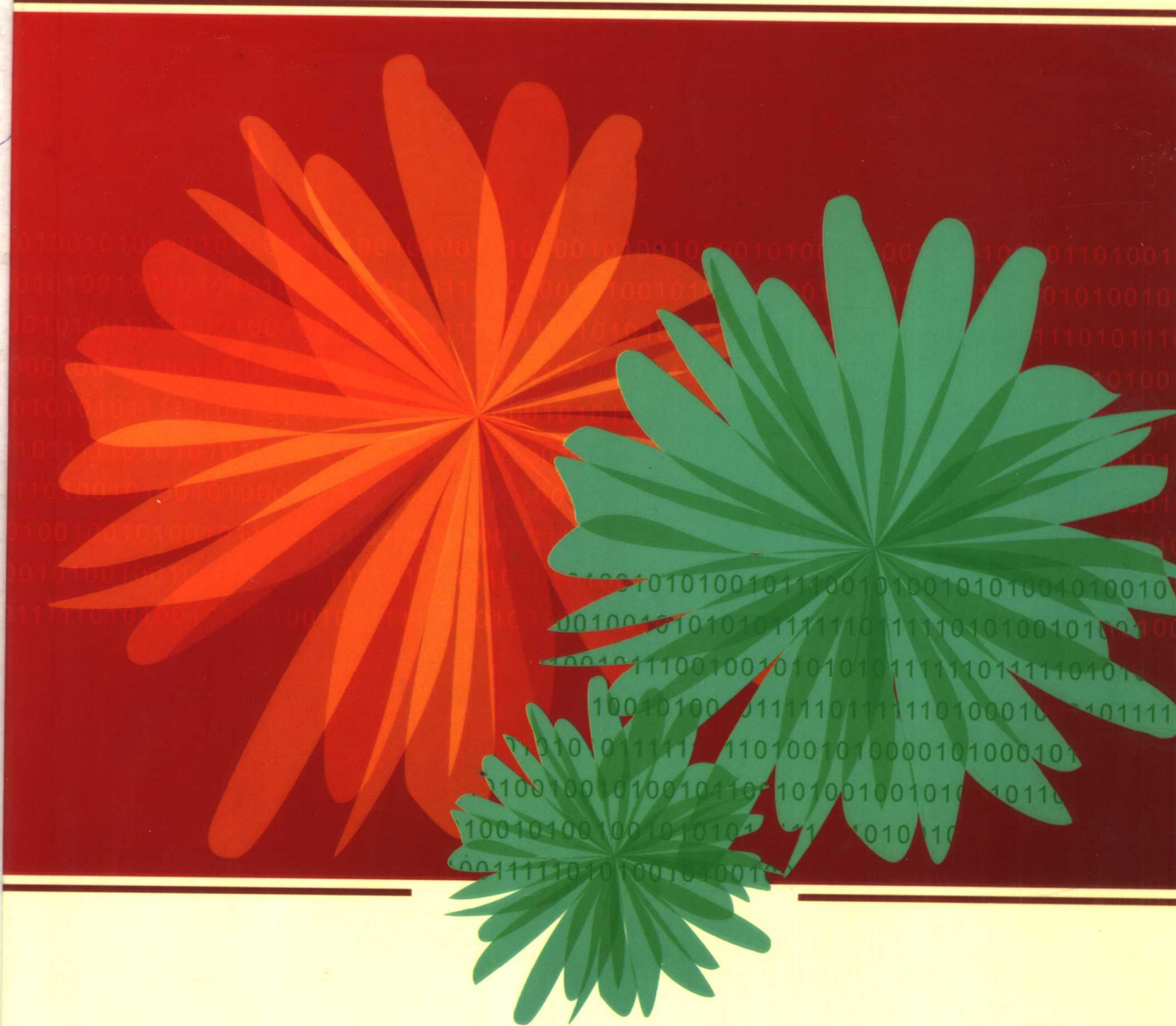




路由器交换机原理及应用

主 编 张应辉 饶云波
副主编 王 津 凌 艳



高职高专“十一五”规划示范教材

路由器交换机原理及应用

主 编 张应辉 饶云波
副主编 王 津 凌 艳

北京航空航天大学出版社

内 容 简 介

本书是根据高职高专教育培养高级技能人才的要求,突出“实践性、实用性、创新性”,并结合作者多年的教学和工程实践经验,以理论够用、实用为主的原则而编写的一本路由器交换机原理及应用教材。主要内容是:交换机概述、交换机配置及应用、路由器基础、局域网协议及配置、虚拟专用网络 VPN、访问控制列表配置、路由器安全配置、VoIP 配置。

本书参考了大量的最新资料,内容丰富翔实,突出了以实例为中心的特点。

本书既可作为承担国家技能型紧缺人才培养的高职高专院校计算机类、信息管理类专业的教材,也可供从事网络研究的技术人员和其他对网络技术有兴趣的人员参考。

图书在版编目(CIP)数据

路由器交换机原理及应用/张应辉等主编. —北京:
北京航空航天大学出版社, 2006. 8

ISBN 7-81077-792-0

I. 路… II. 张… III. ①计算机网络—路由选择
—高等学校: 技术学校—教材②计算机网络—信息交换
机—高等学校: 技术学校—教材 IV. TN915.05

中国版本图书馆 CIP 数据核字(2006)第 084659 号

路由器交换机原理及应用

主 编 张应辉 饶云波

副主编 王 津 凌 艳

策划编辑 蔡 喆 李明富

责任编辑 刘晓明

*

北京航空航天大学出版社出版发行

北京市海淀区学院路 37 号(100083) 发行部电话:010-82317024 传真:010-82328026

<http://www.buaapress.com.cn> E-mail: bhp@263.net

涿州市新华印刷有限公司印装 各地书店经销

*

开本: 787 mm×960 mm 1/16 印张: 14.75 字数: 330 千字

2006 年 8 月第 1 版 2006 年 8 月第 1 次印刷 印数: 4 000 册

ISBN 7-81077-792-0 定价: 22.00 元



高职高专“十一五”规划示范教材

编委会

主 任

张应辉

副主任

(按姓氏笔画排序)

王海春

汤 勇

杨 闯

林训超

饶云波

郭 杰

策划编委

李明富

《路由器交换机原理及应用》编委

(按姓氏笔画排序)

王 龙	王 洵
王 津	刘 峰
刘洪涛	刘晋州
李德智	麦兴隆
卓能文	柴 晟
凌 艳	曹 毅
曾 鹏	曾伟一
谭 力	谭 飞



为了适应网络应用深化带来的挑战,网络的规模和速度都在急剧发展,局域网的速度已从最初的 10 Mbit/s 提高到 100 Mbit/s,目前千兆以太网技术已得到普遍应用。作为网络中最常用的两种设备,路由器和交换机显得特别重要。

全书共分 9 章。

第 1 章是交换机概述,重点讲解了交换机的作用、组成、分类,交换机在网络中的连接及作用,交换技术基础等。

第 2 章是交换机的配置及应用,讲解了生成树协议、二层交换机基本配置和基于端口 VLAN 的划分。

第 3 章是路由器基础,主要讲述了路由器的构成、优缺点,第三层交换机与路由器的区别,路由器的分类,路由器的基本配置,路由器体系结构的发展等。

第 4 章是局域网协议及配置,讲述了路由协议的分类及不同路由协议的特点、静态路由配置、动态路由 RIP 配置、动态路由 OSPF 及 PPP-CHAP 验证实验、动态路由 EIGRP 配置、动态路由和 IGRP 配置等。

第 5 章是广域网协议及配置,讲述了广域网协议与 OSI 参考模型的关系、广域网种类、X.25 配置、帧中继配置、DDN 配置、PPP 协议配置和 ISDN 配置等。

第 6 章是虚拟专用网络 VPN,重点讲述了 VPN 基础、VPN 的建立方式与安全保证、三种 VPN 解决方案、VPN 与隧道协议和用 Cisco 2600 配置 VPDN 等。

第 7 章是访问控制列表配置,重点讲述了 ACL 的概述、ACL 的工作过程、ACL 分类和 ACL 配置等。

第 8 章是路由器安全配置,重点讲述了 NAT 服务配置、CiscoPIX 防火墙、IPSec 协议分析与实现等。

第 9 章是 VoIP 的配置,重点讲述了 IP 电话的基本原理与技术、IP 电话的组成、IP 电话的基本原理与技术、VoIP 的实现方式、IP 电话技术与展望。

关于计算机网络技术基础的书籍,目前出版的比较多,但适合高职高专院校读者的书很少。本书为“‘十一五’规划示范教材”之一,全书遵从高职高专教学规律。教材的编写遵循“实用技术为主、工程实践为线、侧重主流产品”的指导思想,立足于“看得懂、学得会、用得上”的策略。读者只有通过具体的实践,才能加深对所学基础知识的理解,只有经历了实践的全过程,

才能系统地掌握各个环节的基本技能。本书是结合作者多年的教学经验编写出来的,语言通俗易懂,论证由浅入深,内容丰富翔实,突出“实践性、实用性、创新性”。

全书由张应辉、饶云波任主编,王津、凌艳任副主编。其中,第2,5章由张应辉编写;第6章由饶云波编写;第4,7,8,9章由王津编写;第1章由凌艳编写;第3章由曾鹏编写。

本书的出版得到了成都东软信息技术学院的资助,并得到了北京航空航天大学出版社、成都东软信息学院计算机系的大力支持和帮助。周明天教授对本书提出了很好的意见。同时我们也从很多网站和论坛上得到了大量的知识和资源,也向这些站点的所有者和参与者表示真诚的感谢。

由于作者水平有限,加之成书仓促,书中如有不妥与错误之处,恳请读者不吝指正,以便在本书再版时修改和充实。

作 者

2006年7月

目 录

第 1 章 交换机概述

1.1 交换机的作用与组成	1
1.1.1 交换机的作用	1
1.1.2 交换机的组成	2
1.2 交换机的分类	3
1.2.1 OSI 参考模型与数据通信设备	3
1.2.2 交换机的简单分类	5
1.3 交换机在网络中的连接及作用	6
1.3.1 交换机的端口	6
1.3.2 共享式与交换式网络	8
1.4 交换技术基础	10
1.4.1 MAC 地址数据表的建立与路由过滤	10
1.4.2 局域网的三种帧交换方式	15
1.4.3 冗余备份与环路	15
1.5 本章习题	17

第 2 章 交换机的配置和应用

2.1 生成树协议(STP)	19
2.1.1 STP 协议原理	19
2.1.2 STP 的端口状态	22
2.2 二层交换机基本配置及基本端口 VLAN 的划分(Cisco 2950 实现)	23
2.2.1 Cisco 2950 交换机介绍	23
2.2.2 Cisco 交换机配置软件 IOS 介绍	24
2.2.3 Cisco 交换机的基本配置命令	25
2.2.4 VLAN 的概念和划分	31
2.2.5 生成、修改以太网 VLAN	32
2.2.6 删除 VLAN	33

2.2.7 将端口分配给一个 VLAN	34
2.3 二层交换机实现 Trunk 及 VTP 的配置(Cisco 2950 实现)	35
2.3.1 Trunk 以及 Trunk 的优点	35
2.3.2 VTP	37
2.3.3 配置 Trunk 和 VTP	38
2.4 三层交换机实现 VLAN 及 DHCP 配置(Cisco 3350 实现)	40
2.4.1 三层交换机的概念和特点	40
2.4.2 三层交换机的 VLAN 配置	41
2.4.3 三层交换机的 DHCP 配置	43
2.5 本章习题	45

第3章 路由器基础

3.1 路由器概述	47
3.1.1 路由器的基本构成	48
3.1.2 路由器的原理	49
3.1.3 路由器的基本功能	51
3.1.4 路由器的作用	52
3.1.5 路由器的优缺点	52
3.2 第三层交换机与路由器的区别	53
3.2.1 路由器与交换机的区别	53
3.2.2 路由器与第三层交换机的区别	53
3.3 路由器的分类	55
3.4 Cisco 路由器概述	56
3.5 Cisco 路由器接口及模块简介	58
3.5.1 普通 RJ-45 接口	58
3.5.2 Cisco 路由器模块	59
3.6 路由器的基本配置	62
3.6.1 路由器的硬件配置	62
3.6.2 路由器的硬件连接	65
3.7 路由器体系结构的发展	70
3.8 本章习题	72

第4章 局域网协议及配置

4.1 路由协议的分类	75
-------------------	----

4.1.1 路由协议	75
4.1.2 路由协议分类	76
4.2 不同路由协议及其特点	76
4.2.1 RIP 路由协议	77
4.2.2 OSPF 路由协议	77
4.2.3 IGRP 路由协议	78
4.2.4 EIGRP 路由协议	80
4.2.5 IS-IS 路由协议	81
4.2.6 BGP 路由协议	81
4.3 路由器配置	83
4.3.1 路由器配置概述	83
4.3.2 路由配置命令	84
4.4 静态路由配置	86
4.4.1 静态路由配置概述	86
4.4.2 静态路由配置实例	87
4.5 动态路由 RIP 配置	88
4.5.1 RIP 配置概述	88
4.5.2 RIP 配置实例	88
4.6 动态路由 OSPF 及 PPP-CHAP 验证实验	90
4.6.1 OSPF 配置概述	90
4.6.2 OSPF 配置实例	91
4.6.3 PPP-CHAP 原理及配置	91
4.7 动态路由和 IGRP 配置	95
4.7.1 IGRP 配置概述	95
4.7.2 IGRP 配置实例	96
4.8 动态路由和 EIGRP 配置	97
4.8.1 EIGRP 配置概述	97
4.8.2 EIGRP 配置实例	98
4.9 本章习题	99
 第 5 章 广域网协议及配置	
5.1 广域网协议与 OSI 参考模型的关系	101
5.1.1 广域网 WAN	101
5.1.2 OSI 参考模型	102

5.1.3 广域网协议以及与 OSIRM 的对应	102
5.2 广域网的种类	103
5.2.1 广域网分类	103
5.2.2 各种类型中的典型广域网介绍	103
5.3 X.25 配置	104
5.3.1 X.25 的配置命令及其功能	104
5.3.2 X.25 通信原理以及 DTE 配置实例	105
5.4 帧中继配置	112
5.4.1 帧中继的配置命令及其功能	112
5.4.2 帧中继通信原理以及配置实例	112
5.5 DDN 配置	117
5.5.1 DDN 数字数据网	117
5.5.2 DDN 基本命令	118
5.6 PPP 协议配置	119
5.6.1 PPP 点到点协议	119
5.6.2 PPP 协议的配置	120
5.7 ISDN 配置	121
5.7.1 ISDN 综合数字业务网	121
5.7.2 ISDN 配置示例	123
5.8 本章习题	124

第 6 章 虚拟专用网络 VPN

6.1 VPN 基础	126
6.1.1 什么是 VPN	126
6.1.2 VPN 的特点	127
6.2 VPN 的建立与安全保证	128
6.2.1 VPN 的建立方式	128
6.2.2 VPN 的安全保证	129
6.3 三种 VPN 解决方案	130
6.3.1 Access VPN	130
6.3.2 Intranet VPN	131
6.3.3 Extranet VPN	131
6.4 VPN 与隧道技术	132
6.4.1 隧道技术与隧道协议	132

6.4.2 L2TP 隧道的呼叫建立过程	136
6.5 用 Cisco 2600 配置 VPDN	140
6.5.1 认证步骤配置	140
6.5.2 VPDN 配置的三个组成部分及其配置步骤	141
6.6 本章习题	147
 第 7 章 访问控制列表配置	
7.1 ACL 的概述	150
7.1.1 什么是 ACL	150
7.1.2 ACL 的功能	151
7.2 ACL 的工作过程	153
7.2.1 ACL 的操作过程	153
7.2.2 ACL 的逻辑测试过程	154
7.3 ACL 的分类	158
7.3.1 标准的访问控制列表	158
7.3.2 扩展的访问控制列表	160
7.3.3 编号的访问控制列表	161
7.3.4 命名的访问控制列表	161
7.3.5 时间相关的访问控制列表	162
7.4 ACL 配置	162
7.4.1 创建 ACL	162
7.4.2 将 ACL 绑定到某个端口	163
7.4.3 命名的 ACL 设置和绑定	164
7.4.4 时间相关的 ACL 设置	166
7.5 本章习题	169
 第 8 章 路由器安全配置	
8.1 NAT 服务配置	172
8.1.1 网络地址转换 NAT	172
8.1.2 NAT 的特征和实现	174
8.1.3 NAT 的配置	179
8.2 Cisco PIX 防火墙	182
8.3 IPSec 协议分析与实现	186
8.3.1 IPSec 概述	186

8.3.2 IPsec 设计与实现	191
8.4 本章习题	197

第9章 VoIP 配置

9.1 IP 电话的基本原理与技术	199
9.1.1 Internet 电话带来的冲击	199
9.1.2 Internet 电话的原理	200
9.2 IP 电话技术与展望	201
9.2.1 IP 电话技术与传统电话的对比	201
9.2.2 Internet 电话展望	206
9.3 IP 电话系统组成	206
9.4 实现 VoIP 的方式	208
9.4.1 IP 话机方式与 VoIP 语音网关方式的比较	209
9.4.2 IP 话机方式在语音网关方式中的应用	210
9.5 VoIP 网络设备	211
9.6 VoIP 业务的试验平台	212
9.7 Cisco 路由器实现 VoIP	214
9.8 本章习题	218

参考文献

第 1 章 交换机概述

本章教学目标

- ◇ 了解交换机的结构和组成
- ◇ 掌握交换机的分类
- ◇ 掌握交换机在网络中的连接及作用
- ◇ 理解交换技术基础

交换机工作在 ISO 参考模型的第二层——数据链路层。在计算机网络系统中,交换概念的提出是对于共享工作模式的改进。交换机是一种基于物理地址识别的、可以完成存储转发报文功能的局域网设备。在同一时刻,交换机可以传输多个端口对之间的数据。交换机主要是在以太网中广泛使用。

1.1 交换机的作用与组成

1.1.1 交换机的作用

交换机在以太网中起到数据报文转发的作用。它把从某个端口接收到的数据报文从其他端口转发出去,除了连接同种类型的网络之外,还可以在不同类型的网络(以太网和快速以太网)之间起到互联作用。现在一般的交换机所支持的网络主要是以太网、快速以太网和千兆以太网。

交换机最大的作用在于能有效地抑制广播风暴的产生。这主要是因为交换机是基于 MAC 地址进行交换的,通过分析 MAC 帧的帧头信息(源 MAC 地址、目的 MAC 地址、MAC 帧长等),取得目的 MAC 地址后,查找交换机中存储的 MAC 地址表(与 MAC 地址相对应的交换机的端口号),确认有此 MAC 地址的网卡连接在交换机的哪个端口上,然后将数据报文发送到相应的端口上。这也是交换机不同于物理层的设备——集线器的最大不同点。交换机和集线器的冲突域如图 1-1 所示。

交换机还将连接的交换网络的每个网段都单独划分开来,有效降低以太网中广播信道的冲突,所以支持更多的网络节点,这就使得很多局域网可以形成一个很大的以太网。

另外,交换机的成本比较便宜,容易安装和维护,具有自适应功能。这些优势使得交换机在短短数年内已经被广泛用于各种应用场合。现在 Cisco 公司的 Catalyst 系列交换机是目前全世界最流行的交换机,所使用的配置命令都是兼容的。



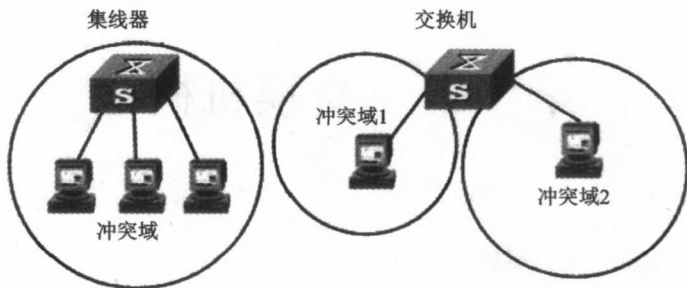


图 1-1 交换机和集线器的冲突域

1.1.2 交换机的组成

交换机由以下几个部分组成。

- MPU(MAC 处理器): 交换机的 MPU 是专用的集成电路芯片 ASIC。它比通用的 CPU 更专业化,针对 MAC 数据报文的处理速度更快,可以实现高速的数据传输。处理器随着具体的交换机模型不同而不同。
- 背板交换矩阵,主要是完成 $N \times N$ 的高速交换的功能。
- PHY(物理层处理器): 交换机的 PHY 和 HUB(集线器)的端口电路芯片是一样的,完成 bit 级数据的收发。
- RAM/DRAM: 主存储单元,也被称作内存。它可以存储交换机需要运行的配置。
- Flash: 存储系统软件和配置文件等的可程式存储器,也被称为“闪存”。
- RJ-45: 以太网的标准接口。它由 4 对连线组成,总共 8 个连接。这种接口就是现在最常见的网络设备接口,俗称“水晶头”,属于双绞线以太网接口类型。RJ-45 插头只能沿固定方向插入,设有一个塑料弹片与 RJ-45 插槽卡住,以防止脱落。图 1-2 是 RJ-45 的实物示意图。

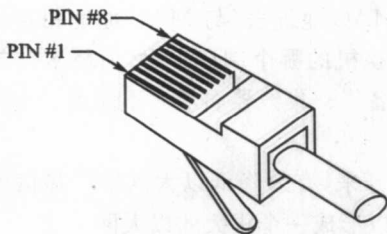


图 1-2 RJ-45 实物示意图

- 启动软件: 启动软件一般是固化存储在 ROM 或者 Flash 存储芯片中的,如果存储在 ROM 之中,那么,产品一旦成型,就不能改动启动程序;如果是采用 Flash 芯片存储启动程序,那么一旦启动程序异常,就可以利用配置命令将缺省的启动程序从本地计算机下载到交换机内部,不但可以减少维修交换机所使用的成本,也可以使得交换机具有健壮性。

- 配置软件：交换机的辅助软件，便于交换机的启动以及各种管理和配置。比较典型的配置软件是 Cisco 公司的 IOS 系统，它是非常重要的一个部分。它有以下功能：
 - ◆ 使网络管理员可以登录到用户模式或者私有模式，对交换机进行相关的配置；
 - ◆ 使用上下文关联进行配置的帮助；
 - ◆ 使用命令行帮助功能，帮助管理员了解命令格式和作用；
 - ◆ 检查交换机的状态和各个硬件元素(RAM,ROM 等)的存储内容。

1.2 交换机的分类

1.2.1 OSI 参考模型与数据通信设备

OSI(Open System Interconnection)参考模型是国际标准化组织(ISO)提出的一个关于由不同供应商提供的不同设备和应用软件之间的网络通信的概念性框架结构。现在它被公认为是计算机通信和 Internet 网络通信的一种基本结构模型。当今使用的大多数网络通信协议都是基于 OSI 模型结构。

OSI 模型有 7 层，逻辑上分为 2 个部分：低层的 1~4 层关心的是原始数据的传输，高层的 5~7 层关心的是网络下的应用程序。OSI 采用了 3 级抽象，即体系结构、服务定义和协议规格说明。体系结构部分定义 OSI 的层次结构、各层关系及各层可能的服务；服务定义部分详细说明了各层所提供的功能；协议规格部分的各种协议精确定义了每一层在通信中发送控制信息及解释信息的过程。

OSI 将网络划分为 7 个层次，如图 1-3 所示。

(1) 物理层

物理层(physical layer)是 OSI 的最底层，主要功能是利用物理传输介质为数据链路层提供连接，以透明地传输比特流。物理层也是有协议规范的，主要是规定了传输介质的种类和接口的电器特性。以太网中最常用的莫过于 RJ-45 接口和 UTP 线缆了。其他常用的物理介质和接口协议还有：EIA/TIA-232(通常也被称作 RS-232)，RS-449，V.35，V.24 等。

(2) 数据链路层

数据链路层(datalink layer)在通信的实体间建立数据链路连接，传送以帧为单位的数据，并采用相应方法使有差错的物理线路变成无差错的数据链路。数据链路层的主要功能是差错控制和流量控制，还有链路管理和帧同步等功能。由于以太网采用了共享信道技术，而在共享信道数中会出现多个接收者的情况，所以必须利用一个局域网的地址来区分不同的接收者。

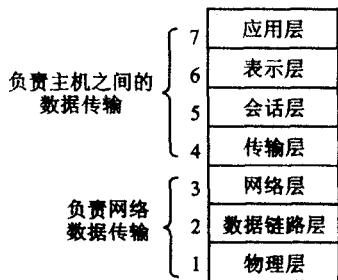


图 1-3 OSI 7 层参考模型

数据链路层指定了两个有物理连接的节点之间如何通过物理连接通信的方式和方法。例如：采用光纤环状共享物理连接时，使用 FDDI 协议来控制数据的发送和接收。而如果在以太网和快速以太网中，则使用的就是 IEEE 802.3 协议。当然，还有其他的链路层协议，包括 HDLC、PPP、帧中继、IEEE 802.2 和 IEEE 802.11 等。交换机现在基本采用的是 IEEE 802.3 协议，目前是低成本和高性能的最佳结合。

(3) 网络层

网络层(network layer)的功能是进行路由选择，阻塞控制与网络互联等。网络层定义了如何端到端传递数据报文。因为中间需要中继传递，为了保证数据报文能够在一个网状结构的网络中被正确传递，因此，网络中需要规定一个网络层的地址——IP 地址。而且网络层还定义了学习和寻找路径的机制，在传送和转发数据报文和消息的时候，路由器或终端节点能够自动学习，将数据报文发送到路由器对应的端口。这一层的典型协议是 IP 协议。

(4) 传输层

传输层(transport layer)的功能是向用户提供可靠的端到端服务，透明地传送报文，是关键的一层。最典型的协议就是 TCP 和 UDP。TCP 是面向连接的传输协议；而 UDP 是面向无连接的传输协议。TCP 建立连接的过程就类似于平常打电话。首先，一方呼叫另一方，等待对方确认可以通信后，双方开始建立通信，而且中间所发送的数据报文都必须确保无误，否则接收方会要求发送方重新发送。而 UDP 则相反，一方不管对方是否在，也不管线路是否通畅，只管将数据报文发送出去，不需要对方确认发送的数据报文是否到达。

(5) 会话层

会话层(session layer)的功能是组织两个会话进程间的通信，并管理数据的交换。这一层定义了如何开始、控制和结束一个会话(session)。它包括控制和管理多个双向消息，可以让上层的应用程序知道消息是否已经发送/接收完成。这一层的典型控制协议有：RPC, SQL, NetBios, AppleTalk ASP 等。

(6) 表示层

表示层(presentation layer)主要用于处理两个通信系统中交换信息的表示方式，包括数据格式变换、数据加密、数据压缩与恢复等功能。表示层的主要目的是为了定义数据格式，例如：ASCII 文本、二进制文本、JPG 格式的图片、JPEG 格式的图像等，同时还包括一些加密的信息方式。

(7) 应用层

应用层(application layer)是 OSI 参考模型中的最高层。应用层确定进程之间通信的性质，以满足用户的需要。它在提供应用进程所需要的信息交换和远程操作的同时，还要作为应用进程的用户代理，来完成一些为进行信息交换所必需的功能。应用层的目的是为了计算机之间的应用程序能够互相通信。应用层的协议一般指的是是一些应用协议，例如：FTP 协议、HTTP 协议(WWW 浏览)、Telnet、NFS、SMTP、SNMP 等。

