

COURSE
TECHNOLOGY
THOMSON LEARNING

NETWORKING

Guide to TCP/IP

Laura A. Chappell
Ed Tittel



Includes coverage of IPv6
and EtherPeek® demo software

TABLE OF
Contents

PREFACE

xvii

CHAPTER ONE

Introducing TCP/IP

	1
What is TCP/IP?	2
The Origins and History of TCP/IP	2
TCP/IP's Design Goals	2
A TCP/IP Chronology	3
Who "Owns" TCP/IP?	5
TCP/IP Standards and RFCs	7
OSI Network Reference Model Overview	8
Models Break Networking into Layers	8
The ISO/OSI Network Reference Model	10
How Protocol Layers Behave	10
The TCP/IP Networking Model	15
TCP/IP Network Access Layer	16
TCP/IP Network Access Layer Protocols	17
TCP/IP Internet Layer Functions	17
Internet Layer Protocols	18
TCP/IP Transport Layer Functions	19
TCP/IP Transport Layer Protocols	19
TCP/IP Application Layer	19
TCP/IP Protocols, Services, Sockets, and Ports	20
TCP/IP Protocol Numbers	21
TCP/IP Port Numbers	22
TCP/IP Sockets	23
Data Encapsulation in TCP/IP	23
About Protocol Analysis	24
Useful Roles for Protocol Analysis	24
Protocol Analyzer Elements	25
Placing a Protocol Analyzer on a Network	29
Chapter Summary	30
Key Terms	32
Review Questions	43
Hands-on Projects	48
Case Projects	52

CHAPTER TWO

IP Addressing and Related Topics

	53
IP Addressing Basics	54
Anatomy of an IP Address	56
IP Address Classes	56
More About Class A Addresses	57
More About Class B Addresses	58

More About Class C Addresses	59
More About Address Classes D and E	60
Network, Broadcast, Multicast, and Other Special IP Addresses	60
Broadcast Packet Structures	61
Multicast Packet and Address Structures	62
The Vanishing IP Address Space	64
Understanding Basic Binary Arithmetic	66
Converting Decimal to Binary	66
Converting Binary to Decimal	68
High-order Bit Patterns	68
Low-order Bit Patterns	68
Of IP Networks, Subnets, and Masks	69
IP Subnets and Supernet	70
Classless Inter-Domain Routing (CIDR)	75
Public Versus Private IP Addresses	77
Managing Access to IP Address Information	79
Obtaining Public IP Addresses	80
IP Addressing Schemes	80
The Network Space	80
The Host Space	82
Chapter Summary	83
Key Terms	84
Review Questions	88
Hands-on Projects	92
Case Projects	95

CHAPTER THREE

Data Link and Network Layer TCP/IP Protocols	99
Data Link Protocols	100
The Serial Line Internet Protocol (SLIP)	101
Point-to-Point Protocol (PPP)	102
Special Handling for PPP Links	104
Frame Types	105
Ethernet Frame Types	105
Token Ring Frame Types	112
Hardware Addresses in the IP Environment	116
ARP Packet Fields and Functions	119
ARP Cache	122
Proxy ARP	124
Reverse ARP (RARP)	125
Network Layer Protocols	125
About Internet Protocol (IP)	126
Sending IP Datagrams	126
Route Resolution Process	127
Lifetime of an IP Datagram	130
Fragmentation and Reassembly	131
Service Delivery Options	135
Precedence	135
Type of Service (TOS)	135
IP Header Fields and Functions	137
Version Field	137
Header Length Field	137

Type of Service Field	137
Total Length Field	139
Identification Field	140
Flags Field	140
Fragment Offset Field	141
Time to Live (TTL) Field	141
Protocol Field	141
Header Checksum Field	142
Source Address Field	142
Destination Address Field	142
Options Fields	142
Chapter Summary	143
Key Terms	145
Review Questions	151
Hands-on Projects	155
Case Projects	159
CHAPTER FOUR	
Internet Control Message Protocol (ICMP)	161
About the Internet Control Message Protocol	162
Overview of ICMP and RFC 792	162
ICMP's Vital Roles on IP Networks	163
Testing and Troubleshooting Sequences for ICMP	164
Connectivity Testing with PING	164
Path Discovery with TRACEROUTE	166
Path Discovery with PATHPING	168
Path MTU Discovery with ICMP	168
Routing Sequences for ICMP	171
Security Issues for ICMP	175
ICMP Packet Fields and Functions	176
Constant ICMP Fields	177
The Varying ICMP Structures and Functions	180
Chapter Summary	197
Key Terms	198
Review Questions	202
Hands-on Projects	206
Case Projects	210
CHAPTER FIVE	
Transport Layer TCP/IP Protocols	211
Understanding Connectionless Transport Protocols	212
User Datagram Protocol (UDP)	213
UDP Header Fields and Functions	214
UDP Port Numbers and Processes	218
Understanding Connection-Oriented Protocols	219
Transmission Control Protocol (TCP)	219
TCP Startup Connection Process (TCP Handshake)	221
TCP Keep-Alive Process	225
TCP Connection Termination	226
TCP Sequence and Acknowledgment Process	228
TCP Error-Detection and Error-Recovery Process	230

TCP Congestion Control	232
TCP Sliding Window	234
TCP Header Fields and Functions	235
Common and Appropriate Uses for TCP and UDP	240
Chapter Summary	241
Key Terms	242
Review Questions	245
Hands-on Projects	249
Case Projects	251
CHAPTER SIX	
Basic TCP/IP Services	253
How Upper-layer IP Protocols Work and Behave	254
Understanding FTP	256
FTP Elements	256
Sample FTP Communications	259
Understanding Telnet	262
Telnet Elements	262
Sample Telnet Communications	264
Understanding SMTP	266
SMTP Elements	267
Sample SMTP Communications	269
Understanding HTTP	271
HTTP Elements	271
Sample HTTP Communications	274
Other Common IP-based Services	276
Echo	277
Quote of the Day (QOD)	277
Character Generator (Chargen)	277
Windows 2000 and Simple TCP/IP Utilities	277
Whois	278
TFTP	278
Finger	279
Remote Procedure Call (RPC)	279
Simple Network Management Protocol (SNMP)	280
NetBIOS Over TCP/IP	280
Decoding Upper-layer Protocols	281
Chapter Summary	283
Key Terms	284
Review Questions	287
Hands-on Projects	291
Case Projects	296
CHAPTER SEVEN	
Domain Name System (DNS)	297
DNS History and Background	298
DNS Database Structure	299
A DNS Overview	301
DNS Database Records	301
Delegating DNS Authority	302
Types of DNS Servers	303
The Client Side of DNS	304

How Domain Name Servers Work	305
DNS Root-level Servers	305
The Importance of DNS Caching	307
DNS Configuration Files and Resource Record Formats	308
Start of Authority (SOA) Record	309
Address and Alias Records	310
Mapping Addresses to Names	311
Handling the Loopback Address	312
Obtaining and Storing Root Server Data	312
The NSLOOKUP Command	314
NSLOOKUP Details	315
Using NSLOOKUP	315
DNS Query/Response Packet Formats	317
DNS Implementation	324
The Trouble with DNS	325
Chapter Summary	327
Key Terms	328
Review Questions	332
Hands-on Projects	336
Case Projects	343

CHAPTER EIGHT

The Dynamic Host Configuration Protocol (DHCP)

CHAPTER EIGHT	345
The Dynamic Host Configuration Protocol (DHCP)	345
Introducing DHCP	346
DHCP's Origins	348
DHCP Software Elements	348
DHCP Lease Types	349
More About DHCP Leases	350
Understanding IP Address Management with DHCP	351
The Standard Address Discovery Process	351
The Discover Packet	352
The Offer Packet	354
The Request Packet	355
The Acknowledgment Packet	357
The Address Renewal Process	358
The Renewal Time (T1)	358
The Rebinding Time (T2)	358
The DHCP Address Release Process	360
DHCP Packet Structures	360
DHCP Options Fields	362
Broadcast and Unicast in DHCP	366
DHCP Relay Agents	367
Microsoft DHCP Scopes and Classes	368
The Future of DHCP	369
Troubleshooting DHCP	369
Chapter Summary	370
Key Terms	370
Review Questions	373
Hands-on Projects	378
Case Projects	380

CHAPTER NINE**Securing TCP/IP Environments****381**

Understanding Computer and Network Security	382
The Three Legs of Network Security	382
Understanding Typical IP Attacks, Exploits, and Break-ins	383
Common Types of IP-Related Attacks	385
What IP Services Are Most Vulnerable?	386
Of Holes, Back Doors, and Other Illicit Points of Entry	387
Principles of IP Security	389
Common IP Points of Attack	390
Viruses, Worms, and Trojan Horse Programs	390
Denial of Service (DoS) Attacks	392
Distributed Denial of Service Attacks (DDoS)	394
Buffer Overflows	395
Spoofing	395
TCP Session Hijacking	396
The Anatomy of IP Attacks	397
Network Sniffing	399
Fixing IP Security Problems	401
The Importance of Patches and Fixes	401
Knowing Which Ports to Block	402
Recognizing Attack Signatures	402
IP Security	405
About Firewalls, Proxy Servers, and Other Boundary Devices	405
Windows 2000: Another Generation of Network Security	415
Updating Anti-Virus Engines and Virus Lists	416
Testing Your Network	417
Chapter Summary	418
Key Terms	420
Review Questions	425
Hands-on Projects	430
Case Projects	433

CHAPTER TEN**Routing in the IP Environment****435**

Understanding Routing	436
Distance Vector Routing Protocols	439
Link-State Routing Protocols	441
Routing Characteristics	443
Route Convergence	443
Split Horizon	443
Poison Reverse	444
Time to Live (TTL)	444
Multicast Versus Broadcast Update Behavior	445
ICMP Router Advertisements	445
Black Holes	445
Areas, Autonomous Systems, and Border Routers	446
Interior Gateway Protocols (IGPs)	448
RIP	448
Open Shortest Path First (OSPF)	451
Enhanced Interior Gateway Routing Protocol (EIGRP)	456
Exterior Gateway Protocols (EGPs)	456
Border Gateway Protocol (BGP)	457

Managing Routing on an In-House Internetwork	457
Hybrid Networks	458
Routing On and Off a Wide Area Network	459
Several Small Offices	459
Hub and Spoke	459
Multiprotocol	460
Mobile Users	460
Routing To and From the Internet	461
Securing Routers and Routing Behavior	462
Troubleshooting IP Routing	463
Chapter Summary	463
Key Terms	464
Review Questions	467
Hands-on Projects	471
Case Projects	473

CHAPTER ELEVEN

Monitoring and Managing Ip Networks

Monitoring and Managing Ip Networks	475
Understanding Network Management Practices and Principle	476
Network Management Architectures	476
OSI Network Management Model	478
Practical Network Management	479
In-band Versus Out-of-band Management	480
Understanding SNMP	482
Management Information Base (MIB) Objects	483
SNMP Agents	488
SNMP Managers	488
SNMP Messages	488
SNMP Security	490
Installing and Configuring SNMP Agents and Consoles	491
Agent Configuration	492
Console Installation	493
Console Configuration	494
SNMP Consoles, Tools, Utilities, and Key Files	494
Integrating SNMP With Other Management Environments	495
Troubleshooting SNMP	496
Chapter Summary	496
Key Terms	498
Review Questions	500
Hands-on Projects	505
Case Projects	507

CHAPTER TWELVE

TCP/IP, NetBIOS, And WINS

TCP/IP, NetBIOS, And WINS	509
What is NetBIOS (and Why Do I Care)?	510
Historic Limitations of NetBIOS	510
NetBIOS in Windows 2000	511
NetBIOS in Perspective	512
What is NetBIOS Used For?	514
How Does NetBIOS Work?	514

NetBIOS Names	517
Structure of NetBIOS Names	517
NetBIOS Name Types and Suffixes	518
NetBIOS Scope Identifier	518
NetBIOS Name Registration and Resolution	519
Name Resolution Regimes by Node Type	520
NetBIOS Name Cache and LMHOSTS File	521
WINS Name Registration and Resolution	522
DNS and the HOSTS File	524
NetBIOS Over TCP/IP	525
NetBIOS Names and IP Names	526
WINS Servers	528
How WINS Works	528
Different WINS Configurations	529
Troubleshooting WINS and NetBIOS	535
Tools for Troubleshooting NetBIOS and WINS Problems	536
Typical Errors in NetBIOS and WINS	538
Chapter Summary	539
Key Terms	539
Review Questions	541
Hands-on Projects	545
Case Projects	552

CHAPTER THIRTEEN

Internet Protocol Version 6 (IPv6)

555

Why Create a New Version of IP?	556
The IPv6 Address Space	557
Address Format and Allocations	557
Address Types	560
Address Allocations	566
Routing Considerations	568
Neighbor Discovery and Router Advertisement	568
Path MTU Discovery and Changes in Fragmentation	570
IPv6 Packet Formats	570
Basic IPv6 Header Format	571
Extension Headers	575
New and Enhanced IPv6 Features	581
Autoconfiguration	581
Security	584
Quality of Service (QoS)	588
Mobile Users	590
Transition: Coexistence of IPv4 and IPv6	593
Dual Stack Approach	594
Tunneling Through the IPv4 Cloud	594
Native IPv6	595
Chapter Summary	595
Key Terms	596
Review Questions	601
Hands-on Projects	606
Case Projects	608