

“十三五”高等职业教育计算机类专业规划教材

# 网络管理与维护案例教程

吴小峰 周 军 主编

WANGLUO GUANLI YU WEIHU  
ANLI JIAOCHENG

中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

“十三五”高等职业教育计算机类专业规划教材

# 网络管理与维护案例教程

吴小峰 周 军 主编

刘振宇 周学全 黄华林 王 璐 副主编

中国铁道出版社  
CHINA RAILWAY PUBLISHING HOUSE

---

## 内 容 简 介

本书主要以一个典型的中小型企业网络规划设计、建设及管理为背景,将所需知识合理安排进单独案例。全书共 11 章,38 个案例,每个案例设“学习目标”“案例描述”“相关知识”“案例实施”,理论联系实际、由浅入深地介绍企业网在规划建设管理过程中交换机和路由器等设备的配置知识。

本书适合作为高等职业院校计算机网络技术专业理论与实训一体化教材,也可作为社会职业技能培训教材,还可供从事网络设备管理维护的技术人员参考使用。

### 图书在版编目(CIP)数据

网络管理与维护案例教程/吴小峰,周军主编. —  
北京:中国铁道出版社,2016.1

“十三五”高等职业教育计算机类专业规划教材  
ISBN 978-7-113-21202-5

I. ①网… II. ①吴… ②周… III. ①计算机网络管  
理—高等教育—教材 ②计算机网络—计算机维护—高  
等职业教育—教材 IV. ①TP393.07

中国版本图书馆 CIP 数据核字(2015)第 320934 号

书 名:网络管理与维护案例教程  
作 者:吴小峰 周 军 主编

策 划:汪 敏  
责任编辑:秦绪好 徐盼欣  
封面设计:付 巍  
封面制作:白 雪  
责任校对:汤淑梅  
责任印制:李 佳

读者热线:(010) 63550836

出版发行:中国铁道出版社(100054,北京市西城区右安门西街 8 号)

网 址:<http://www.51eds.com>

印 刷:北京尚品荣华印刷有限公司

版 次:2016 年 1 月第 1 版 2016 年 1 月第 1 次印刷

开 本:787 mm×1 092 mm 1/16 印张:15 字数:362 千

书 号:ISBN 978-7-113-21202-5

定 价:36.80 元

版权所有 侵权必究

凡购买铁道版图书,如有印制质量问题,请与本社教材图书营销部联系调换。电话:(010) 63550836

打击盗版举报电话:(010) 51873659

随着计算机的不断普及和推广,各企业为了自身的生存和发展,基本都要建设自己的网络来实现网络化和信息化。它们的规模大小不等,但一般均要有自己的局域网和相应的广域网接入。如何规划设计好一个网络,更好地配置、管理和利用现有的网络资源,搭建一个尽可能安全的网络环境,使之更好更有效地为公司服务……是每一个网络规划设计者要考虑的问题。企业网络系统是一个庞大而复杂的系统,不仅为综合信息管理和办公自动化等一系列应用提供基本操作平台,而且应能提供多种应用服务,使信息及时、准确地传送给各个系统,实现企业内部资源的共享,降低企业成本,同时可以更好地与外界进行沟通,让外部更加了解企业。

本书主要以一个典型的中小型企业网络规划设计、建设及管理案例为出发点,以案例驱动任务导向,详细介绍在网络规划设计、建设及管理过程中,需要考虑的各种因素及需要使用的网络技术。本书共分 11 章:第 0 章为企业网络规划设计案例的引入,第 1 章为管理交换网络,第 2 章为管理局域网中的冗余链路,第 3 章为管理网络路由,第 4 章为管理广域网链路,第 5 章为网络安全管理,第 6 章为网络设备 DHCP 服务配置,第 7 章为交换技术高级应用,第 8 章为路由技术高级应用,第 9 章为访问列表高级应用,第 10 章为 IPv6 技术应用。

本书所有案例均采用锐捷公司的网络设备完成,为便于没有该硬件设备的读者学习,本书中前 6 章“案例实施”小节采用思科公司的免费模拟器 Cisco Packet Tracer 完成,有需要的读者可以去官方网站下载。另外,锐捷公司和思科公司网络设备的配置命令有些许区别,请读者注意区分。

为统一图标格式,本书网络拓扑图采用如下图标并规定其含义:



本书由吴小峰、周军任主编,刘振宇、周学全、黄华林、王璐任副主编,余鑫海、王来丽参与编写。尽管本书编写人员在编写过程中反复多次校验,但由于编者水平有限,加之时间仓促,书中难免会有疏漏和不妥之处,敬请广大读者批评指正。

编者

2015 年 10 月

**第 0 章 案例引入 ..... 1**

- 0.1 网络规划设计背景 ..... 1
- 0.2 网络规划设计中的需求分析 ..... 1
- 0.3 网络规划设计的原则 ..... 2
- 0.4 企业网络总体设计 ..... 3
- 0.5 企业网络规划设计案例引入及  
本书学习情境案例分解 ..... 5
- 习题 0 ..... 8

**第 1 章 管理交换网络 ..... 9**

## 1.1 【案例 1】认识交换机 ..... 9

## 相关知识

- 1. 交换机简介 ..... 10
- 2. 交换机功能及作用 ..... 10
- 3. 交换机的分类 ..... 10
- 4. 交换机的选购与性能  
参数 ..... 11
- 5. 交换机的工作原理 ..... 12
- 6. 交换机的端口/编号和  
指示灯 ..... 15
- 7. 交换机的访问方式 ..... 15
- 8. 交换机的命令模式 ..... 15

## 1.2 【案例 2】远程登录交换机 ..... 18

## 相关知识

- 1. 交换机的常用配置命令 ..... 18
- 2. 交换机远程登录功能配置  
步骤和方法 ..... 21

1.3 【案例 3】使用 VLAN 技术  
隔离子网 ..... 23

## 相关知识

- 1. 什么是 VLAN ..... 23
- 2. 为什么要用 VLAN ..... 23
- 3. VLAN 类型 ..... 24
- 4. VLAN 的技术标准 ..... 25
- 5. VLAN 工作原理 ..... 26
- 6. VLAN 配置命令 ..... 27

1.4 【案例 4】跨交换机实现 VLAN  
内部通信 ..... 29

## 相关知识

- 1. VLAN Trunk ..... 29
- 2. Native VLAN ..... 30
- 3. Trunk 接口的访问  
许可列表 ..... 30
- 4. 工作原理 ..... 31

## 习题 1 ..... 34

**第 2 章 管理局域网中的冗余  
链路 ..... 36**2.1 【案例 1】使用生成树协议解决  
备份链路中的环路问题 ..... 36

## 相关知识

- 1. 冗余交换模型 ..... 37
- 2. 交换环路 ..... 37
- 3. 广播风暴 ..... 37
- 4. 生成树协议 ..... 38
- 5. STP、RSTP 配置命令 ..... 44

2.2 【案例 2】使用交换机端口聚合  
技术实现负载均衡及链路  
备份 ..... 46

## 相关知识

- 1. 端口聚合概念 ..... 46
- 2. 二层聚合端口与三层  
聚合端口 ..... 47
- 3. 流量平衡 ..... 47
- 4. 聚合端口配置命令 ..... 47

## 习题 2 ..... 50

**第 3 章 管理网络路由 ..... 52**

## 3.1 【案例 1】认识路由器 ..... 52

## 相关知识

- 1. 路由器简介 ..... 53
- 2. 路由器功能及作用 ..... 53
- 3. 路由器的分类 ..... 54

|                                         |    |
|-----------------------------------------|----|
| 4. 路由器的选购与性能参数.....                     | 55 |
| 5. 路由器的工作原理.....                        | 56 |
| 6. 路由器的接口及编号.....                       | 57 |
| 7. 路由器的访问方式.....                        | 58 |
| 8. 路由器的命令模式.....                        | 58 |
| 3.2 【案例2】远程登录路由器.....                   | 60 |
| 相关知识.....                               |    |
| 1. 路由器的常用配置命令.....                      | 60 |
| 2. 路由器远程登录功能配置<br>步骤和方法.....            | 63 |
| 3.3 【案例3】利用单臂路由实现<br>VLAN之间路由.....      | 66 |
| 相关知识.....                               |    |
| 1. 直连路由与非直连路由.....                      | 67 |
| 2. 路由器子接口.....                          | 67 |
| 3. 默认网关.....                            | 68 |
| 3.4 【案例4】利用三层交换机实现<br>VLAN之间路由.....     | 70 |
| 相关知识.....                               |    |
| 1. 三层交换机与二层<br>交换机区别.....               | 70 |
| 2. 三层交换机与路由器<br>的区别.....                | 70 |
| 3. 三层交换端口.....                          | 71 |
| 3.5 【案例5】利用静态路由实现<br>各区域子网互通.....       | 73 |
| 相关知识.....                               |    |
| 1. 建立路由的三种途径.....                       | 74 |
| 2. 静态路由配置.....                          | 74 |
| 3. 默认路由.....                            | 75 |
| 3.6 【案例6】利用RIP路由协议<br>实现各区域子网互通.....    | 77 |
| 相关知识.....                               |    |
| 1. 动态路由与动态<br>路由算法.....                 | 77 |
| 2. 路由器协议分类.....                         | 78 |
| 3. RIP路由协议.....                         | 79 |
| 3.7 【案例7】利用OSPF动态路由<br>协议实现各区域子网互通..... | 86 |

|                    |    |
|--------------------|----|
| 相关知识.....          |    |
| 1. OSPF工作原理.....   | 87 |
| 2. OSPF协议中的区域..... | 88 |
| 3. OSPF网络类型.....   | 89 |
| 4. OSPF的进程.....    | 89 |
| 5. OSPF的配置.....    | 91 |

|          |    |
|----------|----|
| 习题3..... | 93 |
|----------|----|

## 第4章 管理广域网链路..... 95

|                                  |    |
|----------------------------------|----|
| 4.1 【案例1】在路由器接口<br>上封装广域网协议..... | 95 |
|----------------------------------|----|

|                    |    |
|--------------------|----|
| 相关知识.....          |    |
| 1. 广域网的定义.....     | 96 |
| 2. 广域网接入技术分类.....  | 96 |
| 3. 封装广域网协议的方法..... | 97 |

|                                          |    |
|------------------------------------------|----|
| 4.2 【案例2】利用PPP PAP认证<br>实现广域网链路的安全性..... | 98 |
|------------------------------------------|----|

|                                             |     |
|---------------------------------------------|-----|
| 相关知识.....                                   |     |
| 1. PPP (Point to Point Protocol)<br>概述..... | 99  |
| 2. PPP协议体系结构.....                           | 99  |
| 3. PPP的工作原理.....                            | 100 |
| 4. PPP的PAP验证方式.....                         | 101 |
| 5. PPP的PAP配置方式.....                         | 101 |

|                                           |     |
|-------------------------------------------|-----|
| 4.3 【案例3】利用PPP CHAP认证<br>实现广域网链路的安全性..... | 103 |
|-------------------------------------------|-----|

|                             |     |
|-----------------------------|-----|
| 相关知识.....                   |     |
| 1. PPP CHAP认证.....          | 104 |
| 2. PPP CHAP配置方法.....        | 104 |
| 3. CHAP认证与PAP认证<br>的比较..... | 105 |

|          |     |
|----------|-----|
| 习题4..... | 107 |
|----------|-----|

## 第5章 网络安全管理..... 109

|                                     |     |
|-------------------------------------|-----|
| 5.1 【案例1】利用交换机端口安全<br>功能限制用户接入..... | 109 |
|-------------------------------------|-----|

|                   |     |
|-------------------|-----|
| 相关知识.....         |     |
| 1. 交换机端口安全概述..... | 110 |
| 2. 端口安全的默认配置..... | 111 |
| 3. 端口安全的配置方法..... | 111 |

|           |                                         |     |
|-----------|-----------------------------------------|-----|
| 5.2       | 【案例 2】利用 IP 标准访问列表控制网络流量 .....          | 113 |
|           | 相关知识                                    |     |
|           | 1. 访问列表概述 .....                         | 113 |
|           | 2. ACL 工作原理及规则 .....                    | 114 |
|           | 3. 访问列表种类 .....                         | 117 |
|           | 4. 配置 IP 标准 ACL 的方法 .....               | 117 |
| 5.3       | 【案例 3】利用 IP 扩展访问列表限制访问服务器 .....         | 120 |
|           | 相关知识                                    |     |
|           | 1. 编号的扩展 ACL .....                      | 120 |
|           | 2. 命名的扩展 ACL .....                      | 123 |
| 5.4       | 【案例 4】利用动态 NAT 技术实现高效安全访问 Internet..... | 125 |
|           | 相关知识                                    |     |
|           | 1. NAT 概念 .....                         | 126 |
|           | 2. NAT 用途 .....                         | 126 |
|           | 3. NAT 分类 .....                         | 126 |
|           | 4. NAT 术语 .....                         | 127 |
|           | 5. NAT 的工作过程 .....                      | 128 |
|           | 6. NAT 的配置方法 .....                      | 129 |
| 5.5       | 【案例 5】利用静态 NAT 安全发布内网 Internet 服务 ..... | 131 |
|           | 相关知识                                    |     |
|           | 1. NAT 工作过程 .....                       | 131 |
|           | 2. NAT 配置方法 .....                       | 132 |
| 5.6       | 【案例 6】使用防火墙实现安全的访问控制 .....              | 135 |
|           | 相关知识                                    |     |
|           | 1. 防火墙概念 .....                          | 135 |
|           | 2. 防火墙作用 .....                          | 135 |
|           | 3. 防火墙分类及工作原理 .....                     | 136 |
|           | 4. 防火墙工作模式 .....                        | 137 |
|           | 5. 防火墙三种模式的工作过程 .....                   | 137 |
|           | 6. 防火墙初始化配置方法 .....                     | 138 |
| 习题 5..... |                                         | 150 |

|            |                                 |     |
|------------|---------------------------------|-----|
| 第 6 章      | 网络设备 DHCP 服务配置.....             | 152 |
| 6.1        | 【案例 1】启用网络设备的 DHCP 服务 .....     | 152 |
|            | 相关知识                            |     |
|            | 1. DHCP 简介 .....                | 153 |
|            | 2. DHCP 的工作过程 .....             | 153 |
|            | 3. 配置命令 .....                   | 154 |
| 6.2        | 【案例 2】DHCP 中继服务 .....           | 156 |
|            | 相关知识                            |     |
|            | 1. DHCP 中继代理简介 .....            | 157 |
|            | 2. DHCP 中继代理的原理 .....           | 157 |
|            | 3. 配置命令 .....                   | 158 |
| 习题 6 ..... |                                 | 160 |
| 第 7 章      | 交换技术高级应用 .....                  | 162 |
| 7.1        | 【案例 1】应用 MSTP 实现网络冗余和负载均衡 ..... | 162 |
|            | 相关知识                            |     |
|            | 1. MSTP 产生的背景 .....             | 163 |
|            | 2. MSTP 的基本概念 .....             | 163 |
|            | 3. MSTP 的基本原理 .....             | 166 |
| 7.2        | 【案例 2】交换机端口限速 .....             | 170 |
|            | 相关知识                            |     |
|            | 1. QoS 概述 .....                 | 171 |
|            | 2. QoS 处理流程 .....               | 171 |
| 7.3        | 【案例 3】交换机端口镜像 .....             | 173 |
|            | 相关知识                            |     |
|            | 1. 理解 SPAN .....                | 174 |
|            | 2. SPAN 概念和术语 .....             | 174 |
|            | 3. 配置 SPAN .....                | 175 |
| 习题 7 ..... |                                 | 176 |
| 第 8 章      | 路由技术高级应用 .....                  | 178 |
| 8.1        | 【案例 1】OSPF 多区域互联 .....          | 178 |
|            | 相关知识                            |     |
|            | 1. OSPF 简介 .....                | 179 |
|            | 2. OSPF 的区域 .....               | 179 |
|            | 3. OSPF 的进程号 .....              | 179 |

- 8.2 【案例2】对 OSPF 邻居进行明文认证 ..... 181

相关知识

1. OSPF 认证技术 ..... 182
2. OSPF 认证的类型 ..... 182
3. OSPF 认证的配置 ..... 182
4. 明文认证 ..... 182
5. 密文认证 ..... 182

- 8.3 【案例3】对 OSPF 邻居进行密文认证 ..... 184

- 8.4 【案例4】实现动态路由重分配 ..... 187

相关知识

1. 路由重分布的概念 ..... 187
2. 路由重分布的配置 ..... 187

- 8.5 【案例5】使用 VRRP 实现路由备份 ..... 189

相关知识

1. VRRP 概念介绍 ..... 190
2. VRRP 的工作机制 ..... 191
3. VRRP 的配置 ..... 191

- 习题 8 ..... 193

## 第 9 章 访问列表高级应用 ..... 198

- 9.1 【案例1】基于时间的访问控制列表应用 ..... 198

相关知识

1. 基于时间的访问控制列表概述 ..... 199
2. 基于时间的访问控制列表配置 ..... 199

- 9.2 【案例2】专家级的访问控制列表应用 ..... 203

相关知识

1. 专家级的访问控制列表概述 ..... 203
2. 专家级的访问控制列表的配置 ..... 203

- 习题 9 ..... 207

## 第 10 章 应用 IPv6 技术 ..... 215

- 10.1 【案例1】学习 IPv6 基本知识 ..... 215

相关知识

1. IPv6 的主要特点 ..... 216
2. IPv6 地址格式 ..... 217
3. IPv6 地址类型 ..... 217

- 10.2 【案例2】通过手工 IPv6 隧道实现 IPv6 网络通信 ..... 220

相关知识

1. IPv6 隧道配置概述 ..... 221
2. IPv6 隧道类型 ..... 221
3. IPv6 隧道的配置 ..... 223
4. Windows XP 主机上手工配置 IPv6 地址 ..... 225

- 10.3 【案例3】配置 6 to 4 隧道实现 IPv6 接入子网 IPv6 主干网 ... 226

- 10.4 【案例4】建立 ISATAP 自动隧道 ..... 228

- 习题 10 ..... 229

## 参考文献 ..... 232

# 第0章

## 案例引入

### 能力目标

能为中小型企业规划设计网络方案。

### 知识目标

- 了解企业网络规划设计的需求。
- 了解并掌握企业网络体系结构与规划设计方法。

本章是企业网络规划设计案例的引入，主要内容包括计算网络的基本概念、组成及功能；Internet 的历史与发展；TCP/IP、IP 地址、域名和 IPv6；Internet 常用术语等。

## 0.1 网络规划设计背景

中小型企业网络与其他局域网一样，企业拥有自我建设、自我管理和自我使用的权利，因此，受经费、技术水平及其他方面的影响，企业网络在规划设计、资源建设和应用上很不平衡，差别很大，特别是在 IT 界目前还未实施网络工程监理的条件下存在很多问题，如有些中小型企业不考虑自身需求，一味追求高性能、高配置，构建的网络往往造成不必要的浪费；另一方面，有些中小型企业建成的网络根本达不到应用自身对网络性能的需求。因此，根据企业需求进行合理的网络规划和设计尤为重要，网络规划设计是网络工程的第一步，合理的网络规划设计可以让建好的网络更快、更有效率、更安全地运行。

本书主要以一个典型的中小型企业网络规划设计、建设及管理为出发点，介绍在网络规划设计、建设及管理过程中，需要考虑的各种因素及需要使用的网络技术。譬如，网络规划设计步骤、需求分析、规划设计原则、设计模型、交换技术、路由技术、安全技术等。

## 0.2 网络规划设计中的需求分析

### 0.2.1 网络规划设计中的需求分析概述

网络系统的规划设计主要分为六个阶段：需求分析、逻辑设计、物理设计、设计优化、实施及测试、监测及性能优化。在需求分析阶段，网络分析人员通过与用户和技术人员进行交流来获取用户对新的或升级系统的商业和技术目标，然后归纳出当前网络的特征，分析出当前和将来的网络通信量、网络性能，包括流量、负载、协议行为和服务质量要求。需求分析是开发过程中最关键的阶段，需求分析中的一个小的偏差，可能会导致以后各级工作的严重偏移，从而导致整个网络系统无法达到预期的效果。

## 0.2.2 网络规划设计中的需求分析过程

通过需求分析可以获取网络系统各方面的需求情况,网络设计人员通过咨询用户和专业技术人员,了解一个全新的或者升级的网络系统的商业和技术目标,然后描述现有网络,最后分析当前和未来的网络通信量。在需求分析过程中,主要考虑业务需求、用户需求、应用需求、计算机平台需求、网络需求这五个方面的需求。

(1) 业务需求调查是理解业务本质的关键,同一个企业有不同的职能分工,存在不同的业务需求,需要对不同的用户进行特定业务信息的搜集。通过获取组织结构图,了解该企业中岗位设置及岗位职责;通过确定各阶段及关键时间点制定日程表;通过投资规模确定网络工程的设计思路、技术线路、设备购置以及服务水平;通过确定业务活动来明确网络的需求;通过预测增长率来明确网络的伸缩性;通过网络的可靠性和可用性、Web 站点和 Internet 的连接性、网络的安全性、远程访问来确定网络的设计思路和技术路线。

(2) 用户需求针对的是当前网络用户,通过与用户群的交流了解用户需要的重要服务以及功能,并通过用户服务表对收集到的信息进行归档。

(3) 应用需求主要从应用系统自身的特点以及应用对资源的访问这两个角度去考虑应用的类型和地点、使用方法、需求增长、可靠性和可用性需求以及网络响应,最终编制出相应需求表。

(4) 计算机平台需求主要是了解用户进行各项操作对所运行的计算机软硬件方面有哪些需求,最终编制出相应需求表。

(5) 网络需求主要是考虑网络管理员的需求,包括局域网功能、网络拓扑结构、性能、网络管理、网络安全以及城域网/广域网的选择,最终编制出相应需求表。

## 0.2.3 网络规划设计中的需求分析

对用户的需求调查是需求分析的第一步,也是非常重要的一步,在很大程度上决定了整个工程设计的成败。需求分析包括提炼、分析已收集到的信息并得出正式的需求分析报告,并及时查漏补缺。提炼、分析的目的在于总结出精确的需求用以设计出高质量的网络系统。要形成文档以及需求表交与用户,并及时收集用户的反馈信息,再次提炼、分析,直到用户满意为止。在遇到一些专业问题时,应尽可能详细地告知投资者所存在的利弊,以满足用户的需求作为最大的目标。

在进行需求分析时除了考虑用户的需求还需要考虑外界的一些条件,否则也会导致网络系统无法实现。

(1) 政策约束。政策约束包括法律、法规、行业规定、业务规范、技术规范等方面的约束。在开发系统的过程中应遵照相关规定进行设计,确保工程正常顺利开展直至最终使用。

(2) 预算约束。在不超出用户预算的情况下采取优良的设计,若突破用户的预算再优良的设计也无法实现。

(3) 时间约束。在项目进度方面,需要编制合理的项目进度表,保证系统按时完工。

## 0.3 网络规划设计的原则

中小型企业网络的规划设计有多种解决方案,根据企业网络的类型、规模和性质不同,企

业网络的设计方案有所不同,体现在技术、应用上更是不同。在传统的语音服务无法满足中小型企业各种业务信息需求的今天,中小型企业对图形、图像、视频等多媒体信息的需求不断增长,多媒体信息已成为中小型企业依赖计算机网络进行信息共享和交流的重要资源。企业网络应分为内部网络和外部网络两个部分,其中还包括在这两部分上的实际应用。中小型企业在网络设计之初就应该充分考虑自身的需求,通过这些需求来具体设计适合自己的网络。

### 0.3.1 目标原则

用户的需求往往有分阶段的近期目标和远期目标,要明确不同阶段的建设目标,考虑到网络系统的规模。必须确定协议集、体系结构、计算模式、网络上最多站点数目和网络最大覆盖范围等的类型和范围,同时应对整个系统的数据量、数据流量和数据流向有个清醒的估计,遵循近期建设目标所确定的网络方案有利于升级和扩展到最终建设目标的原则。

依据企业建网资金的安排,在听取有关专家意见的基础上,结合企业的业务内容及其发展的需要,制定一个在未来五年中的近期、中期及长期的建设规划,以保持网络建设的延续性,保护先前的投资(含各种硬件、软件及信息资源),并能融合不断涌现的新技术和新应用。

### 0.3.2 组网原则

(1) 先进性。网络系统的先进性是规划设计人员要首先考虑的。采用先进的组网技术,能使所建网络在长时间内保持先进性和可用性,在相当长的一段时间内不至于落后或淘汰,而且能适应近期及中远期业务的需求。

(2) 可扩充性。采用模块式和结构化设计,并采用分步实施的建设策略,使网络系统配置灵活。同时,留有合理的扩充余地,既能满足用户数量的扩充,又能满足因技术发展需要而实现低成本扩展和升级的需求。

(3) 安全可靠。安全与可靠是组网的重要原则之一。应从安全体系、网络结点、通信线路、网络拓扑等多方面考虑,保证整个系统的安全性和保密性。如在局域网和广域网的互联点上设置防火墙,在多层次上以多种方式实现安全性控制等,以抵御来自网络内部或外部的攻击。

(4) 可管理维护性。在网络设计中,要建立全面的网络管理解决方案。不仅要保证整个网络系统集成规划设计的合理性,还应配置相关的检测设备和管理设施,重视售前和售后维护工作。

(5) 开放互联性。采用符合当前最新的软硬件国际标准的通信协议和设备,支持开放的技术、结构、系统组件及用户接口,使网络系统与多种协议计算机有良好的通信互联能力。

(6) 经济实用性。充分利用投入的资金,以较高的性价比构建网络系统。根据用户的需求,在满足系统性能以及在可预见期间内不失先进性的前提下,尽量使整个系统投资合理且实用性强。

## 0.4 企业网络总体设计

企业网络解决方案总体设计以高可靠性、高性能、高安全性、良好的可扩展性、可管理性和统一的网管系统及可靠组播为原则,考虑到技术的先进性、成熟性,采用模块化的设计方法。

### 0.4.1 企业网络层次化结构设计

在企业园区网络整体设计中,采用层次化、模块化的网络设计结构,并严格定义各层功

能模型,不同层次关注不同的特性配置。典型的企业园区网络结构可以分成接入层、汇聚层、核心层,如图 0-1 所示。

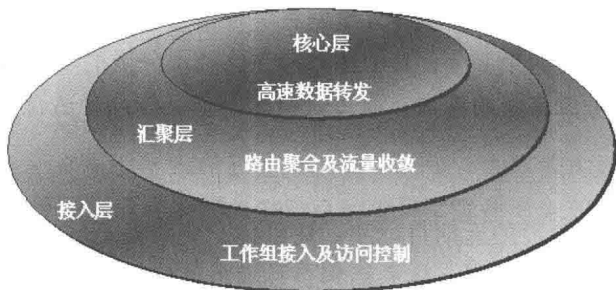


图 0-1 网络设计分层结构图

(1) 接入层。提供网络的第一级接入功能,完成简单的二、三层交换,接入安全、Qos 和 POE 功能都位于这一层。对应于企业园区网的接入层设备。

(2) 汇聚层。汇聚来自配线间的流量和执行策略,当路由协议应用于这一层时,具有负载均衡、快速收敛和易于扩展等特点,这一层还可作为接入设备的第一跳网关;对于企业网的汇聚层设备,应该能够承载企业网的多种融合业务。

(3) 核心层。网络的主干,必须能够提供高速数据交换和路由快速收敛,要求具有较高的可靠性、稳定性和易扩展性等。对于企业园区网核心层,必须提供高性能、高可靠的网络结构,采用高可靠的环网结构或多设备冗余的星形结构。对于企业网核心层设备,应该在提供大容量、高性能 L2/L3 交换服务基础上,能够进一步融合硬件 IPv6、网络安全、网络业务分析等智能特性,可为企业网构建融合业务的基础网络平台,进而帮助企业实现 IT 资源整合的需求。

在企业网络设计中,使用层次化模型有许多好处,列举如下:

(1) 节省成本。在采用层次模型之后,各层次各司其职,不再在同一个平台上考虑所有的事情。层次模型模块化的特性使网络中的每一层都能够很好地利用带宽,减少了对系统资源的浪费。

(2) 易于理解。层次化设计使得网络结构清晰明了,可以在不同的层次实施不同难度的管理,降低了管理成本。

(3) 易于扩展/在网络设计中,模块化具有的特性使得网络增长时网络的复杂性能限制在子网中,而不会蔓延到网络的其他地方。而如果采用扁平化和网状设计,任何一个结点的变动都将对整个网络产生很大影响。

(4) 易于排错。层次化设计能够使网络拓扑结构分解为易于理解的子网,网络管理者能够轻易地确定网络故障的范围,从而简化了排错过程。

#### 0.4.2 层次化模型应用方案

基于网络分层结构设计的思想,结合企业的实际情况,层次化模型主要有如下两种应用方案。

(1) 基于交换的层次结构。这种应用方案(见图 0-2),所有层次上使用的都是交换机设备。核心层、汇聚层、接入层这种层次化的网络设备模型,特别适合于具有上千台工作站的大中型企业网络的设计,如果是只有几百台计算机的中小型网络,可以采用将核心层和汇聚层合二为一的方案。

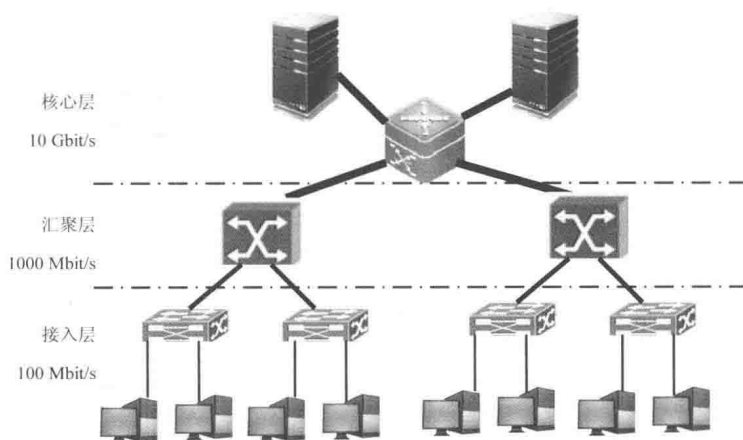


图 0-2 基于交换的层次结构

（2）基于路由的层次结构。这种应用方案（见图 0-3）在汇聚层提供策略交换速率的是路由器设备，由于路由交换要比交换机慢（这是路由器自身工作原理决定的），所以这种方案比较适用于数据流量不是很大的场合。如果数据流量比较大，又要避免网络拥塞，就需要购买高性能路由器。

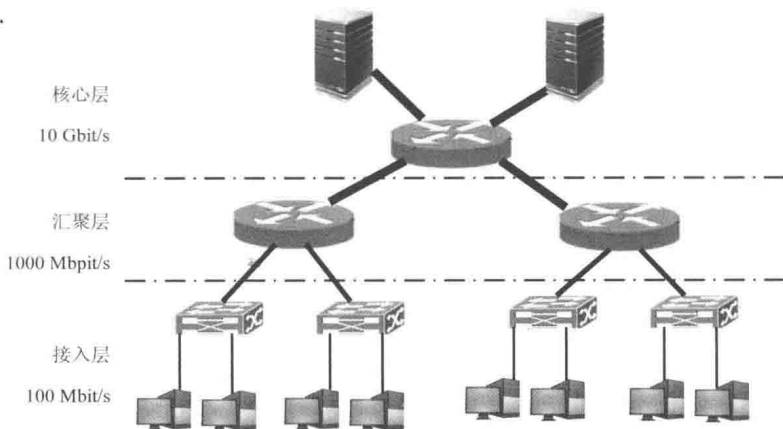


图 0-3 基于路由的层次结构

## 0.5 企业网络规划设计案例引入及 本书学习情境案例分解

为了学习网络规划设计与建设所涉及的知识或技术，本书引入一个典型企业网络规划设计案例展开讨论。

图 0-4 所示是一个典型企业网络拓扑图，它也是网络层次化模型的一个应用方案。根据企业网络的拓扑图与应用需求，要能建设与管理好这样的网络，对网络管理员来说需要掌握大量网络管理与设备配置方面的知识。结合这一企业网络案例的建设，我们把要学习的知识分解为以下各章节与学习案例，在各个案例学习过程中穿插介绍相关知识点或网络管理与建设的关键技术。

### 1. 管理交换网络

交换网络是整个企业网络的基础和核心,交换网络建设的好坏对网络性能的发挥、网络应用的运行以及是否便于管理网络都有着直接的影响。而交换网络的核心设备就是交换机,为此首先要认识交换机,学习交换机的工作原理等;其次为了便于进行网络管理,需配置交换机远程登录功能、在交换机上配置 VLAN 等。因此将本章节案例分解为:

- 【案例 1】认识交换机。
- 【案例 2】远程登录交换机。
- 【案例 3】使用 VLAN 技术隔离子网。
- 【案例 4】跨交换机实现 VLAN 内部通信。

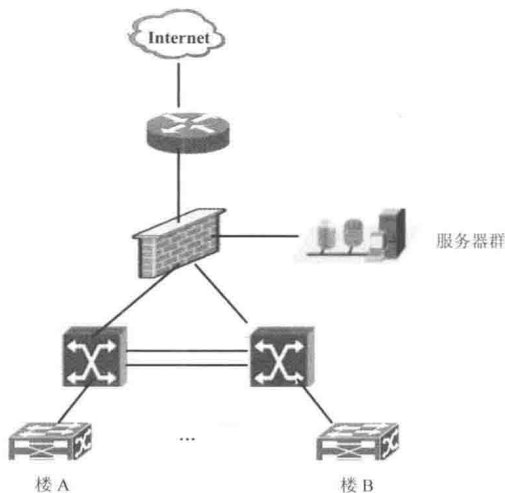


图 0-4 典型企业网络拓扑图

### 2. 管理局域网中的冗余链路

在交换网络中,为了提高链路的安全性,往往在网络规划和建设时会增加交换机等设备,有时还会在交换机设备间增加多条链路(如图 0-4 中,两台三层交换机之间使用两根网线相连),达到冗余备份或增加带宽的目的。但在交换机增加链路的同时,也带来一些负面影响,如广播风暴、MAC 地址表抖动等问题,严重情况下会导致网络瘫痪,所以必须有相应的技术作保障,如生成树协议、端口聚合技术等。因此将本章节案例分解为:

- 【案例 1】使用生成树协议解决备份链路中的环路问题。
- 【案例 2】使用交换机端口聚合技术实现负载均衡及链路备份。

### 3. 管理网络路由

在 TCP/IP 网络中,每个网段是相互分隔的,不能直接交换数据。为了实现在不同网络间转发数据单元的功能,必须借助于三层设备,最典型的代表就是路由器和三层交换机。路由器的主要工作就是为经过路由器的每个数据单元寻找一条最佳传输路径,并将该数据有效地传送到目的站点。因此在本章节中,要认识路由器这种设备,学习路由器工作原理等;其次为了便于进行网络管理,需配置路由器远程登录功能、在路由器或三层交换机上配置路由策略来实现子网互联。因此将本章节案例分解为:

- 【案例 1】认识路由器。
- 【案例 2】远程登录路由器。
- 【案例 3】利用单臂路由实现 VLAN 之间路由。
- 【案例 4】利用三层交换机实现 VLAN 之间路由。
- 【案例 5】利用静态路由实现各区域子网互通。
- 【案例 6】利用 RIP 路由协议实现各区域子网互通。
- 【案例 7】利用 OSPF 动态路由协议实现各区域子网互通。

### 4. 管理广域网链路

为了能够访问外部的网络(如 Internet),在企业局域网络建好后,一般要向 ISP 申请广域网链路接入 Internet。一般的做法是使用路由设备(企业出口路由器)与 ISP 的路由设备相

连接（见图 0-4）。为了实现安全接入，一般要对这种广域网链路进行认证，常见的有 PPP 协议的 PAP 认证和 CHAP 认证。因此将本章节案例分解为：

【案例 1】在路由器接口上封装广域网协议。

【案例 2】利用 PPP PAP 认证实现广域网链路的安全性。

【案例 3】利用 PPP CHAP 认证实现广域网链路的安全性。

## 5. 网络安全管理

随着互联网发展和 IT 的普及，网络和 IT 已经日渐深入人们的日常生活和工作当中，社会信息化和信息网络化突破了应用信息在时间和空间上的障碍，使信息的价值不断提高。但是与此同时，网页篡改、计算机病毒、系统非法入侵、数据泄密、网站欺骗、服务瘫痪、漏洞非法利用等信息安全事件时有发生。

在企业规划建设网络的过程中，如何保证网络安全运行也是网络规划设计者必须考虑的问题。目前常用的方法或技术手段主要有：接入控制、访问控制列表 ACL、地址转换技术 NAT、防火墙技术等。因此将本章节案例分解为：

【案例 1】利用交换机端口安全功能限制用户接入。

【案例 2】利用 IP 标准访问列表控制网络流量。

【案例 3】利用 IP 扩展访问列表限制访问服务器。

【案例 4】利用动态 NAT 技术实现高效安全访问 Internet。

【案例 5】利用静态 NAT 安全发布内网 Internet 服务。

【案例 6】使用防火墙实现安全的访问控制。

## 6. 网络设备 DHCP 服务配置

DHCP 服务是一种常用的服务器技术，主要功能是给网络上的 PC 自动分配 IP 地址、子网掩码、网关、DNS 服务器地址等信息，一般是在安装了服务器操作系统的服务器上配置。本章介绍如何在网络设备上配置。因此将本章节案例分解为：

【案例 1】启用网络设备的 DHCP 服务。

【案例 2】DHCP 中继服务。

## 7. 交换技术高级应用

MSTP 是一种多生成树技术，可以让不同的 VLAN 数据走不同的路径，提供了比生成树和快速生成树更优秀的网络冗余和负载均衡；交换机是 PC 的直接接入端，在交换机上进行端口限速可以在网络的最末端限制 PC 的上网速度，限速更有效率且更可靠；当网络上的交换机出现异常情况的时候，通过交换机端口镜像功能，可以很好地分析网络流量包。因此将本章节案例分解为：

【案例 1】应用 MSTP 实现网络冗余和负载均衡。

【案例 2】交换机端口限速。

【案例 3】交换机端口镜像。

## 8. 路由技术高级应用

OSPF 是一种链路状态路由选择算法，它在工作的时候必须有一个主工作区 0，当网络规模比较大的时候还有更多的工作区，如工作区 1、工作区 2 等，这时必须解决不同工作区互联的问题；OSPF 算法在工作的时候需要跟邻居路由器不断地收集数据，而不安全的路由器会

利用这种机制传来不安全的数据,因此 OSPF 对邻居进行认证很有必要;当把运行不同路由算法的网络互联时,一个很重要的工作就是让路由信息从一个网络到达另一个网络,这就是路由重分配;路由器的工作是在不同的网络中寻路,如果路由器出现故障,很可能会导致部分网络不通,因此对路由器进行冗余备份也很重要。因此将本章节案例分解为:

【案例 1】OSPF 多区域互联。

【案例 2】对 OSPF 邻居进行明文认证。

【案例 3】对 OSPF 邻居进行密文认证。

【案例 4】实现动态路由重分配。

【案例 5】使用 VRRP 实现路由备份。

### 9. 访问列表高级应用

通过在三层设备上配置访问控制列表,可以对流经三层设备的数据流进行精确的控制,高级访问列表可以实现更高级、更精细的匹配条件,进而实现更复杂的数据流控制。因此将本章节案例分解为:

【案例 1】基于时间的访问控制列表应用。

【案例 2】专家级的访问控制列表应用。

### 10. 应用 IPv6 技术

随着上网设备的增加,IPv4 提供的 IP 地址已用完,这种情况下推出了第六版本的 IP 协议 IPv6,IPv6 可以提供更大的 IP 地址空间,为上网设备的增加提供可能,但目前仍有大量的 IPv4 网络存在,为了实现 IPv4 和 IPv6 网络共存和互联,必须使用隧道技术。因此将本章节案例分解为:

【案例 1】学习 IPv6 基本知识。

【案例 2】通过手工 IPv6 隧道实现 IPv6 网络通信。

【案例 3】配置 6 to 4 隧道实现 IPv6 接入 IPv6 主干网。

【案例 4】建立 ISATAP 自动隧道。

## 习 题 0

1. 简述网络层次化规划设计的好处。
2. 谈谈你对网络规划设计重要性的认识。

# 第1章

## ➡ 管理交换网络

### 能力目标

能针对不同的网络环境使用相应的方法或手段对园区网中的交换网络部分进行简单配置和管理。

### 知识目标

- 了解交换机的登录方式，掌握配置交换机的远程登录服务的方法。
- 掌握交换机的工作原理及常用配置命令。
- 掌握交换机的 VLAN 技术及应用。

### 章节案例及分析

在一个园区网络的管理中，对交换网络的管理占很大的比重，交换网络配置管理直接影响网络的性能，并且会影响网络管理员的工作强度。因此，要管好一个园区网，首先需要熟悉交换技术，掌握交换机的配置管理命令。在交换机管理中最常使用的技术是 VLAN 技术，所以要掌握 VLAN 技术并能应用在交换网络管理中。为了方便管理，又要提供对交换机远程管理的支持。对应典型的企业网络（见图 0-4），我们要在各级交换机上做相应配置，保证各部门数据交换顺利，并且方便管理员对设备进行管理。

本章分为四个案例：一是让学者对交换机有所认识，主要介绍交换机的外观、接口、指示灯等，同时对交换机的工作原理作一个简要阐述；二是介绍如何远程登录交换机，包括对交换机如何配置远程登录功能以及如何使用 telnet 命令远程登录交换机，同时熟悉交换机的命令模式和常用配置命令等；三是介绍如何在交换机上通过创建 VLAN 对子网进行隔离，同时介绍 VLAN 的概念、用途、种类、标准及配置命令等；四是介绍如何跨交换机实现同一 VLAN 子网内部互通，并且对实现该案例所需的知识，如 VLAN Trunk、Native VLAN 和 Trunk 接口的许可访问列表等作介绍。

## 1.1 【案例 1】认识交换机

### 学习目标

- (1) 认识交换机设备，了解交换机各种接口类型、功能及作用、外观、指示灯。
- (2) 了解交换机的一些性能参数（背板能力、吞吐量等）。
- (3) 掌握交换机工作原理。
- (4) 熟悉交换机的访问方式及命令模式。