

Inhaltsverzeichnis

1	Netzwerke	1
1.1	Netzwerkstandards	2
1.1.1	OSI als Grundlage	2
1.1.2	IEEE-Normen	3
1.1.3	Sonstige Standards	7
1.2	Netzwerkvarianten	8
1.2.1	Ethernet	9
1.2.2	Token Ring	13
1.2.3	Fiber Distributed Data Interface (FDDI)	16
1.2.4	Integrated Services Digital Network (ISDN)	18
1.2.5	Digital Subscriber Line (xDSL)	20
1.2.6	Asynchronous Transfer Mode (ATM)	20
1.2.7	Wireless LAN (WLAN)	21
1.2.8	Bluetooth	27
1.3	Netzwerkkomponenten	28
1.3.1	Repeater	28
1.3.2	Brücke	28
1.3.3	Switch	32
1.3.4	Gateway	37
1.3.5	Router	38
2	TCP/IP – Grundlagen	39
2.1	Wesen eines Protokolls	40
2.1.1	Versuch einer Erklärung	40
2.1.2	Verbindungsorientierte und verbindungslose Protokolle	42

2.2	Low-Layer-Protokolle	43
2.2.1	Protokolle der Datensicherungsschicht (Layer 2)	43
2.2.2	Media Access Control (MAC)	44
2.2.3	Logical Link Control (LLC)	45
2.2.4	Service Access Point (SAP)	47
2.2.5	Subnetwork Access Protocol (SNAP)	48
2.3	Protokolle der Netzwerkschicht (Layer 3)	49
2.3.1	Internet Protocol (IP)	50
2.3.2	Internet Control Message Protocol (ICMP)	59
2.3.3	Address Resolution Protocol (ARP)	64
2.3.4	Reverse Address Resolution Protocol (RARP)	66
2.3.5	Routing-Protokolle	66
2.4	Protokolle der Transportschicht (Layer 4)	67
2.4.1	Transmission Control Protocol (TCP)	69
2.4.2	User Datagram Protocol (UDP)	76
2.5	Protokolle der Anwendungsschicht (Layer 5–7)	77
2.6	Sonstige Protokolle	78
2.6.1	X.25	79
2.6.2	Frame Relay	80
2.6.3	Serial Line Internet Protocol (SLIP)	82
2.6.4	Point-to-Point Protocol (PPP)	82
2.6.5	Point-to-Point Tunneling Protocol (PPTP)	82
2.6.6	PPP over Ethernet (PPPoE)	82
2.6.7	Layer 2 Tunneling Protocol (L2TP)	82
3	Adressierung im IP-Netzwerk	83
3.1	Adresskonzept	83
3.1.1	Adressierungsverfahren	83
3.1.2	Adressregistrierung	85
3.1.3	Adressaufbau und Adressklassen	85
3.2	Subnetzadressierung	88
3.2.1	Prinzip	89
3.2.2	Typen der Subnetzmaske	89
3.2.3	Design der Subnetzmaske	90
3.2.4	Verwendung privater IP-Adressen	92
3.2.5	Internetdomain und Subnetz	94

3.3	Dynamische Adressvergabe	94
3.3.1	Bootstrap Protocol (BootP)	95
3.3.2	Dynamic Host Configuration Protocol (DHCP)	97
3.3.3	DHCP im Windows-Netzwerk	106
4	Routing	113
4.1	Grundlagen	114
4.1.1	Aufgaben und Funktion	114
4.1.2	Anforderungen	114
4.1.3	Funktionsweise	116
4.1.4	Router-Architektur	118
4.1.5	Routing-Verfahren	120
4.1.6	Routing-Algorithmus	121
4.1.7	Einsatzkriterien für Router	124
4.2	Routing-Protokolle	126
4.2.1	Routing Information Protocol (RIP)	127
4.2.2	RIP-Version 2	129
4.2.3	Open Shortest Path First (OSPF)	130
4.2.4	HELLO	143
4.2.5	Interior Gateway Routing Protocol (IGRP)	144
4.2.6	Enhanced IGRP	144
4.2.7	Intermediate System – Intermediate System (IS-IS)	145
4.2.8	Border Gateway Protocol (BGP)	147
4.3	Betrieb und Wartung	147
4.3.1	Router-Initialisierung	148
4.3.2	Out-Of-Band-Access	149
4.3.3	Hardware-Diagnose	150
4.3.4	Router-Steuerung	150
4.3.5	Sicherheitsaspekte	151
5	Namensauflösung	153
5.1	Prinzip der Namensauflösung	153
5.1.1	Symbolische Namen	154
5.1.2	Namenshierarchie	155
5.1.3	Funktionsweise	157

5.2	Verfahren zur Namensauflösung	157
5.2.1	Host-Datei	157
5.2.2	WINS	161
5.2.3	Domain Name System	163
5.3	Domain Name System	163
5.3.1	Aufgaben und Funktionen	164
5.3.2	Auflösung von Namen	164
5.3.3	DNS-Struktur	166
5.3.4	DNS-Anfragen	167
5.3.5	Umgekehrte Auflösung	169
5.3.6	Standard Resource Records	169
5.3.7	DNS-Message	171
5.3.8	Dynamic DNS (DDNS)	172
5.3.9	Zusammenspiel von DNS und Active Directory	173
5.3.10	Auswahl der Betriebssystemplattform	176
5.3.11	Fazit	177
5.4	Namensauflösung in der Praxis	177
5.4.1	Vorgaben und Funktionsweise	178
5.4.2	DNS mit Windows-Servern	181
5.4.3	DNS-Konfiguration unter Linux	190
5.4.4	Client-Konfiguration	194
5.4.5	DNS-Datenfluss	198
6	Protokolle und Dienste	203
6.1	Exkurs: Client-Server-Konzept	203
6.2	TELNET	205
6.2.1	Network Virtual Terminal	206
6.2.2	Negotiated Options	206
6.2.3	Zugriffsschutz	209
6.2.4	Kommunikation und Protokollierung	210
6.2.5	TELNET-Anweisungen	211
6.2.6	TELNET auf einem Windows-Client	214
6.2.7	Sonderfall: TELNET 3270 (tn3270)	215
6.3	Dateiübertragung mit FTP	216
6.3.1	Funktion	216
6.3.2	FTP-Sitzungsprotokoll	220
6.3.3	FTP-Befehlsübersicht	223

6.3.4	FTP-Meldungen	227
6.3.5	Anonymus FTP	227
6.3.6	Trivial File Transfer Protocol (TFTP)	228
6.4	HTTP	229
6.4.1	Eigenschaften	230
6.4.2	Adressierung	230
6.4.3	HTTP-Message	231
6.4.4	HTTP-Request	233
6.4.5	HTTP-Response	234
6.4.6	Statuscodes	234
6.4.7	Methoden	236
6.4.8	MIME-Datentypen	237
6.4.9	Einsatz eines Web-Servers	240
6.5	E-Mail	252
6.5.1	Simple Mail Transfer Protocol (SMTP)	254
6.5.2	Post Office Protocol 3 (POP3)	258
6.5.3	Internet Message Access Protocol 4 (IMAP4)	260
6.5.4	E-Mail-Einsatz in der Praxis	261
6.6	Voice over IP	265
6.7	Chat	266
6.8	Newsgroups	266
6.9	Lightweight Directory Access Protocol (LDAP)	267
6.9.1	Konzeption	267
6.9.2	Application Programming Interface (API)	268
6.10	NFS	269
6.10.1	Remote Procedure Calls (Layer 5)	270
6.10.2	External Data Representation (XDR)	272
6.10.3	Prozeduren und Anweisungen	273
6.10.4	Network Information Services (NIS) – YELLOW PAGES ...	275
6.11	Kerberos	276
6.12	Simple Network Management Protocol (SNMP)	279
6.12.1	SNMP und CMOT – zwei Entwicklungsrichtungen	280
6.12.2	SNMP-Architektur	281
6.12.3	SNMP-Komponenten	282
6.12.4	Structure and Identification of Management Information (SMI)	284

6.12.5	Management Information Base (MIB)	286
6.12.6	SNMP-Anweisungen	292
6.12.7	SNMP-Message-Format	293
6.12.8	SNMP-Sicherheit	294
6.12.9	SNMP-Nachfolger	295
7	TCP/IP und Betriebssysteme	301
7.1	TCP/IP unter Windows	302
7.1.1	Windows als Desktop-System	302
7.1.2	Windows als Server-System	306
7.2	TCP/IP beim Apple Macintosh	309
7.3	TCP/IP unter Linux	311
7.3.1	Netzwerkverbindung testen und konfigurieren	311
7.3.2	Konfiguration des Name Resolver	313
7.3.3	Loopback Interface	316
7.3.4	Routing im Linux-Netzwerk	316
7.3.5	Netzwerkdienste	319
8	Sicherheit im IP-Netzwerk	321
8.1	Interne Sicherheit	322
8.1.1	Hardware-Sicherheit	323
8.1.2	UNIX-Zugriffsrechte	324
8.1.3	Windows-Zugriffsrechte	329
8.1.4	Benutzerauthentifizierung	331
8.1.5	Die R-Kommandos	333
8.1.6	Remote Execution (rexec)	336
8.2	Externe Sicherheit	337
8.2.1	Öffnung isolierter Netzwerke	337
8.2.2	Das LAN/WAN-Sicherheitsrisiko	338
8.3	Organisatorische Sicherheit	339
8.3.1	Data Leakage	339
8.3.2	Nutzung potenziell gefährlicher Applikationen	340
8.3.3	Prozessnetzwerke und ihr Schutz	341

8.4	Angriffe aus dem Internet	341
8.4.1	»Hacker« und »Cracker«	343
8.4.2	Scanning-Methoden	344
8.4.3	Denial of Service Attack	347
8.4.4	DNS-Sicherheitsprobleme	350
8.4.5	Schwachstellen des Betriebssystems	353
8.5	Aufbau eines Sicherheitssystems	358
8.5.1	Grundschutzhandbuch für IT-Sicherheit des BSI	359
8.6	Das Drei-Komponenten-System	362
8.6.1	Firewall-System	366
8.6.2	Content Security System	373
8.6.3	Intrusion Detection System und Intrusion Response System	373
8.7	Public Key Infrastructure (PKI)	376
8.7.1	Authentifizierung	377
8.7.2	Verschlüsselung	379
8.7.3	Zertifikate	385
8.7.4	Signaturen	386
8.8	Virtual Private Network (VPN)	390
8.8.1	Grundlagen	390
8.8.2	Beispielkonfiguration	391
8.9	Sicherheitsprotokoll IPsec	394
8.9.1	IPsec-Merkmale	395
8.9.2	IP- und IPsec-Paketformat	396
8.9.3	Transport- und Tunnelmodus	398
8.9.4	IPsec-Protokolle AH und ESP	399
8.9.5	Internet Key Exchange (IKE)	401
8.9.6	IPsec-RFCs	405
9	TCP/IP im Internet	407
9.1	Was ist das Internet?	407
9.2	Aufbau des Internets	409
9.2.1	TCP/IP als Grundlage	409
9.2.2	Dienste im Internet	409

9.3	Internet-Sicherheit	410
9.3.1	Sicherheitslücken	411
9.3.2	Bedrohung durch Viren	414
9.3.3	Hacking und Cracking	415
9.3.4	Risikoabschätzung und -schutz	416
9.4	Suche im WWW	418
9.4.1	Suche nach Dateien	418
9.4.2	Einsatz von Suchmaschinen	419
9.5	Geschwindigkeit und Bandbreite	424
10	Weiterentwicklungen	427
10.1	Gründe für eine Neuentwicklung	428
10.2	Lösungsansätze	430
10.2.1	Lösungen auf Basis von IPv6	431
10.2.2	ROAD-Arbeitsgruppe	433
10.3	IPv6-Leistungsmerkmale	435
10.3.1	Erweiterung des Adressraums	435
10.3.2	Abbildung von Hierarchien	436
10.3.3	IP-Header-Struktur	436
10.3.4	Priorisierung	436
10.3.5	Sicherheit	436
10.3.6	Vereinfachte Konfiguration	437
10.3.7	Multicasting	437
10.4	IP-Header der Version 6	437
10.5	Stand der Einführung von IPv6	439
10.5.1	Test-Netzwerk	440
10.5.2	Adressen in der Konvergenzphase	441
10.6	NAT, CIDR und RSIP als Alternativen	442
10.6.1	Network Address Translation (NAT)	442
10.6.2	Classless Inter Domain Routing (CIDR)	443
10.6.3	RSIP	444
10.7	Fazit	444

11 Troubleshooting in IP-Netzwerken	447
11.1 Analysemöglichkeiten	448
11.1.1 Der Netzwerk-Trace	448
11.1.2 Netzwerkstatistik	450
11.1.3 Remote Network Monitoring (RMON)	451
11.1.4 Analyse in Switched LANs	454
11.2 Verbindungstest mit PING	455
11.2.1 Selbsttest	455
11.2.2 Test anderer Endgeräte	456
11.2.3 Praktische Vorgehensweise im Fehlerfall	458
11.3 Informationen per NETSTAT	459
11.4 ROUTE zur Wegewahl	462
11.5 Wegeermittlung per TRACEROUTE	463
11.6 Knotenadressen per ARP	464
11.7 Aktuelle Konfiguration mit IFCONFIG	464
11.8 NSLOOKUP zur Nameserver-Suche	466
A Anhang	469
A.1 Geschichtliches	469
A.1.1 ARPANET – Die Anfänge	470
A.1.2 Entwicklung zum Internet	473
A.1.3 Request For Comment (RFC)	476
A.2 Literatur und Quellenverzeichnis	478
Stichwortverzeichnis	481