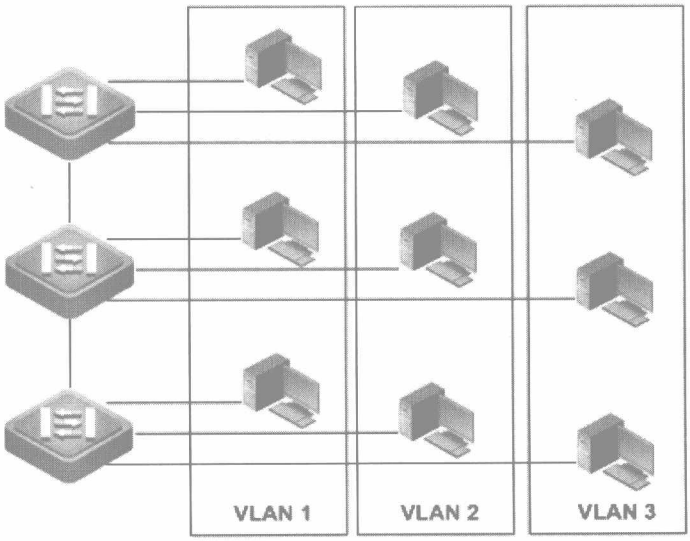


图 1-2　划分 VLAN

VLAN 有多种不同的划分方式：基于端口的、基于协议的、基于 IP 地址的、基于 MAC 地址的。其中最常用的是基于端口划分 VLAN。

通过划分 VLAN 的方法，可以在二层交换网络中对广播域进行划分，将大的广播域划分为小的广播域，从而减少网络中的广播流量。划分 VLAN 后，如果某 VLAN 中的一台设备发出广播包，那么在这同一 VLAN 中的其他成员都会收到此广播包，而对于属于其他 VLAN 的端口和设备则无法收到此广播包。

VLAN 划分的逻辑子网尽管与物理局域网实现同一目的——隔离广播，但是它和物理子网不同，VLAN 划分的逻辑子网是由相互通信并且与物理位置无关的设备组成，这决定了 VLAN 的划分与物理位置无关。例如在基于端口划分 VLAN 时，可以将同一交换机不连续的端口划分到一个 VLAN 中，也可以将不同交换机上的端口划分到同一个 VLAN 中。划分到同一个 VLAN 的端口与设备，属于同一个 LAN，即同一个广播域，因此在规划 IP 地址时，同一个 VLAN 内的设备应属于同一个子网。

1.1.1　实施 VLAN 技术的好处

通过在交换网络中 VLAN 技术的实施，可以为网络带来很多诸如隔离广播、安全、故障隔离等好处。

- **隔离广播：**在交换网络中，通过对广播域的隔离，可以大大减少网络中泛洪的广播包，提高网络带宽的利用率。但与此同时，由于在二层网络中划分了广播域，那么不同广播域（VLAN）之间的数据通信需要通过三层网络设备才能实现。
- **安全性：**通过在二层网络划分 VLAN，可以实现在二层网络中不同 VLAN 间的数据隔离。在二层网络中划分 VLAN 后，不但广播包不能通过，而且无法进行正常的数据通信。这时通过使用三层设备，可以实现不同 VLAN 间的数据转发。在三层设备接口上（如 VLAN 接口），可以应用其他安全措施。还可以通过访问控制列表，对网络中不同 VLAN 间的通信进行访问控制。

- **故障隔离**：通过 VLAN 的划分，将设备划分到不同的广播域当中，可以减小网络故障的影响。例如网络中的环路，可能会导致大量的广播包扩散或是广播风暴的情况，在划分 VLAN 后，这些故障的影响被控制在一个广播域内，即一个 VLAN 内，对网络中的其他 VLAN 没有影响。特别是现在网络当中经常遇到的 ARP 病毒，经常会导致某网络内主机无法正常通信，通过 VLAN 的划分，可以将这个影响的范围减小到一个 VLAN 的范围，同时也方便故障的定位和排除。

1.1.2 802.1q

在交换机上划分 VLAN 后，交换机会判断接收到的数据帧属于哪个 VLAN，从而控制数据帧发送到其他 VLAN 的范围中。如果基于端口方式来划分 VLAN，交换机会通过从哪个端口接收到的数据帧，判断数据帧属于哪个 VLAN。例如将交换机的 1 号端口划分到 VLAN10，那么连接在 1 号端口的设备发送数据帧时，交换机可以判断此数据帧为 VLAN10 中的数据帧。当数据帧只在同一交换机上传输时，交换机可以判断此数据帧的身份。但是前面讲过，数据帧的划分不受地理位置的限制，因此对于其他交换机来说，需要有一个标签来标明数据帧属于哪个 VLAN。802.1q 标签（Tag）就可以实现这个目的，支持 802.1q VLAN 的交换机收到数据帧后，会在数据帧中插入长度为 4 字节的 802.1q 标签。如图 1-3 所示，其中有 12 比特表示 VLAN 编号，表示的范围是 0~4095，但用户在设备上可以配置的 VLAN 范围是 1~4094，其中，VLAN1 为默认 VLAN，不可以删除，并且默认情况下交换机上所有端口都属于默认的 VLAN1。

802.1q 标签共 4 个字节，其中 3 个比特表示 802.1P 优先级（Priority），1 个比特表示 CFI 信息（Canonical Format Indicator），用于压缩 Token Ring 数据包，以使其可以在以太网主干内传输，12 个比特用于标识 VLAN ID 信息。

图 1-3 802.1q Tag

1.1.3 VLAN Trunk

在交换机上划分 VLAN 时，经常会遇到同一 VLAN 跨越多台交换机的问题。如图 1-4 所示，由于交换机上默认的端口都属于 VLAN1，而级联的链路也属于 VLAN1，所以其他 VLAN 的数据无法在该链路上传输。因此对于跨交换机实现同 VLAN 数据通信的场合，需要在交换机间建立 Trunk（干道）链路。Trunk 链路的特点是允许多个 VLAN 的数据流通过，所有 VLAN 的数据都可以通过 Trunk 链路进行传输。

在交换机上需要将连接 Trunk 链路的端口模式设置为 Trunk 模式，连接主机的端口模式为 Access 模式。802.1q 数据帧在经过 Trunk 链路传输时，为了让接

收的交换机知道此数据帧属于哪个 VLAN，需要携带 802.1q 标签。如果数据帧从 Access 端口发出时，由于主机并不需要区分数据帧属于哪个 VLAN，所以需要去掉 802.1q 标签。Native VLAN（本地 VLAN）是 VLAN 网络中特殊的一类 VLAN。在网络中，为了提高数据的处理效率，对 Native VLAN 这类 VLAN 可以省略打标签的过程，但是网络中只能有一个 Native VLAN。如锐捷交换机默认情况下的 Native VLAN 是 VLAN1。

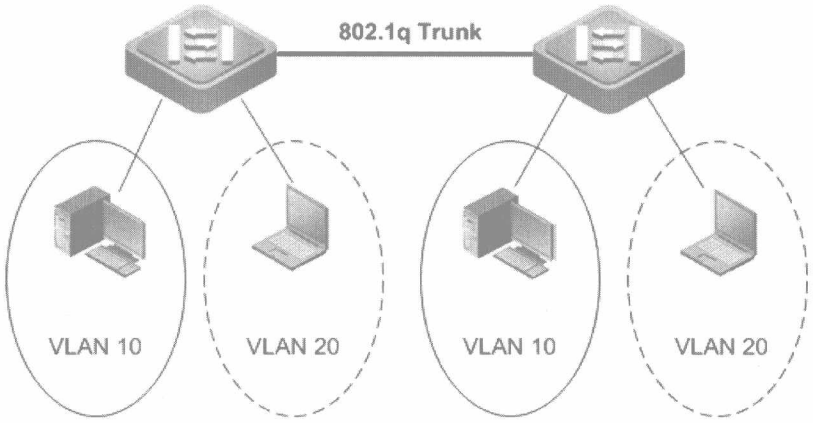


图 1-4　跨交换机实现 VLAN 间通信

1.1.4　配置 VLAN

锐捷网络全系列的网管交换机都支持 VLAN 配置。VLAN1 为默认 VLAN，VLAN1 不可删除。在交换机上可以配置的 VLAN 编号范围是 1~4094。

当创建 VLAN 后，系统将为其赋予一个默认的名称。VLAN 的名称用于友好地标识不同的 VLAN，VLAN 名称不会出现在数据帧中。

1. 创建 VLAN

步骤 1　进入全局配置模式。

Switch#**configure terminal**

步骤 2　创建 VLAN。

Switch(config)#**vlan** *vlan-id*

步骤 3　（可选）命名 VLAN。

Switch(config-vlan)#**name** *vlan-name*

2. 将交换机端口加入到 VLAN 中

步骤 1　进入端口配置模式。

Swtich(config)#**interface** *interface*

步骤 2　将端口模式设置为接入端口。

Switch(config-if)#**switchport mode access**

步骤 3　将端口添加到特定 VLAN。

Switch(config-if)#**switchport access vlan** *vlan-id*

示例 1-1 介绍了如何将交换端口 fastEthernt 0/1 加入到 VLAN10 中。

示例 1-1　将端口 fastEthernet 0/1 添加到 VLAN10 中

```
Switch#configure terminal
```