

# Contents

|                                                     |                  |
|-----------------------------------------------------|------------------|
| <i>Preface</i>                                      | <i>page</i> xiii |
| <i>Note to instructors</i>                          | xv               |
| <i>Acknowledgements</i>                             | xvi              |
| <i>General conventions</i>                          | xvii             |
| <i>List of abbreviations</i>                        | xviii            |
| <hr/>                                               |                  |
| <b>0 TCP/IP overview</b>                            | 1                |
| <hr/>                                               |                  |
| 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               |
| <hr/>                                               |                  |
| <b>1 Linux and TCP/IP networking</b>                | 26               |
| <hr/>                                               |                  |
| 1.1 Objectives                                      | 26               |
| 1.2 Linux and TCP/IP implementations                | 26               |
| 1.3 Linux commands and tools                        | 31               |
| 1.4 Diagnostic tools                                | 35               |

| viii     | Contents                                       |    |
|----------|------------------------------------------------|----|
|          | 1.5 Exercises with Linux commands              | 36 |
|          | 1.6 Exercises with diagnostic tools            | 39 |
|          | 1.7 Exercises on port numbers                  | 41 |
| <b>2</b> | <b>A single segment network</b>                | 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 |
| <b>3</b> | <b>Bridges, LANs and the Cisco IOS</b>         | 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 |
| <b>4</b> | <b>Static and dynamic routing</b>              | 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 |

| ix       | Contents                                        |     |
|----------|-------------------------------------------------|-----|
|          | 4.8 OSPF exercise                               | 97  |
|          | 4.9 Static routing experiment                   | 98  |
|          | 4.10 Traceroute experiment                      | 99  |
| <b>5</b> | <b>UDP and its applications</b>                 | 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 |
| <b>6</b> | <b>TCP study</b>                                | 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 |
| <b>7</b> | <b>Multicast and realtime service</b>           | 134 |
|          | 7.1 Objectives                                  | 134 |
|          | 7.2 IP multicast                                | 134 |

| x        | Contents                               |                                                     |
|----------|----------------------------------------|-----------------------------------------------------|
|          | 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              |
| <b>8</b> | <b>The Web, DHCP, NTP and NAT</b>      | <b>159</b>                                          |
|          | 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                    |
| <b>9</b> | <b>Network management and security</b> | <b>187</b>                                          |
|          | 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   |

|           |                                                                    |
|-----------|--------------------------------------------------------------------|
| <b>xi</b> | <b>Contents</b>                                                    |
|           | <hr/>                                                              |
|           | <b>References and further reading</b> 214                          |
|           | <br><b>Appendix A: instructor's guide</b> 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                                            |
|           | <br><b>Appendix B: initial configuration of the routers</b> 233    |
|           | B.1 Initial configuration of router1 233                           |
|           | B.2 Initial configurations of the other routers 235                |
|           | <br><b>Appendix C: source code</b> 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                             |
|           | <br><b>Appendix D: list of key requests for comments (RFC)</b> 253 |
|           | <br><i>Index</i> 258                                               |