

TCP/IP Illustrated, Volume 1 Second Edition

The Protocols

Kevin R. Fall
W. Richard Stevens



Foreword by Vint Cerf, *Internet pioneer*

◆ ADDISON-WESLEY PROFESSIONAL COMPUTING SERIES

Table of Contents

Foreword xxv

Preface to the Second Edition xxvii

Adapted Preface to the First Edition xxxiii

Chapter 1: Introduction 1

1.1 Architectural Principles 2

1.2 Design and Implementation 8

1.3 The Architecture and Protocols of the TCP/IP Suite 13

1.4 Internets, Intranets, and Extranets 19

1.5 Designing Applications 20

1.6 Standardization Process 22

1.7 Implementations and Software Distributions 24

1.8 Attacks Involving the Internet Architecture 25

1.9 Summary 26

1.10 References 28

Chapter 2: The Internet Address Architecture 31

2.1 Introduction 31

2.2 Expressing IP Addresses 32

2.3 Basic IP Address Structure 34

2.4 CIDR and Aggregation 46

2.5 Special-Use Addresses 50

2.6 Allocation 62

- 2.7 Unicast Address Assignment 65
- 2.8 Attacks Involving IP Addresses 70
- 2.9 Summary 71
- 2.10 References 72

Chapter 3: Link Layer 79

- 3.1 Introduction 79
- 3.2 Ethernet and the IEEE 802 LAN/MAN Standards 80
- 3.3 Full Duplex, Power Save, Autonegotiation, and 802.1X Flow Control 94
- 3.4 Bridges and Switches 98
- 3.5 Wireless LANs—IEEE 802.11(Wi-Fi) 111
- 3.6 Point-to-Point Protocol (PPP) 130
- 3.7 Loopback 145
- 3.8 MTU and Path MTU 148
- 3.9 Tunneling Basics 149
- 3.10 Attacks on the Link Layer 154
- 3.11 Summary 156
- 3.12 References 157

Chapter 4: ARP: Address Resolution Protocol 165

- 4.1 Introduction 165
- 4.2 An Example 166
- 4.3 ARP Cache 169
- 4.4 ARP Frame Format 170
- 4.5 ARP Examples 171

4.6 ARP Cache Timeout 174

4.7 Proxy ARP 174

4.8 Gratuitous ARP and Address Conflict Detection (ACD) 175

4.9 The arp Command 177

4.10 Using ARP to Set an Embedded Device's IPv4 Address 178

4.11 Attacks Involving ARP 178

4.12 Summary 179

4.13 References 179

Chapter 5: The Internet Protocol (IP) 181

5.1 Introduction 181

5.2 IPv4 and IPv6 Headers 183

5.3 IPv6 Extension Headers 194

5.4 IP Forwarding 208

5.5 Mobile IP 215

5.6 Host Processing of IP Datagrams 220

5.7 Attacks Involving IP 226

5.8 Summary 226

5.9 References 228

Chapter 6: System Configuration: DHCP and Autoconfiguration 233

6.1 Introduction 233

6.2 Dynamic Host Configuration Protocol (DHCP) 234

6.3 Stateless Address Autoconfiguration (SLAAC) 276

6.4 DHCP and DNS Interaction 285

6.5 PPP over Ethernet (PPPoE) 286

6.6 Attacks Involving System Configuration 292

6.7 Summary 292

6.8 References 293

Chapter 7: Firewalls and Network Address Translation (NAT) 299

7.1 Introduction 299

7.2 Firewalls 300

7.3 Network Address Translation (NAT) 303

7.4 NAT Traversal 316

7.5 Configuring Packet-Filtering Firewalls and NATs 334

7.6 NAT for IPv4/IPv6 Coexistence and Transition 339

7.7 Attacks Involving Firewalls and NATs 345

7.8 Summary 346

7.9 References 347

Chapter 8: ICMPv4 and ICMPv6: Internet Control Message Protocol 353

8.1 Introduction 353

8.2 ICMP Messages 355

8.3 ICMP Error Messages 361

8.4 ICMP Query/Informational Messages 380

8.5 Neighbor Discovery in IPv6 395

8.6 Translating ICMPv4 and ICMPv6 424

8.7 Attacks Involving ICMP 428

8.8 Summary 430

8.9 References 430

Chapter 9: Broadcasting and Local Multicasting (IGMP and MLD) 435

9.1 Introduction 435

9.2 Broadcasting 436

9.3 Multicasting 441

9.4 The Internet Group Management Protocol (IGMP) and Multicast Listener Discovery Protocol (MLD) 451

9.5 Attacks Involving IGMP and MLD 469

9.6 Summary 470

9.7 References 471

Chapter 10: User Datagram Protocol (UDP) and IP Fragmentation 473

10.1 Introduction 473

10.2 UDP Header 474

10.3 UDP Checksum 475

10.4 Examples 478

10.5 UDP and IPv6 481

10.6 UDP-Lite 487

10.7 IP Fragmentation 488

10.8 Path MTU Discovery with UDP 493

10.9 Interaction between IP Fragmentation and ARP/ND 496

10.10 Maximum UDP Datagram Size 497

10.11 UDP Server Design 498

10.12 Translating UDP/IPv4 and UDP/IPv6 Datagrams 505

10.13 UDP in the Internet 506

10.14 Attacks Involving UDP and IP Fragmentation 507

10.15 Summary 508

10.16 References 508

Chapter 11: Name Resolution and the Domain Name System (DNS) 511

11.1 Introduction 511

11.2 The DNS Name Space 512

11.3 Name Servers and Zones 516

11.4 Caching 517

11.5 The DNS Protocol 518

11.6 Sort Lists, Round-Robin, and Split DNS 565

11.7 Open DNS Servers and DynDNS 567

11.8 Transparency and Extensibility 567

11.9 Translating DNS from IPv4 to IPv6 (DNS64) 568

11.10 LLMNR and mDNS 569

11.11 LDAP 570

11.12 Attacks on the DNS 571

11.13 Summary 572

11.14 References 573

Chapter 12: TCP: The Transmission Control Protocol (Preliminaries) 579

12.1 Introduction 579

12.2 Introduction to TCP 584

12.3 TCP Header and Encapsulation 587

12.4 Summary 591

12.5 References 591

Chapter 13: TCP Connection Management 595

13.1 Introduction 595

13.2 TCP Connection Establishment and Termination 595

13.3 TCP Options 605

13.4 Path MTU Discovery with TCP 612

13.5 TCP State Transitions 616

13.6 Reset Segments 625

13.7 TCP Server Operation 631

13.8 Attacks Involving TCP Connection Management 640

13.9 Summary 642

13.10 References 643

Chapter 14: TCP Timeout and Retransmission 647

14.1 Introduction 647

14.2 Simple Timeout and Retransmission Example 648

14.3 Setting the Retransmission Timeout (RTO) 651

14.4 Timer-Based Retransmission 664

14.5 Fast Retransmit 667

14.6 Retransmission with Selective Acknowledgments 671

14.7 Spurious Timeouts and Retransmissions 677

14.8 Packet Reordering and Duplication 682

14.9 Destination Metrics 685

14.10 Repacketization 686

14.11 Attacks Involving TCP Retransmission 687

14.12 Summary 688

14.13 References 689

Chapter 15: TCP Data Flow and Window Management 691

15.1 Introduction 691

15.2 Interactive Communication 692

15.3 Delayed Acknowledgments 695

15.4 Nagle Algorithm 696

15.5 Flow Control and Window Management 700

15.6 Urgent Mechanism 719

15.7 Attacks Involving Window Management 723

15.8 Summary 723

15.9 References 724

Chapter 16: TCP Congestion Control 727

16.1 Introduction 727

16.2 The Classic Algorithms 730

16.3 Evolution of the Standard Algorithms 739

16.4 Handling Spurious RTOs—the Eifel Response Algorithm 744

16.5 An Extended Example 745

16.6 Sharing Congestion State 767

16.7 TCP Friendliness 768

16.8 TCP in High-Speed Environments 770

16.9 Delay-Based Congestion Control 777

- 16.10 Buffer Bloat 781
- 16.11 Active Queue Management and ECN 782
- 16.12 Attacks Involving TCP Congestion Control 785
- 16.13 Summary 786
- 16.14 References 788

Chapter 17: TCP Keepalive 793

- 17.1 Introduction 793
- 17.2 Description 795
- 17.3 Attacks Involving TCP Keepalives 802
- 17.4 Summary 802
- 17.5 References 803

Chapter 18: Security: EAP, IPsec, TLS, DNSSEC, and DKIM 805

- 18.1 Introduction 805
- 18.2 Basic Principles of Information Security 806
- 18.3 Threats to Network Communication 807
- 18.4 Basic Cryptography and Security Mechanisms 809
- 18.5 Certificates, Certificate Authorities (CAs), and PKIs 821
- 18.6 TCP/IP Security Protocols and Layering 832
- 18.7 Network Access Control: 802.1X, 802.1AE, EAP, and PANA 833
- 18.8 Layer 3 IP Security (IPsec) 840
- 18.9 Transport Layer Security (TLS and DTLS) 876
- 18.10 DNS Security (DNSSEC) 894
- 18.11 DomainKeys Identified Mail (DKIM) 915

18.12 Attacks on Security Protocols 918

18.13 Summary 919

18.14 References 922

Glossary of Acronyms 933

Index 963