

TCP/IP

Grundlagen und Praxis

Protokolle, Routing, Dienste, Sicherheit

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhalt

1	Netzwerke	1
1.1	Netzwerkstandards	1
1.1.1	OSI als Grundlage	2
1.1.2	IEEE-Normen	3
1.2	Netzwerkvarianten	7
1.2.1	Ethernet	8
1.2.2	Wireless LAN (IEEE 802.11)	12
1.2.3	Bluetooth	19
1.2.4	Sonstige Varianten	20
1.3	Netzwerkkomponenten	24
1.3.1	Repeater	25
1.3.2	Brücke	25
1.3.3	Switch	28
1.3.4	Gateway	34
1.3.5	Router	34
2	TCP/IP – Grundlagen	37
2.1	Wesen eines Protokolls	38
2.2	Low-Layer-Protokolle	40
2.2.1	Protokolle der Datensicherungsschicht (Layer 2)	40
2.2.2	Media Access Control (MAC)	41
2.2.3	Logical Link Control (LLC)	42
2.2.4	Service Access Point (SAP)	44
2.2.5	Subnetwork Access Protocol (SNAP)	45
2.3	Protokolle der Netzwerkschicht (Layer 3)	46
2.3.1	Internet Protocol (IP)	46
2.3.2	Internet Control Message Protocol (ICMP)	56
2.3.3	Address Resolution Protocol (ARP)	61
2.3.4	Reverse Address Resolution Protocol (RARP)	63
2.3.5	Routing-Protokolle	63

2.4	Protokolle der Transportschicht (Layer 4)	64
2.4.1	Transmission Control Protocol (TCP)	66
2.4.2	User Datagram Protocol (UDP)	74
2.5	Protokolle der Anwendungsschicht (Layer 5–7)	75
2.6	Sonstige Protokolle	76
3	Adressierung im IP-Netzwerk	79
3.1	Adresskonzept	79
3.1.1	Adressierungsverfahren	79
3.1.2	Adressregistrierung	81
3.1.3	Adressaufbau und Adressklassen	82
3.2	Subnetzadressierung	84
3.2.1	Prinzip	85
3.2.2	Typen und Design der Subnetzmaske	85
3.2.3	Verwendung privater IP-Adressen	88
3.2.4	Internetdomain und Subnetz	90
3.3	Dynamische Adressvergabe	91
3.3.1	Bootstrap Protocol (BootP)	92
3.3.2	Dynamic Host Configuration Protocol (DHCP)	94
3.4	IP-Version 6 (IPv6)	101
3.4.1	Gründe für eine Neuentwicklung	102
3.4.2	Lösungsansätze	105
3.4.3	IPv6-Leistungsmerkmale	108
3.4.4	IP-Header der Version 6	111
3.4.5	Stand der Einführung von IPv6	113
3.4.6	NAT, CIDR und RSIP als Alternativen	114
3.4.7	Fazit	116
4	Routing	119
4.1	Grundlagen	120
4.1.1	Aufgaben und Funktion	120
4.1.2	Anforderungen	121
4.1.3	Funktionsweise	122
4.1.4	Router-Architektur	124
4.1.5	Routing-Verfahren	126
4.1.6	Routing-Algorithmus	128
4.1.7	Einsatzkriterien für Router	130
4.2	Routing-Protokolle	132
4.2.1	Routing Information Protocol (RIP)	133
4.2.2	RIP-Version 2	135

4.2.3	Open Shortest Path First (OSPF)	137
4.2.4	HELLO	149
4.2.5	Interior Gateway Routing Protocol (IGRP)	150
4.2.6	Enhanced IGRP	151
4.2.7	Intermediate System – Intermediate System (IS-IS)	152
4.2.8	Border Gateway Protocol (BGP)	153
4.3	Betrieb und Wartung	153
4.3.1	Router-Initialisierung	154
4.3.2	Out-Of-Band Access	155
4.3.3	Hardwarediagnose	156
4.3.4	Router-Steuerung	157
4.3.5	Sicherheitsaspekte	157
4.4	Software Defined Networking (SDN)	158
4.4.1	Netzwerk Virtualisierung	159
4.4.2	Switching Fabrics	159
4.4.3	WAN Traffic Engineering	160
4.4.4	SD-WAN	160
4.4.5	Access Networks	160
5	Namensauflösung	161
5.1	Prinzip der Namensauflösung	162
5.1.1	Symbolische Namen	163
5.1.2	Namenshierarchie	163
5.1.3	Funktionsweise	164
5.2	Statische Namensauflösung	165
5.3	Dynamische Namensauflösung	168
5.3.1	Aufgaben und Funktionen	169
5.3.2	Auflösung von Namen	170
5.3.3	DNS-Struktur	171
5.3.4	DNS-Anfragen	173
5.3.5	Umgekehrte Auflösung	174
5.3.6	Standard Resource Records	175
5.3.7	DNS-Message	176
5.3.8	Dynamic DNS (DDNS)	177
5.3.9	Zusammenspiel von DNS und Active Directory	178
5.3.10	Auswahl der Betriebssystemplattform	182
5.4	Namensauflösung in der Praxis	182
5.4.1	Vorgaben und Funktionsweise	182
5.4.2	DNS-Konfiguration	185
5.4.3	Client-Konfiguration	190

6	Protokolle und Dienste	191
6.1	TELNET	191
6.2	SSH (Secure Shell)	192
6.2.1	SSH-Server-Einrichtung	192
6.2.2	SSH-Client-Einrichtung	194
6.3	Dateiübertragung mit FTP	195
6.3.1	Funktion	196
6.3.2	Sicheres FTP (FTPS und SFTP)	199
6.3.3	Anonymus FTP	201
6.3.4	Trivial File Transfer Protocol (TFTP)	201
6.4	HTTP	202
6.4.1	Eigenschaften	203
6.4.2	Adressierung	203
6.4.3	HTTP-Message	204
6.4.4	HTTP-Request	206
6.4.5	HTTP-Response	207
6.4.6	Statuscodes	208
6.4.7	Methoden	208
6.4.8	MIME-Datentypen	209
6.4.9	HTTP Version 2 (HTTP/2)	211
6.4.10	HTTP/3 und QUIC	211
6.4.11	HTTPS	212
6.5	E-Mail	212
6.5.1	Simple Mail Transfer Protocol (SMTP)	214
6.5.2	Post Office Protocol 3 (POP3)	218
6.5.3	Internet Message Access Protocol 4 (IMAP4)	220
6.6	Unified Collaboration and Communication (UCC)	221
6.6.1	Presence Manager	222
6.6.2	Instant Messaging (IM)	222
6.6.3	Conferencing	223
6.6.4	Telephony	223
6.6.5	Application Integration	224
6.6.6	Mobility	224
6.6.7	CTI und Call Control	225
6.6.8	Federation	225
6.7	Lightweight Directory Access Protocol (LDAP)	225
6.7.1	Konzeption	226
6.7.2	Application Programming Interface (API)	227
6.8	NFS	227
6.8.1	Remote Procedure Calls (Layer 5)	228
6.8.2	External Data Representation (XDR)	230
6.8.3	Prozeduren und Anweisungen	230
6.8.4	Network Information Services (NIS) – YELLOW PAGES	231

6.9	Kerberos	232
6.10	Simple Network Management Protocol (SNMP)	235
6.10.1	SNMP und CMOT – zwei Entwicklungsrichtungen	236
6.10.2	SNMP-Architektur	238
6.10.3	SNMP-Komponenten	238
6.10.4	Structure and Identification of Management Information (SMI)	240
6.10.5	Management Information Base (MIB)	242
6.10.6	SNMP-Anweisungen	245
6.10.7	SNMP-Message-Format	246
6.10.8	SNMP-Sicherheit	247
6.10.9	SNMP-Nachfolger	248
7	Sicherheit im IP-Netzwerk	253
7.1	Interne Sicherheit	254
7.1.1	Hardware-sicherheit	256
7.1.2	UNIX-Zugriffsrechte	256
7.1.3	Windows- und macOS-Zugriffsrechte	261
7.1.4	Benutzerauthentifizierung	262
7.1.5	Die R-Kommandos	263
7.1.6	Remote Execution (rexec)	265
7.2	Externe Sicherheit	266
7.2.1	Öffnung isolierter Netzwerke	266
7.2.2	Das LAN/WAN-Sicherheitsrisiko	268
7.3	Organisatorische Sicherheit	269
7.3.1	Data Leakage	269
7.3.2	Nutzung potenziell gefährlicher Applikationen	270
7.3.3	Prozessnetzwerke und ihr Schutz	270
7.4	Angriffe aus dem Internet	271
7.4.1	»Hacker« und »Cracker«	272
7.4.2	Scanning-Methoden	272
7.4.3	Denial of Service Attack	274
7.4.4	DNS-Sicherheitsprobleme	277
7.4.5	Schwachstellen des Betriebssystems	280
7.5	Virtual Private Network (VPN)	280
7.6	Sicherheitsprotokoll IPsec	282
7.6.1	IPsec-Merkmale	282
7.6.2	IP- und IPsec-Paketformat	284
7.6.3	Transport- und Tunnelmodus	285
7.6.4	IPsec-Protokolle AH und ESP	286
7.6.5	Internet Key Exchange (IKE)	289

7.7	Weitere Überlegungen	293
7.7.1	Grundschutzhandbuch für IT-Sicherheit des BSI	293
7.7.2	Patching	293
7.7.3	Der Schutz des Perimeters	294
7.7.4	Public Key Infrastructure (PKI)	295
7.7.5	Security Incident und Event Management (SIEM)	295
7.7.6	Datenschutz-Grundverordnung (DSGVO)	296
7.7.7	Der Sicherheitsschild	296
8	Troubleshooting in IP-Netzwerken	299
8.1	Analysemöglichkeiten	300
8.1.1	Der Netzwerk-Trace	300
8.1.2	Netzwerkstatistik	302
8.1.3	Remote Network Monitoring (RMON)	303
8.1.4	Analyse in Switched LANs	306
8.2	Verbindungstest mit PING	306
8.2.1	Selbsttest	307
8.2.2	Test anderer Endgeräte	308
8.2.3	Praktische Vorgehensweise im Fehlerfall	310
8.2.4	Informationen per NETSTAT	311
8.3	ROUTE zur Wegekongfiguration	313
8.4	Wegeermittlung per TRACEROUTE	315
8.5	Knotenadressen per ARP	316
8.6	Aktuelle Konfiguration	317
8.7	NSLOOKUP zur Nameserver-Suche	318
8.8	Netzwerkanalyse mit WireShark	321
8.8.1	Installation und Konfiguration	321
8.8.2	Szenario: Web-Surfing	323
8.8.3	Diverse Auswertungen	325
A	Anhang: Das neue TCP/IP-Umfeld	329
A.1	Internet of Things (IoT)	329
A.1.1	IoT in der Industrie	330
A.1.2	IoT im öffentlichen Sektor	331
A.1.3	IoT im privaten Haushalt	332
A.2	Industrie 4.0	332
B	Anhang: TCP/IP-Konfigurationen	335
B.1	Microsoft Windows	335
B.2	Apple macOS	338
B.3	Debian Linux	340
B.4	Android	341
B.5	Apple IOS	343
	Index	345