CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

TCP/IP Essentials

The TCP/IP family of protocols have become the de facto standard in the world of networking, are found in virtually all computer communication systems, and form the basis of today's Internet. *TCP/IP Essentials* is a hands-on guide to TCP/IP technologies, and shows how the protocols operate in practice. The book contains a series of carefully designed and extensively tested laboratory experiments that span the various elements of protocol definition and behavior. Topics covered include bridges, routers, LANs, static and dynamic routing, multicast and realtime service, and network management and security. The experiments are described in a Linux environment, with parallel notes on Solaris implementation. The book includes many exercises, and supplementary material for instructors is available. The book is aimed at students of electrical and computer engineering or computer science who are taking courses in networking. It is also an ideal guide for engineers studying for networking certifications.

SHIVENDRA S. PANWAR is a professor in the Electrical and Computer Engineering Department at Polytechnic University, Brooklyn, New York, USA. He is currently the Director of the New York State Center for Advanced Technology in Telecommunications (CATT). He is the author of over 80 refereed papers.

SHIWEN MAO is a research associate in the Bradley Department of Electrical and Computer Engineering, Virginia Polytechnic Institute and State University, Blacksburg, VA, USA.

JEONG-DONG RYOO is a senior member of research staff at the Electronics and Telecommunications Research Institute, Daejon, South Korea.

YIHAN LI is a research associate in the Department of Electrical Engineering, Polytechnic University, Brooklyn, New York, USA.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

TCP/IP Essentials

A Lab-Based Approach

Shivendra S. Panwar

Department of Electrical and Computer Engineering,
Polytechnic University, Brooklyn, New York

Shiwen Mao

The Bradley Department of Electrical and Computer Engineering,
Virginia Polytechnic Institute and State University
Blacksburg, Virginia

Jeong-dong Ryoo

Electronics and Telecommunications Research Unit,
Daejeon, South Korea

Yihan Li

Department of Electrical and Computer Engineering,
Polytechnic University,
Brooklyn, New York

CAMBRIDGE
UNIVERSITY PRESS

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

PUBLISHED BY THE PRESS SYNDICATE OF THE UNIVERSITY OF CAMBRIDGE
The Pitt Building, Trumpington Street, Cambridge, United Kingdom

CAMBRIDGE UNIVERSITY PRESS
The Edinburgh Building, Cambridge CB2 2RU, UK
40 West 20th Street, New York, NY 10011-4211, USA
477 Williamstown Road, Port Melbourne, VIC 3207, Australia
Ruiz de Alarcón 13, 28014 Madrid, Spain
Dock House, The Waterfront, Cape Town 8001, South Africa

http://www.cambridge.org

© Cambridge University Press 2004

This book is in copyright. Subject to statutory exception
and to the provisions of relevant collective licensing agreements,
no reproduction of any part may take place without
the written permission of Cambridge University Press.

First published 2004

Printed in the United Kingdom at the University Press, Cambridge

Typefaces Times 11/14.5 pt. and Helvetica *System* LaTeX 2_ε [TB]

A catalog record for this book is available from the British Library

Library of Congress Cataloging in Publication data

TCP/IP essentials : a lab-based approach / Shivendra S. Panwar . . . [et al.]
p. cm.
Includes bibliographical references and index.
ISBN 0 521 84144 5 (hardback) ISBN 0 521 60124 X (paperback)
1. TCP/IP (Computer network protocol) 2. Computer networks. I. Panwar, Shivendra S.

TK5105.585.T355 2004
004.6′2–dc22 2004045664

ISBN 0 521 84144 5 hardback
ISBN 0 521 60124 X paperback

The publisher has used its best endeavors to ensure that the URLs for external websites referred to in this book are correct and active at the time of going to press. However, the publisher has no responsibility for the websites and can make no guarantee that a site will remain live or that the content is or will remain appropriate.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

To my wife, Shruti, my parents, and Choti.

Shivendra Panwar

To my wife, Kweesook, my children, James and Michelle, and my parents.

Jeong-dong Ryoo

To our son, Eric, and our parents.

Yihan Li and Shiwen Mao

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

Contents

Preface *page* xiii
Note to instructors xv
Acknowledgements xvi
General conventions xvii
List of abbreviations xviii

0 TCP/IP overview 1

0.1 The Internet 1
0.2 TCP/IP protocols 2
0.3 Internetworking devices 5
0.4 Encapsulation and multiplexing 7
0.5 Naming and addressing 8
0.6 Multiple access 15
0.7 Routing and forwarding 16
0.8 Congestion control and flow control 17
0.9 Error detection and control 18
0.10 Header formats of the protocols 19
0.11 An example: how TCP/IP protocols work together 22

1 Linux and TCP/IP networking 26

1.1 Objectives 26
1.2 Linux and TCP/IP implementations 26
1.3 Linux commands and tools 31
1.4 Diagnostic tools 35

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

1.5 Exercises with Linux commands 36
1.6 Exercises with diagnostic tools 39
1.7 Exercises on port numbers 41

2 A single segment network 43

2.1 Objectives 43
2.2 Local area networks 43
2.3 Network interface 50
2.4 The Internet Control Message Protocol 52
2.5 The Sock traffic generator 54
2.6 Network interface exercises 54
2.7 ARP exercises 55
2.8 Exercises with ICMP and ping 58
2.9 Exercises with IP address and subnets mask 59

3 Bridges, LANs and the Cisco IOS 61

3.1 Objectives 61
3.2 Ethernet bridges 61
3.3 Configuring a bridge or router 66
3.4 Exercises on Cisco IOS 71
3.5 A simple bridge experiment 73
3.6 Spanning tree exercises 75
3.7 Exercise on the Cisco IOS web browser UI 76

4 Static and dynamic routing 77

4.1 Objectives 77
4.2 Static and dynamic routing 77
4.3 Manipulating routing tables 89
4.4 Traceroute 90
4.5 A simple router experiment 91
4.6 RIP exercises 93
4.7 Routing experiments with ICMP 95

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

4.8 OSPF exercise 97
4.9 Static routing experiment 98
4.10 Traceroute experiment 99

5 UDP and its applications 100

5.1 Objectives 100
5.2 The User Datagram Protocol 100
5.3 MTU and IP fragmentation 101
5.4 Client–server applications 102
5.5 Using the sock program 106
5.6 UDP exercises 106
5.7 Path MTU discovery exercise 107
5.8 Exercises with FTP and TFTP 108

6 TCP study 111

6.1 Objectives 111
6.2 TCP service 111
6.3 Managing the TCP connection 112
6.4 Managing the TCP data flow 114
6.5 Tuning the TCP/IP kernel 123
6.6 TCP diagnostic tools 124
6.7 Exercises on TCP connection control 126
6.8 Exercise on TCP interactive data flow 127
6.9 Exercise on TCP bulk data flow 128
6.10 Exercises on TCP timers and retransmission 128
6.11 Other exercises 129
6.12 Exercises with DBS and NIST Net 130

7 Multicast and realtime service 134

7.1 Objectives 134
7.2 IP multicast 134

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

7.3 Realtime multimedia streaming 145
7.4 Simple multicast exercises 152
7.5 IGMP exercises 154
7.6 Multicast routing exercises 156
7.7 Multicast video streaming exercise 158

8 The Web, DHCP, NTP and NAT 159

8.1 Objectives 159
8.2 The HyperText Transfer Protocol 159
8.3 The Dynamic Host Configuration Protocol 164
8.4 The Network Time Protocol 169
8.5 The IP network address translator 172
8.6 Socket programming in a nutshell 175
8.7 HTTP exercises 178
8.8 DHCP exercises 180
8.9 NTP exercises 181
8.10 NAT exercises 182
8.11 Socket programming exercises 185

9 Network management and security 187

9.1 Objectives 187
9.2 Network management 187
9.3 Network security overview 192
9.4 Encryption, confidentiality, and authentication 193
9.5 Application layer security 198
9.6 Transport layer and web security 200
9.7 Network layer security 203
9.8 System security 205
9.9 SNMP exercises 208
9.10 Exercises on secure applications 209
9.11 Exercises on a secure Apache server 210
9.12 Exercises on firewalls and iptables 211
9.13 Exercises on auditing and intrusion detection 212

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

References and further reading 214

Appendix A: instructor's guide 216

A.1 Lab operation mechanism 216
A.2 Lab equipment 217
A.3 Software installation and configuration 219
A.4 Estimated budget 229
A.5 Root privilege for system commands 230
A.6 Internet access 232

Appendix B: initial configuration of the routers 233

B.1 Initial configuration of router1 233
B.2 Initial configurations of the other routers 235

Appendix C: source code 236

C.1 Command files for the DBS experiments 236
C.2 Netspy source code 239
C.3 HTML and CGI files 245
C.4 Socket programming source code 246

Appendix D: list of key requests for comments (RFC) 253

Index 258

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

Preface

You can know the name of a bird in all the languages of the world, but when you're finished, you'll know absolutely nothing whatever about the bird . . . So let's look at the bird and see what it's doing – that's what counts. I learned very early the difference between knowing the name of something and knowing something.

Richard Feynman (1918–1988)

As the title of this book suggests, this book is a *minimalist* approach to teaching TCP/IP *using laboratory-based experiments*. It is minimalist in that it provides one, possibly idiosyncratic, choice of topics at a depth we felt was sufficient to learn the basics of TCP/IP. The intention was not to write a reference text on the subject. The laboratory was important in giving students the experience of observing the TCP/IP protocols in action. The act of observing and drawing some conclusions from those observations, brings to life the often dry study of network protocols, and motivates students to learn more about them.

Appendix A is necessary reading only for the instructor who is in charge of setting up the lab. We have attempted to keep costs down so that only the most Scrooge-like University administrator would raise an eyebrow over the cost of the lab equipment (as for lab space, that may be another matter!). We assume that the students have a basic background in networking, perhaps from a previous course, or perhaps as part of a course that back loads the experiments in this book after providing a general lecture-based introduction to networks. Chapter 0 is a quick overview of TCP/IP that serves two purposes. It provides an overview of the TCP/IP stack, and serves as the framework for the rest of the book. Chapters 1 to 9 have the following common structure. Each of them provides introductory material suitable for presentation in the lecture part of the course followed by a lab experiment. The lab experiments should follow lectures that provide the

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

students with the basic knowledge they need to perform the experiments and derive insights from their observations during the course of the experiments. Each lab experiment is designed to take no more than 3 hours to complete.

The experiments were developed on the basis of a course taught at the Polytechnic University over the course of over eight years. Initially, we used SUN workstations with the Solaris operating system, but have now switched to Linux machines. The primary operating system in this book is Linux, but with Solaris commands provided when they differ from Linux commands. Chapter 1 provides an introduction to Linux, since many students may be unfamiliar with this operating system. It also introduces key tools used in subsequent experiments such as tcpdump and Ethereal. Chapter 2 introduces network interfaces, ping and IP addresses. Chapter 3 introduces bridges, also known as layer two switches, bridge/router configuration, and the Cisco IOS. Chapter 4 focuses on routing, with RIP and OSPF as the routing protocols studied, along with the useful traceroute utility. Chapter 5 introduces UDP and FTP. Chapter 6 follows up with TCP, including a study of its congestion control mechanism. These six chapters are sufficient in many cases to introduce students to the basics of TCP/IP. Nonetheless, the next three chapters are important for students who wish to link the basic plumbing of TCP/IP with applications. Chapter 7 deals with IP multicast and realtime applications. The web, DHCP, NTP and NAT are some key applications that are presented in Chapter 8, as well as a brief introduction to socket programming. Network management and security are arguably two of the most important features that students need to know, at least at a basic level. Chapter 9 provides a brief introduction to this material, which can easily be the subject of a separate course. A list of key RFCs is provided at the end of the book.

There are several alternative ways of teaching this material with this book. A general knowledge of networking is assumed as a prerequisite for this book. However, an introductory course in networking could be combined with the first six experiments, back-loaded at the end of the course, to illustrate the lowest four layers of the protocol stack. For computer scientists, a top-down approach is sometimes the preferred approach in teaching networking. In that case the lab experiments can be re-ordered to focus on the higher layers.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

Note to instructors

Additional course material, including lecture transparencies, sample lab reports, homework assignments, examinations, and errata, are available at the course website: www.cambridge.org/052160124X.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

Acknowledgements

The authors would like to acknowledge the support of Polytechnic University, the National Science Foundation, the New York State Office of Science, Technology and Academic Research (NYSTAR), and the Securities Industries Automation Corporation (SIAC). In particular, it was our work with SIAC, a company responsible for the networking and system needs of the New York and American Stock Exchanges, which initially inspired us. In particular, we would like to thank Andrew Bach, Joseph Kubat, Michael Lamberg, Darko Mrakovcic, and Dror Segal of SIAC for their support. A special thanks to Dr. Nitin Gogate, who helped with the initial version of the experiments, and all the graduate students who followed. We would like to thank Jeffrey (Zhifeng) Tao, Yanming Shen and Pei Liu, who helped proofread and test the lab experiments. We would also like to thank the following faculty members who have also taught this course over the years at Poly: Malathi Veeraraghavan, John (Zheng-Xue) Zhao, and Jorg Liebeherr.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

General conventions

The following conventions are used all through this book.

- In paragraphs, Linux, Unix and Cisco IOS commands are written in a bold font, such as: **telnet** and **enable**.
- In a compound command with options and parameters, the command and options are in bold, while the parameters are in italics. For example, in

  tcpdump -enx host *ip_addr1* **and** *ip_addr2*,

  the command **tcpdump** uses options **-e, -n** and **-x**. In the filter that follows, key words such as **host, and, not, or** etc., are also in bold. The parameters are *ip_addr1* and *ip_addr2*, which should be replaced with the corresponding IP addresses during the exercise.

  The following exemplary command,

  /etc/init.d/snmpd start|stop,

  uses two options. Either **start** or **stop** can be used, but not at the same time.
- The name of a host or router is in the `Typewriter` typestyle, e.g., `shakti` or `Router4`.
- A protocol header field is also in the `Typewriter` typestyle, e.g., `Length` or `Source IP Address`.
- Questions in the LAB REPORT section of each exercise should be answered in the lab report. For example, for Exercise 1 in Chapter 1, students need to answer the following question in Lab Report 1.

  LAB REPORT What is the default directory when you open a new command tool? What is your working directory?
- In this guide, we focus on the Linux operating system. However, this guide can also be used with the Sun Solaris operating system. In the following text, Linux-specific material, or general material that apply to both operating systems are used, while the Solaris specific materials are enclosed between horizontal lines.

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

Abbreviations

ACK	Acknowledgement
AIMD	Additive-Increase-Multiplicative-Decrease
API	Application Programming Interface
ARP	Address Resolution Protocol
ARPA	Advanced Research Projects Agency
API	Application Programming Interface
AS	Autonomous System
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
BOOTP	Bootstrap Protocol
BPDU	Bridge Protocol Data Unit
BSD	Berkely Software Distribution
CDE	Common Desktop Environment
CIDR	Classless Interdomain Routing
CBT	Core-Based Tree
CGI	Common Gateway Interface
CRC	Cyclic Redundancy Check
CSMA/CA	Carrier Sense Multiple Access/Collision Avoidance
CSMA/CD	Carrier Sense Multiple Access/Collision Detection
DBS	Distributed Benchmark System
DES	Data Encryption Standard
DHCP	Dynamic Host Configuration Protocol
DNS	Domain Name System
DSS	Digital Signature Standard
DVMRP	Distance Vector Multicast Routing Protocol

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

EGP	Exterior Gateway Protocol
FDDI	Fiber Distributed Data Interface
FEC	Forward Error Correction
FIN	Finish Flag
FTP	File Transfer Protocol
GPS	Global Positioning System
HTML	HyperText Markup Language
HTTP	HyperText Transfer Protocol
IAB	Internet Architecture Board
ICANN	Internet Corporation for Assigned Names and Numbers
ICMP	Internet Control Message Protocol
IETF	Internet Engineering Task Force
IGP	Interior Gateway Protocol
IGMP	Internet Group Management Protocol
InterNIC	Internet Network Information Center
IP	Internet Protocol
IRTF	Internet Research Task Force
ISOC	Internet Society
ISN	Initial Sequence Number
LAN	Local Area Network
LSA	Link State Advertisement
MAC	Medium Access Control
MAC	Message Authentication Code
MIB	Management Information Base
MOSPF	Multicast Extension to OSPF
MPLS	Multiprotocol Label Switching
MSL	Maximum Segment Life
MSS	Maximum Segment Size
MTU	Maximum Transmission Unit

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

NAT	Network Address Translator
NFS	Network File System
NIST	National Institute of Standards and Technology
NTP	Network Time Protocol
OSPF	Open Shortest Path First
PAT	Port Address Translation
PDA	Personal Digital Assistant
PDU	Protocol Data Unit
PIM	Protocol Independent Multicast
PNG	Portable Network Graphics
PPP	Point-to-Point Protocol
QoS	Quality of Service
RIP	Routing Information Protocol
RARP	Reverse Address Resolution Protocol
RBAC	Role-Based Access Control
RFC	Request for Comments
RPC	Remote Procedure Call
RRQ	Read Request
RSA	Rivest–Shamir–Adleman
RST	Reset Flag
RTO	Retransmission Timeout
RTCP	Realtime Transport Control Protocol
RTP	Realtime Transport Protocol
RTSP	Real Time Streaming Protocol
RTT	Round-Trip Time
SACK	Selective Acknowledgment
SHA	Secure Hash Algorithm
SIP	Session Initiation Protocol
SMI	Structure of Management Information
SMTP	Simple Mail Transfer Protocol
SNMP	Simple Network Management Protocol
SPF	Shortest Path First

© Cambridge University Press www.cambridge.org

CAMBRIDGE

Cambridge University Press
0521841445 - TCP/IP Essentials: A Lab-Based Approach
Shivendra S. Panwar, Shiwen Mao, Jeong-dong Ryoo and Yihan Li
Frontmatter
More information

SSL	Secure Sockets Layer
STDIN	Standard Input
STDOUT	Standard Output
SYN	Synchronize Sequence Number Flag
TCP	Transmission Control Protocol
TE	Traffic Engineering
TFTP	Trivial File Transfer Protocol
TTL	Time-to-Live
UDP	User Datagram Protocol
UI	User Interface
VoIP	Voice over IP
VPN	Virtual Private Network
WAN	Wide Area Network
Wi-Fi	Wireless Fidelity
WWW	World Wide Web

© Cambridge University Press www.cambridge.org