

Inhaltsverzeichnis

1	Netzwerke	1
1.1	Netzwerkstandards	2
1.1.1	OSI als Grundlage	2
1.1.2	IEEE-Normen	4
1.1.3	Sonstige Standards	7
1.2	Netzwerkvarianten	9
1.2.1	Ethernet	10
1.2.2	Token Ring	13
1.2.3	Fiber Distributed Data Interface (FDDI)	17
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
2.6.8	MPLS (Multi Protocol Label Switching)	83
3	Adressierung im IP-Netzwerk	85
3.1	Adresskonzept	85
3.1.1	Adressierungsverfahren	85
3.1.2	Adressregistrierung	87
3.1.3	Adressaufbau und Adressklassen	87
3.2	Subnetzadressierung	90
3.2.1	Prinzip	91
3.2.2	Typen der Subnetzmaske	91
3.2.3	Design der Subnetzmaske	92
3.2.4	Verwendung privater IP-Adressen	94
3.2.5	Internetdomain und Subnetz	96

3.3	Dynamische Adressvergabe	96
3.3.1	Bootstrap Protocol (BootP)	97
3.3.2	Dynamic Host Configuration Protocol (DHCP)	99
3.3.3	DHCP im Windows-Netzwerk	108
4	Routing	115
4.1	Grundlagen	116
4.1.1	Aufgaben und Funktion	116
4.1.2	Anforderungen	116
4.1.3	Funktionsweise	118
4.1.4	Router-Architektur	120
4.1.5	Routing-Verfahren	122
4.1.6	Routing-Algorithmus	123
4.1.7	Einsatzkriterien für Router	126
4.2	Routing-Protokolle	128
4.2.1	Routing Information Protocol (RIP)	129
4.2.2	RIP-Version 2	131
4.2.3	Open Shortest Path First (OSPF)	132
4.2.4	HELLO	146
4.2.5	Interior Gateway Routing Protocol (IGRP)	147
4.2.6	Enhanced IGRP	148
4.2.7	Intermediate System – Intermediate System (IS-IS)	149
4.2.8	Border Gateway Protocol (BGP)	150
4.3	Betrieb und Wartung	151
4.3.1	Router-Initialisierung	151
4.3.2	Out-Of-Band Access	152
4.3.3	Hardwarediagnose	153
4.3.4	Router-Steuerung	154
4.3.5	Sicherheitsaspekte	154
5	Namensauflösung	155
5.1	Prinzip der Namensauflösung	155
5.1.1	Symbolische Namen	157
5.1.2	Namenshierarchie	157
5.1.3	Funktionsweise	159

5.2	Verfahren zur Namensauflösung	160
5.2.1	Host-Datei	160
5.2.2	WINS	164
5.2.3	Domain Name System	166
5.3	Domain Name System	166
5.3.1	Aufgaben und Funktionen	166
5.3.2	Auflösung von Namen	167
5.3.3	DNS-Struktur	169
5.3.4	DNS-Anfragen	170
5.3.5	Umgekehrte Auflösung	171
5.3.6	Standard Resource Records	172
5.3.7	DNS-Message	173
5.3.8	Dynamic DNS (DDNS)	175
5.3.9	Zusammenspiel von DNS und Active Directory	175
5.3.10	Auswahl der Betriebssystemplattform	179
5.3.11	Fazit	179
5.4	Namensauflösung in der Praxis	180
5.4.1	Vorgaben und Funktionsweise	180
5.4.2	DNS mit Windows-Servern	183
5.4.3	DNS-Konfiguration unter Linux	192
5.4.4	Client-Konfiguration	197
5.4.5	DNS-Datenfluss	200
6	Protokolle und Dienste	205
6.1	TELNET	205
6.1.1	Network Virtual Terminal	206
6.1.2	Negotiated Options	207
6.1.3	Zugriffsschutz	210
6.1.4	Kommunikation und Protokollierung	210
6.1.5	TELNET-Anweisungen	211
6.1.6	TELNET auf einem Windows-Client	215
6.1.7	Sonderfall: TELNET 3270 (tn3270)	215
6.2	Dateiübertragung mit FTP	216
6.2.1	Funktion	216
6.2.2	FTP-Sitzungsprotokoll	220
6.2.3	FTP-Befehlsübersicht	223
6.2.4	FTP-Meldungen	227

6.2.5	Anonymus FTP	227
6.2.6	Trivial File Transfer Protocol (TFTP)	228
6.2.7	Sicheres FTP	229
6.3	HTTP	229
6.3.1	Eigenschaften	230
6.3.2	Adressierung	230
6.3.3	HTTP-Message	232
6.3.4	HTTP-Request	233
6.3.5	HTTP-Response	234
6.3.6	Statuscodes	234
6.3.7	Methoden	236
6.3.8	MIME-Datentypen	238
6.4	E-Mail	239
6.4.1	Simple Mail Transfer Protocol (SMTP)	241
6.4.2	Post Office Protocol 3 (POP3)	245
6.4.3	Internet Message Access Protocol 4 (IMAP4)	247
6.4.4	E-Mail-Einsatz in der Praxis	248
6.5	Unified Communications (UC)	252
6.5.1	Presence Manager	253
6.5.2	Instant Messaging (IM)	253
6.5.3	Conferencing	254
6.5.4	Telephony	254
6.5.5	Application Integration	255
6.5.6	Mobility	256
6.5.7	CTI und Call Control	256
6.5.8	Federation	256
6.6	Lightweight Directory Access Protocol (LDAP)	257
6.6.1	Konzeption	257
6.6.2	Application Programming Interface (API)	258
6.7	NFS	259
6.7.1	Remote Procedure Calls (Layer 5)	259
6.7.2	External Data Representation (XDR)	262
6.7.3	Prozeduren und Anweisungen	263
6.7.4	Network Information Services (NIS) – YELLOW PAGES ...	264
6.8	Kerberos	266

6.9 Simple Network Management Protocol (SNMP)	268
6.9.1 SNMP und CMOT – zwei Entwicklungsrichtungen	270
6.9.2 SNMP-Architektur	271
6.9.3 SNMP-Komponenten	272
6.9.4 Structure and Identification of Management Information (SMI)	273
6.9.5 Management Information Base (MIB)	275
6.9.6 SNMP-Anweisungen	281
6.9.7 SNMP-Message-Format	282
6.9.8 SNMP-Sicherheit	283
6.9.9 SNMP-Nachfolger	284
7 TCP/IP und Betriebssysteme	289
7.1 TCP/IP unter Windows	290
7.1.1 Windows als Desktop-System	290
7.1.2 Windows als Serversystem	294
7.2 TCP/IP beim Apple Macintosh	297
7.3 TCP/IP unter Linux	299
7.3.1 Netzwerkverbindung testen und konfigurieren	299
7.3.2 Konfiguration des Name Resolver	301
7.3.3 Loopback Interface	304
7.3.4 Routing im Linux-Netzwerk	304
7.3.5 Netzwerkdienste	307
8 Sicherheit im IP-Netzwerk	309
8.1 Interne Sicherheit	310
8.1.1 Hardwaresicherheit	311
8.1.2 UNIX-Zugriffsrechte	312
8.1.3 Windows-Zugriffsrechte	317
8.1.4 Benutzeroauthentifizierung	320
8.1.5 Die R-Kommandos	321
8.1.6 Remote Execution (rexec)	324
8.2 Externe Sicherheit	325
8.2.1 Öffnung isolierter Netzwerke	325
8.2.2 Das LAN/WAN-Sicherheitsrisiko	327

8.3	Organisatorische Sicherheit	328
8.3.1	Data Leakage	328
8.3.2	Nutzung potenziell gefährlicher Applikationen	329
8.3.3	Prozessnetzwerke und ihr Schutz	329
8.4	Angriffe aus dem Internet	330
8.4.1	»Hacker« und »Cracker«	332
8.4.2	Scanning-Methoden	333
8.4.3	Denial of Service Attack	336
8.4.4	DNS-Sicherheitsprobleme	339
8.4.5	Schwachstellen des Betriebssystems	342
8.5	Aufbau eines Sicherheitssystems	347
8.5.1	Grundschutzhandbuch für IT-Sicherheit des BSI	348
8.6	Das Drei-Komponenten-System	351
8.6.1	Firewall-System	355
8.6.2	Content Security System	362
8.6.3	Intrusion Detection System und Intrusion Response System	362
8.7	Public Key Infrastructure (PKI)	365
8.7.1	Authentifizierung	366
8.7.2	Verschlüsselung	368
8.7.3	Zertifikate	374
8.7.4	Signaturen	375
8.8	Virtual Private Network (VPN)	379
8.8.1	Grundlagen	379
8.8.2	Beispielkonfiguration	380
8.9	Sicherheitsprotokoll IPsec	384
8.9.1	IPsec-Merkmale	384
8.9.2	IP- und IPsec-Paketformat	385
8.9.3	Transport- und Tunnelmodus	387
8.9.4	IPsec-Protokolle AH und ESP	388
8.9.5	Internet Key Exchange (IKE)	391
8.9.6	IPsec-RFCs	395

9 TCP/IP im Internet	397
9.1 Was ist das Internet?	397
9.2 Aufbau des Internets	399
9.2.1 TCP/IP als Grundlage	399
9.2.2 Dienste im Internet	399
9.3 Sicherheit im Internet	400
9.3.1 Sicherheitslücken	401
9.3.2 Bedrohung durch Viren	404
9.3.3 Hacking und Cracking	405
9.3.4 Risikoabschätzung und -schutz	406
9.4 Suche im WWW	408
9.4.1 Suche nach Dateien	408
9.4.2 Einsatz von Suchmaschinen	409
9.5 Geschwindigkeit und Bandbreite	414
9.6 Internet der Dinge	416
10 Weiterentwicklungen	417
10.1 Gründe für eine Neuentwicklung	418
10.2 Lösungsansätze	420
10.2.1 Lösungen auf Basis von IPv6	421
10.2.2 ROAD-Arbeitsgruppe	423
10.3 IPv6-Leistungsmerkmale	425
10.3.1 Erweiterung des Adressraums	426
10.3.2 Abbildung von Hierarchien	426
10.3.3 IP-Header-Struktur	426
10.3.4 Priorisierung	426
10.3.5 Sicherheit	427
10.3.6 Vereinfachte Konfiguration	427
10.3.7 Multicasting	428
10.4 IP-Header der Version 6	428
10.5 Stand der Einführung von IPv6	430
10.5.1 Test-Netzwerk	430
10.5.2 Adressen in der Konvergenzphase	431

10.6 NAT, CIDR und RSIP als Alternativen	432
10.6.1 Network Address Translation (NAT)	433
10.6.2 Classless Inter Domain Routing (CIDR)	434
10.6.3 RSIP	434
10.7 Fazit	435
11 Troubleshooting in IP-Netzwerken	437
11.1 Analysemöglichkeiten	438
11.1.1 Der Netzwerk-Trace	438
11.1.2 Netzwerkstatistik	440
11.1.3 Remote Network Monitoring (RMON)	441
11.1.4 Analyse in Switched LANs	444
11.2 Verbindungstest mit PING	445
11.2.1 Selbsttest	445
11.2.2 Test anderer Endgeräte	446
11.2.3 Praktische Vorgehensweise im Fehlerfall	448
11.3 Informationen per NETSTAT	449
11.4 ROUTE zur Wegewahl	452
11.5 Wegeermittlung per TRACEROUTE	453
11.6 Knotenadressen per ARP	454
11.7 Aktuelle Konfiguration	454
11.8 NSLOOKUP zur Nameserver-Suche	456
A Anhang	459
A.1 Geschichtliches	459
A.1.1 ARPANET – Die Anfänge	460
A.1.2 Entwicklung zum Internet	463
A.1.3 Request for Comment (RFC)	466
A.2 Literatur und Quellenverzeichnis	468
Stichwortverzeichnis	471