

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	32
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	39
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	52
2.1.9 Kennzeichnen, Suchen und Finden von Kabelverbindungen	56
2.1.10 Power over Ethernet (PoE)	58
2.2 Lichtwellenleiter, Kabel und Verbinder	58
2.2.1 Übersicht über die Netzwerkstandards mit Glasfaserkabel	60
2.2.2 Aufbau und Funktion von Glasfaserkabeln	62
2.2.3 Dauerhafte Glasfaserverbindungen	66

2.2.4	Lichtwellenleiter-Steckverbindungen	66
2.2.5	Umgang mit der LWL-Technik	69
2.2.6	Aufbau eines einfachen Leitungs- und Kabeltesters	72
2.2.7	Prüfen von LWL-Kabeln und -Verbindungen	72
2.3	Datenübertragung per Funktechnik	73
2.3.1	WLAN (Wireless LAN, Wi-Fi)	73
2.3.2	Datenübertragung über öffentliche Funknetze	75
2.3.3	Powerline Communication (PLC)	76
2.4	Technische Anbindung von Rechnern und Netzen	77
2.5	Weitere Netzwerkkomponenten	77
2.6	Zugriffsverfahren	78
2.6.1	CSMA/CD, Kollisionserkennung	78
2.6.2	CSMA/CA, Kollisionsvermeidung	79
2.7	Prüfungsfragen	79

3	Adressierung im Netzwerk – Theorie	81
3.1	Physikalische Adresse (MAC-Adresse)	81
3.2	Ethernet-Pakete (Ethernet-Frames)	83
3.3	Zusammenführung von MAC- und IP-Adresse	84
3.3.1	Address Resolution Protocol (ARP), IPv4	85
3.3.2	Neighbor Discovery Protocol (NDP), IPv6	86
3.4	IP-Adressen	89
3.5	IPv4-Adressen	90
3.5.1	Netzwerkklassen im IPv4	91
3.5.2	Netz- und Subnetzmaske, Unterteilung von Netzen	92
3.5.3	Berechnungen	95
3.5.4	Private Adressen des IPv4	97
3.5.5	Zeroconf – konfigurationsfreie Vernetzung von Rechnern	98
3.5.6	Localnet und Localhost	99
3.5.7	Weitere reservierte Adressen	100
3.6	IPv6-Adressen	101
3.6.1	Adressarten des IPv6	104

3.6.2	IPv6-Loopback-Adresse	107
3.6.3	Unspezifizierte Adresse	108
3.6.4	IPv4- in IPv6-Adressen und umgekehrt	108
3.6.5	Tunnel-Adressen	109
3.6.6	Kryptografisch erzeugte Adressen (CGA)	110
3.6.7	Lokale Adressen	111
3.6.8	Übersicht der Präfixe von IPv6-Adressen	111
3.6.9	Adresswahl und -benutzung	112
3.7	Internetprotokoll	113
3.7.1	Der IPv4-Header	114
3.7.2	Der IPv6-Header	116
3.8	Prüfungsfragen	118
3.8.1	Berechnungen	118
3.8.2	IP-Adressen	118

4 MAC- und IP-Adressen in der Praxis

4.1	MAC-Adressen	119
4.1.1	Ermitteln der MAC-Adresse	119
4.1.2	Ändern der MAC-Adresse	121
4.1.3	Manuelles Setzen und Ändern von MAC-Adressen mittels »arp«	122
4.1.4	ARP-Spoofing erkennen	122
4.2	IP-Adressen setzen	123
4.2.1	Netzwerkkonfiguration von PCs	125
4.2.2	IP-Adresskonfiguration von weiteren Netzwerkgeräten	133
4.2.3	Zentrale IP-Adressverwaltung mit dem DHCP-Server	135
4.2.4	Zeroconf	142
4.3	Verwendung von Rechnernamen	143
4.3.1	Der Urtyp: Adressauflösung in der »hosts«-Datei	143
4.3.2	Der Domain Name Server (DNS) und seine Konfiguration	144
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 Netzwerk-diagnoseprogrammen	161
4.5	Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene	163
4.5.1	Bridges – Verbinden von Netzwerkteilen	163
4.5.2	Hubs – die Sammelschiene für TP-Netze	164
4.6	Switches – Verbindungsknoten ohne Kollisionen	165
4.6.1	Funktionalität	165
4.6.2	Schleifen – Attentat oder Redundanz?	166
4.6.3	Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)	169
4.6.4	Virtuelle Netze (VLAN)	170
4.6.5	Switch und Sicherheit	173
4.6.6	Geräteauswahl	174
4.6.7	Anzeigen und Anschlüsse am Switch	176
4.6.8	Konfiguration eines Switchs allgemein	177
4.6.9	Spanning Tree am Switch aktivieren	177
4.6.10	VLAN-Konfiguration von Switches	179
4.6.11	Konfiguration von Rechnern für tagged VLANs	180
4.7	Routing – Netzwerkgrenzen überschreiten	184
4.7.1	Gemeinsame Nutzung einer IP-Adresse mit PAT	187
4.7.2	Festlegen des Standardgateways	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	195
4.9.3	Switches	195
4.9.4	MAC- und IP-Adressen	195
4.9.5	Namensauflösung	195
4.9.6	Routing	196
4.9.7	Sicherheit im lokalen Netz	196

5 Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen

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

6 Datentransport mit TCP und UDP

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	218
6.4.1	Integration der Firewall in das Netzwerk	219
6.4.2	Regeln definieren	221
6.5	Der Proxyserver	225
6.5.1	Lokaler Proxyserver	226
6.5.2	Proxyserver als eigenständiger Netzwerkteilnehmer	226
6.5.3	Squid, ein Proxyserver	227
6.6	Port and Address Translation (PAT), Network Address Translation (NAT)	228
6.7	Praxis	230
6.7.1	Verbindungsaufbau zu einem Dienst mit geänderter Port-Nummer	230
6.7.2	Durchführen von Portscans zum Austesten von Sicherheitsproblemen	231
6.7.3	Schließen von Ports	232

6.8 Prüfungsfragen	233
6.8.1 TCP-Protokoll	234
6.8.2 Ports und Sockets	234
6.8.3 Firewall	234

7 Kommunikation und Sitzung

7.1 SMB/CIFS (Datei-, Druck- und Nachrichtendienste)	235
7.1.1 Grundlagen	236
7.1.2 Freigaben von Verzeichnissen und Drucken unter Windows	236
7.1.3 »nmbd« und »smbd« unter Linux/FreeBSD	238
7.1.4 Die Samba-Konfigurationsdatei »smb.conf«	238
7.1.5 Testen der Konfiguration	242
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 und 8/8.1)	244
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	274
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 Secure Copy (scp), Ersatz für Remote Copy (rcp)	286
9.1.5 SSHFS: entfernte Verzeichnisse lokal nutzen	287
9.2 SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung	288
9.3 Aufbau eines SSH-Tunnels	290
9.4 Fernsitzungen	291
9.4.1 Telnet	291
9.4.2 Secure Shell (SSH), nur Textdarstellung	292
9.4.3 Display-Umleitung für X11-Sitzungen	293
9.4.4 SSH zur Display-Umleitung für X11	293
9.4.5 Virtual Network Computing (VNC)	294
9.4.6 X2Go (Server und Client)	297
9.4.7 Remote Desktop Protocol (RDP)	309

10 Netzwerkpraxis 311

10.1 Planung von Netzwerken	311
10.1.1 Bedarf ermitteln	311

10.1.2	Ermitteln des Ist-Zustands	313
10.1.3	Berücksichtigung räumlicher und baulicher Verhältnisse	314
10.1.4	Investitionssicherheit	315
10.1.5	Ausfallsicherheiten vorsehen	315
10.1.6	Zentrales oder verteiltes Switching	316
10.2	Netzwerke mit Kupferkabeln	318
10.2.1	Kabel (Cat. 5 und Cat. 7)	319
10.2.2	Anforderungen an Kabeltrassen und Installationskanäle	319
10.2.3	Dosen und Patchfelder	320
10.3	Netzwerke mit Glasfaserkabeln	322
10.3.1	Kabeltrassen für LWL-Kabel	323
10.3.2	Dosen- und Patchfelder	324
10.3.3	Medienkonverter	324
10.3.4	LWL-Multiplexer	325
10.4	Geräte für Netzwerkverbindungen und -dienste	325
10.4.1	Netzwerkkarten	326
10.4.2	WLAN-Router und -Sticks	326
10.4.3	Router	327
10.4.4	Switches	347
10.4.5	Printserver	349
10.4.6	Netzwerkspeicher (NAS)	351
10.4.7	Modems für den Netzzugang	351
10.5	Einbindung externer Netzwerkeinnehmer	354
10.6	Sicherheit	355
10.6.1	Abschottung wichtiger Rechner	356
10.6.2	Netzwerkverbindung mit einem Virtual Private Network (VPN)	358
10.6.3	WLAN sicher konfigurieren	364
10.6.4	SSH-Tunnel mit PuTTY aufbauen	365
10.6.5	Sichere Konfiguration von Printservern	368
10.6.6	Sicherer E-Mail-Verkehr	371
10.6.7	Sicherer Internetzugang mit IPv6	372
10.7	Prüf- und Diagnoseprogramme für Netzwerke	373
10.7.1	Rechtliche Hinweise	373
10.7.2	Verbindungen mit »netstat« anzeigen	374
10.7.3	Hosts und Ports mit »nmap« finden	375
10.7.4	Datenverkehr protokollieren (Wireshark, tcpdump)	378

10.7.5	Netzaktivitäten mit »darkstat« messen	381
10.7.6	Netzlast mit »fping« erzeugen	383
10.7.7	Weitere Einsatzmöglichkeiten von »fping«	383
10.7.8	Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen	386
Anhang		387
A	Fehlertafeln	389
B	Auflösungen zu den Prüfungsfragen	397
C	Netzwerkbeigriffe kurz erklärt	403
Index		419