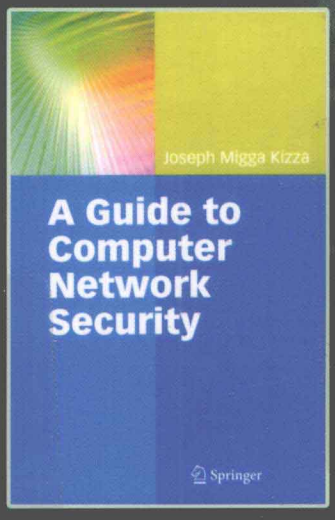
国 外 计 算 机 科 学 教 材 系 列

Springer

计算机网络安全概论

A Guide to Computer Network Security



[美] Joseph Migga Kizza 著

陈向阳 胡征兵 王海晖 译

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

国外计算机科学教材系列

计算机网络安全概论

A Guide to Computer Network Security

[美] Joseph Migga Kizza 著

陈向阳 胡征兵 王海晖 译

電子工業出版社
Publishing House of Electronics Industry
北京 · BEIJING

内 容 简 介

本书主要探讨了当前网络基础设施和协议中的安全威胁和漏洞，并描述了目前解决网络安全问题的努力方向。具体内容包括：网络漏洞、网络犯罪、恶意脚本、安全评估、灾害管理、认证、加密、入侵检测与防御、网络取证、安全评估、安全协议、无线网络和传感器网络的安全。

本书可以作为高等院校“信息安全”、“计算机网络安全”、“电子商务安全”、“网络攻防”等课程的教材或参考书，也适合计算机及电子、通信和自控专业的本、专科学生及成教学生阅读。

版权贸易合同登记号　图字：01-2010-8178

图书在版编目(CIP)数据

计算机网络安全概论/(美)克扎(Kizza,J. M.)著；陈向阳，胡征兵，王海晖译.
北京：电子工业出版社，2012.6
书名原文：A Guide to Computer Network Security
国外计算机科学教材系列

ISBN 978-7-121-15220-7

Ⅰ. ①计… Ⅱ. ①克… ②陈… ③胡… ④王… Ⅲ. ①计算机网络-安全技术-高等学校-教材 Ⅳ. ①TP393.08

中国版本图书馆 CIP 数据核字(2011)第 241391 号

策划编辑：马　岚
责任编辑：许菊芳
印　　刷：涿州市京南印刷厂
装　　订：
出版发行：电子工业出版社
　　北京市海淀区万寿路 173 信箱　邮编　100036
开　　本：787×1092　1/16　印张：20.75　字数：531.2 千字
印　　次：2012 年 6 月第 1 次印刷
定　　价：45.00 元

凡所购买电子工业出版社图书有缺损问题，请向购买书店调换。若书店售缺，请与本社发行部联系，联系及邮购电话：(010)88254888。

质量投诉请发邮件至 zlts@phei.com.cn，盗版侵权举报请发邮件至 dbqq@phei.com.cn。

服务热线：(010)88258888。

前　言

如果摩尔定律是正确的，那么过去的每一天技术领域都在发生着新的和更高级的改变。我们在对计算设备的微型化感到惊讶的同时，也在享受着由于计算速度的提升所带来的愉悦。世界上的一切似乎都处于不停的变化和快速移动之中，我们也在快速地向着普适计算的方向发展。为了实现(达到)这种计算境界，就必须开发出新的、容易使用的、无缝计算的用户接口。如果你有丰富的数字设备程序开发经验，相信你会像我一样期待着这种崭新的计算前景的到来。

如果可以以历史为鉴，在信息安全方面来讲也是如此，那么每一个计算设备的新老用户，都必须面对充满着各种问题的未来。在进入这种快速、小型化和可以隐藏的普适计算设备的世界的同时，许多多疑、(恶作剧)淘气和恶意的人们也将与我们同处一地，我们必须对此加以防范。正如预料到的那样，帮助只会姗姗来迟，因为我们很难得到训练有素的、经验丰富的专业人员，而且即使能够找到专业人员，就目前的情形而言费用也会很可观。

其次，如今的安全协议和最优方法是以最快的、可以保证网络管理员不断地更改它们的速度持续地变化着的。再次，就目前的情形而言，很难及时发现最新的安全缺陷并为它们及时打补丁。换句话讲，计算环境一方面肯定会变化，而另一方面又保持不变。

正是由于这些原因，即使在没有先进的计算机和信息安全协议和最优方法的情形下，我们最好仍要保持警惕，因为脆弱的计算机网络系统频繁遭到攻击并不是危言耸听，而且在今后这种攻击将会持续增加。

因此设计自适应的、可扩展的安全协议和最优方法及实现大规模的广泛认知，都需要更多的努力，才能满足这种不断增长的挑战，并且要提高公众水平，以便让他们成为创新的计算世界中的主动安全参与者。

本书是一本综合性的教材，不仅涉及计算和信息安全保障的每一个主要话题，而且也会介绍一些最新的计算技术，例如将来大有可为的无线传感器网络，其中安全性很可能会成为最大的问题。本书的目的是带来大规模的安全问题的教育和认知，以及对一般网络空间的关注。特别是在计算机世界中，安全认知对社会利益、用户所面对的安全问题和危险具有防御作用，并有助于开发出更好的算法和协议。综合起来，全书可分成四个部分，共22章。

第一部分讲解计算机网络的工作原理与安全形势。第二部分根据不断出现的安全威胁，向读者展示最主要的安全形势，其中概述了几种安全威胁类型。第三部分，也是最大的部分，构成了本书的核心并提供了大多数最优方法和当前使用的解决方案。第四部分为工程项目实践。除了算法、协议和解决方案外，还给出了前面讨论过的每一个安全项目的几种产品和服务。

总之，本书试图达到如下目的：

1. 教育公众有关一般意义上的网络安全，特别是与因特网有关的计算机系统安全。
2. 警告公众有关计算机网络脆弱性、漏洞，以及计算机基础设施弱点的重要性。
3. 让公众注意有效的安全方案和最优方法，专家对这些方案的意见，以及随机自组织实现这类方案的可能性。
4. 了解立法、法规和执法在计算机安全努力中所扮演的角色。
5. 最后，发起一场对开发效率、综合算法、协议及信息安全最优方法的讨论。

本书覆盖了广泛的安全话题、算法、解决方案和最优方法，既可以用于教学，也可以充当对学习计算机网络安全问题感兴趣的所有人的参考工具书，并可从中学到防止信息系统攻击的技术。书中深入探讨、分析了大多数计算机网络安全问题，加上安全算法和解决方案的讨论，使得本书成为计算机安全人员、网络安全策略制订者理想的参考资料。此外，本书通过列举有效的立法、法规、社会和伦理安全问题，包括在个人隐私和集体、个人安全需求之间不断消失的界限，来激发读者的想像力。

本书的目标读者为计算机科学、信息科学、技术研究、图书馆学、工程以及艺术和科学类专业中对信息科学感兴趣的部分本科学生。此外，信息管理科学专业的学生会发现本书特别有帮助。工程技术人员，特别是那些工作在信息领域的人员，也会发现本书是一本很好的参考资料。对于那些对信息安全和保障方面感兴趣的人，以及那些仅想成为网络作家的人来说，本书也非常具有参考价值。

课本资源

每章的最后都有两种类型的练习：易于快速完成的基本练习和需要深入思考的高级练习，前一种练习的答案可以从学习过的课文中很快找到，而回答后一种练习需要研究学习本书以外的内容。第22章专门用做试验练习。有三种类型的试验练习：单周或双周作业，既可通过简单的阅读也可用准备好的软件和硬件工具来完成；稍难一些的学期项目，可能会需要更长的时间、团队合作和进一步学习研究才能成功地完成；难的开放性研究项目，需要很多思考、花费很多时间并需要做广泛的研究。我们尽可能在整本书中使用开放源代码的软件工具，这样做有两个结果：其一是在专用软件价格不断上升的情况下，使得本书有一定参考意义；其二，可以使书中内容和相关软件工具能够长久使用，因为内容和对应的练习不是建立在随时都可能过时的特殊专用软件之上的。

教学支持资料

如果打算考虑使用本书，就可以申请我们设计的教学辅助资料，以便有助于课堂教学。教师和学生的辅助资料包括如下：

- 教学大纲。为教师而准备的教学大纲。
- 教学幻灯片 PPT。这些资料非常详细，有助于教师教学，特别是有利于那些初次讲授本课程的教师。
- 选择性地给出了每章后面部分练习的答案。
- 实验。由于网络安全是一门实用性的课程，学生要花费相当多的时间安排实验练习。本书最后一章包含几个实验练习和工程项目。配套网站上包含更多项目和更新。
- 教师指导手册。为班级教学准备资料的教师的日常工作提供指导。
- 学生实验资料。在本部分中，将继续张贴出最新的实验练习、软件和挑战工程项目。

这些资料既可以在出版商的 Web 站点 http://www.springeronline.com，也可以在作者的网站 http://www.utc.edu/Faculty/Joseph-Kizza/上找到。

Joseph Migga Kizza

美国田纳西州查塔努加

目　录

第一部分　理解计算机网络安全

第 1 章　计算机网络基础 …… 2
1.1　简介 …… 2
1.2　计算机网络模型 …… 3
1.3　计算机网络类型 …… 3
1.4　数据通信媒体与技术 …… 4
1.5　网络拓扑 …… 8
1.6　网络连接性和协议 …… 11
1.7　网络服务 …… 14
1.8　网络连接设备 …… 16
1.9　网络技术 …… 22
1.10　总结 …… 26
练习 …… 26
高级练习 …… 26
参考文献 …… 27

第 2 章　理解计算机网络安全 …… 28
2.1　简介 …… 28
2.2　计算机网络安全保护 …… 29
2.3　保护的形式 …… 30
2.4　安全标准 …… 32
练习 …… 37
高级练习 …… 38
参考文献 …… 38

第二部分　计算机网络的安全挑战

第 3 章　计算机网络的安全威胁 …… 40
3.1　简介 …… 40
3.2　安全威胁来源 …… 41
3.3　安全威胁动机 …… 51
3.4　安全威胁管理 …… 53
3.5　安全威胁关联 …… 54
3.6　安全威胁认知 …… 54
练习 …… 55
高级练习 …… 56
参考文献 …… 56

第 4 章　计算机网络漏洞 …… 57
4.1　定义 …… 57
4.2　漏洞的来源 …… 57
4.3　漏洞评估 …… 66
练习 …… 67
高级练习 …… 68
参考文献 …… 68

第 5 章　网络犯罪与黑客 …… 69
5.1　简介 …… 69
5.2　网络犯罪 …… 69
5.3　黑客 …… 72
5.4　不断上升的网络犯罪应对处理 …… 84
5.5　总结 …… 85
练习 …… 85
高级练习 …… 85
参考文献 …… 86

第 6 章　恶意脚本 …… 87
6.1　简介 …… 87
6.2　公共网关接口(CGI)简介 …… 87
6.3　三次握手中的 CGI 脚本 …… 88
6.4　服务器端的 CGI 接口 …… 89
6.5　CGI 脚本安全问题 …… 89
6.6　Web 脚本安全问题 …… 90
6.7　处理脚本安全问题 …… 91
6.8　脚本语言 …… 91
练习 …… 93
高级练习 …… 94
参考文献 …… 94
其他参考文献 …… 94

第 7 章　安全评估，分析与保障 …… 95
7.1　简介 …… 95
7.2　系统安全策略 …… 96
7.3　构建安全策略 …… 98
7.4　安全需求规范 …… 102
7.5　威胁鉴别 …… 103
7.6　威胁分析 …… 105
7.7　漏洞鉴别与评估 …… 106
7.8　安全认证 …… 109
7.9　安全监控与审计 …… 109

7.10 产品与服务 …… 111
练习 …… 111
高级练习 …… 112
参考文献 …… 112
其他参考文献 …… 112

第三部分 网络安全挑战的应对方式

第 8 章 灾害管理 …… 114
8.1 简介 …… 114
8.2 灾害预防 …… 115
8.3 灾难响应 …… 117
8.4 灾难恢复 …… 117
8.5 为商业灾难做好准备 …… 120
8.6 灾难规划与恢复资源 …… 121
练习 …… 121
高级练习——案例研究 …… 122
参考文献 …… 122

第 9 章 访问控制和授权 …… 123
9.1 定义 …… 123
9.2 访问权限 …… 123
9.3 访问控制系统 …… 128
9.4 授权 …… 131
9.5 授权系统的类型 …… 132
9.6 授权规则 …… 133
9.7 授权粒度 …… 134
9.8 Web 访问与授权 …… 134
练习 …… 135
高级练习 …… 135
参考文献 …… 136

第 10 章 认证 …… 137
10.1 定义 …… 137
10.2 认证的多种因素和有效性 …… 138
10.3 认证元素 …… 139
10.4 认证类型 …… 140
10.5 认证方法 …… 141
10.6 设计一种身份验证策略 …… 148
练习 …… 148
高级练习 …… 149
参考文献 …… 149

第 11 章　密码学 …… 150
11.1　定义 …… 150
11.2　对称加密 …… 152
11.3　公共密钥加密 …… 154
11.4　增强安全:对称加密和公钥加密方法的结合 …… 157
11.5　密钥管理:产生，传输和发布 …… 157
11.6　公钥基础设施(PKI) …… 161
11.7　哈希函数 …… 162
11.8　数字签名 …… 163
练习 …… 164
高级练习 …… 164
参考文献 …… 165

第 12 章　防火墙 …… 166
12.1　定义 …… 166
12.2　防火墙的类型 …… 168
12.3　防火墙配置和实现 …… 176
12.4　非军事区 …… 177
12.5　通过防火墙提高安全性 …… 179
12.6　防火墙取证 …… 180
12.7　防火墙服务及其局限性 …… 180
练习 …… 181
高级练习 …… 182
参考文献 …… 182

第 13 章　入侵检测与防御系统 …… 183
13.1　定义 …… 183
13.2　入侵检测 …… 183
13.3　入侵检测系统 …… 185
13.4　入侵检测系统的类型 …… 187
13.5　IDS 工具的多变性 …… 193
13.6　其他类型的入侵检测系统 …… 193
13.7　系统入侵的响应 …… 195
13.8　入侵检测系统面临的挑战 …… 196
13.9　入侵检测系统的实现 …… 196
13.10　入侵防御系统 …… 197
13.11　入侵检测工具 …… 198
练习 …… 200
高级练习 …… 200
参考文献 …… 200

第 14 章　计算机和网络取证 …… 202
14.1　定义 …… 202

14.2 计算机取证 …… 203
14.3 网络取证 …… 214
14.4 取证工具 …… 218
练习 …… 222
高级练习 …… 223
参考文献 …… 223

第 15 章 病毒和内容过滤 …… 224
15.1 定义 …… 224
15.2 扫描，过滤和阻塞 …… 224
15.3 病毒过滤 …… 227
15.4 内容过滤 …… 233
15.5 垃圾邮件 …… 235
练习 …… 236
高级练习 …… 237
参考文献 …… 237

第 16 章 标准化与安全规范:计算机产品的安全评估 …… 238
16.1 简介 …… 238
16.2 产品的标准化 …… 238
16.3 安全评估 …… 240
16.4 主要的安全评估规范 …… 242
16.5 评估就意味着安全吗 …… 245
练习 …… 245
高级练习 …… 246
参考文献 …… 246

第 17 章 计算机网络安全协议 …… 247
17.1 简介 …… 247
17.2 应用层安全 …… 247
17.3 运输层的安全 …… 256
17.4 网络层的安全 …… 259
17.5 链路层和局域网的安全 …… 264
练习 …… 266
高级练习 …… 267
参考文献 …… 267

第 18 章 无线网络及设备安全 …… 269
18.1 简介 …… 269
18.2 蜂窝无线通信网络基础设施 …… 269
18.3 无线局域网(WLAN)或无线保真(Wi-Fi) …… 275
18.4 无线网络标准 …… 278
18.5 无线网络安全 …… 280

练习 …… 285
高级练习 …… 286
参考文献 …… 286

第 19 章　传感器网络安全 …… 288
19.1　简介 …… 288
19.2　传感器网络的成长 …… 289
19.3　传感器网络的设计因素 …… 289
19.4　传感器网络中的安全 …… 292
19.5　传感器网络的安全机制和最优方法 …… 294
19.6　传感器网络安全研究趋势 …… 295
练习 …… 297
高级练习 …… 297
参考文献 …… 297

第 20 章　保证信息和计算机网络安全的其他努力 …… 299
20.1　简介 …… 299
20.2　立法 …… 299
20.3　法规 …… 300
20.4　自律 …… 300
20.5　教育 …… 301
20.6　报告中心 …… 302
20.7　市场力量 …… 302
20.8　公益活动 …… 303
练习 …… 303
高级练习 …… 304
参考文献 …… 304

第 21 章　计算机网络以外的安全:信息保证 …… 305
21.1　简介 …… 305
21.2　集体安全动机和最优方法 …… 305
参考文献 …… 308

第四部分　安全项目

第 22 章　项目 …… 310
22.1　简介 …… 310
22.2　第一部分:单周/双周试验安排 …… 310
22.3　第二部分:学期项目 …… 312
22.4　用于增强 Web 应用程序安全的工具 …… 316
22.5　第三部分: 研究项目 …… 317

第一部分　理解计算机网络安全

第 1 章　计算机网络基础

第 2 章　理解计算机网络安全

第1章　计算机网络基础

1.1　简介

在所有通信类型的基本概念中，为了能够通信必须包括三种组件。首先，必须有两个实体，分别称为发送者和接收者，二者必须具有某种共享的东西。其次，必须存在某种媒体，以便通过它将共享的项目连接起来，也就是所谓的传输媒体。最后，必须有达成一致的一组通信规则或协议。这三部分适用于任何一类或任何一种通信结构。

本章将集中研究计算机网络中的上述三种组件。那么什么是计算机网络呢？计算机网络是一种分布式系统，由松散耦合的计算机或其他设备所组成。其中任意两台设备（不失一般性，不妨称之为网络元素或传输元素）可以经过通信媒体相互通信。为了使这些互连的设备成为所谓的通信网络，就必须有一组网络中的每台设备应该遵守的规则或协议，以便与网络中的另外一台设备进行通信。硬件和软件的组合就是计算机通信网络或简称为计算机网络。图1.1显示了一个计算机网络。

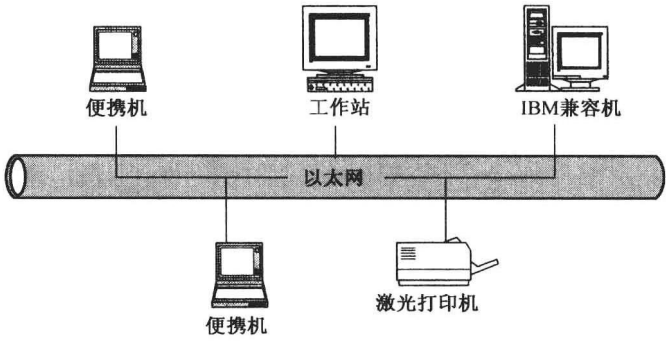


图1.1　计算机网络

硬件组件由一组节点形成的网络元素构成，包括一般称为主机的终端系统以及由集线器、网桥、路由器和网关组成的中间交换元素，我们将它们统称为网络元素。

网络元素可以有自己的局部资源或全局资源。网络软件由所有的应用程序和网络协议组成，用来同步、协调并在网络元素之间实现资源共享和数据交换。网络软件也使得在网络中共享昂贵的资源成为可能。网络元素、网络软件和用户全部都在一起工作，以便于单个用户可以交换信息和共享在本地不能提供的位于其他系统上的资源。网络元素和资源可以采用多种硬件技术并且软件也可以尽可能不同，但是全部组合必须一起协调工作。

网络互连技术使得多种、分散的底层硬件技术和不同软件能够异构互连起来并使它们顺利地通信。任何计算机通信网络的工作都是通过网络元素提供的底层机制以及运行在通信元素上的软件提供的高层通信设施取得的。在讨论这些网络如何工作之前，先探讨一下不同的网络类型。

1.2　计算机网络模型

计算机网络的配置模型有多种,其中最常用的是集中式模型和分布式模型。在集中式模型中，多台计算机和设备互连起来并且能够互相通信。但是，仅有一台称为主机的中央计算机，所有的通信必须通过它才能进行。从属的计算机称为代理，可能具有较少的本地资源(如内存)，共享的全局资源受处在中心位置的主机控制。与集中式模型不同，分布式网络中松散耦合的计算机通过由互连的元素和通信信道组成的通信网络互连而成。计算机本身可能拥有本地局部资源,或者也可能从远程计算机请求资源。这些计算机就是所谓的包括主机、客户机或节点的一串名字。如果一台主机具有其他主机需要的资源，那么这台主机就称为服务器。通信和资源的共享不是由中央计算机控制，而是由网络中的两个通信节点来决定。图 1.2和图 1.3 分别显示了一个集中式网络模型和一个分布式网络模型。

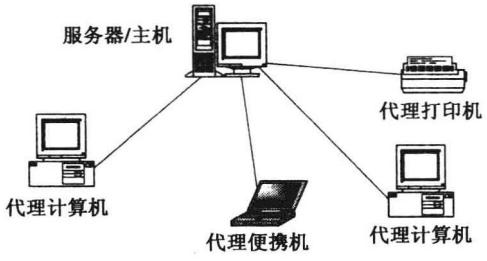


图 1.2　集中式网络模型

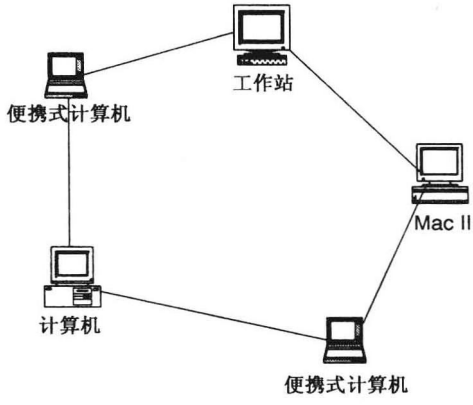


图 1.3　分布式网络模型

1.3　计算机网络类型

计算机网络规模各有不同。每一个网络都是由一簇网络元素及其资源组成，簇的大小决定着网络的类型。一般来讲有两种网络类型:局域网和广域网。

1.3.1　局域网

带有两台或多台计算机或一簇网络及其资源，由通信媒介连接共享通信协议，并且局限于小的地理区域(如建筑物的不同楼层或一栋建筑物)或一些相邻的建筑物的计算机网络，被称为局域网(LAN)。局域网的优势在于所有的网络元素紧靠在一起，以便于通信链路维护较高的数据移动速度。也由于较近的通信元素的原因，就可以使用昂贵的和高质量的通信元素提供更好的服务和高可靠性。图 1.4 显示了一个局域网网络。

1.3.2　广域网

广域网(WAN)是由一簇或多簇网络元素及其资源构成的网络，簇的元素或簇本身不局限于一个很小的区域内，而是分散到广阔的地理区域，如在一个国家区域内，跨越整个国家、几个国家甚至是全球的因特网。

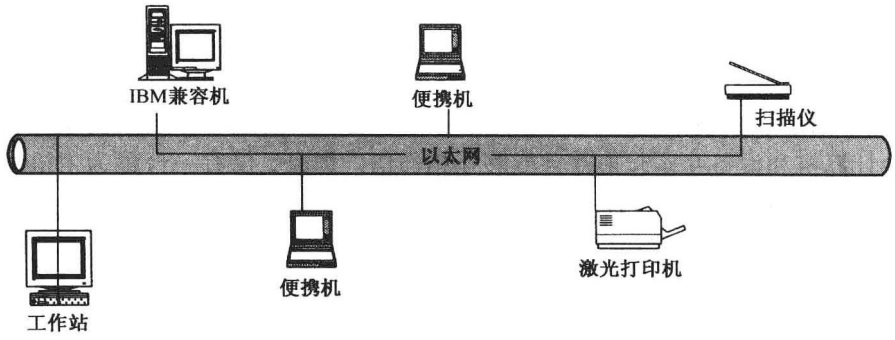


图 1.4 局域网

广域网的优点包括可以将服务分布到更广的团体、提供局域网所不能提供的硬件和软件资源。但是，因为广域网覆盖了广阔的地理面积，导致通信介质很慢并且经常不可靠。图 1.5 显示了一个广域网。

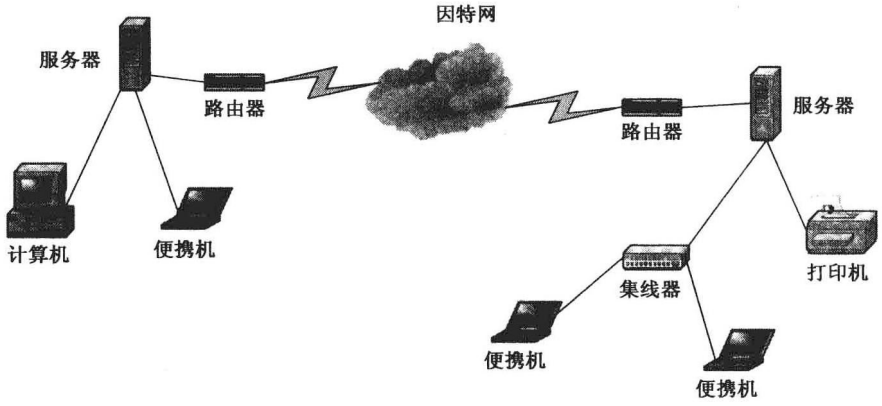


图 1.5 广域网

1.3.3 城域网

介于局域网和广域网之间有一种中等规模的网络，称为城域网(MAN)，因为其覆盖范围要比局域网稍大，但是又没有广域网那么大。覆盖一座城市或者城市一部分的居民网络就是城域网的一个很好例子。一般很少谈及城域网，是因为它介于局域网和广域网之间。

1.4 数据通信媒体与技术

某种类型网络的性能极大地依赖于网络中所使用的传输技术和所使用的媒体。让我们分别对这两者进行讨论。

1.4.1 传输技术

传输信息的媒体决定了所使用的信号。某些媒体仅允许传输模拟信号，但某些既允许传输模拟信号又允许传输数字信号。根据涉及的媒体类型以及其他方面的考虑，输入的数据既

可以表示成数字信号也可以表示成模拟信号。在模拟格式下，数据以某一时间间隔内的连续电磁波表示的(如语音和视频等)，在各种媒体(如铜导线、双绞线对或同轴电缆、光纤或无线)中传播。后面会分别讨论这些媒体。另一方面，以数字格式表示时，数据是以数字信号的形式发送的，由一系列电压脉冲表示成一串二进制比特。模拟和数字数据两者都能传播，并且大多数情况下既可以表示成模拟也可以表示成数字。

传输本身就是在网络元素之间传播并处理数据信号。为了传输而表示的数据，既可以是模拟信号又可以是数字信号，被称为编码方案。编码后的数据通过连接所有网络元素的传输媒体进行传输。

编码方案有两种，分别是模拟和数字。模拟编码传播表示模拟数据的模拟信号(例如声波和语音数据)，而数字编码传播既可以表示模拟信号也可以表示通过两个电压等级形成的二进制流数字数据的数字信号。

因为本书中我们的兴趣在于数字网络，因此将重点介绍数字编码。

1.4.1.1　数字数据的模拟编码

数字信息是以 1 或 0 的形式表示的。为了通过如电话线等某些具有有限带宽的媒体发送信息，数字数据需要使用调制及解调生成模拟信号的方式进行编码。编码使用连续的震荡波形，通常是正弦波形，具有恒定频率的信号称为载波信号。载波具有三个调制特性：振幅、频率和相移。然后使用调制解调器(一种调制解调对)，根据三个载波特性之一或者某种组合调制和解调数据信号。结果波形位于载波两边频率范围之间，如下所示：

- 振幅调制中的每个二进制值由不同振幅的载波频率表示。没有载波或低载波频率就表示为 0，而其他频率表示为 1。但是这是一种效率很低的调制技术，因此仅用于最多为 1200 bps 的低频率的语音级线路上。
- 频率调制也是通过利用接近载波频率的两个频率来表示二进制值的。较高的频率代表 1，较低的频率代表 0。这种方案不容易出错。
- 相移调制更改载波的定时，通过移动载波的相位来编码数据。1 编码成更改 180 度相位，而 0 编码成载波信号更改为 0 相位。这是三种编码方案中最有效的一种，传输速率可以达到 9600 bps。

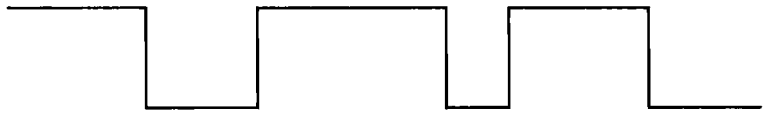
1.4.1.2　数字数据的数字编码

这种编码方案中提供了一种最常见和最容易的传输数字信号方法，两个二进制数字常被表示成两种不同的电压。在计算机内，这些电压一般用 0 V 和 5 V 表示。另一方法使用两种代码表示：不归零编码(NRZ-L)和不归零反相编码(NRZ-I)，NRZ-L 中负电压表示二进制中的 1 而正电压表示 0。这两种编码例子参见图 1.6 和图 1.7。在 NRZ-L 中，只要出现了 1，就从一个电压跳变到另外一个电压，用来表示信号信息。NRZ 信号编码技术的问题之一是需要接收机和发射机之间能很好地进行时钟同步。也就是至少要发送一个单独的时钟信号。还有其他的表示方法，例如曼彻斯特和差分曼彻斯特，则是将时钟信息编码到数据之中。

人们不禁会问，为什么还要麻烦使用数字编码和传输？这是因为它与模拟编码相比具有如下几个优点：

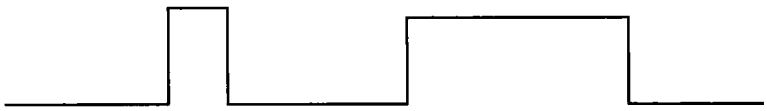
- 可以降低数字电路的费用
- 更加有效地集成语音、视频、文本和图像

- 因为使用了中继器，可以降低噪音和其他信号损失
- 使用数字技术可以最好地利用信道的容量
- 便于加密，因此要比模拟传输具有更好的安全性



0000000000000011111111110000000000000000000011111110000000000000000011111111

图 1.6 NRZ-L 不归零编码的表示



00000000000000011111000000000000000000111111111111111111110000000000

图 1.7 NRZ-I 不归零反相编码对多个 1 的表示

1.4.1.3 传输信号的多路复用

在网络媒体上传输数据期间，经常会出现传输数据的容量远远低于媒体容量的情况。发生这种情况时，可以让多个信号载波共享同一传输媒体，这就是所谓的多路复用。有两种方法实现多路复用：时分多路复用(TMD)和频分多路复用(FDM)。

在 FDM 中，所有的数据信道首先转换成模拟形式。因为在一个载波上可以承载多个信号，每个模拟信号就被一个分隔开的不同载波频率所调制，这样一来就可以在解调处理中将信号恢复出来。频率被捆绑到载波上。在接收端，解调器可以选择需要的载波信号并以一种带宽不重叠的方式用它从信道中提取数据信号。FDM 具有支持全双工通信的优点。

TDM 则不同，它通过将信道分成时隙，在数据流发送之前将时隙分配给数据流来工作。在传输的两端，如果发送方和接收方同意时隙的分配，那么接收方就能很容易地恢复并重构原来的数据流。因此多个数字信号通过准时交叉插入每个信号的一部分就可以在同一载波上承载。

1.4.2 传输媒体

正如我们所观察到的，任何形式的通信必须经过媒体，也只有通过媒体才能实现通信。因此为了通信，网络中的网络元素就离不开媒体。没有传输媒体，网络就不能起作用，因为传输元素之间没有连接起来。传输媒体在网络性能中占据重要的位置。总体来讲，网络性能质量、可靠性以及网络的整体性能极大地依赖于传输媒体。传输媒体也确定了网络的容量、网络流量、网络可靠性、以覆盖距离表示的网络大小以及传输速率。网络传输媒体既可以是有线的，也可以是无线的。

1.4.2.1 有线传输媒体

有线传输媒体用于物理地连接固定网络中的每个网络元素。有各种不同类型的物理媒体，其中最常用的是铜导线、双绞线、同轴电缆和光纤。

铜导线用于传统通信中是由于传输电流时的低电阻，从而使得信号传输得更远。但是铜导线易受环境中电磁波的干扰，正因为此，必须总是将铜导线加以绝缘。