

Auf einen Blick

1	Grundlagen moderner Netzwerke	19
2	Netzwerktechnik	29
3	Adressierung im Netzwerk – Theorie	83
4	MAC- und IP-Adressen in der Praxis	121
5	Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen	197
6	Datentransport mit TCP und UDP	203
7	Kommunikation und Sitzung	235
8	Standards für den Datenaustausch	275
9	Netzwerkanwendungen	281
10	Netzwerkpraxis	315

Inhalt

Geleitwort des Fachgutachters	15
Vorwort	17

1 Grundlagen moderner Netzwerke 19

1.1 Definition und Eigenschaften von Netzwerken	20
1.2 Die Netzwerkprotokollfamilie TCP/IP	22
1.3 OSI-Schichtenmodell und TCP/IP-Referenzmodell	23
1.4 Räumliche Abgrenzung von Netzwerken	27
1.5 Regel- und Nachschlagewerk für TCP/IP-Netze (RFCs)	27
1.6 Prüfungsfragen	28

2 Netzwerktechnik 29

2.1 Elektrische Netzwerkverbindungen und -standards	30
2.1.1 Netzwerke mit Koaxialkabeln	31
2.1.2 Netze mit Twisted-Pair-Kabeln	34
2.1.3 Aufbau, Bezeichnung und Kategorien von Twisted-Pair-Kabeln	36
2.1.4 Stecker- und Kabelbelegungen	40
2.1.5 Anschlusskomponenten für Twisted-Pair-Kabel	43
2.1.6 Herstellung von Kabelverbindungen mit der Schneid- Klemmtechnik (LSA)	45
2.1.7 Montage von RJ45-Steckern	48
2.1.8 Prüfen von Kabeln und Kabelverbindungen	51
2.1.9 Kennzeichnen, Suchen und Finden von Kabelverbindungen	56
2.1.10 Power over Ethernet (PoE)	58
2.2 Lichtwellenleiter, Kabel und Verbinder	59
2.2.1 Übersicht über die Netzwerkstandards mit Glasfaserkabel	61
2.2.2 Aufbau und Funktion von Glasfaserkabeln	63
2.2.3 Dauerhafte Glasfaserverbindungen	67
2.2.4 Lichtwellenleiter-Steckverbindungen	68

2.2.5	Umgang mit der LWL-Technik	70
2.2.6	Aufbau eines einfachen Leitungs- und Kabeltesters	73
2.2.7	Prüfen von LWL-Kabeln und -Verbindungen	73
2.3	Datenübertragung per Funktechnik	74
2.3.1	WLAN (Wireless LAN, Wi-Fi)	74
2.3.2	Datenübertragung über öffentliche Funknetze	77
2.3.3	Powerline Communication (PLC)	78
2.4	Technische Anbindung von Rechnern und Netzen	79
2.5	Weitere Netzwerkkomponenten	79
2.6	Zugriffsverfahren	80
2.6.1	CSMA/CD, Kollisionserkennung	80
2.6.2	CSMA/CA, Kollisionsvermeidung	80
2.7	Prüfungsfragen	81
3	Adressierung im Netzwerk – Theorie	83
<hr/>		
3.1	Physikalische Adresse (MAC-Adresse)	83
3.2	Ethernet-Pakete (Ethernet-Frames)	85
3.3	Zusammenführung von MAC- und IP-Adresse	86
3.3.1	Address Resolution Protocol (ARP), IPv4	86
3.3.2	Neighbor Discovery Protocol (NDP), IPv6	88
3.4	IP-Adressen	91
3.5	IPv4-Adressen	92
3.5.1	Netzwerkklassen im IPv4	92
3.5.2	Netz- und Subnetzmaske, Unterteilung von Netzen	93
3.5.3	Berechnungen	97
3.5.4	Private Adressen des IPv4	100
3.5.5	Zeroconf – konfigurationsfreie Vernetzung von Rechnern	100
3.5.6	Localnet und Localhost	101
3.5.7	Weitere reservierte Adressen	102
3.6	IPv6-Adressen	103
3.6.1	Adresstypen des IPv6	105
3.6.2	IPv6-Loopback-Adresse	108
3.6.3	Unspezifizierte Adresse	109
3.6.4	IPv4- in IPv6-Adressen und umgekehrt	109

3.6.5	Tunnel-Adressen	110
3.6.6	Kryptografisch erzeugte Adressen (CGA)	112
3.6.7	Lokale Adressen	112
3.6.8	Übersicht der Präfixe von IPv6-Adressen	113
3.6.9	Adresswahl und -benutzung	113
3.7	Internetprotokoll	114
3.7.1	Der IPv4-Header	115
3.7.2	Der IPv6-Header	117
3.8	Prüfungsfragen	119
3.8.1	Berechnungen	119
3.8.2	IP-Adressen	119
4	MAC- und IP-Adressen in der Praxis	121
4.1	MAC-Adressen	121
4.1.1	Ermitteln der MAC-Adresse	121
4.1.2	Ändern der MAC-Adresse	123
4.1.3	Manuelles Setzen und Ändern von MAC-Adressen mittels »arp«	124
4.1.4	ARP-Spoofing erkennen	124
4.2	IP-Adressen setzen	124
4.2.1	Netzwerkconfiguration von PCs	126
4.2.2	IP-Adresskonfiguration von weiteren Netzwerkgeräten	134
4.2.3	Zentrale IP-Adressverwaltung mit dem DHCP-Server	136
4.2.4	Zeroconf	143
4.3	Verwendung von Rechnernamen	143
4.3.1	Der Urtyp: Adressauflösung in der »hosts«-Datei	144
4.3.2	Der Domain Name Server (DNS) und seine Konfiguration	145
4.3.3	Einstellungen beim Client	155
4.4	Überprüfung der Erreichbarkeit und Namensauflösung von Hosts	157
4.4.1	Prüfung der Erreichbarkeit und Namensauflösung mit »ping« bzw. »ping6«	157
4.4.2	Werkzeuge für Nameserver-Abfragen (»nslookup«, »host«, »dig«)	159
4.4.3	Mitschnitte von DNS-Abfragen mit Netzwerkdiagnoseprogrammen ...	162
4.5	Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene	164
4.5.1	Bridges – Verbinden von Netzwerkteilen	164
4.5.2	Hubs – die Sammelschiene für TP-Netze	165

4.6	Switches – Verbindungsknoten ohne Kollisionen	166
4.6.1	Funktionalität	166
4.6.2	Schleifen – Attentat oder Redundanz?	167
4.6.3	Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)	169
4.6.4	Virtuelle Netze (VLAN)	171
4.6.5	Switch und Sicherheit	173
4.6.6	Geräteauswahl	175
4.6.7	Anzeigen und Anschlüsse am Switch	176
4.6.8	Konfiguration eines Switchs allgemein	178
4.6.9	Spanning Tree am Switch aktivieren	178
4.6.10	VLAN-Konfiguration von Switches	179
4.6.11	Konfiguration von Rechnern für tagged VLANs	181
4.7	Routing – Netzwerkgrenzen überschreiten	184
4.7.1	Gemeinsame Nutzung einer IP-Adresse mit PAT	187
4.7.2	Festlegen des Standard-Gateways	187
4.7.3	Routing-Tabelle abfragen (»netstat«)	188
4.7.4	Routenverfolgung mit »traceroute«	189
4.7.5	Route manuell hinzufügen (»route add«)	190
4.7.6	Route löschen (»route«)	192
4.8	Multicast-Routing	193
4.9	Praxisübungen	194
4.9.1	Glasfasern	194
4.9.2	TP-Verkabelung	194
4.9.3	Switches	194
4.9.4	MAC- und IP-Adressen	195
4.9.5	Namensauflösung	195
4.9.6	Routing	195
4.9.7	Sicherheit im lokalen Netz	195

5 Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen 197

5.1	ICMP-Pakete (IPv4)	198
5.2	ICMPv6-Pakete	199

6	Datentransport mit TCP und UDP	203
6.1	Transmission Control Protocol (TCP)	203
6.1.1	Das TCP-Paket	204
6.1.2	TCP: Verbindungsaufbau	206
6.1.3	TCP: Transportkontrolle	207
6.1.4	TCP: Verbindungsabbau	208
6.2	User Datagram Protocol (UDP)	209
6.2.1	UDP: Der UDP-Datagram-Header	210
6.3	Nutzung von Services mittels Ports und Sockets	211
6.3.1	Sockets und deren Schreibweise	212
6.3.2	Übersicht über die Port-Nummern	213
6.3.3	Ports und Sicherheit	215
6.4	Die Firewall	217
6.4.1	Integration der Firewall in das Netzwerk	218
6.4.2	Regeln definieren	220
6.5	Der Proxyserver	224
6.5.1	Lokaler Proxyserver	225
6.5.2	Proxyserver als eigenständiger Netzwerkteilnehmer	225
6.5.3	Squid, ein Proxyserver	226
6.6	Port and Address Translation (PAT), Network Address Translation (NAT)	227
6.7	Praxis	229
6.7.1	Verbindungsaufbau zu einem Dienst mit geänderter Port-Nummer	229
6.7.2	Durchführen von Portscans zum Austesten von Sicherheitsproblemen	230
6.7.3	Schließen von Ports	231
6.8	Prüfungsfragen	232
6.8.1	TCP-Protokoll	232
6.8.2	Ports und Sockets	233
6.8.3	Firewall	233
7	Kommunikation und Sitzung	235
7.1	SMB/CIFS (Datei-, Druck- und Nachrichtendienste)	235
7.1.1	Grundlagen	236
7.1.2	Freigaben von Verzeichnissen und Druckern unter Windows	236

7.1.3	»nmbd« und »smbd« unter Linux/FreeBSD	237
7.1.4	Die Samba-Konfigurationsdatei »smb.conf«	238
7.1.5	Testen der Konfiguration	241
7.1.6	Aufnehmen und Bearbeiten von Samba-Benutzern	242
7.1.7	Starten, Stoppen und Neustart der Samba-Daemons	243
7.1.8	Netzlaufwerk verbinden (Windows 7, 8/8.1 und 10)	243
7.1.9	Client-Zugriffe unter Linux/FreeBSD	244
7.1.10	Zugriffskontrolle mit »smbstatus«	247
7.1.11	Die »net«-Befehle für die Windows-Batchprogrammierung	248
7.2	Network File System (NFS)	249
7.2.1	Konfiguration des NFS-Servers	249
7.2.2	Konfiguration des NFS-Clients	252
7.3	HTTP für die Informationen im Internet	253
7.3.1	Grundlagen des HTTP-Protokolls	253
7.3.2	Serverprogramme	258
7.3.3	Client-Programme	259
7.3.4	Webbrowser und Sicherheit	260
7.4	Mail-Transport	261
7.4.1	Grundlagen des SMTP/ESMTP-Protokolls	261
7.4.2	Konfigurationshinweise	265
7.4.3	Anhänge von E-Mails, MIME, S/MIME	267
7.5	Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS)	271
7.5.1	Secure Shell (SSH)	271
7.5.2	SSL und TLS	272
7.6	Praxisübungen	273
7.6.1	Konfiguration des Samba-Servers	273
7.6.2	NFS-Server	273
7.6.3	HTTP, Sicherheit	274
7.6.4	E-Mail	274

8 Standards für den Datenaustausch 275

9 Netzwerkanwendungen 281

9.1	Datenübertragung	281
9.1.1	File Transfer Protocol (FTP), Server	281
9.1.2	File Transfer Protocol (FTP), Clients	282
9.1.3	Benutzerkommandos für FTP- und SFTP-Sitzungen	284
9.1.4	Datentransfer mit »netread« und »netwrite«	286
9.1.5	Verschlüsselte Datentransfers und Kommandoausgaben mit »cryptcat«	288
9.1.6	Secure Copy (scp), Ersatz für Remote Copy (rcp)	290
9.1.7	SSHFS: entfernte Verzeichnisse lokal nutzen	290
9.2	SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung	292
9.3	Aufbau eines SSH-Tunnels	294
9.4	Fernsitzungen	295
9.4.1	Telnet	295
9.4.2	Secure Shell (SSH), nur Textdarstellung	295
9.4.3	Display-Umleitung für X11-Sitzungen	296
9.4.4	SSH zur Display-Umleitung für X11	297
9.4.5	Virtual Network Computing (VNC)	298
9.4.6	X2Go (Server und Client)	300
9.5	Telefonie-Anwendungen über Netzwerke (VoIP)	305
9.5.1	Grundlagen	305
9.5.2	Endeinrichtungen und ihre Konfiguration	308
9.5.3	Besonderheiten der Netzwerkinfrastruktur für VoIP	310
9.5.4	Sonderfall Fax: T38	310
9.5.5	Sicherheit	311
9.5.6	Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP	312
9.5.7	Remote Desktop Protocol (RDP)	312

10 Netzwerkpraxis 315

10.1	Planung von Netzwerken	315
10.1.1	Bedarf ermitteln	315
10.1.2	Ermitteln des Ist-Zustands	317
10.1.3	Berücksichtigung räumlicher und baulicher Verhältnisse	318

10.1.4	Investitionssicherheit	319
10.1.5	Ausfallsicherheiten vorsehen	319
10.1.6	Zentrales oder verteiltes Switching	320
10.2	Netzwerke mit Kupferkabeln	322
10.2.1	Kabel (Cat. 5 und Cat. 7)	323
10.2.2	Anforderungen an Kabeltrassen und Installationskanäle	323
10.2.3	Dosen und Patchfelder	324
10.3	Netzwerke mit Glasfaserkabeln	326
10.3.1	Kabeltrassen für LWL-Kabel	327
10.3.2	Dosen und Patchfelder	328
10.3.3	Medienkonverter	328
10.3.4	LWL-Multiplexer	329
10.4	Geräte für Netzwerkverbindungen und -dienste	329
10.4.1	Netzwerkkarten	329
10.4.2	WLAN-Router und -Sticks	330
10.4.3	Router	331
10.4.4	Switches	355
10.4.5	Printserver	357
10.4.6	Netzwerkspeicher (NAS)	365
10.4.7	Modems für den Netzzugang	366
10.5	Einbindung externer Netzwerkteilnehmer	368
10.6	Sicherheit	368
10.6.1	Abschottung wichtiger Rechner	369
10.6.2	Netzwerkverbindung mit einem Virtual Private Network (VPN)	371
10.6.3	WLAN sicher konfigurieren	377
10.6.4	SSH-Tunnel mit PuTTY aufbauen	378
10.6.5	Sichere Konfiguration von Printservern	381
10.6.6	Sicherer E-Mail-Verkehr	384
10.6.7	Sicherer Internetzugang mit IPv6	385
10.6.8	Mit Portknocking Brute Force-Angriffe vermeiden	386
10.7	Prüf- und Diagnoseprogramme für Netzwerke	389
10.7.1	Rechtliche Hinweise	389
10.7.2	Verbindungen mit »netstat« anzeigen	389
10.7.3	Hosts und Ports mit »nmap« finden	391
10.7.4	MAC-Adressen-Inventur: netdiscover	394
10.7.5	Datenverkehr protokollieren (Wireshark, tcpdump)	395
10.7.6	Netzaktivitäten mit »darkstat« messen	397

10.7.7	Netzlast mit »fping« erzeugen	399
10.7.8	Weitere Einsatzmöglichkeiten von »fping«	399
10.7.9	Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen	401
10.7.10	»cryptcat«: im Dienste der Sicherheit	402
10.7.11	Weitere Systemabfragen auf Linux-Systemen	405

Anhang 407

A	Fehlertafeln	409
B	Auflösungen zu den Prüfungsfragen	417
C	Netzwerkbegriffe kurz erklärt	423
Index		441