

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	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	65
2.2.4	Lichtwellenleiter-Steckverbindungen	66

2.2.5	Umgang mit der LWL-Technik	69
2.2.6	Aufbau eines einfachen Leitungs- und Kabeltesters	71
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)	75
2.4	Technische Anbindung von Rechnern und Netzen	76
2.5	Weitere Netzwerkkomponenten	77
2.6	Zugriffsverfahren	78
2.6.1	CSMA/CD, Kollisionserkennung	78
2.6.2	CSMA/CA, Kollisionsvermeidung	78
2.7	Prüfungsfragen	78

3 Adressierung im Netzwerk – Theorie 79

3.1	Physikalische Adresse (MAC-Adresse)	79
3.2	Ethernet-Pakete (Ethernet-Frames)	81
3.3	Zusammenführung von MAC- und IP-Adresse	82
3.3.1	Address Resolution Protocol (ARP), IPv4	82
3.3.2	Neighbor Discovery Protocol (NDP), IPv6	84
3.4	IP-Adressen	87
3.5	IPv4-Adressen	88
3.5.1	Netzwerkklassen im IPv4	88
3.5.2	Netz- und Subnetzmaske, Unterteilung von Netzen	89
3.5.3	Berechnungen	92
3.5.4	Private Adressen des IPv4	94
3.5.5	Zeroconf – konfigurationsfreie Vernetzung von Rechnern	95
3.5.6	Localnet und Localhost	96
3.5.7	Weitere reservierte Adressen	97
3.6	IPv6-Adressen	98
3.6.1	Adresstypen des IPv6	100
3.6.2	IPv6-Loopback-Adresse	103
3.6.3	Unspezifizierte Adresse	104

3.6.4	IPv4- in IPv6-Adressen und umgekehrt	104
3.6.5	Tunnel-Adressen	105
3.6.6	Kryptografisch erzeugte Adressen (CGA)	107
3.6.7	Lokale Adressen	107
3.6.8	Übersicht der Präfixe von IPv6-Adressen	107
3.6.9	Adresswahl und -benutzung	108
3.7	Internetprotokoll	109
3.7.1	Der IPv4-Header	110
3.7.2	Der IPv6-Header	112
3.8	Prüfungsfragen	114
3.8.1	Berechnungen	114
3.8.2	IP-Adressen	114
4	MAC- und IP-Adressen in der Praxis	115
4.1	MAC-Adressen	115
4.1.1	Ermitteln der MAC-Adresse	115
4.1.2	Ändern der MAC-Adresse	117
4.1.3	Manuelles Setzen und Ändern von MAC-Adressen mittels »arp«	118
4.1.4	ARP-Spoofing erkennen	118
4.2	IP-Adressen setzen	118
4.2.1	Netzwerkkonfiguration von PCs	120
4.2.2	IP-Adresskonfiguration von weiteren Netzwerkgeräten	128
4.2.3	Zentrale IP-Adressverwaltung mit dem DHCP-Server	130
4.2.4	Zeroconf	137
4.3	Verwendung von Rechnernamen	137
4.3.1	Der Urtyp: Adressauflösung in der »hosts«-Datei	138
4.3.2	Der Domain Name Server (DNS) und seine Konfiguration	139
4.3.3	Einstellungen beim Client	149
4.4	Überprüfung der Erreichbarkeit und Namensauflösung von Hosts	151
4.4.1	Prüfung der Erreichbarkeit und Namensauflösung mit »ping« bzw. »ping6«	151
4.4.2	Werkzeuge für Nameserver-Abfragen (»nslookup«, »host«, »dig«)	153
4.4.3	Mitschnitte von DNS-Abfragen mit Netzwerkdiagnose- programmen	155

4.5	Zentrale Netzwerkgeräte auf Sicherungs- und Vermittlungsebene	157
4.5.1	Bridges – Verbinden von Netzwerkteilen	157
4.5.2	Hubs – die Sammelschiene für TP-Netze	158
4.6	Switches – Verbindungsknoten ohne Kollisionen	159
4.6.1	Funktionalität	159
4.6.2	Schleifen – Attentat oder Redundanz?	160
4.6.3	Verbindungen zwischen Switches (Link Aggregation, Port Trunking, Channel Bundling)	162
4.6.4	Virtuelle Netze (VLAN)	164
4.6.5	Switch und Sicherheit	166
4.6.6	Geräteauswahl	168
4.6.7	Anzeigen und Anschlüsse am Switch	169
4.6.8	Konfiguration eines Switchs allgemein	171
4.6.9	Spanning Tree am Switch aktivieren	171
4.6.10	VLAN-Konfiguration von Switches	172
4.6.11	Konfiguration von Rechnern für tagged VLANs	174
4.7	Routing – Netzwerkgrenzen überschreiten	177
4.7.1	Gemeinsame Nutzung einer IP-Adresse mit PAT	180
4.7.2	Festlegen des Standard-Gateways	180
4.7.3	Routing-Tabelle abfragen (»netstat«)	181
4.7.4	Routenverfolgung mit »traceroute«	182
4.7.5	Route manuell hinzufügen (»route add«)	183
4.7.6	Route löschen (»route«)	185
4.8	Multicast-Routing	186
4.9	Praxisübungen	187
4.9.1	Glasfasern	187
4.9.2	TP-Verkabelung	187
4.9.3	Switches	187
4.9.4	MAC- und IP-Adressen	188
4.9.5	Namensauflösung	188
4.9.6	Routing	188
4.9.7	Sicherheit im lokalen Netz	188

5	Steuer- und Fehlercodes mit ICMP und ICMPv6 übertragen	191
5.1	ICMP-Pakete (IPv4)	192
5.2	ICMPv6-Pakete	193
6	Datentransport mit TCP und UDP	197
6.1	Transmission Control Protocol (TCP)	197
6.1.1	Das TCP-Paket	198
6.1.2	TCP: Verbindungsaufbau	200
6.1.3	TCP: Transportkontrolle	201
6.1.4	TCP: Verbindungsabbau	202
6.2	User Datagram Protocol (UDP)	203
6.2.1	UDP: Der UDP-Datagram-Header	204
6.3	Nutzung von Services mittels Ports und Sockets	205
6.3.1	Sockets und deren Schreibweise	206
6.3.2	Übersicht über die Port-Nummern	207
6.3.3	Ports und Sicherheit	209
6.4	Die Firewall	211
6.4.1	Integration der Firewall in das Netzwerk	212
6.4.2	Regeln definieren	214
6.5	Der Proxyserver	218
6.5.1	Lokaler Proxyserver	219
6.5.2	Proxyserver als eigenständiger Netzwerkteilnehmer	219
6.5.3	Squid, ein Proxyserver	220
6.6	Port and Address Translation (PAT), Network Address Translation (NAT)	221
6.7	Praxis	223
6.7.1	Verbindungsaufbau zu einem Dienst mit geänderter Port-Nummer	223
6.7.2	Durchführen von Portscans zum Austesten von Sicherheitsproblemen	224
6.7.3	Schließen von Ports	225

6.8	Prüfungsfragen	226
6.8.1	TCP-Protokoll	226
6.8.2	Ports und Sockets	227
6.8.3	Firewall	227

7 Kommunikation und Sitzung 229

7.1	SMB/CIFS (Datei-, Druck- und Nachrichtendienste)	229
7.1.1	Grundlagen	230
7.1.2	Freigaben von Verzeichnissen und Druckern unter Windows	230
7.1.3	»nmbd« und »smbd« unter Linux/FreeBSD	231
7.1.4	Die Samba-Konfigurationsdatei »smb.conf«	232
7.1.5	Testen der Konfiguration	235
7.1.6	Aufnehmen und Bearbeiten von Samba-Benutzern	236
7.1.7	Starten, Stoppen und Neustart der Samba-Daemons	237
7.1.8	Netzlaufwerk verbinden (Windows 7, 8/8.1 und 10)	237
7.1.9	Client-Zugriffe unter Linux/FreeBSD	238
7.1.10	Zugriffskontrolle mit »smbstatus«	241
7.1.11	Die »net«-Befehle für die Windows-Batchprogrammierung	242
7.2	Network File System (NFS)	243
7.2.1	Konfiguration des NFS-Servers	243
7.2.2	Konfiguration des NFS-Clients	246
7.3	HTTP für die Informationen im Internet	247
7.3.1	Grundlagen des HTTP-Protokolls	247
7.3.2	Serverprogramme	252
7.3.3	Client-Programme	253
7.3.4	Webbrowser und Sicherheit	254
7.4	Mail-Transport	255
7.4.1	Grundlagen des SMTP/ESMTP-Protokolls	255
7.4.2	Konfigurationshinweise	259
7.4.3	Anhänge von E-Mails, MIME, S/MIME	261
7.5	Secure Shell (SSH) und Secure Socket Layer (SSL), Transport Layer Security (TLS)	265
7.5.1	Secure Shell (SSH)	265
7.5.2	SSL und TLS	266

7.6	Praxisübungen	267
7.6.1	Konfiguration des Samba-Servers	267
7.6.2	NFS-Server	267
7.6.3	HTTP, Sicherheit	268
7.6.4	E-Mail	268

8 Standards für den Datenaustausch 269

9 Netzwerkanwendungen 275

9.1	Datenübertragung	275
9.1.1	File Transfer Protocol (FTP), Server	275
9.1.2	File Transfer Protocol (FTP), Clients	276
9.1.3	Benutzerkommandos für FTP- und SFTP-Sitzungen	278
9.1.4	Datentransfer mit »netread« und »netwrite«	280
9.1.5	Verschlüsselte Datentransfers und Kommandoausgaben mit »cryptcat«	282
9.1.6	Secure Copy (scp), Ersatz für Remote Copy (rcp)	284
9.1.7	SSHFS: entfernte Verzeichnisse lokal nutzen	284
9.2	SSH, SFTP und SCP: Schlüssel erzeugen zur Erhöhung der Sicherheit oder zur kennwortfreien Anmeldung	286
9.3	Aufbau eines SSH-Tunnels	288
9.4	Fernsitzungen	289
9.4.1	Telnet	289
9.4.2	Secure Shell (SSH), nur Textdarstellung	289
9.4.3	Display-Umleitung für X11-Sitzungen	290
9.4.4	SSH zur Display-Umleitung für X11	291
9.4.5	Virtual Network Computing (VNC)	292
9.4.6	X2Go (Server und Client)	294
9.5	Telefonie-Anwendungen über Netzwerke (VoIP)	306
9.5.1	Grundlagen	306
9.5.2	Endeinrichtungen und ihre Konfiguration	310
9.5.3	Besonderheiten der Netzwerkinfrastruktur für VoIP	311

9.5.4	Sonderfall Fax: T38	312
9.5.5	Sicherheit	312
9.5.6	Anwendungsbeispiel: »Gegensprechanlage« im LAN mittels VoIP	313
9.5.7	Remote Desktop Protocol (RDP)	314

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	Netzwerkarten	329
10.4.2	WLAN-Router und -Sticks	330
10.4.3	Router	331
10.4.4	Switches	355
10.4.5	Printserver	356
10.4.6	Netzwerkspeicher (NAS)	358
10.4.7	Modems für den Netzzugang	359
10.5	Einbindung externer Netzwerkteilnehmer	361
10.6	Sicherheit	362
10.6.1	Abschottung wichtiger Rechner	363
10.6.2	Netzwerkverbindung mit einem Virtual Private Network (VPN)	365

10.6.3	WLAN sicher konfigurieren	371
10.6.4	SSH-Tunnel mit PuTTY aufbauen	372
10.6.5	Sichere Konfiguration von Printservern	375
10.6.6	Sicherer E-Mail-Verkehr	378
10.6.7	Sicherer Internetzugang mit IPv6	379
10.6.8	Mit Portknocking Brute Force-Angriffe vermeiden	380
10.7	Prüf- und Diagnoseprogramme für Netzwerke	383
10.7.1	Rechtliche Hinweise	383
10.7.2	Verbindungen mit »netstat« anzeigen	383
10.7.3	Hosts und Ports mit »nmap« finden	384
10.7.4	Datenverkehr protokollieren (Wireshark, tcpdump)	388
10.7.5	Netzaktivitäten mit »darkstat« messen	390
10.7.6	Netzlaster mit »fping« erzeugen	392
10.7.7	Weitere Einsatzmöglichkeiten von »fping«	392
10.7.8	Die Erreichbarkeit von Hosts mit »ping« bzw. »ping6« prüfen	394
10.7.9	»cryptcat«: im Dienste der Sicherheit	395
10.7.10	Weitere Systemabfragen auf Linux-Systemen	398

Anhang 401

A	Fehlertafeln	401
B	Auflösungen zu den Prüfungsfragen	409
C	Netzwerkbegriffe kurz erklärt	415
Index		433