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 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 ... 84
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 ... 90
3.5.2 Netz- und Subnetzmaske, Unterteilung von Netzen ... 91
3.5.3 Berechnungen ... 95
3.5.4 Private Adressen des IPv4 ... 96
3.5.5 Zeroconf – konfigurationsfreie Vernetzung von Rechnern ... 97
3.5.6 Localnet und Localhost ... 98
3.5.7 Weitere reservierte Adressen ... 99

3.6 IPv6-Adressen ... 100
3.6.1 Adresstypen des IPv6 ... 102
3.6.2 IPv6-Loopback-Adresse ... 105
3.6.3 Unspezifizierte Adresse ... 106
3.6.4 IPv4- in IPv6-Adressen und umgekehrt ... 106

3.6.5 Tunnel-Adressen ... 107
3.6.6 Kryptografisch erzeugte Adressen (CGA) ... 109
3.6.7 Lokale Adressen ... 109
3.6.8 Übersicht der Präfixe von IPv6-Adressen ... 110
3.6.9 Adresswahl und -benutzung ... 110

3.7 Internetprotokoll ... 111
3.7.1 Der IPv4-Header ... 112
3.7.2 Der IPv6-Header ... 114

3.8 Prüfungsfragen ... 116
3.8.1 Berechnungen ... 116
3.8.2 IP-Adressen ... 116

4 MAC- und IP-Adressen in der Praxis 117

4.1 MAC-Adressen ... 117
4.1.1 Ermitteln der MAC-Adresse ... 117
4.1.2 Ändern der MAC-Adresse ... 119
4.1.3 Manuelles Setzen und Ändern von MAC-Adressen mittels »arp« ... 120
4.1.4 ARP-Spoofing erkennen ... 120

4.2 IP-Adressen setzen ... 120
4.2.1 Netzwerkkonfiguration von PCs ... 122
4.2.2 IP-Adresskonfiguration von weiteren Netzwerkgeräten ... 130
4.2.3 Zentrale IP-Adressverwaltung mit dem DHCP-Server ... 132
4.2.4 Zeroconf ... 139

4.3 Verwendung von Rechnernamen ... 139
4.3.1 Der Urtyp: Adressauflösung in der »hosts«-Datei ... 140
4.3.2 Der Domain Name Server (DNS) und seine Konfiguration ... 141
4.3.3 Einstellungen beim Client ... 151

4.4 Überprüfung der Erreichbarkeit und Namensauflösung von Hosts ... 153
4.4.1 Prüfung der Erreichbarkeit und Namensauflösung mit »ping« bzw. »ping6« ... 153
4.4.2 Werkzeuge für Nameserver-Abfragen (»nslookup«, »host«, »dig«) ... 155
4.4.3 Mitschnitte von DNS-Abfragen mit Netzwerkdiagnoseprogrammen ... 158

4.5 Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene ... 160
4.5.1 Bridges – Verbinden von Netzwerkteilen ... 160
4.5.2 Hubs – die Sammelschiene für TP-Netze ... 161

4.6 Switches – Verbindungsknoten ohne Kollisionen ... 162
4.6.1 Funktionalität ... 162
4.6.2 Schleifen – Attentat oder Redundanz? ... 163
4.6.3 Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling) ... 165
4.6.4 Virtuelle Netze (VLAN) ... 167
4.6.5 Switch und Sicherheit ... 169
4.6.6 Geräteauswahl ... 171
4.6.7 Anzeigen und Anschlüsse am Switch ... 172
4.6.8 Konfiguration eines Switchs allgemein ... 174
4.6.9 Spanning Tree am Switch aktivieren ... 174
4.6.10 VLAN-Konfiguration von Switches ... 175
4.6.11 Konfiguration von Rechnern für tagged VLANs ... 177

4.7 Routing – Netzwerkgrenzen überschreiten ... 180
4.7.1 Gemeinsame Nutzung einer IP-Adresse mit PAT ... 183
4.7.2 Festlegen des Standard-Gateways ... 183
4.7.3 Routing-Tabelle abfragen (»netstat«) ... 184
4.7.4 Routenverfolgung mit »traceroute« ... 185
4.7.5 Route manuell hinzufügen (»route add«) ... 186
4.7.6 Route löschen (»route«) ... 188

4.8 Multicast-Routing ... 189

4.9 Praxisübungen ... 190
4.9.1 Glasfasern ... 190
4.9.2 TP-Verkabelung ... 190
4.9.3 Switches ... 190
4.9.4 MAC- und IP-Adressen ... 191
4.9.5 Namensauflösung ... 191
4.9.6 Routing ... 191
4.9.7 Sicherheit im lokalen Netz ... 191

5 Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen ... 193

5.1 ICMP-Pakete (IPv4) ... 194

5.2 ICMPv6-Pakete ... 195

6 Datentransport mit TCP und UDP 199

6.1 Transmission Control Protocol (TCP) ... 199
6.1.1 Das TCP-Paket ... 200
6.1.2 TCP: Verbindungsaufbau ... 202
6.1.3 TCP: Transportkontrolle ... 203
6.1.4 TCP: Verbindungsabbau ... 204

6.2 User Datagram Protocol (UDP) ... 205
6.2.1 UDP: Der UDP-Datagram-Header ... 206

6.3 Nutzung von Services mittels Ports und Sockets ... 207
6.3.1 Sockets und deren Schreibweise ... 208
6.3.2 Übersicht über die Port-Nummern ... 209
6.3.3 Ports und Sicherheit ... 211

6.4 Die Firewall ... 213
6.4.1 Integration der Firewall in das Netzwerk ... 214
6.4.2 Regeln definieren ... 216

6.5 Der Proxyserver ... 220
6.5.1 Lokaler Proxyserver ... 221
6.5.2 Proxyserver als eigenständiger Netzwerkteilnehmer ... 221
6.5.3 Squid, ein Proxyserver ... 222

6.6 Port and Address Translation (PAT), Network Address Translation (NAT) ... 223

6.7 Praxis ... 225
6.7.1 Verbindungsaufbau zu einem Dienst mit geänderter Port-Nummer ... 225
6.7.2 Durchführen von Portscans zum Austesten von Sicherheitsproblemen 226
6.7.3 Schließen von Ports ... 227

6.8 Prüfungsfragen ... 228
6.8.1 TCP-Protokoll ... 228
6.8.2 Ports und Sockets ... 229
6.8.3 Firewall ... 229

7 Kommunikation und Sitzung 231

7.1 SMB/CIFS (Datei-, Druck- und Nachrichtendienste) ... 231
7.1.1 Grundlagen ... 232
7.1.2 Freigaben von Verzeichnissen und Druckern unter Windows ... 232

7.1.3 »nmbd« und »smbd« unter Linux/FreeBSD ... 233
7.1.4 Die Samba-Konfigurationsdatei »smb.conf« ... 234
7.1.5 Testen der Konfiguration ... 237
7.1.6 Aufnehmen und Bearbeiten von Samba-Benutzern ... 238
7.1.7 Starten, Stoppen und Neustart der Samba-Daemons ... 239
7.1.8 Netzlaufwerk verbinden (Windows 7, 8/8.1 und 10) ... 239
7.1.9 Client-Zugriffe unter Linux/FreeBSD ... 240
7.1.10 Zugriffskontrolle mit »smbstatus« ... 243
7.1.11 Die »net«-Befehle für die Windows-Batchprogrammierung ... 244

7.2 Network File System (NFS) ... 245
7.2.1 Konfiguration des NFS-Servers ... 245
7.2.2 Konfiguration des NFS-Clients ... 248

7.3 HTTP für die Informationen im Internet ... 249
7.3.1 Grundlagen des HTTP-Protokolls ... 249
7.3.2 Serverprogramme ... 254
7.3.3 Client-Programme ... 255
7.3.4 Webbrowser und Sicherheit ... 256

7.4 Mail-Transport ... 257
7.4.1 Grundlagen des SMTP/ESMTP-Protokolls ... 257
7.4.2 Konfigurationshinweise ... 261
7.4.3 Anhänge von E-Mails, MIME, S/MIME ... 263

7.5 Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS) ... 267
7.5.1 Secure Shell (SSH) ... 267
7.5.2 SSL und TLS ... 268

7.6 Praxisübungen ... 269
7.6.1 Konfiguration des Samba-Servers ... 269
7.6.2 NFS-Server ... 269
7.6.3 HTTP, Sicherheit ... 270
7.6.4 E-Mail ... 270

8 Standards für den Datenaustausch 271

9 Netzwerkanwendungen 277

9.1 Datenübertragung ... 277
9.1.1 File Transfer Protocol (FTP), Server ... 277
9.1.2 File Transfer Protocol (FTP), Clients ... 278
9.1.3 Benutzerkommandos für FTP- und SFTP-Sitzungen ... 280
9.1.4 Datentransfer mit »netread« und »netwrite« ... 282
9.1.5 Verschlüsselte Datentransfers und Kommandoausgaben mit »cryptcat« ... 284
9.1.6 Secure Copy (scp), Ersatz für Remote Copy (rcp) ... 286
9.1.7 SSHFS: entfernte Verzeichnisse lokal nutzen ... 286

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 ... 291
9.4.3 Display-Umleitung für X11-Sitzungen ... 292
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) ... 296

9.5 Telefonie-Anwendungen über Netzwerke (VoIP) ... 308
9.5.1 Grundlagen ... 308
9.5.2 Endeinrichtungen und ihre Konfiguration ... 312
9.5.3 Besonderheiten der Netzwerkinfrastruktur für VoIP ... 313
9.5.4 Sonderfall Fax: T38 ... 314
9.5.5 Sicherheit ... 314
9.5.6 Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP ... 315
9.5.7 Remote Desktop Protocol (RDP) ... 316

10 Netzwerkpraxis 317

10.1 Planung von Netzwerken ... 317
10.1.1 Bedarf ermitteln ... 317
10.1.2 Ermitteln des Ist-Zustands ... 319
10.1.3 Berücksichtigung räumlicher und baulicher Verhältnisse ... 320

10.1.4 Investitionssicherheit ... 321
10.1.5 Ausfallsicherheiten vorsehen ... 321
10.1.6 Zentrales oder verteiltes Switching ... 322

10.2 Netzwerke mit Kupferkabeln ... 324
10.2.1 Kabel (Cat. 5 und Cat. 7) ... 325
10.2.2 Anforderungen an Kabeltrassen und Installationskanäle ... 325
10.2.3 Dosen und Patchfelder ... 326

10.3 Netzwerke mit Glasfaserkabeln ... 328
10.3.1 Kabeltrassen für LWL-Kabel ... 329
10.3.2 Dosen und Patchfelder ... 330
10.3.3 Medienkonverter ... 330
10.3.4 LWL-Multiplexer ... 331

10.4 Geräte für Netzwerkverbindungen und -dienste ... 331
10.4.1 Netzwerkkarten ... 331
10.4.2 WLAN-Router und -Sticks ... 332
10.4.3 Router ... 333
10.4.4 Switches ... 357
10.4.5 Printserver ... 358
10.4.6 Netzwerkspeicher (NAS) ... 366
10.4.7 Modems für den Netzzugang ... 367

10.5 Einbindung externer Netzwerkteilnehmer ... 369

10.6 Sicherheit ... 369
10.6.1 Abschottung wichtiger Rechner ... 370
10.6.2 Netzwerkverbindung mit einem Virtual Private Network (VPN) ... 372
10.6.3 WLAN sicher konfigurieren ... 378
10.6.4 SSH-Tunnel mit PuTTy aufbauen ... 379
10.6.5 Sichere Konfiguration von Printservern ... 382
10.6.6 Sicherer E-Mail-Verkehr ... 385
10.6.7 Sicherer Internetzugang mit IPv6 ... 386
10.6.8 Mit Portknocking Brute Force-Angriffe vermeiden ... 387

10.7 Prüf- und Diagnoseprogramme für Netzwerke ... 390
10.7.1 Rechtliche Hinweise ... 390
10.7.2 Verbindungen mit »netstat« anzeigen ... 390
10.7.3 Hosts und Ports mit »nmap« finden ... 392
10.7.4 MAC-Adressen-Inventur: netdiscover ... 395
10.7.5 Datenverkehr protokollieren (Wireshark, tcpdump) ... 396
10.7.6 Netzaktivitäten mit »darkstat« messen ... 398

10.7.7 Netzlast mit »fping« erzeugen 400
10.7.8 Weitere Einsatzmöglichkeiten von »fping« 400
10.7.9 Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen 402
10.7.10 »cryptcat«: im Dienste der Sicherheit 403
10.7.11 Weitere Systemabfragen auf Linux-Systemen 406

Anhang 409

A Fehlertafeln 409

B Auflösungen zu den Prüfungsfragen 417

C Netzwerkbegriffe kurz erklärt 423

Index 441