

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	72
2.2.6	Aufbau eines einfachen Leitungs- und Kabeltesters	75
2.2.7	Prüfen von LWL-Kabeln und -Verbindungen	76
2.3	Datenübertragung per Funktechnik	76
2.3.1	WLAN (Wireless LAN, Wi-Fi)	77
2.3.2	Datenübertragung über öffentliche Funknetze	79
2.3.3	Powerline Communication (PLC)	80
2.4	Technische Anbindung von Rechnern und Netzen	81
2.5	Weitere Netzwerkkomponenten	81
2.6	Zugriffsverfahren	82
2.6.1	CSMA/CD, Kollisionserkennung	82
2.6.2	CSMA/CA, Kollisionsvermeidung	82
2.7	Prüfungsfragen	83
3	Adressierung im Netzwerk – Theorie	85
<hr/>		
3.1	Physikalische Adresse (MAC-Adresse)	85
3.2	Ethernet-Pakete (Ethernet-Frames)	87
3.3	Zusammenführung von MAC- und IP-Adresse	88
3.3.1	Address Resolution Protocol (ARP), IPv4	88
3.3.2	Neighbor Discovery Protocol (NDP), IPv6	90
3.4	IP-Adressen	93
3.5	IPv4-Adressen	94
3.5.1	Netzwerkklassen im IPv4	94
3.5.2	Netz- und Subnetzmaske, Unterteilung von Netzen	95
3.5.3	Berechnungen	99
3.5.4	Private Adressen des IPv4	102
3.5.5	Zeroconf – konfigurationsfreie Vernetzung von Rechnern	102
3.5.6	Localnet und Localhost	103
3.5.7	Weitere reservierte Adressen	104
3.6	IPv6-Adressen	105
3.6.1	Adresstypen des IPv6	107
3.6.2	IPv6-Loopback-Adresse	110
3.6.3	Unspezifizierte Adresse	111
3.6.4	IPv4- in IPv6-Adressen und umgekehrt	111

3.6.5	Tunnel-Adressen	112
3.6.6	Kryptografisch erzeugte Adressen (CGA)	114
3.6.7	Lokale Adressen	114
3.6.8	Übersicht der Präfixe von IPv6-Adressen	115
3.6.9	Adresswahl und -benutzung	115
3.7	Internetprotokoll	116
3.7.1	Der IPv4-Header	117
3.7.2	Der IPv6-Header	119
3.8	Prüfungsfragen	121
3.8.1	Berechnungen	121
3.8.2	IP-Adressen	121
4	MAC- und IP-Adressen in der Praxis	123
4.1	MAC-Adressen	123
4.1.1	Ermitteln der MAC-Adresse	123
4.1.2	Ändern der MAC-Adresse	125
4.1.3	Manuelles Setzen und Ändern von MAC-Adressen mittels »arp«	126
4.1.4	ARP-Spoofing erkennen	126
4.2	IP-Adressen setzen	126
4.2.1	Netzwerkconfiguration von PCs	128
4.2.2	IP-Adressconfiguration von weiteren Netzwerkgeräten	136
4.2.3	Zentrale IP-Adressverwaltung mit dem DHCP-Server	138
4.2.4	Zeroconf	145
4.3	Verwendung von Rechnernamen	145
4.3.1	Der Urtyp: Adressauflösung in der »hosts«-Datei	146
4.3.2	Der Domain Name Server (DNS) und seine Konfiguration	147
4.3.3	Einstellungen beim Client	157
4.4	Überprüfung der Erreichbarkeit und Namensauflösung von Hosts	159
4.4.1	Prüfung der Erreichbarkeit und Namensauflösung mit »ping« bzw. »ping6«	159
4.4.2	Werkzeuge für Nameserver-Abfragen (»nslookup«, »host«, »dig«)	161
4.4.3	Mitschnitte von DNS-Abfragen mit Netzwerkdiagnoseprogrammen ...	164
4.5	Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene	166
4.5.1	Bridges – Verbinden von Netzwerkteilen	166
4.5.2	Hubs – die Sammelschiene für TP-Netze	167

4.6	Switches – Verbindungsknoten ohne Kollisionen	168
4.6.1	Funktionalität	168
4.6.2	Schleifen – Attentat oder Redundanz?	169
4.6.3	Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)	171
4.6.4	Virtuelle Netze (VLAN)	173
4.6.5	Switch und Sicherheit	175
4.6.6	Geräteauswahl	177
4.6.7	Anzeigen und Anschlüsse am Switch	178
4.6.8	Konfiguration eines Switchs allgemein	180
4.6.9	Spanning Tree am Switch aktivieren	180
4.6.10	VLAN-Konfiguration von Switches	181
4.6.11	Konfiguration von Rechnern für tagged VLANs	183
4.7	Routing – Netzwerkgrenzen überschreiten	186
4.7.1	Gemeinsame Nutzung einer IP-Adresse mit PAT	189
4.7.2	Festlegen des Standard-Gateways	189
4.7.3	Routing-Tabelle abfragen (»netstat«)	190
4.7.4	Routenverfolgung mit »traceroute«	191
4.7.5	Route manuell hinzufügen (»route add«)	192
4.7.6	Route löschen (»route«)	194
4.8	Multicast-Routing	195
4.9	Praxisübungen	196
4.9.1	Glasfasern	196
4.9.2	TP-Verkabelung	196
4.9.3	Switches	196
4.9.4	MAC- und IP-Adressen	197
4.9.5	Namensauflösung	197
4.9.6	Routing	197
4.9.7	Sicherheit im lokalen Netz	197

5 Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen 199

5.1	ICMP-Pakete (IPv4)	200
5.2	ICMPv6-Pakete	201

6	Datentransport mit TCP und UDP	205
6.1	Transmission Control Protocol (TCP)	205
6.1.1	Das TCP-Paket	206
6.1.2	TCP: Verbindungsaufbau	208
6.1.3	TCP: Transportkontrolle	209
6.1.4	TCP: Verbindungsabbau	210
6.2	User Datagram Protocol (UDP)	211
6.2.1	UDP: Der UDP-Datagram-Header	212
6.3	QUIC	213
6.4	Nutzung von Services mittels Ports und Sockets	213
6.4.1	Sockets und deren Schreibweise	215
6.4.2	Übersicht über die Port-Nummern	215
6.4.3	Ports und Sicherheit	217
6.5	Die Firewall	220
6.5.1	Integration der Firewall in das Netzwerk	221
6.5.2	Regeln definieren	223
6.6	Der Proxyserver	226
6.6.1	Lokaler Proxyserver	227
6.6.2	Proxyserver als eigenständiger Netzwerkteilnehmer	228
6.6.3	Squid, ein Proxyserver	229
6.7	Port and Address Translation (PAT), Network Address Translation (NAT)	229
6.8	Praxis	231
6.8.1	Verbindungsaufbau zu einem Dienst mit geänderter Port-Nummer	231
6.8.2	Durchführen von Portscans zum Austesten von Sicherheitsproblemen	232
6.8.3	Schließen von Ports	234
6.9	Prüfungsfragen	235
6.9.1	TCP-Protokoll	235
6.9.2	Ports und Sockets	235
6.9.3	Firewall	235
7	Kommunikation und Sitzung	237
7.1	SMB/CIFS (Datei-, Druck- und Nachrichtendienste)	237
7.1.1	Grundlagen	238

7.1.2	Freigaben von Verzeichnissen und Druckern unter Windows	238
7.1.3	»nmbd« und »smbd« unter Linux/FreeBSD	239
7.1.4	Die Samba-Konfigurationsdatei »smb.conf«	240
7.1.5	Testen der Konfiguration	243
7.1.6	Aufnehmen und Bearbeiten von Samba-Benutzern	244
7.1.7	Starten, Stoppen und Neustart der Samba-Daemons	245
7.1.8	Netzlaufwerk verbinden (Windows 7, 8/8.1 und 10)	245
7.1.9	Client-Zugriffe unter Linux/FreeBSD	246
7.1.10	Zugriffskontrolle mit »smbstatus«	249
7.1.11	Die »net«-Befehle für die Windows-Batchprogrammierung	250
7.2	Network File System (NFS)	251
7.2.1	Konfiguration des NFS-Servers	251
7.2.2	Konfiguration des NFS-Clients	254
7.3	HTTP für die Informationen im Internet	255
7.3.1	Grundlagen des HTTP-Protokolls	255
7.3.2	Serverprogramme	261
7.3.3	Client-Programme	262
7.3.4	Webbrowser und Sicherheit	263
7.4	Mail-Transport	264
7.4.1	Grundlagen des SMTP/ESMTP-Protokolls	264
7.4.2	Konfigurationshinweise	268
7.4.3	Anhänge von E-Mails, MIME, S/MIME	270
7.5	Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS)	274
7.5.1	Secure Shell (SSH)	274
7.5.2	SSL und TLS	275
7.6	Praxisübungen	276
7.6.1	Konfiguration des Samba-Servers	276
7.6.2	NFS-Server	277
7.6.3	HTTP, Sicherheit	277
7.6.4	E-Mail	277
8	Standards für den Datenaustausch	279

9 Netzwerkanwendungen 285

9.1	Datenübertragung	285
9.1.1	File Transfer Protocol (FTP), Server	285
9.1.2	File Transfer Protocol (FTP), Clients	286
9.1.3	Benutzerkommandos für FTP- und SFTP-Sitzungen	288
9.1.4	Datentransfer mit »netread« und »netwrite«	290
9.1.5	Verschlüsselte Datentransfers und Kommandoausgaben mit »cryptcat«	292
9.1.6	Secure Copy (scp), Ersatz für Remote Copy (rcp)	294
9.1.7	SSHFS: entfernte Verzeichnisse lokal nutzen	294
9.2	SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung	296
9.3	Aufbau eines SSH-Tunnels	298
9.4	Fernsitzungen	299
9.4.1	Telnet	299
9.4.2	Secure Shell (SSH), nur Textdarstellung	299
9.4.3	Display-Umleitung für X11-Sitzungen	300
9.4.4	SSH zur Display-Umleitung für X11	301
9.4.5	Virtual Network Computing (VNC)	302
9.4.6	X2Go (Server und Client)	304
9.5	Telefonie-Anwendungen über Netzwerke (VoIP)	309
9.5.1	Grundlagen	309
9.5.2	Endeinrichtungen und ihre Konfiguration	312
9.5.3	Besonderheiten der Netzwerkinfrastruktur für VoIP	314
9.5.4	Sonderfall Fax: T38	314
9.5.5	Sicherheit	315
9.5.6	Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP	316
9.5.7	Remote Desktop Protocol (RDP)	316

10 Netzwerkpraxis 319

10.1	Planung von Netzwerken	319
10.1.1	Bedarf ermitteln	319
10.1.2	Ermitteln des Ist-Zustands	321
10.1.3	Berücksichtigung räumlicher und baulicher Verhältnisse	322

10.1.4	Investitionssicherheit	323
10.1.5	Ausfallsicherheiten vorsehen	323
10.1.6	Zentrales oder verteiltes Switching	324
10.2	Netzwerke mit Kupferkabeln	326
10.2.1	Kabel (Cat. 5 und Cat. 7)	327
10.2.2	Anforderungen an Kabeltrassen und Installationskanäle	327
10.2.3	Dosen und Patchfelder	328
10.3	Netzwerke mit Glasfaserkabeln	330
10.3.1	Kabeltrassen für LWL-Kabel	331
10.3.2	Dosen und Patchfelder	332
10.3.3	Medienkonverter	332
10.3.4	LWL-Multiplexer	333
10.4	Geräte für Netzwerkverbindungen und -dienste	333
10.4.1	Netzwerkkarten	333
10.4.2	WLAN-Router und -Sticks	334
10.4.3	Router	335
10.4.4	Switches	353
10.4.5	Printserver	356
10.4.6	Netzwerkspeicher (NAS)	364
10.4.7	Modems für den Netzzugang	365
10.5	Einbindung externer Netzwerkteilnehmer	366
10.6	Sicherheit	367
10.6.1	Abschottung wichtiger Rechner	368
10.6.2	Netzwerkverbindung mit einem Virtual Private Network (VPN)	370
10.6.3	WLAN sicher konfigurieren	376
10.6.4	SSH-Tunnel mit PuTTY aufbauen	377
10.6.5	Sichere Konfiguration von Printservern	380
10.6.6	Sicherer E-Mail-Verkehr	383
10.6.7	Sicherer Internetzugang mit IPv6	384
10.6.8	Mit Portknocking Brute Force-Angriffe vermeiden	385
10.7	Prüf- und Diagnoseprogramme für Netzwerke	388
10.7.1	Rechtliche Hinweise	388
10.7.2	Verbindungen mit »netstat« anzeigen	388
10.7.3	Hosts und Ports mit »nmap« finden	390
10.7.4	MAC-Adressen-Inventur: netdiscover	393
10.7.5	Datenverkehr protokollieren (Wireshark, tcpdump)	394
10.7.6	Netzaktivitäten mit »darkstat« messen	396

10.7.7	Netzlast mit »fping« erzeugen	398
10.7.8	Weitere Einsatzmöglichkeiten von »fping«	398
10.7.9	Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen	400
10.7.10	»cryptcat«: im Dienste der Sicherheit	401
10.7.11	Weitere Systemabfragen auf Linux-Systemen	404

Anhang 407

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