

Inhaltsverzeichnis



Vorwort	25
Vorwort der Erstausgabe	27
Einführung	29
1 Einführung und Übersicht	33
1.1 Internetworking – die Beweggründe	33
1.2 Das TCP/IP-Internet	34
1.3 Internet-Services.	35
1.3.1 Internet-Services der Anwendungsebene	35
1.3.2 Internet-Services auf Netzwerkebene	36
1.4 Geschichte und Tragweite des Internets	38
1.5 Internet Architecture Board	40
1.6 Reorganisation des IAB.	41
1.7 Die Internet Society	42
1.8 Internet Request for Comments.	42
1.9 Internetprotokolle und Standardisierung	43
1.10 Künftiges Wachstum und künftige Technologien	43
1.11 Wie dieser Test organisiert ist	44
1.12 Zusammenfassung	45
1.13 Weiterführende Hinweise	45
1.14 Aufgaben	46
2 Übersicht über die zugrunde liegenden Netzwerktechnologien	47
2.1 Einführung	47
2.2 Zwei Ansätze für die Netzwerkkommunikationen	47
2.3 Wide Area und Local Area Networks.	48
2.3.1 Hardwareadressen im Netzwerk	49

Inhaltsverzeichnis

2.4	Ethernet-Technologie	50
2.4.1	Thin-Ethernet	52
2.4.2	Twisted-Pair-Ethernet	53
2.4.3	Die Leistung des Ethernet	54
2.4.4	Fast-Ethernet	55
2.4.5	10/100-Ethernet	55
2.4.6	Gigabit-Ethernet	56
2.4.7	Eigenschaften eines Ethernets	56
2.4.8	Kollisionserkennung und -Recovery	56
2.4.9	Ethernet-Hardwareadressen	57
2.4.10	Ethernet-Rahmenformat	58
2.4.11	Wie ein Ethernet mit Repeatern verlängert wird	59
2.4.12	Wie ein Ethernet mit Bridges verlängert wird	59
2.5	Fiber Distributed Data Interconnect (FDDI)	61
2.5.1	Eigenschaften eines FDDI-Netzwerks	61
2.5.2	Gegenläufig rotierende FDDI-Dualringe	62
2.5.3	FDDI-Rahmenformat	63
2.6	Asynchronous Transfer Mode	64
2.6.1	ATM-Zellengröße	64
2.6.2	Verbindungsorientierte Netzwerke	64
2.7	WAN-Technologien: ARPANET	65
2.7.1	ARPANET-Adressierung	67
2.8	National Science Foundation Networking	68
2.8.1	Der ursprüngliche NSFNET-Backbone	68
2.8.2	Das zweite NSFNET-Backbone 1988-1989	69
2.8.3	NSFNET-Backbone 1989-1990	70
2.9	ANSNET	71
2.10	Very High Speed Backbone (vBNS)	72
2.10.1	Kommerzielle Internet-Backbones	72
2.11	Andere Technologien, über die TCP/IP gefahren wurde	72
2.11.1	X25NET und Tunnels	72
2.11.2	Point-to-Point-Netzwerke	74
2.11.3	IP über Dial-Up-Netzwerke	75
2.11.4	Andere Token-Ring-Technologien	75
2.11.5	Wireless-Netzwerktechnologien	76
2.12	Zusammenfassung	76
2.13	Weiterführende Hinweise	77
2.14	Aufgaben	77

3	Internetworking: Konzept und architektonisches Modell	79
3.1	Einführung	79
3.2	Connectivity auf Anwendungsebene	79
3.3	Connectivity auf Netzwerkebene	80
3.4	Eigenschaften des Internetworks	81
3.5	Internetwork-Architektur	81
3.6	Interconnection durch IP-Router	82
3.7	Aus der Sicht des Anwenders	83
3.8	Alle Netzwerke sind gleich	84
3.9	Die offenen Fragen.	84
3.10	Zusammenfassung	85
3.11	Weiterführende Hinweise	85
3.12	Aufgaben	86
4	Klassenbestimmte Internet-Adressen	87
4.1	Einführung	87
4.2	Universelle Kennungen.	87
4.3	Das ursprüngliche klassenbestimmte Adressierungsschema	87
4.4	Mit Adressen werden Netzwerkverbindungen spezifiziert	89
4.5	Netzwerk- und gezielte Broadcast-Adressen	89
4.6	Begrenzte Broadcasts	90
4.7	Wie die Null als »diesen« / »dieses« interpretiert wird	90
4.8	Subnetz- und Supernetz-Erweiterungen.	91
4.9	IP-Multicast-Adressen	91
4.10	Schwächen der Internet-Adressierung	91
4.11	Dotted-Decimal-Notation	93
4.12	Loopback-Adresse	93
4.13	Überblick der speziellen Adresskonventionen	94
4.14	Internet-Adressierungsbehörde.	94
4.15	Reservierte Adresspräfixe	95
4.16	Ein Beispiel.	95

4.17	Netzwerk-Bytereihenfolge	97
4.18	Zusammenfassung	98
4.19	Weiterführende Hinweise	98
4.20	Aufgaben	99
5	Die Zuordnung von Internet-Adressen zu physischen Adressen (ARP)	101
5.1	Einführung	101
5.2	Das Problem der Adressauflösung	101
5.3	Zwei physische Adresstypen	102
5.4	Auflösung durch direkte Zuordnung	102
5.5	Auflösung durch dynamische Bindung	103
5.6	Address-Resolution-Cache	104
5.7	ARP-Cache-Zeitüberschreitung	104
5.8	Verbesserungen von ARP	105
5.9	Beziehung zwischen ARP und anderen Protokollen	105
5.10	ARP-Implementierung	106
5.11	ARP-Verkapselung und Identifikation	107
5.12	ARP-Protokollformat	107
5.13	Zusammenfassung	108
5.14	Weiterführende Informationen	109
5.15	Aufgaben	109
6	Feststellen einer Internet-Adresse beim Systemstart (RARP)	111
6.1	Einführung	111
6.2	Reverse Address Resolution Protocol (RARP)	112
6.3	Das Timing von RARP-Transaktionen	113
6.4	Zusammenfassung	114
6.5	Weiterführende Hinweise	114
6.6	Aufgaben	115

7	Internet Protocol: Verbindungslose Zustellung von Datagrammen	117
7.1	Einführung	117
7.2	Ein virtuelles Netzwerk	117
7.3	Internetworking-Architektur und Philosophie	117
7.4	Organisatorisches Konzept der Services	118
7.5	Verbindungsloses Delivery-System	118
7.6	Zweck des Internet Protocols	118
7.7	Das Internet-Datagramm	119
7.7.1	Datagramm-Format	119
7.7.2	Datagramm-Servicetyp und Unterscheidung der Services	120
7.7.3	Verkapselung von Datagrammen	122
7.7.4	Datagrammgröße, Netzwerk-MTU und Fragmentierung	123
7.7.5	Reassemblierung von Fragmenten	125
7.7.6	Fragmentierungssteuerung	125
7.7.7	Time-to-Live (TTL)	126
7.7.8	Andere Datagramm-Header-Felder	127
7.8	Internet-Datagramm-Optionen	128
7.8.1	Die Option Record Route (Route aufnehmen)	129
7.8.2	Source Route-Optionen	130
7.8.3	Zeitstempel-Option	131
7.8.4	Verarbeitungsoptionen während der Fragmentierung	132
7.9	Zusammenfassung	132
7.10	Weiterführende Hinweise	133
7.11	Aufgaben	133
8	Internet Protocol: Wie IP-Datagramme geroutet werden	135
8.1	Einführung	135
8.2	Routing in einem Internetwork	135
8.3	Direkte und indirekte Zustellung	136
8.3.1	Datagramm-Zustellung über ein einzelnes Netzwerk	137
8.3.2	Indirekte Zustellung	137
8.4	Auf Tabellen basiertes IP-Routing	138
8.5	Next-Hop-Routing	138
8.6	Standardrouten	140
8.7	Hostspezifische Routen	140

8.8	Der IP-Routing-Algorithmus	141
8.9	Routing mit IP-Adressen	141
8.10	Behandlung von eingehenden Datagrammen	143
8.11	Wie Routing-Tabellen aufgebaut werden.	144
8.12	Zusammenfassung	144
8.13	Weiterführende Hinweise	145
8.14	Aufgaben	145
9	Internet Protocol: Fehlermeldungen und Steuerungsnachrichten (ICMP)	147
9.1	Einführung	147
9.2	Internet Control Message Protocol	147
9.3	Fehlermeldungen vs. Fehlerkorrektur	148
9.4	Zustellung von ICMP-Meldungen	149
9.5	ICMP-Nachrichtenformat	149
9.6	Erreichbarkeit und Status eines Ziels testen (ping)	150
9.7	Echo Request- und Reply-Nachrichtenformate	151
9.8	Unerreichbare Ziele melden	151
9.9	Überlastung und Flusskontrolle der Datagramme	153
9.10	Source Quench-Format	153
9.11	Route Change-Anforderungen von Routern.	154
9.12	Schleifen oder übermäßig lange Routen erkennen	155
9.13	Andere Probleme melden	156
9.14	Zeitsynchronisierung und Schätzung der Übertragungszeit	157
9.15	Information Request- und -Reply-Nachrichten	158
9.16	Subnetzmaske entdecken	158
9.17	Router entdecken	159
9.18	Router anfordern	160
9.19	Zusammenfassung	160
9.20	Weiterführende Hinweise	161
9.21	Aufgaben	161

10	Klassenlose und Subnetz-Adresserweiterungen (CIDR)	163
10.1	Einführung	163
10.2	Übersicht der relevanten Fakten	163
10.3	Minimierung der Netzwerknummern	164
10.4	Transparente Router	164
10.5	Proxy-ARP	166
10.6	Subnetz-Adressierung	167
10.7	Flexibilität in der Subnetz-Adresszuordnung	169
10.8	Subnetze mit variabler Länge	170
10.9	Maskenbasierte Implementierung von Subnetzen	170
10.10	Darstellung der Subnetzmaske	171
10.11	Routing in Zusammenhang mit Subnetzen	172
10.12	Subnetz-Routing-Algorithmus	173
10.13	Ein einheitlicher Routing-Algorithmus	174
10.14	Subnetzmasken verwalten	174
10.15	Broadcasting in Subnetzen	175
10.16	Anonyme Point-to-Point-(Endpunkt-) Netzwerke	176
10.17	Classless Addressing (Klassenlose Adressierung – Supernetting)	177
10.18	Auswirkung des Supernettings auf das Routing	178
10.19	CIDR-Adressblöcke und –Bitmasken	178
10.20	Adressblöcke und CIDR-Notation	179
10.21	Beispiel für die klassenlose Adressierung	180
10.22	Datenstrukturen und Algorithmen für klassenlose Lookups	180
10.22.1	Hashing und klassenbestimmte Adressen	181
10.22.2	Suche nach Maskenlänge	181
10.22.3	Binäre Trie-Strukturen	181
10.23	Longest-Match-Routing und gemischte Routing-Typen	183
10.23.1	PATRICIA und die Ebenen-Komprimierung (Level Compressed Tries) . .	184
10.24	CIDR-Blöcke, die für private Netzwerke reserviert sind	184
10.25	Zusammenfassung	185

10.26	Weiterführende Hinweise	185
10.27	Aufgaben	186
11	Protokollschichten	189
11.1	Einführung	189
11.2	Die Notwendigkeit multipler Protokolle	189
11.3	Konzeptuelle Ebenen der Protokollsoftware	190
11.4	Funktionalität der Schichten	192
11.4.1	Das 7-Schichten-ISO-Referenzmodell	192
11.5	X.25 und seine Beziehung zum ISO-Modell	193
11.5.1	Das 5-Schichten-TCP/IP-Referenzmodell	194
11.6	Unterschiede zwischen den ISO- und den Internetschichten	196
11.6.1	Sicherungsschicht vs. Verlässlichkeit zwischen Endpunkten	196
11.6.2	Ort der Intelligenz und der Entscheidungsfindung	197
11.7	Das Schichtenprinzip der Protokolle	197
11.7.1	Schichten in einer TCP/IP-Internet-Umgebung	198
11.8	Das Schichtenprinzip im Kontext der Netzwerksstruktur	199
11.9	Zwei wichtige Grenzen im TCP/IP-Modell	201
11.9.1	High-Level-Protokoll-Adressgrenze	201
11.9.2	Betriebssystemgrenze	201
11.10	Nachteile des Schichtenprinzips	202
11.11	Der grundlegende Gedanke von Multiplexing und Demultiplexing	202
11.12	Zusammenfassung	203
11.13	Weiterführende Hinweise	204
11.14	Aufgaben	204
12	User Datagram Protocol (UDP)	205
12.1	Einführung	205
12.2	Wie das endgültige Ziel identifiziert wird	205
12.3	User Datagram Protocol	206
12.4	Format von UDP-Nachrichten	206
12.5	UDP-Pseudo-Header	207
12.6	UDP-Verkapselung und Protokollschichten	208
12.7	Schichten und die Berechnung der UDP-Prüfsumme	209

12.8	UDP-Multiplexing, -Demultiplexing und –Ports.	210
12.9	Reservierte und verfügbare UDP-Portnummern	211
12.10	Zusammenfassung	212
12.11	Weiterführende Hinweise	213
12.12	Aufgaben	213
13	Der verlässliche Stream-Transport-Service (TCP)	215
13.1	Einführung	215
13.2	Warum die Stream-Zustellung erforderlich ist	215
13.3	Eigenschaften des verlässlichen Delivery-Services	216
13.4	Wie Verlässlichkeit gewährleistet wird	217
13.5	Das Konzept der Sliding-Windows.	218
13.6	Das Transmission Control Protocol	220
13.7	Ports, Verbindungen und Endpunkte	221
13.8	Passives und aktives Öffnen	223
13.9	Segmente, Streams und Sequenzzahlen	223
13.10	Variable Fenstergröße und Flusssteuerung	224
13.11	TCP-Segment-Format	225
13.12	Out-of-Band-Daten	226
13.13	Option – Maximale Segmentgröße	227
13.14	Berechnung der TCP-Prüfsumme.	228
13.15	Bestätigungen und erneute Übertragungen.	228
13.16	Zeitüberschreitung und erneute Übertragung	229
13.17	Genauere Messung von Round Trip Samples	231
13.18	Karns Algorithmus und Timer-Backoff	232
13.19	Die Behandlung von großen Abweichungen der Verzögerung	233
13.20	Die Handhabung der Überlastung	235
13.21	Überlastung, Tail-Drop und TCP	237
13.22	Random Early Discard (RED – Richtlinie für frühzeitiges Verwerfen beliebiger Segmente)	238
13.23	Aufbau einer TCP-Verbindung	240

13.24	Ausgangswerte der Sequenzzahlen	241
13.25	Beenden einer TCP-Verbindung	242
13.26	Zurücksetzen einer TCP-Verbindung	243
13.27	TCP-State-Machine (-Zustandsautomat)	243
13.28	Erzwungene Datenzustellung	244
13.29	Reservierte TCP-Portnummern.	245
13.30	TCP-Leistung	245
13.31	Das Silly-Window-Syndrom und kleine Pakete.	246
13.32	Vermeidung des Silly-Window-Syndroms.	247
13.32.1	Empfängerseitige Vermeidung des Silly-Window-Syndroms	248
13.32.2	Verzögerte Bestätigungen	248
13.32.3	Senderseitige Vermeidung des Silly-Window-Syndroms	249
13.33	Zusammenfassung	250
13.34	Weiterführende Hinweise	251
13.35	Aufgaben	251
14	Routing: Cores, Peers und Algorithmen	253
14.1	Einführung	253
14.2	Der Ursprung der Routing-Tabellen.	253
14.3	Routing mit partiellen Informationen.	254
14.4	Die ursprüngliche Internet-Architektur und Cores	256
14.5	Core-Router	257
14.6	Jenseits der Core-Architektur zu Peer-Backbones.	259
14.7	Automatisches Propagieren von Routen.	260
14.8	Distance-Vector-(Bellman-Ford-)Routing	261
14.9	Gateway-to-Gateway Protocol (GGP)	262
14.10	Distance Factoring	263
14.11	Verlässlichkeit und Routing-Protokolle.	264
14.12	Link-State-Routing (SPF)	264
14.13	Zusammenfassung	265
14.14	Weiterführende Hinweise	266
14.15	Aufgaben	266

15	Routing: Externe Gateway-Protokolle und autonome Systeme (BGP)	269
15.1	Einführung	269
15.2	Dem architektonischen Modell werden weitere Stufen der Komplexität hinzugefügt	269
15.3	Eine sinnvolle Grenze für die Gruppengröße festlegen	270
15.4	Ein grundlegender Gedanke: Zusätzliche Hops	271
15.5	Verdeckte Netzwerke	272
15.6	Konzept der autonomen Systeme	273
15.7	Vom Core zu unabhängigen autonomen Systemen	273
15.8	Ein Exterior-Gateway-Protokoll	274
15.9	Eigenschaften von BGP	275
15.10	BGP-Funktionalität und Nachrichtentypen	276
15.11	BGP-Nachrichtenheader	277
15.12	Nachricht BGP OPEN	278
15.13	BGP UPDATE-Nachricht	279
15.14	Komprimierte Maske/Adress-Paare	279
15.15	BGP-Pfadattribute	280
15.16	BGP KEEPALIVE-Nachricht	281
15.17	Informationen aus der Perspektive des Empfängers	282
15.18	Die wichtigste Beschränkung der Exterior Gateway-Protokolle	283
15.19	Das Internet-Routing-Arbiter-System	284
15.20	BGP NOTIFICATION-Nachricht	285
15.21	Dezentralisierung der Internet-Architektur	286
15.22	Zusammenfassung	287
15.23	Weiterführende Hinweise	287
15.24	Aufgaben	287
16	Das Routing in einem autonomen System (RIP, OSPF, HELLO)	289
16.1	Einführung	289
16.2	Statische vs. dynamische Interior-Routen	289

16.3	Routing Information Protocol (RIP)	291
16.3.1	Die Geschichte von RIP	291
16.3.2	RIP-Operationen	292
16.3.3	Die Lösung des Problems der langsamen Konvergenz	294
16.3.4	RIP1-Nachrichten Format	295
16.3.5	RIP1-Adressierungskonventionen	296
16.3.6	RIP1-Routen-Interpretation und -Aggregation	297
16.3.7	RIP2-Erweiterungen	297
16.3.8	RIP2-Nachrichtenformat	298
16.3.9	Übertragung von RIP-Nachrichten	298
16.3.10	Der Nachteil von RIP-Hop-Counts	299
16.4	Das HELLO-Protokoll	299
16.5	Verzögerungsmetrik und Oszillation	300
16.6	RIP, HELLO und BGP kombinieren	301
16.7	Routing zwischen autonomen Systemen	302
16.8	Gated: Die Kommunikation zwischen autonomen Systemen	302
16.9	Das Open SPF-Protokoll (OSPF)	303
16.9.1	OSPF-Nachrichtenformat	304
16.9.2	OSPF-Hello-Nachrichtenformat	305
16.9.3	Nachrichtenformat der OSPF-Datenbase-Description	306
16.9.4	Nachrichtenformat der OSPF-Link-Status-Anforderung	307
16.9.5	Nachrichtenformat der OSPF-Link-Status-Update-Nachricht	307
16.10	Routing mit partiellen Informationen	308
16.11	Zusammenfassung	309
16.12	Weiterführende Hinweise	309
16.13	Aufgaben	309
17	Internet-Multicasting	313
17.1	Einführung	313
17.2	Hardware-Broadcast	313
17.3	Hardware-Ursprünge von Multicast	314
17.4	Ethernet-Multicast	314
17.5	IP-Multicast	315
17.6	Die konzeptuellen Elemente	315
17.7	IP-Multicast-Adressen	316
17.8	Multicast-Adress-Semantik	318

17.9	Zuordnung von IP-Multicast zu Ethernet-Multicast	318
17.10	Hosts und die Multicast-Zustellung	319
17.11	Multicast-Bereiche	319
17.12	Erweiterung der Host-Software für den Umgang mit Multicasting.	320
17.13	Internet Group Management Protocol	320
17.14	IGMP-Implementierung	321
17.15	Zustandsübergänge der Gruppenmitgliedschaft	322
17.16	IGMP-Nachrichtenformt	323
17.17	Multicast-Forwarding und Routing-Informationen	324
17.17.1	Die Notwendigkeit des dynamischen Routings	325
17.17.2	Die Unzulänglichkeit des zielbasierten Routings	325
17.17.3	Beliebige Absender	325
17.18	Grundlegende Paradigmen des Multicast-Routings	326
17.19	Auswirkungen von TRPF	327
17.20	Multicast-Bäume.	328
17.21	Das Wesen des Multicast-Routings	329
17.22	Reverse Path Multicasting	330
17.23	Distance Vector Multicast Routing Protocol	331
17.24	Das mrouted-Programm	331
17.25	Alternative Protokolle	333
17.26	Core Based Trees (CBT)	334
17.27	Protocol Independent Multicast (PIM).	335
17.27.1	PIM – Dense Mode (PIM-DM)	335
17.27.2	Protokollunabhängigkeit	335
17.27.3	PIM – Sparse Mode (PIM-SM)	336
17.27.4	Die Umschaltung vom gemeinsamen Baum zu einem Shortest Path Tree	336
17.28	Multicast Extensions to OSPF (MOSPF).	337
17.29	Verlässliches Multicasting und ACK-Implosionen	338
17.30	Zusammenfassung	339
17.31	Weiterführende Hinweise	340
17.32	Aufgaben	340

18	TCP/IP über ATM-Netzwerke	343
18.1	Einführung	343
18.2	ATM-Hardware	343
18.3	Große ATM-Netzwerke	344
18.4	Logische Ansicht eines ATM-Netzwerks	344
18.5	Die zwei Verbindungsparadigmen von ATM	345
18.5.1	Permanent Virtual Circuits (PVC)	345
18.5.2	Switched Virtual Circuits (SVC)	346
18.6	Pfade, Circuits und IDs	346
18.7	ATM-Cell-Transport	347
18.8	ATM-Anpassungsschichten	347
18.9	ATM-Anpassungsschicht Typ 5	348
18.10	AAL5-Konvergenz, -Segmentierung und -Reassemblierung	349
18.11	Datagramm-Verkapselung und IP-MTU-Größe	350
18.12	Pakettyp und Multiplexing	351
18.13	IP-Adressbindungen in einem ATM-Netzwerk	352
18.14	Konzept des logischen IP-Subnetzes	352
18.15	Verbindungsmanagement	353
18.16	Adressbindung innerhalb eines LIS	354
18.17	ATMARP-Paketformat	354
18.17.1	Format der ATM-Adresslängenfelder	356
18.17.2	Operationscodes des ATMARP-Protokolls	356
18.18	Verwendung von ATMARP-Pakete zur Ermittlung einer Adresse	356
18.18.1	Permanente virtuelle Schaltkreise	357
18.18.2	Geschaltete virtuelle Schaltkreise	357
18.19	Zeitüberschreitungen für die ATMARP-Informationen an einem Host oder Router	357
18.20	IP-Switching-Technologien	358
18.21	Switch-Operationen	358
18.22	Optimiertes IP-Forwarding	359
18.23	Klassifizierung, Flows und Switching in den höheren Schichten	359
18.24	Anwendbarkeit der Switching-Technologie	360

18.25	Zusammenfassung	360
18.26	Weiterführende Hinweise	361
18.27	Aufgaben	362
19	Mobiles IP	365
19.1	Einführung	365
19.2	Mobilität, Routing und Adressierung	365
19.3	Eigenschaften des mobilen IPs	365
19.4	Übersicht der Operationen im mobilen IP	366
19.5	Einzelheiten der mobilen Adressierung	367
19.6	Foreign-Agent Discovery.	367
19.7	Registrierung beim Agenten	369
19.8	Format der Registrierungsnachricht.	369
19.9	Kommunikation mit einem Foreign-Agenten	370
19.10	Datagramme übertragen und empfangen.	371
19.11	Das 2X-Problem	371
19.12	Kommunikation mit Computern im Home-Netzwerk	372
19.13	Zusammenfassung	373
19.14	Weiterführende Hinweise	373
19.15	Aufgaben	374
20	Private Netzwerkverbindungen mit NAT und VPN	375
20.1	Einführung	375
20.2	Private und hybride Netzwerke	375
20.3	Ein Virtual Private Network (VPN)	376
20.4	VPN-Adressierung und -Routing	377
20.5	Ein VPN mit privaten Adressen	377
20.6	Network Address Translation (NAT).	379
20.7	Erstellung der NAT-Übersetzungstabelle	379
20.8	NAT mit mehreren Adressen	381
20.9	Port-Mapped NAT.	381

21	Das Client-Server-Interaktionsmodell	387
21.1	Einführung	387
21.2	Client-Server-Modell	387
21.3	Ein einfaches Beispiel: Der UDP-Echo-Server	388
21.4	Zeit- und Datumsserver	389
21.4.1	Darstellung des Datums und der Uhrzeit	389
21.4.2	Lokale und universelle Zeit	390
21.5	Die Komplexität der Server	390
21.6	RARP-Server	391
21.7	Alternativen zum Client-Server-Modell	392
21.8	Zusammenfassung	393
21.9	Weiterführende Hinweise	393
22	Das Socket-Interface	395
22.1	Einführung	395
22.2	Das UNIX-I/O-Paradigma und Netzwerk-I/O	395
22.3	Netzwerk-I/O für UNIX hinzufügen	396
22.4	Die Socket-Abstraktion	396
22.5	Ein Socket erstellen	397
22.6	Socket-Vererbung und –Terminierung	398
22.7	Angabe einer lokalen Adresse	398
22.8	Verknüpfen von Sockets mit Zieladressen	400
22.9	Übertragung von Daten über ein Socket	400
23	Bootstrap und Autokonfiguration (BOOTP, DHCP)	419
23.1	Einführung	419
23.2	Die Notwendigkeit einer Alternative zu RARP	419
23.3	Die Nutzung von IP, um eine IP-Adresse festzustellen	420
23.4	Die BOOTP-Wiederholungsrichtlinie	421
23.5	Das BOOTP-Nachrichtenformat	421
23.6	Die zweistufige Bootstrap-Prozedur	422

23.7	Das herstellerspezifische Feld	423
23.8	Die Notwendigkeit einer dynamischen Konfiguration.	424
23.9	Dynamische Hostkonfiguration	425
24	Das Domain Name System (DNS)	435
24.1	Einführung	435
24.2	Namen für Maschinen	435
24.3	Der flache Namensraum.	436
24.4	Hierarchische Namen	436
24.5	Delegieren der Autorität für Namen	437
24.6	Autorität für eine Subgruppe.	437
24.7	Internet-Domännennamen	438
24.8	Offizielle und inoffizielle Internet-Domännennamen	439
24.9	Benannte Einträge und Namensyntax	441
25	Applikationen: Remote-Login (TELNET, Rlogin)	455
25.1	Einführung	455
25.2	Remote Interactive Computing	455
25.3	TELNET-Protokoll	456
25.4	Heterogenität berücksichtigen.	458
25.5	Befehle zur Steuerung der Remote-Site übergeben	459
25.6	Wie der Server gezwungen wird, eine Steuersequenz zu lesen.	461
25.7	TELNET-Optionen	461
25.8	Aushandeln von TELNET-Optionen	462
25.9	Rlogin (BSD UNIX)	463
26	Applikationen: Dateitransfer und -zugriff (FTP, TFTP, NFS)	467
26.1	Einführung	467
26.2	Dateizugriff und -transfer	467
26.3	Gemeinsamer Online-Zugriff	467

26.4	Gemeinsamer Zugriff durch den Dateitransfer.	468
26.5	FTP: Das wichtigste TCP/IP-Filetransfer-Protokoll	469
26.6	Features von FTP	469
26.7	FTP-Prozessmodell	470
26.8	TCP-Portnummer	471
26.9	FTP aus Sicht des Users.	471
27	Applikationen: Elektronische Mail (SMTP, POP, IMAP, MIME)	479
27.1	Einführung	479
27.2	Elektronische Mail	479
27.3	Mailbox-Namen und -Aliase	480
27.4	Alias-Erweiterung und Mail-Forwarding	480
27.5	Zusammenhang zwischen Internetworking und Mail	482
27.6	TCP/IP-Standards für den elektronischen Mail-Service	483
27.7	Elektronische Mail-Adressen	484
27.8	Pseudo-Domänenadressen	485
27.9	Simple Mail Transfer Protocol (SMTP).	485
27.10.1	Post Office Protocol	488
27.10.2	Internet Message Access Protocol	488
28	Applikationen: World Wide Web (HTTP)	493
28.1	Einführung	493
28.2	Die Wichtigkeit des Webs	493
28.3	Architektonische Komponenten.	493
28.4	Uniform Resource Locator.	494
28.5	Beispiel für ein Dokument.	494
28.6	HyperText Transfer Protocol	495
28.7	HTTP GET-Request	496
28.8	Fehlermeldungen	496
28.9	Persistente Verbindungen und Längen	497

29	Applikationen: Voice- und Video-Over-IP (RTP)	503
29.1	Einführung	503
29.2	Audio-Clips und Kodierungsverfahren	503
29.3	Audio- und Videoübertragung sowie -Wiedergabe	504
29.4	Jitter und Playback-Verzögerung	505
29.5	Real-Time Transport Protocol (RTP)	506
29.6	Streams, Mixing und Multicasting	507
29.7	RTP-Verkapselung	507
29.8	RTP Control Protocol (RTCP)	508
29.9	RTCP-Operationen	508
29.10.1	H.323-Standard	510
29.10.2	Session Initiation Protocol (SIP)	511
30	Applikationen: Internet-Management (SNMP)	515
30.1	Einführung	515
30.2	Die Ebene der Management-Protokolle	515
30.3	Architektonisches Modell	516
30.4	Protokoll-Framework	517
30.4.1	Ein Standard-Netzwerk-Management-Protokoll	518
30.4.2	Ein Standard für die verwalteten Informationen	518
30.5	Beispiele für MIB-Variablen	519
30.6	Die Struktur der Management-Informationen	520
30.7	Formale Definitionen mit ASN.1	520
30.8	Struktur und Darstellung von MIB-Objektnamen	521
30.9	Simple Network Management Protocol	525
30.9.1	Tabellen mithilfe von Namen durchsuchen	526
31	Zusammenfassung der Abhängigkeiten zwischen den Protokollen	535
31.1	Einführung	535
31.2	Abhängigkeiten zwischen den Protokollen	535
31.3	Das Stundenglasmodell	537
31.4	Zugriff durch Anwendungsprogramme	537

31.5	Zusammenfassung	538
31.6	Weiterführende Hinweise	538
31.7	Aufgaben	538
32	Internetworking-Sicherheit und Firewall-Design (IPsec)	541
32.1	Einführung	541
32.2	Ressourcen schützen	541
32.3	Informationsrichtlinie	542
32.4	Sicherheit im Internetwork	542
32.5	IP-Sicherheit (IPsec)	543
32.6	IPsec-Authentifizierungs-Header	543
32.7	Security Association	544
32.8	IPsec Encapsulating Security Payload	545
32.9	Authentifizierung und veränderbare Header-Felder	546
33	Die Zukunft von TCP/IP (IPv6)	557
33.1	Einführung	557
33.2	Wozu die Änderung?	557
33.3	Neue Richtlinien	558
33.4	Die Beweggründe für eine Änderung von IPv4	558
33.5	Der Weg zu einer neuen IP-Version	559
33.6	Der Name der nächsten IP-Version	559
33.7	Features von IPv6	559
33.8	Das allgemeine Format eines IPv6-Datagramms	560
33.9	Format des IPv6-Basis-Headers	561
A	RFCs im Überblick	579
B	Glossar der Internetworking-Begriffe und Abkürzungen	627
	Bibliographie	671
	Index	677