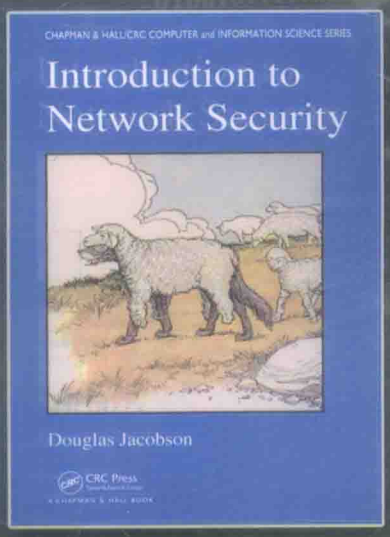
国外计算机科学教材系列

CRC Press
Taylor & Francis Group

网络安全基础
——网络攻防、协议与安全

Introduction to Network Security



[美] Douglas Jacobson 著
仰礼友 赵红宇 译

中国工信出版集团
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

网络安全基础

——网络攻防、协议与安全

Introduction to Network Security

[美] Douglas Jacobson 著

仰礼友 赵红宇 译

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

内 容 简 介

本书从网络攻防、协议与安全解决方案的角度阐述网络安全，把网络看成安全与不安全的源头。全书共分为四部分，第一部分讨论网络概念与威胁的入门知识，分别介绍了网络体系结构、网络协议、互联网和网络漏洞的分类；第二部分讨论低层网络安全，包括物理网络层概述、网络层协议和传输层协议；第三部分讨论应用层安全，包括应用层概述、邮件、Web 安全和远程访问安全；第四部分基于网络防范，介绍了常用的网络安全设备。

本书适合作为计算机科学或计算机工程专业高年级本科或硕士研究生的网络安全课程教材，也适合网络与信息安全相关方向专业人士参考。

Douglas Jacobson: Introduction to Network Security
ISBN: 9781584885436

版权贸易合同登记号　图字：01-2010-5784

图书在版编目(CIP)数据

网络安全基础：网络攻防、协议与安全/(美)雅各布森(Jacobson, D.)著；仰礼友，赵红宇译.
北京：电子工业出版社，2016.5
国外计算机科学教材系列
书名原文：Introduction to Network Security
ISBN 978-7-121-28534-9

Ⅰ. ①网… Ⅱ. ①雅… ②仰… ③赵… 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(2016)第 071755 号

策划编辑：马　岚
责任编辑：马　岚
印　　刷：涿州市京南印刷厂
装　　订：涿州市京南印刷厂
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：18.75　字数：480 千字
版　　次：2016 年 5 月第 1 版
印　　次：2016 年 5 月第 1 次印刷
定　　价：49.00 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)88254888，88258888。
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。

再 版 序

网络一方面给人们的生活、交流、工作与发展带来方式上的巨大变化，同时也对国家与军队的信息安全和人们的个人隐私带来了不可否认的安全威胁与巨大挑战。网络与信息安全不仅严重影响和制约了网络的普及和应用，同时也涉及到国家、军队的信息安全及社会的经济安全，使人们对网络又爱又恨。

本书的作者是美国爱荷华州立大学电子与计算机工程系教授，现任爱荷华州立大学信息确保中心主任，该中心是国家安全局认可的在信息确保教育方面具有学术地位的特许中心。作者从网络和协议存在的固有漏洞的分析出发，提出减少和解决这些安全漏洞的多种解决方案，把网络看成不安全和安全的源头，来考查不同的网络协议，洞察网络的漏洞，提出利用攻击和减少攻击的方法。

本书对于想全面了解网络漏洞产生的根源，想深入探讨如何解决网络安全问题的科研人员来说，是一部很好的参考书。本书结构清晰、内容翔实且每章附有课后作业和实验作业及参考文献，信息量大，所以更是一部很好的大学高年级学生和研究生专业基础课教材。

仰礼友教授和赵红宇副教授组织翻译完成了 Douglas Jacobson 的这本侧重网络安全实践的教材。中译本在 5 年中已多次重印，被许多网络工程相关专业的教师采用作为教材。作者在网站 http：//www. dougj. net/textbook/还提供了一些补充资料。这次出版，两位译者对全书译文进行了修订勘误，尽力以更好的内容质量面对读者。也欢迎广大读者的沟通交流，联系邮箱 malan@phei.com.cn。

前　言

写作思路

本书从网络漏洞、协议与安全解决方案出发，重点论述网络安全，而同类专著关注的是安全和安全方案，他们把网络看成用于通信的目的，而本书把网络看成不安全和安全的源头，从洞察网络的漏洞、探测、攻击和减少攻击的方法入手分析不同的网络协议。

自从有人类历史以来，网络作为通信系统一直就在我们身边存在，通信双方凭借的是信任。早期通信系统凭借通信双方可看得见的识别物来进行通信，并且使用简单的方式来保护数据。例如，借助双方都认识的信使，并使用信件蜡封确保私密。随着技术的进步，传输数据的方法也随之改进了，盗窃与保护数据的方法也同样在改进。然而，直到20世纪末，双方数据的直接传输仍然不是通过今天意义上的网络，双方是借助其他方法来识别数据的归属的。我们今天面临的问题比过去要复杂得多，今天已经有了不受任何实体或组织控制的网络把计算机连接起来。与过去的数据通信不同，今天的网络由无数的设备构成，它们在数据从发送者传送到接收者的过程中对数据进行处理。当初设计这些网络是为了方便通信，只在小范围的可信任的团体和已经认识的个体中使用，设计中并没有考虑安全性。

内容组织

本书第一部分简要讨论网络体系结构与典型网络的层次功能，以及基于网络的漏洞和攻击的分类，这个分类描述的是所涉及的每一协议层的漏洞和攻击的架构，共分为四类：

- 基于头部的漏洞与攻击：修改了协议头部，或使头部无效。
- 基于协议的漏洞与攻击：数据包是有效的，但不能被直接使用。
- 基于验证的漏洞与攻击：修改了发送方与接收方的识别标志。
- 基于流量的漏洞与攻击：借助流量实施攻击。

第二部分从网络的不同层（物理层、网络层与传输层）审视每一层的安全，采用自底向上的网络安全方法，让读者理解网络每一层的漏洞与安全机理。例如，通过理解物理层固有的漏洞及可能的安全防范，进而理解网络层可能存在的漏洞，以及为克服漏洞而采用的安全机制。

第三部分探讨几个普通的网络应用安全案例。在互联网上，这些应用只是把网络底层看成数据准确无误地由一个应用传送到另一个应用的渠道。本书把漏洞看成网络底层提供的网络功能，从而让读者深入理解安全就是要克服这些漏洞。

第四部分描述几个经常部署的并与上述分类相关的基于网络的安全解决方案。

本书采用“界定-攻击-防范”的方法来阐述网络安全。首先简要引入相关的协议，接着详细描述熟知的漏洞，然后介绍可能的攻击方法。本书重点在于描述攻击的方法，而不是具体的攻击工具，具体攻击工具一般作为课后作业或实验引入。读者一旦理解了对某个协议的各种威胁，就能提出可能的解决方案。每章的后面都根据每章的概念给出课后作业及实验室实验，允许读者尝试某些攻击并审视破解攻击方案的有效性。

附录 A 为密码学概述。附录 B 讨论研发或部署一个低成本的实验室，用于支持课堂教学或用来作为合作实验床。附录 C 为课后作业答案。

读者

本书面向两类读者：一是作为计算机科学或计算机工程专业的本科高年级或硕士研究生第一年的网络安全课程教材，二是作为网络安全专业的网络安全课程或网络专业的部分课程教材。当然，本书也可以用于网络或网络安全专业人员的参考书。

本书和其他著作的区别如下：

网络焦点。本书通过剖析网络协议及其弱点和对策来审视网络安全。有几本著作，其主要焦点在几个应用层协议（Kerberos，Secure Email，SecureWeb 等），而不关心底层协议（物理层、网络层与传输层），而许多麻烦的问题是由这些层的漏洞引起的。

网络安全视角。本书采用大多数著作中采用的方法，即通过网络的层提供哪些服务与功能来审视网络安全，并在这些层提供服务与功能时，审视网络存在的漏洞与安全问题。根据这一视角，本书既可作为网络专业的网络安全课程，也可作为网络安全专业的网络安全课程。

实验室实验。本书包含实验室实验课所需的实验材料，这些实验考察网络的攻击与防范，而且本书还提供一个典型的低成本的实验室部署。

Web 网站。本书提供了 Web 网站（http://www.dougj.net/textbook/）。网站包括授课讲义和关于 UNIX、C 及套接字编程的指导手册，还有建设或维护实验室的详细信息。

网络安全实践视角。本书提供了网络安全实践视角，我们考察实际协议，给读者提供详细素材及理解漏洞与研发对策所需的信息。这些将通过实验进一步加以巩固。

攻防方法。本书从攻防视角来考察网络安全，考察当前协议的漏洞及降低攻击的防范机制。本书焦点不在于攻击的工具，而在于攻击的方法。通过实验，学生可以研究网络攻击的效果及安全系统的有效性。

术语定义。本书涉及很多网络与安全术语，其中许多是专属本领域的术语。因此，笔者认为在章节之后列举所涉及术语的简短定义是很重要的，新术语在所在节中给出。在我们开始阐述正文之前，有几个术语需要定义，以使读者有一个通用的参照模式。

定　义
应用 指允许用户连接网络并执行某项任务的计算机程序。
攻击者 指利用网络攻击计算机系统、网络或其他连接在互联网中的设备的个人或群体。
黑客 即攻击者。
主机 连接到网络上的计算机。
互联网 互连众多网络设备的全球网络的集合。
网络 一组互连的设备并可以相互通信。

网络设备

连接到网络上的设备，泛指包括主机或计算机在内的所有设备，这些设备使网络可以运行起来。

目标

黑客试图攻击的设备、主机、用户或目标。

用户

利用网络执行计算机程序的个人，或一般的计算机用户。

致谢

感谢我的妻子 Gwenna，感谢我的孩子们（Sarah，Jordan 和 Jessica），感谢他们的支持与耐心。还要感谢 Sharon Sparks 在本书的编辑方面给予的帮助。

目　录

第一部分　网络概念与威胁入门

第 1 章　网络体系结构 …… 2
1.1　网络的层次结构 …… 3
1.2　协议概述 …… 7
1.3　层次网络模型 …… 9
课后作业和实验作业 …… 12
参考文献 …… 13

第 2 章　网络协议 …… 14
2.1　协议规范 …… 14
2.2　地址 …… 17
2.3　头部 …… 21
课后作业和实验作业 …… 22
参考文献 …… 23

第 3 章　互联网 …… 24
3.1　寻址 …… 25
3.1.1　地址欺骗 …… 28
3.1.2　IP 地址 …… 28
3.1.3　主机名与 IP 地址的匹配 …… 29
3.2　客户-服务器模式 …… 30
3.3　路由 …… 34
课后作业和实验作业 …… 36
参考文献 …… 37

第 4 章　网络漏洞的分类 …… 38
4.1　网络安全威胁模型 …… 38
4.2　分类 …… 43
4.2.1　基于头部的漏洞和攻击 …… 43
4.2.2　基于协议的漏洞和攻击 …… 44
4.2.3　基于验证的漏洞和攻击 …… 45
4.2.4　基于流量的漏洞和攻击 …… 47
4.3　分类方法的应用 …… 47

课后作业和实验作业 …… 49
参考文献 …… 49

第二部分　低层网络安全

第 5 章　物理网络层概述 …… 52
5.1　常见的攻击方法 …… 53
5.1.1　硬件地址欺骗 …… 53
5.1.2　网络嗅探 …… 55
5.1.3　物理攻击 …… 55
5.2　有线网络协议 …… 56
5.2.1　以太网协议 …… 56
5.2.2　基于头部的攻击 …… 62
5.2.3　基于协议的攻击 …… 62
5.2.4　基于验证的攻击 …… 62
5.2.5　基于流量的攻击 …… 64
5.3　无线网络协议 …… 65
5.3.1　基于头部的攻击 …… 70
5.3.2　基于协议的攻击 …… 70
5.3.3　基于验证的攻击 …… 71
5.3.4　基于流量的攻击 …… 73
5.4　常用对策 …… 77
5.4.1　虚拟局域网(VLAN) …… 77
5.4.2　网络访问控制(NAC) …… 78
5.5　一般结论 …… 80
课后作业和实验作业 …… 80
参考文献 …… 81

第 6 章　网络层协议 …… 83
6.1　IPv4 协议 …… 84
6.1.1　IP 寻址 …… 84
6.1.2　路由 …… 87
6.1.3　数据包格式 …… 91
6.1.4　地址解析协议(ARP) …… 93
6.1.5　网际控制消息协议(ICMP) …… 95
6.1.6　把它们组合在一起 …… 97
6.1.7　基于头部的攻击 …… 105
6.1.8　基于协议的攻击 …… 106
6.1.9　基于认证的攻击 …… 106

6.1.10 基于流量的攻击 …… 108
6.2 引导协议(BOOTP)和动态主机配置协议(DHCP) …… 111
6.2.1 引导协议(BOOTP) …… 111
6.2.2 DHCP 协议 …… 113
6.2.3 基于头部的攻击 …… 115
6.2.4 基于协议的攻击 …… 115
6.2.5 基于验证的攻击 …… 115
6.2.6 基于流量的攻击 …… 116
6.3 IPv6 协议 …… 116
6.3.1 数据包格式 …… 117
6.3.2 版本 6 的 ICMP 协议 …… 119
6.4 常用的 IP 层对策 …… 119
6.4.1 IP 过滤 …… 120
6.4.2 网络地址转换(NAT) …… 120
6.4.3 虚拟专用网(VPN) …… 124
6.4.4 IP 安全(IPSEC) …… 126
课后作业和实验作业 …… 128
参考文献 …… 132
第 7 章 传输层协议 …… 135
7.1 传输控制协议(TCP) …… 135
7.1.1 多路复用 …… 135
7.1.2 连接管理 …… 136
7.1.3 数据传输 …… 136
7.1.4 特殊服务 …… 137
7.1.5 错误报告 …… 137
7.1.6 TCP 协议 …… 137
7.1.7 TCP 数据包格式 …… 139
7.1.8 基于头部的攻击 …… 140
7.1.9 基于协议的攻击 …… 140
7.1.10 基于验证的攻击 …… 144
7.1.11 基于流量的攻击 …… 145
7.2 用户数据报协议(UDP) …… 145
7.2.1 数据包格式 …… 146
7.2.2 基于头部和协议的攻击 …… 146
7.2.3 基于验证的攻击 …… 146
7.2.4 基于流量的攻击 …… 146
7.3 域名服务(DNS) …… 146
7.3.1 DNS 协议 …… 148

7.3.2 DNS 数据包格式 …… 149
7.3.3 基于头部的攻击 …… 151
7.3.4 基于协议的攻击 …… 151
7.3.5 基于验证的攻击 …… 151
7.3.6 基于流量的攻击 …… 152
7.4 常用对策 …… 153
7.4.1 传输层安全(TLS) …… 153
课后作业和实验作业 …… 154
参考文献 …… 155

第三部分 应用层安全

第 8 章 应用层概述 …… 158
8.1 套接字 …… 159
8.2 常见攻击方法 …… 161
8.2.1 基于头部的攻击 …… 161
8.2.2 基于协议的攻击 …… 161
8.2.3 基于验证的攻击 …… 162
8.2.4 基于流量的攻击 …… 162
课后作业和实验作业 …… 162
参考文献 …… 163

第 9 章 电子邮件 …… 164
9.1 简单电子邮件传输协议(SMTP) …… 166
9.1.1 漏洞、攻击和对策 …… 168
9.2 POP 和 IMAP …… 172
9.2.1 漏洞、攻击和对策 …… 175
9.3 MIME …… 177
9.3.1 漏洞、攻击和对策 …… 181
9.4 一般电子邮件对策 …… 182
9.4.1 加密和验证 …… 182
9.4.2 电子邮件过滤 …… 185
9.4.3 内容过滤处理 …… 187
9.4.4 电子邮件取证 …… 188
课后作业和实验作业 …… 192
参考文献 …… 194

第 10 章 Web 安全 …… 196
10.1 超文本传输协议(HTTP) …… 198
10.1.1 指令信息 …… 198

10.1.2 回应消息 …… 199
10.1.3 HTTP 消息头部 …… 200
10.1.4 漏洞、攻击和对策 …… 205
10.2 超文本标记语言(HTML) …… 209
10.2.1 漏洞、攻击和对策 …… 211
10.3 服务器端安全 …… 213
10.3.1 漏洞、攻击和对策 …… 214
10.4 客户端安全 …… 215
10.4.1 漏洞、攻击和对策 …… 217
10.5 常用 Web 对策 …… 218
10.5.1 URL 过滤 …… 218
10.5.2 内容过滤 …… 221
课后作业和实验作业 …… 222
参考文献 …… 223
第 11 章 远程访问安全 …… 226
11.1 基于终端的远程访问(TELNET,rlogin 和 X-Windows) …… 226
11.1.1 TELNET …… 226
11.1.2 rlogin …… 229
11.1.3 X-Windows …… 232
11.1.4 漏洞、攻击和对策 …… 233
11.2 文件传输协议 …… 235
11.2.1 文件传输协议(FTP) …… 235
11.2.2 轻量级文件传输协议 …… 240
11.2.3 远程复制协议(RCP) …… 241
11.2.4 漏洞、攻击和对策 …… 241
11.3 对等网络 …… 243
11.3.1 集中式的对等网络 …… 244
11.3.2 KaZaA …… 246
11.3.3 分布式对等网络 …… 247
11.3.4 漏洞、攻击和对策 …… 249
11.4 常用的对策 …… 251
11.4.1 加密远程访问 …… 251
11.4.2 安全外壳协议(SSH) …… 252
11.4.3 远程桌面 …… 254
11.4.4 安全文件传输(SFTP、FTPS 和 HTTPS) …… 254
课后作业和实验作业 …… 255
参考文献 …… 257

第四部分　网络减灾

第 12 章　常用网络安全设备 …… 262
12.1　网络防火墙 …… 262
12.2　基于网络的入侵检测和防护 …… 266
12.3　基于网络的数据丢失保护 …… 268
课后作业和实验作业 …… 270
参考文献 …… 270
附录 A　密码学 …… 273
附录 B　实验室配置 …… 279
附录 C　课后作业答案 …… 283

第一部分　网络概念与威胁入门

第 1 章　网络体系结构
第 2 章　网络协议
第 3 章　互联网
第 4 章　网络漏洞的分类

第一部分介绍基本网络概念和网络漏洞与攻击的分类，已经学习过网络的读者可以跳过这一部分的前3章。第1章讨论支持网络分层方法的概念及如何由通常的网络结构透视网络安全。第2章概述网络协议并讨论与网络安全相关的网络协议的几个关键方面。第3章论述互联网的几项关键内容，如路由、寻址，以及它们如何与安全相关。第4章介绍网络漏洞和攻击的分类，并引入网络威胁模型，这是本书在其余各章剖析网络漏洞、攻击与对策的基础。

第1章　网络体系结构

在探讨网络概念与安全之前，简要回顾一下网络发展的历史[1-9]是有裨益的，因为过去所做的一切对今天的安全是有影响的。图1.1给出了网络发展历史的各个阶段。

图1.1　网络发展的历史

正如图1.1所示，过去30年间发生了许多变化，网络的规模与复杂性都在增加。早期网络设计只提供连通性，并不支持安全。20世纪70年代第一个网络仅限于几个研究机构与大学之间[8,9]，且互连的每一方都是可信任的，安全的问题并不突出。1988年，针对网络上的计算

机的攻击首次出现[10]，直到今天采用相同方法的某些攻击仍然有用。推动网络的创新与增长是网络的简单易用与互连，而不是安全，这一点将贯穿全书。

1.1　网络的层次结构

本节阐述网络是如何实现的，以及网络提供的功能。一个网络可以划分为不同的功能模块，这些功能模块称为层[11,12]，而每一层都被赋予相应的职能，这些层就构成现代网络的全部功能。层可以由软件或硬件实现，但网络上的每一台设备并不对应所有网络层。例如，路由器的设计就不是针对每一层的，因为它不负责数据端到端的传输，它只关心把网上送来的数据传输到下一个节点。本节将从描述网络层的结构开始，然后描述因特网上这些层所提供的服务与功能。

计算机通信的第一个例子，是由两台希望通信的设备通过点对点的连接构成的。在这个例子中，通信需要的软件是自带的，且由销售商独家开发。物理连接既可能是直接采用专线，也可能是采用电话线加调制解调器。数据速率和今天的网络速率相比是很低的，应用往往基于简单的文本通信。这些早期应用一般用于简单的文件传输或远程访问。因为有这些应用，所以在计算机之间不需要数据中继。计算机之间采用数据中继的第一个应用是电子邮件，早期的电子邮件系统设计仅用于同类计算机之间的文本信息传输。由于早期的文件传输系统使用专用软件进行通信，因此异种计算机之间的电子邮件通信很困难。

20 世纪 70 年代，业界开始着力制定标准[13]，旨在让网络上不同种类的设备实现通信。早期标准的制定者决定把问题分成功能模块，即不同的计算机采用不同的方法使之互相通信。每一个模块或每一层执行一组功能，并为它上面的那一层提供一组服务，本层使用它下面那一层提供的服务。图 1.2 是采用黑匣子方法定义的一个层，图 1.2(a)表示任何一个黑匣子的设计方法，输入和输出定义为一组服务和要实现的功能。由某一层提供的服务称为服务访问点(service access point，SAP)，每层实现标准中规定的一组功能，这些功能用于支持一组服务，这些服务通常涉及希望交换数据的两个设备对应层之间的通信。这个内部层之间的通信称为协议。实现这个层的具体方法在标准中没有规定，后面会讲到，这一点会导致一些值得关注的安全问题。这种定义每一层的黑匣子方法，使得不同的提供商能够实现相同的功能与服务。

由图 1.2(b)可以看到，层 A 为上一层提供服务，层 B 为层 A 提供服务，这些服务通常被规定为子程序调用(正如在程序中看到的)。例如，这里有一个由层 A 提供的 send_data(目标、源、数据、选项和长度)服务，这个服务用于发送一个数据块到与其对应的层 A，即由目标地址指定的另一台设备。这个服务有几个参数，用于指定层如何处理服务请求，同时包括要传送到对等层的信息。参数 data 包含层 A 要发送到目标设备上的对应层 A 的数据，每一层利用它的下一层提供的服务实现它要提供的功能。同样，在图 1.2(b)中，层 B 提供的服务为 send_packet(目标、源、数据和选项)。

注意，在这个例子中，层 B 提供发送一个固定长度数据的 send_packet 子程序，它上面的层 A 提供一个发送较大数据量的服务，这就是某一层要提供的功能所在。在这个例子中，层 A 需要提供一个功能，把从上一层收到的数据分成较小的数据包，并发送到下一层，收到数据的对应层 A 需要提供一个功能，把这些小的数据包收集到一起，成为一个数据块，并发送给它的上一层。当某一层和它对应的层通信时，它必须把数据发送到它的下一层。当某一层执行其功能时，它也必须能将控制信息传递到对应的层。根据图 1.2(b)所示的例子，层 A 需要发送

控制信息，以用于接收层 A 把数据包重新组装起来。对等层之间的交互有对应的交互规则，例如，最大的数据包的尺寸、控制信息和数据的格式，以及控制消息的计时与顺序等。这些规则即是协议，而控制信息用于执行协议。每一层定义为服务、功能与协议的集合。图 1.3 说明了控制信息如何封装到数据中，从而每一层依据它处理来自上一层的请求。

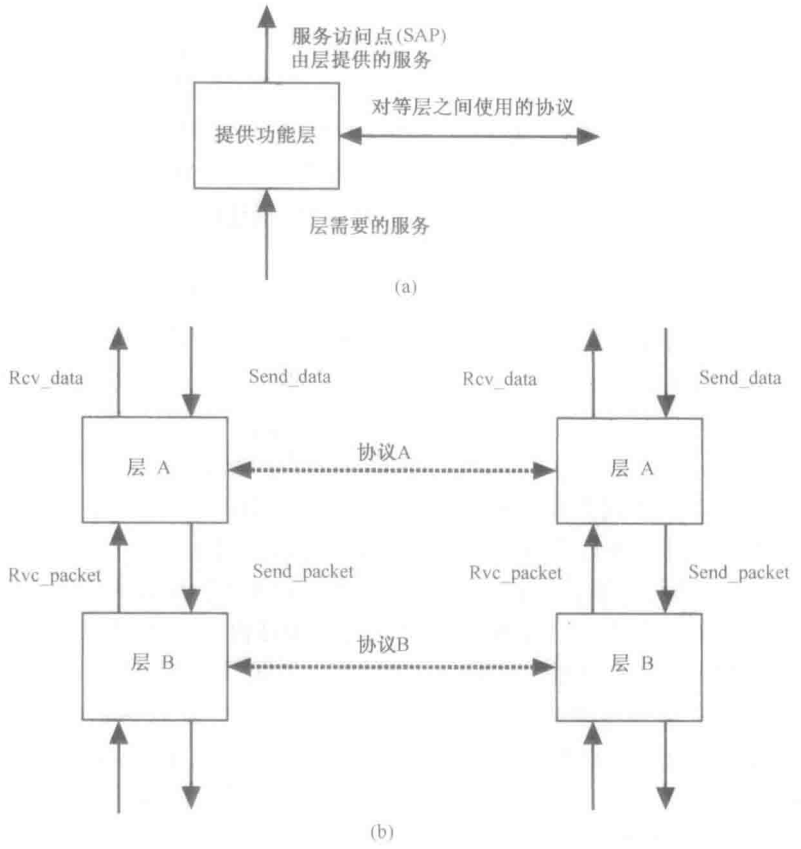


图 1.2 网络的层

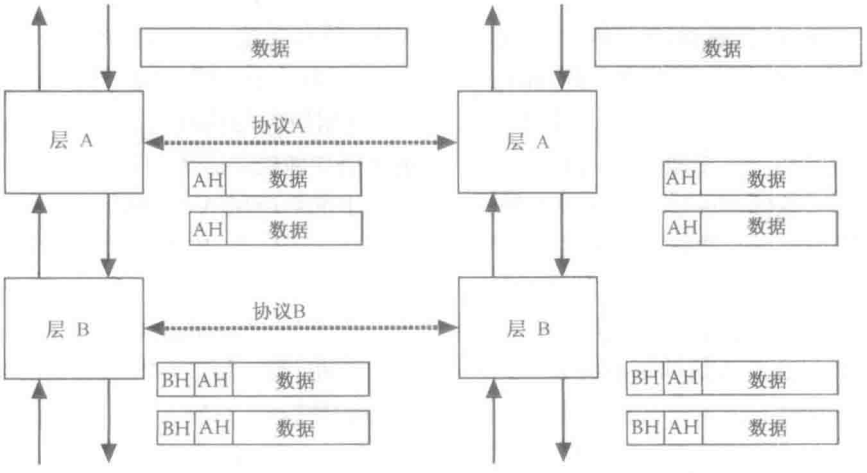


图 1.3 控制信息封装