TurboLinux标准培训教程系列

飞思教育 FECIT-EDUCATION 拓林思（中国）教育培训中心指定用书

TURBOLINUX

网络管理教程

飞思教育产品研发中心 /编著

拓林思（中国）教育培训中心/监制

- TurboLinux网络基础和网络管理
- TurboLinux局域网和以太网技术
- TurboLinux平台上的路由DNS、DHCP、NFS
- TurboLinux平台上的Sendmail、电子邮件、IP层
- TurboLinux平台上的Apache、PPP、ipchains应用
- TurboLinux客户机/服务器模型以及网络安全

電子工業出版社
PUBLISHING HOUSE OF ELECTRONICS INDUSTRY
URL:http://www.phei.com.cn

HIGH PERFORMANCE LINUX

入门与提高系列丛书

AutoCAD 2002 入门与提高

张国宝　编著

人 民 邮 电 出 版 社

内 容 简 介

本书属于《TurboLinux 标准培训教程系列》丛书，是拓林思（中国）教育培训中心指定用书。全书共分 20 章，首先介绍了计算机网络系统模型，包括局域网技术、以太网技术、IP 层、ARP 和 RARP 协议、路由以及传输层；然后以大量实例，详细介绍了如何在 TurboLinux 上构建 PPP、DHCP、DNS、Sendmail、Apache、NFS、Samba 等网络服务和应用。通过对上述内容的学习，再配合每章后精选的习题，相信您可以完成一个基于 TurboLinux 的中小型网络应用系统的设计与实施。

本书主要是为初、中级 TurboLinux 网络用户和网络管理员而编写的，同时，对于高级用户也具有极大的参考价值，特别适合作为培训和自学教材。

图书在版编目（CIP）数据

TurboLinux 网络管理教程 / 飞思教育产品研发中心编著. -北京：电子工业出版社，2000.10
（TurboLinux 标准培训教程系列）
ISBN 7-5053-6186-4

Ⅰ.T… Ⅱ.飞… Ⅲ.操作系统（软件），Linux–教材 Ⅳ.TP316.89

中国版本图书馆 CIP 数据核字（2000）第 70012 号

丛 书 名：TurboLinux 标准培训教程系列
书　　名：TurboLinux 网络管理教程
编　　著：飞思教育产品研发中心
监　　制：拓林思（中国）教育培训中心
责任编辑：郭　晶　王树伟
排版制作：电子工业出版社计算机排版室监制
印 刷 者：北京牛山世兴印刷厂
出版发行：电子工业出版社　　URL：http://www.phei.com.cn
　　北京海淀区万寿路 173 信箱　邮编：100036
经　　销：各地新华书店
开　　本：787×1092　1/16　印张：18.25　字数：467.2 千字
版　　次：2000 年 10 月第 1 版　　2000 年 10 月第 1 次印刷
书　　号：ISBN 7-5053-6186-4
　　TP · 3325
印　　数：6000 册　　定　　价：26.00 元

前　言

关于本丛书

Linux 是一种可以免费使用和自由传播的类 UNIX 操作系统。1991 年，它诞生于芬兰赫尔辛基大学一位名叫 Linus Torvalds 的学生手中，后来，通过世界各地成千上万的程序员的设计而实现。它具有 UNIX 的全部功能，具有多任务、多用户、开放性等众多优秀特性，任何使用 UNIX 操作系统或想要学习 UNIX 操作系统的人都可以从 Linux 中获益，所以 Linux 一出现就受到广大计算机爱好者的喜爱。

在 Linux 领域，TurboLinux 是目前世界上最大的开发软件之一。因其技术先进、本地化工作深入到位，而深受用户欢迎。1999 年 4 月 TurboLinux（拓林思）公司进入中国以来，先后发布 TurboLinux 3.0.2 简体中文版，TurboLinux 4.0 简体中文版；2000 年 3 月又发布了 TurboLinux 6.0 简体中文版的标准版和 Server 版。在此期间，TurboLinux 公司与我国多家电脑生产厂家达成合作协议，将 TurboLinux 作为预装的操作系统与电脑捆绑销售，其中包括长城和 TCL。此外，拓林思公司还积极开展活动，与国内政府机构和著名学府建立合作关系，大力研究和推广 TurboLinux 的应用。

基于当前 TurboLinux 的热门应用以及 TurboLinux 爱好者、TurboLinux 培训班对高质量参考书及教材的渴望，由“飞思教育产品研发中心”精心策划了《TurboLinux 标准培训教程系列》丛书，包括《TurboLinux 中文版教程》、《TurboLinux 简体中文版 6.x 使用指南》、《TurboLinux 用户基础教程》、《TurboLinux 系统管理教程》、《TurboLinux 网络管理教程》。这套丛书从 TurboLinux 的基础应用到中、高级管理，对 Linux 操作系统进行了全面讲解。

培训教程

培训教程是 TurboLinux 认证考试的指定教材。在编写过程中，作者结合自己的实践经验进行讲解，其内容详实、全面、具体，每章分为内容提要、主要知识点、正文、小结、本章习题 5 个部分，最后还附有实验指导。同时，在内容安排上也适合读者循序渐进地学习，是读者通过 TurboLinux 认证考试的最佳选择，也是培训班学员的必备教材。

本教程具有广泛的适用性：

- 适合于有较好计算机基础的初学者作为自学教材。
- 适合于有一定 UNIX 经验的学员作为培训教材。
- 适合于 Linux 专业技术人员作为技术参考手册。
- 适合于精通 TurboLinux 者作为应考拓林思认证工程师（TCE）的复习资料。

关于本书

Linux 操作系统作为当前流行的一种系统平台，具有安全性高、系统功能强、可扩展性好等特点。此外，Linux 操作系统还提供了强大的网络功能。当前流行网站的建设者都

选用 Linux 作为其操作系统平台。本书作为 Linux 用户进行网络管理的培训教材，旨在使用户对计算机网络系统结构、Linux 网络管理功能有一个比较清楚的了解和掌握。

本书共分 20 章（第 20 章为实验），首先介绍了计算机网络系统模型，包括局域网技术、以太网技术、IP 层、ARP 和 RARP 协议、路由以及传输层；然后以大量实例，详细介绍了如何在 TurboLinux 上构建 PPP、DHCP、DNS、Sendmail、Apache、NFS、Samba 等网络服务和应用。

本书自成系统，讲解深入浅出，每章后附有相当数量的精选习题，便于自学。适合于作为 TurboLinux 系统网络管理的教材，亦可作为 Linux 爱好者进行网络功能应用和开发的参考书。本书内容覆盖面较广，读者在使用本书时可根据不同情况各有取舍。

我们最大的心愿和目的就是可以让读者熟练地掌握一些基本的操作技巧和实用工具来完成日常工作和学习任务。

本书由飞思教育产品研发中心策划并编著，同时得到了叶伟、刘晓华、李欣的支持和帮助。但由于时间仓促，作者水平有限，经验不足，加之 Linux 技术发展更新得很快，书中错误遗漏的地方还请广大读者批评指正。我们的联系方式：

电话：（010）68131648　（010）68251220　E-mail：fecit@fecit.com.cn

网址：http://www.fecit.com.cn

本书约定

对本书统一运用的符号解释如下：

【　】表示快捷键。

注意　表示某一操作过程中的注意事项。

说明　表示进一步解释。

飞思教育产品研发中心

目　录

TurboLinux网络管理教程

1

网络基础

本章内容提要

本章是本书乃至计算机网络技术的基础。本章介绍了网络传输技术、计算机网络的 ISO/OSI 七层模型、TCP/IP 协议的体系结构和 IP 地址的技术。

本章重点内容如下：

- OSI 协议分层（各层的名称、功能）
- TCP/IP 协议
- IP 地址

1.1 网络传输技术

传输，从信号类型上可以分成光信号传输和电信号传输，从信号本身的特征来讲，有模拟信号传输和数字信号传输。在本书中，只需从一个较高的层次上来看，而不必陷入技术细节。今天所使用的传输技术，从广义上讲，可以分为两类：广播式和点到点。

广播式网络

广播式网络仅有一条通信信道，由网络上的所有机器共享。如同在同一个教室里，老师和学生们共享空气作为声音的传输通道。在此类网络中传输的消息按某种语法组织为分组或包。这些分组可以被任何机器发送并被其他所有机器接收。分组的传送采用类似于信件发收的按地址区分不同接收者的方式。当收到分组时，各机器将检查它的地址字段，如果是发给自己的则处理该分组，否则就应丢弃此分组。

广播系统通常也允许在目的地址字段中使用一种特殊代码，以便使分组被网络上的所有目标接收处理。这种操作被称为广播。如同老师的授课，每位同学都可以听，并且思考。某些广播系统还支持向网络的一个子集发送的功能，即多点发送。一种常见的方案是保留地址字段的某一位来指示多点发送，而剩下的 n-1 位地址字段存放组号（假设地址字段共 n 位）。每台机器可以注册到任意某几组或所有的组。当某一分组被发送给某个小组时，所有机器都将检查该分组，若指示多点发送的那一位为有效，就检查分组中的组号是否属于自己组号的集合，如果是则接收并处理它。

广播网络的保密性很差，网络上的每台机器都可以接受并处理所有的分组，这些机器可能是网络管理员用于分析的，也可能是不怀好意的使用者在窃听。但是，因为您共享着信道，所以不必为每两人建一个信道，这样可以大量节省建设网络的成本。使用广播信道也有利于多人合作完成任务时所需的通信。

点到点网络

点到点网络是由一对对机器之间的多条联接构成。全连通网络就是点到点网络的一种特殊情况，即每两台机器之间就有一条通道（也有可能不止一条）。这种网络下的通信，只须发信方确定谁来收信，并将信息包放在连接两方的那条通道上就可以了，收方认为所有接收到的包都是发给自己的。

但是因为建设全连通网络的代价太高，n 个节点的网络，须至少铺设 n（n-1）条通道。实际上往往不在所有的节点之间都建立通道，而只要保证任意两个节点能够互通就行。这时，为了能从源端到达目的地，网络上的分组传送可能必须通过一台或多台中间机器。通常又存在多条从源端到达目的地的路径，并且可能长度不一样。这样，就出现了路径选择的问题，即路由问题。在点到点网络中路由选择算法是十分重要的。

此时，应保证网络上传送的分组由一台机器发出后，由指定的机器接收处理，其余机器不会接收到，最多实现包的转发而已。

点到点网络的保密性较高，但是有路由功能的节点有些特殊，应区别对待，将在后面第 6 章中进行介绍。

一般地，本地规模较小的网络采用广播方式，而大的广域网络则采用点到点方式。

1.2　网 络 模 型

网络通信不是说在两台机器间存在一个通信信道就可以了，但还存在不同层次上的问题。计算机的处理能力与通信的结合，使计算机网络具有强大的能力，但处理能力和通信能力是怎样结合起来的呢？这就需要计算机网络模型。网络模型是协议分层的，各层专注于自己资源的利用，形成功能，为上层提供服务。

这里有必要介绍一下协议的概念。在通信中，协议指双方为完成通信而预先做的一些关于控制方面的规定。如分组本身的定义和解释方式、通信的开始和结束等等。

1.2.1　协议分层

为了减少协议设计的复杂性，大多数网络都按层或级的方式来组织，每一层都建立在它的下层之上。不同的网络，层的数量、各层的名字、内容和功能都不尽相同。然而，在所有的网络中，每一层的目的都是向它的上一层提供一定的服务，而把如何实现这一服务的细节对上一层加以屏蔽。

一台机器上的第 n 层与另一台机器上的第 n 层进行对话。对话的规则被称为第 n 层上的协议。如果违反协议将导致通信困难甚至难以进行。图 1-1 说明了一个 5 层的协议。不同的机器里包含对应层的实体叫对等进程（peer）。正是对等进程利用协议在进行通信。

图 1-1　对等进程通信模型

实际上，数据不是从一台机器的第 n 层直接传送到另一台机器的第 n 层，而是每一层把数据和控制信息交给它的下一层，直到最下层。第 1 层下是物理介质，在这里进行实际的通信。在图 1-1 中，虚线表示虚拟通信，实线表示物理通信。

每一对相邻层之间都有一个接口。接口定义下层向上层提供的原语操作和服务。网络设计者在决定一个网络包括多少层，每一层应当做什么时，在相邻层之间定义一个清晰的接口是很重要的。为达到这些目的，要求每一层能完成一组特定的有明确含义的功能。

层和协议的集合称为网络体系结构。体系结构的描述必须包含足够的信息，使实现者

可以用来为每一层编写程序和设计硬件，并使之符合有关协议。某系统所使用的协议列表，每层一个协议，被称为协议栈。

协议分层的较低层次常常以硬件或固件的形式实现，以提高信息的处理速度。

计算机网络的某些关键问题在好几层的设计中都会出现。下面简要介绍其中一些较重要的问题。

每一层都需要识别发送方和接收方的机制。因为网络中通常有很多计算机，其中一些有多个进程。某台计算机上需要建立连接的进程必须能有某种手段来指定和谁通信。因为有多个目标，所以需要有某种寻址手段来指明特定的目标。

物理通信链路并非是完美无缺的，所以差错控制也是一个很重要的问题。已知的检错和纠错代码有多种，连接的双方必须一致同意使用哪一种。另外，接收方还应该通知发送方哪些报文已经被正确的收到了，哪些还没有收到。为了解决可能出现的顺序错误。协议必须明确保证接收方能够把各报文按原来的顺序重新组合在一起。

另一个必须在好几层中解决的问题是，所有的进程都应该能接受任意长的报文。这一特性要求用户能在不同层上把报文分割、传输和重组装。

1.2.2 服务与接口

首先，介绍几个术语。

实体：每一层的活动元素通常被称为实体。实体可以是软件实体（如一个进程），也可以是硬件实体（如智能输入/输出芯片）。不同机器上同一层的实体叫对等实体。

服务和服务接入点：服务是在服务接入点 SAP（Service Access Point）提供给上层使用的。n 层 SAP 就是 n+1 层可以访问 n 层服务的地方。

协议数据单元：为了传递 SDU，n 层实体可能将 SDU 分成几段，每一段加上一个报头后就构成协议数据单元（PDU：Protocol Data Unit）。例如，分组就是 PDU。PDU 被对等实体用于执行它们的同等协议。它们被用于分辨哪些 PDU 包含数据，哪些 PDU 包含控制信息，并提供序号和计数等。

连接和非连接：面向连接的服务和面向无连接的服务。在使用面向连接的服务时，用户首先要建立连接，使用连接，然后释放连接；面向无连接的系统中，每个报文带有完整的目的地址，且独立于其他报文，经由系统选定的路线传递。文件传输比较适合于面向连接的服务。面向无连接的服务通常被称为数据报服务。

在这里，n 层实体实现的服务为 n+1 层所利用。在这种情况下，n 层被称为服务提供者，n+1 层为服务用户。n 层利用 n-1 层的服务来提供它自己的服务。相邻层之间需要交换信息，对接口必须有一致统一的规则。在典型的接口上，n+1 层实体通过 SAP（如图 1-2 所示）把一个接口数据单元 IDU（Interface Data Unit）传递给 n 层实体。IDU 由服务数据单元 SDU（Service Data Unit）和一些控制信息组成。SDU 是将要跨过网络传递给对等实体，然后向上交给 n+1 层的信息。控制信息用于帮助下一层完成任务（如 SDU 中的字节数），它本身不是数据的一部分。

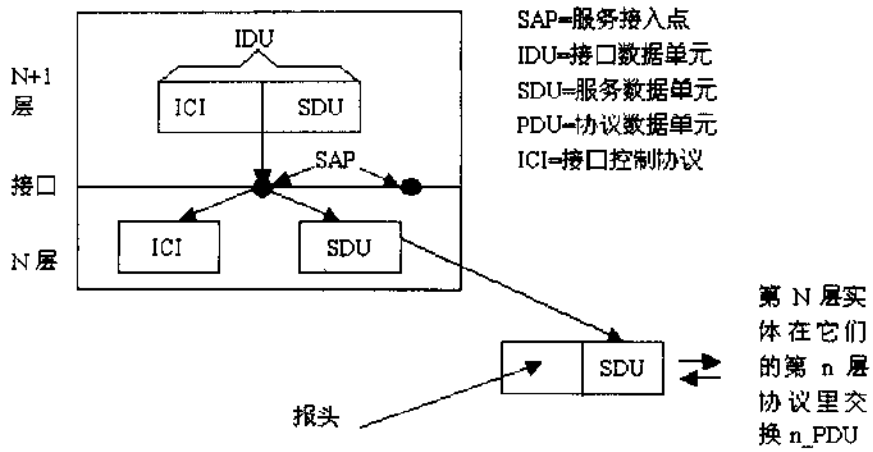

图 1-2　处于接口两边的两层之间的关系

1.2.3　ISO/OSI 七层网络模型

OSI 参考模型基于国际标准化组织（ISO）的建议，作为各种层上使用的协议国际标准化的第一步而发展起来的。这一模型被称作 ISO/OSI 开放系统互联参考模型（简称 OSI 模型）。

OSI 模型根据以下原则分成 7 层：

- 根据不同层次的抽象分层。
- 每层应当实现一个定义明确的功能。
- 每层功能的选择应该有助于指定网络协议的国际标准。
- 各层的边界的选择应该尽量减少跨过接口的通信量。
- 层数应该足够多，以避免不同的功能混杂到同一层里，但也不能太多，否则体系结构会过于庞大。

下面从最下层开始，依次讨论 OSI 参考模型的各层。请注意 OSI 模型并不是网络体系结构的全部内容，它并没有确切的描述用于各层的协议和服务，仅告诉用户每一层应该做什么。

物理层

物理层涉及到通信在信道上传输的原始 bit 流。设计时必须保证一方发出二进制“1”时，另一方收到的也是“1”而不是“0”。这里的典型问题是用多少伏特的电压表示“1”，多少伏特的电压表示“0”；一个 bit 持续多少微秒；传输是否在两个方向上同时进行；如何建立最初的连接及如何在完成通信后终止连接；网络接插件有多少针以及各针的用途等。这里的设计主要是处理机械的、电气的和过程的接口，以及物理层下的物理传输介质等问题。

数据链路层

数据链路层的主要任务是加强物理层传输原始 bit 的功能，使之对网络层显现为一条

无错链路。发送方把输入数据封装在数据帧里（典型的数据帧为几百或几千字节），按顺序发送各帧，并处理接收方返回的确认帧。因为物理层仅仅接收和传送 bit 流，而不关心它的意义和结构，所以只能依赖各链路层来产生和识别帧边界。可以通过在帧的前面和后面附加上特殊的二进制编码模式来达到这一目的。

数据链路层要解决由于帧的破坏、丢失和重复出现的问题。也要防止高速的发送方的数据把低速的接收方“淹没”，即所谓的差错控制和流量控制。

广播式网络在数据链路层还要处理新的问题，即如何控制对共享信道的访问。数据链路层的一个特殊的子层——介质访问子层，就是专门处理这个问题的。

网络层

网络层关系到子网的运行控制，其中一个关键问题是确定分组从源端到目的端如何选择路由。路由既可以选用网络中固定的静态路由表，几乎保持不变，也可以在每一次会话开始时决定，还可以根据当前网络的负载状况，高度灵活的为每一个分组决定路由。

如果在子网里同时出现过多的分组，它们将相互阻塞通路，形成瓶颈。此类拥塞控制也属于网络层的范围。

网络层常常设有记账功能，还要解决跨网络跨协议传送的问题。

在广播网络中，选择路由问题很简单。因此网络层很弱，甚至不存在。

传输层

传输层的基本功能是从会话层接收数据，并在必要时把它分成较小的单元，传递给网络层，并确保到达对方的各段信息正确无误，而且，这些任务都必须高效率的完成。从某种意义上讲，传输层使会话层不受硬件技术变化的影响。

传输层也要决定向会话层，最终向网络用户提供什么样的服务。

传输层是真正的从源到目的的“端到端”的层。

会话层

会话层允许不同的机器上的用户建立会话关系。会话层允许进行类似传输层的普通数据的传输，并提供了对某些应用有用的增强服务会话，也可以用于远程登录到分时系统或在两台机器间传递文件。

会话层的服务之一是管理会话。会话层允许信息同时进行双向传输，或任一时刻只能单向传输。

另一会话服务是同步。会话层提供了在数据流中插入检查点的办法解决断点重新传递的问题。

表示层

表示层完成某些特定的功能，由于这些功能常被请求，因此人们希望找到通用的解决办法，而不是让每个用户来实现。值得一提的是，表示层以下的各层只关心可靠的的传输 bit 流，而表示层关心的是所传输的信息的语法和语义。

应用层

应用层包含大量人们普遍需要的协议。

如文件传输。不同的文件系统有不同的文件命名原则，不同系统之间传输文件所需处理的各种不兼容问题，也同样属于应用层的工作。此外，还有电子邮件、远程作业输入、名录查询和其他各种通用和专用的功能，将在后面章节作较详细地介绍。

1.3　TCP/IP 网络

今天的 Internet 连接了世界各地数以亿计的计算机，它们各不相同，可能是由很多不同的厂家生产的型号和运行完全不同的操作系统，但它们能很好的互相通信、交互，产生着巨大的财富。这就是 TCP/IP（Transmission Control Protocol / Internet Protocol）协议的功劳了。TCP/IP 协议是一个真正的开放系统，是整个因特网（Internet）的基础。

本节针对 TCP/IP 协议进行概述，其目的是为本书其余章节提供充分的背景知识。

1.3.1　TCP/IP 的历史

TCP/IP 起源于 60 年代末美国政府资助的一个分组交换网络研究项目，到现在已发展成为计算机之间最常应用的联网形式。最初，不同的计算机之间的通信使用着不同的传输介质，使得基于异种机的网络互联成为网络通信技术的难点。70 年代初期，为了实现网际互联，不得不开始研究一些在不同网络之间自由通信的技术，以使不同体系结构的计算机交互。1973 年，美国国防部高级研究计划署 DARPA（Defence Advanced Research Projects Agency）率先开始了适应并完善分组网络互联的协议及其他一些技术的研究，以支持基于异种硬件体系结构、异种操作系统、异种通信技术的网络彼此互联。网际协议 TCP/IP 就是在这种环境下产生的，发展到目前为止，TCP/IP 协议系列已成为一个满足异种机互联要求的成熟的网络协议体系。

1969 年美国国防部高级研究计划署 DARPA 建立了一个只有四个节点的、存储转发方式的分组交换广域网 ARPANET。这是世界上第一个分组交换网，该网是用以验证远程分组交换网的可行性而进行的一项试验工程。1972 年首次公布了 ARPANET，验证了远程分组交换技术的可行性，并开始了网络控制协议 NCP 的设计工作。70 年代中，国际信息处理联合会 IFIP 的 6.1 工作组进一步补充和完善了 DARPA 在 NCP 方面的开发工作，从而产生了 TCP/IP。

随着 UNIX 在学术界和研究机构的流行，斯坦福大学、BBN（Bolt Beranck and Newman）公司等单位推出了世界上第一个 TCP 实现原型。80 年代初，美国加州大学伯克利分校推出了 4.1BSD 和 4.2BSD UNIX 操作系统，其内核中包含了 TCP 实现。1983 年，TCP/IP 取代 NCP，并正式作为美国军用标准发表。与此同时，Sun Microsystem 公司将 TCP/IP 带进了广阔的商业领域。

此后，TCP/IP 协议迅猛发展，成为支持众多厂商、不同机型、不同网络互联通信的事实上的国际标准协议。TCP/IP 协议已成为建设计算机局域网、广域网，特别是因特网（Internet）的最重要的核心通信协议。

1.3.2 TCP/IP 体系结构

TCP/IP 协议可看作是符合 ISO/OSI 七层网络模型的，但是作了许多简化，以使它能更高效率的工作。对应于 ISO/OSI 七层网络模型，TCP 是一种传输层协议，IP 是一种网络层协议。TCP/IP 协议是一组不同的协议组合在一起构成的协议族。尽管通常称该协议族为 TCP/IP 协议，但 TCP 和 IP 只是其中最常用到两个协议而已。

TCP/IP 协议族采用了分层体系结构，如下图 1-3 所示，每层有自己特定的功能，低层为高层提供服务。整个系统遵循对等实体通信原则。

TCP 提供相当于 OSI 参考模型中传输层的服务。IP 则提供网络层的服务，TCP/IP 之上是该协议族提供的各种应用服务，而底层网络可以是各种不同的物理网络，如 Ethernet、Token Ring、X.25 公共分组交换网等等。

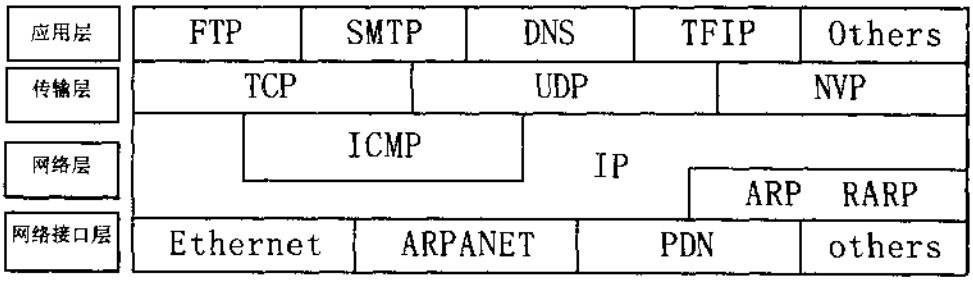

图 1-3 TCP/IP 体系结构

在 TCP/IP 协议族中，网络层 IP 协议提供的是一种不可靠的服务。也就是说，它只是尽可能快地把分组从源节点送到目的节点，但是并不提供任何可靠性保证。TCP/IP 协议有一个很重要的思想，就是 Best Effort（尽最大努力），指的就是这个。

而另一方面，TCP 在不可靠的 IP 层上提供了一个可靠的运输层。为了提供这种可靠的服务，TCP 采用了超时重新传递，发送和接收的端到端确认分组等机制。

以下对图中各个模块做一下简要介绍：

底层网络对应于 ISO/OSI 中的数据链路层以及物理层，数据链路层不是 TCP/IP 协议族中的一部分，但它是 TCP/IP 赖以存在的各种物理网络与 TCP/IP 之间的接口。这些网络包括多种局域网和广域网，如 Ethernet、ARPANET 等。

网络层相当于 ISO/OSI 中的网络层

- ICMP（Internet Control Message Protocol）是 IP 协议的附属协议。IP 层用它来与其他主机或路由器交换错误报文和其他重要信息。尽管 ICMP 主要被 IP 协议使用，但应用程序也有可能访问它。两个流行的诊断工具，Ping 和 Traceroute 都使用它。
- ARP（Address Resolution Protocol，地址解析协议）和 RARP（Reverse Address Resolution Protocol，逆地址解析协议）是某些网络接口（如以太网和令牌环网）使用的特殊协议，用来转换 IP 层和网络接口层所使用的地址。其中，ARP 用于将 Internet 地址（也称作 IP 地址）转换到网络接口层地址，而 RARP 用于将网络接口层地址转换到 Internet 地址。