

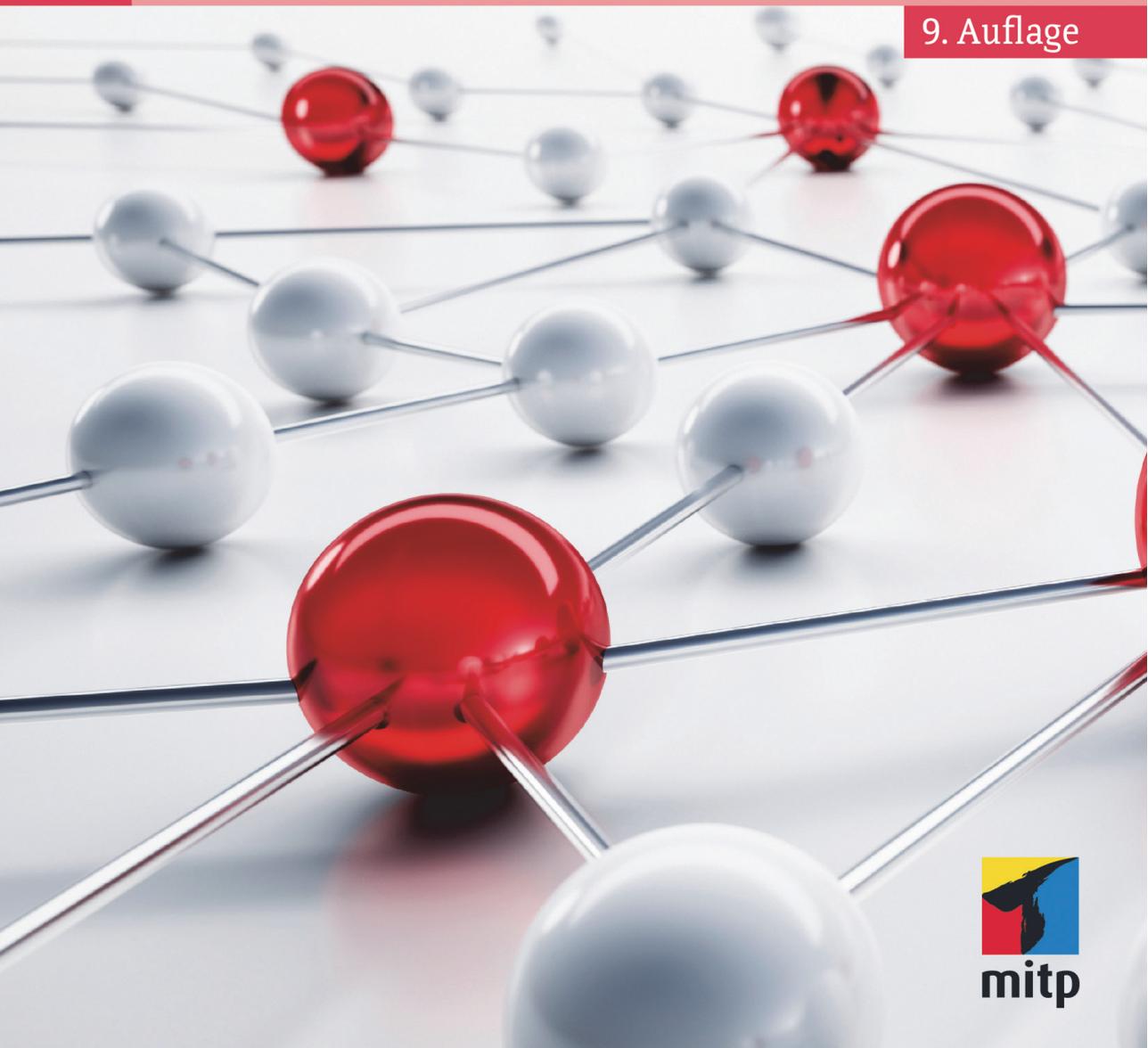
Markus Kammermann

# CompTIA Network+

Computer-Netzwerke verständlich erläutert

Vorbereitung auf die Prüfung N10-009

9. Auflage



# Inhaltsverzeichnis

<b>1</b>	<b>Einführung</b> . . . . .	<b>17</b>
1.1	Das Ziel dieses Buches . . . . .	18
1.2	Die CompTIA-Network+-Zertifizierung . . . . .	18
1.3	Das Weiterbildungsprogramm von CompTIA . . . . .	20
1.4	Voraussetzungen für CompTIA Network+ . . . . .	20
1.5	Danksagung zur 9. Auflage . . . . .	21
1.6	Eintrittstest zur Standortbestimmung . . . . .	22
<b>2</b>	<b>Entwicklungen und Modelle</b> . . . . .	<b>29</b>
2.1	Es war einmal ein Netzwerk . . . . .	30
2.2	Was ist denn eigentlich ein Netzwerk? . . . . .	31
2.2.1	Netzwerkelemente . . . . .	32
2.2.2	Netzwerkmodelle . . . . .	33
2.2.3	Netzwerkmanagement . . . . .	35
2.3	Vom Nutzen von Referenzmodellen . . . . .	35
2.4	Die Architektur des OSI-Modells . . . . .	37
2.5	Das beschreiben die einzelnen Schichten . . . . .	41
2.5.1	Bitübertragungsschicht (Physical Layer) . . . . .	41
2.5.2	Sicherungsschicht (Data Link Layer) . . . . .	41
2.5.3	Vermittlungsschicht (Network Layer) . . . . .	43
2.5.4	Transportschicht (Transport Layer) . . . . .	43
2.5.5	Sitzungsschicht (Session Layer) . . . . .	44
2.5.6	Darstellungsschicht (Presentation Layer) . . . . .	44
2.5.7	Anwendungsschicht (Application Layer) . . . . .	44
2.6	Das DoD-Modell . . . . .	45
2.7	Fragen zu diesem Kapitel . . . . .	47
<b>3</b>	<b>Grundbegriffe der Telematik</b> . . . . .	<b>49</b>
3.1	Multiplikatoren und Zahlensysteme . . . . .	49
3.2	Elektrische Eigenschaften . . . . .	53
3.3	Allgemeine Übertragungstechnik . . . . .	54
3.3.1	Das Sinussignal . . . . .	54
3.3.2	Dämpfung . . . . .	55

3.3.3	Frequenzbereiche . . . . .	56
3.4	Grundlagen der Datenübertragung . . . . .	57
3.4.1	Analoge Datenübertragung . . . . .	58
3.4.2	Digitale Übertragung . . . . .	58
3.5	Multiplexing . . . . .	59
3.6	Übertragungsarten. . . . .	61
3.6.1	Seriell – Parallel . . . . .	61
3.6.2	Bitrate . . . . .	62
3.6.3	Einfach oder hin und zurück? . . . . .	63
3.6.4	Synchrone und asynchrone Datenübertragung . . . . .	63
3.7	Bandbreite und Latenz . . . . .	64
3.8	Von Bits und Frames. . . . .	66
3.9	Fragen zu diesem Kapitel . . . . .	66
<b>4</b>	<b>Hardware im lokalen Netzwerk . . . . .</b>	<b>69</b>
4.1	Die wichtigsten Übertragungsmedien . . . . .	69
4.1.1	Twisted-Pair-Kabel . . . . .	71
4.1.2	Unshielded Twisted Pair . . . . .	72
4.1.3	Shielded Twisted Pair. . . . .	78
4.1.4	Koaxialkabel. . . . .	80
4.1.5	Lichtwellenleiter . . . . .	81
4.1.6	Auch das geht: Daten via Stromnetz. . . . .	87
4.2	Netzwerkkarten . . . . .	87
4.3	Repeater, Hubs und Bridges . . . . .	89
4.3.1	Repeater. . . . .	90
4.3.2	Hub . . . . .	90
4.3.3	Bridge . . . . .	90
4.4	So funktionieren Switches . . . . .	92
4.4.1	Methoden der Durchleitung . . . . .	92
4.4.2	Switches im Netz organisieren . . . . .	93
4.4.3	Spanning Tree Protocol . . . . .	93
4.4.4	Shortest Path Bridging und TRILL . . . . .	95
4.4.5	Managed Switches . . . . .	97
4.5	Konvertieren und Verbinden . . . . .	99
4.5.1	Medienkonverter. . . . .	99
4.5.2	Modems. . . . .	101
4.5.3	Multiplexer . . . . .	102
4.5.4	CSU/DSU . . . . .	103
4.6	Router verbinden diese (Netzwerk-)Welt . . . . .	104

4.7	Virtuelle Netzwerkkomponenten . . . . .	105
4.8	Fragen zu diesem Kapitel . . . . .	108
<b>5</b>	<b>Topologie und Verbindungsaufbau . . . . .</b>	<b>111</b>
5.1	Physische Topologien . . . . .	111
5.2	Bandbreitenverwendung . . . . .	117
5.2.1	Basisbandübertragung . . . . .	118
5.2.2	Breitbandübertragung . . . . .	118
5.3	Leitungsvermittelt – paketvermittelt . . . . .	118
5.3.1	Leitungsvermittelte Netzwerke . . . . .	118
5.3.2	Paketvermittelte Netzwerke . . . . .	119
5.3.3	Nachrichtenvermittlung . . . . .	119
5.4	Verbindungslos – verbindungsorientiert . . . . .	119
5.5	Unicast, Multicast, Broadcast, Anycast . . . . .	120
5.6	Fragen zu diesem Kapitel . . . . .	121
<b>6</b>	<b>Die Standards der IEEE-802.x-Reihe . . . . .</b>	<b>123</b>
6.1	Das Ethernet-Verfahren . . . . .	124
6.2	Von Fast Ethernet bis 100 Gigabit . . . . .	128
6.2.1	Fast Ethernet . . . . .	129
6.2.2	Gigabit-Ethernet . . . . .	129
6.2.3	Und schon folgen die 10 Gigabit/s . . . . .	129
6.2.4	Es werde schneller: 40 Gbps und 100 Gbps . . . . .	131
6.2.5	Power over Ethernet . . . . .	132
6.3	Dazu dienen VLANs . . . . .	133
6.4	Strukturierte Verkabelung . . . . .	138
6.5	Fragen zu diesem Kapitel . . . . .	141
<b>7</b>	<b>Netzwerk ohne Kabel: Drahtlostechnologien . . . . .</b>	<b>145</b>
7.1	Wenn sich das LAN plötzlich WLAN nennt . . . . .	146
7.1.1	Unterschiedliche Übertragungsverfahren . . . . .	148
7.1.2	Die Verbindungsarten eines WLAN . . . . .	149
7.1.3	Wie verbinden sich Sender und Empfänger? . . . . .	152
7.1.4	Verbindung über WPS . . . . .	153
7.2	Standards für drahtlose lokale Netzwerke . . . . .	153
7.2.1	Die Standards IEEE 802.11a/b/g . . . . .	153
7.2.2	Die nächsten Schritte: IEEE 802.11n und 802.11ac . . . . .	154
7.2.3	IEEE 802.11ax alias Wi-Fi 6 . . . . .	157
7.2.4	Die Gegenwart hört auf den Begriff IEEE 802.11be . . . . .	159
7.2.5	Frequenzträger und Kanalbreite . . . . .	160

7.3	Ein WLAN richtig aufbauen . . . . .	162
7.3.1	Aufbau der Hardware. . . . .	162
7.3.2	Konfiguration des drahtlosen Netzwerks . . . . .	164
7.4	Die Sicherheit im WLAN. . . . .	166
7.4.1	Wired Equivalent Privacy . . . . .	167
7.4.2	WPA und 802.11i . . . . .	167
7.5	Unterschiedliche Sendeverfahren . . . . .	169
7.5.1	Infrarot . . . . .	170
7.5.2	Mikrowellen . . . . .	170
7.5.3	Radiowellen (Funkwellen) . . . . .	173
7.6	Kommunikation auf kurze Distanzen . . . . .	173
7.6.1	Die Bluetooth-Technologie. . . . .	173
7.6.2	Zigbee und Z-Wave . . . . .	175
7.6.3	RFID . . . . .	175
7.6.4	NFC . . . . .	177
7.7	Fragen zu diesem Kapitel . . . . .	177
<b>8</b>	<b>WAN-Datentechniken auf OSI-Layer 1 bis 3 . . . . .</b>	<b>181</b>
8.1	Von POTS zu ISDN . . . . .	181
8.2	Breitband-ISDN und seine Nachfolger . . . . .	183
8.2.1	Synchrone digitale Hierarchie . . . . .	184
8.2.2	Sonet . . . . .	184
8.2.3	ATM. . . . .	186
8.3	Next Generation Network (NGN) . . . . .	188
8.4	Die wichtigsten DSL-Varianten. . . . .	191
8.4.1	Die DSL-Technologie . . . . .	191
8.4.2	DSL-Verfahren . . . . .	191
8.4.3	Probleme beim DSL-Einsatz . . . . .	194
8.5	TV-Kabelnetze . . . . .	195
8.6	Fiber to the Home . . . . .	196
8.7	Satelliten . . . . .	197
8.8	LPWAN. . . . .	198
8.9	Mobile Datennetze. . . . .	199
8.10	Fragen zu diesem Kapitel . . . . .	202
<b>9</b>	<b>Mein Name ist IP – Internet Protocol . . . . .</b>	<b>205</b>
9.1	Die Geschichte von TCP/IP . . . . .	205
9.2	Der Aufbau der Adressierung. . . . .	207
9.3	Die Grundlagen der IP-Adressierung. . . . .	209
9.3.1	CIDR statt Adressklassen. . . . .	212

9.3.2	Private Netzwerke unter IPv4 . . . . .	214
9.3.3	Ausnahmen und besondere Adressen . . . . .	215
9.3.4	Der IPv4-Header. . . . .	215
9.4	IPv6. . . . .	217
9.4.1	Der Header von IPv6 . . . . .	218
9.4.2	Konzepte und spezielle Adressen unter IPv6. . . . .	220
9.5	Fragen zu diesem Kapitel . . . . .	223
<b>10</b>	<b>Weitere Protokolle im TCP/IP-Stack . . . . .</b>	<b>227</b>
10.1	ICMP und IGMP . . . . .	227
10.2	ARP. . . . .	228
10.3	NAT und noch mehr Abkürzungen. . . . .	230
10.3.1	NAT und PAT. . . . .	230
10.3.2	Universal Plug and Play. . . . .	231
10.4	Das TCP-Protokoll. . . . .	232
10.4.1	Verbindungsmanagement. . . . .	233
10.4.2	Datenflusssteuerung . . . . .	234
10.4.3	Schließen der Verbindung. . . . .	235
10.5	Die Alternative: UDP. . . . .	235
10.6	Die Geschichte mit den Ports . . . . .	236
10.7	Voice over IP und Videokonferenzen . . . . .	239
10.8	Fragen zu diesem Kapitel . . . . .	244
<b>11</b>	<b>Stets zu Diensten. . . . .</b>	<b>247</b>
11.1	Routing-Protokolle. . . . .	247
11.1.1	RIP, RIPv2, IGRP. . . . .	250
11.1.2	OSPF und IS-IS . . . . .	252
11.1.3	BGP . . . . .	253
11.1.4	CARP und VRRP . . . . .	254
11.1.5	FHRP und HSRP . . . . .	255
11.2	Dynamic Host Configuration Protocol . . . . .	255
11.3	DNS (Domain Name System). . . . .	258
11.3.1	hosts . . . . .	258
11.3.2	Der Windows Internet Naming Service (WINS) . . . . .	259
11.3.3	Das Domain Name System . . . . .	259
11.3.4	Der Aufbau von DNS . . . . .	260
11.3.5	DNSSec, DoH und DoT. . . . .	266
11.3.6	Das Konzept des dynamischen DNS. . . . .	267
11.4	Web- und Mail-Protokolle. . . . .	267
11.4.1	HTTP. . . . .	267

11.4.2	FTP .....	270
11.4.3	TFTP .....	272
11.4.4	NNTP.....	272
11.4.5	SMTP.....	273
11.4.6	POP3 und IMAP4.....	274
11.5	Weitere Dienstprotokolle.....	276
11.5.1	NTP .....	276
11.5.2	SSH .....	278
11.5.3	Telnet.....	278
11.6	Fragen zu diesem Kapitel .....	280
<b>12</b>	<b>Netzwerke betreiben .....</b>	<b>283</b>
12.1	Grundlagen der Verwaltung .....	283
12.1.1	Arbeitsgruppen und Domänen .....	284
12.1.2	Der Client/Server-Ansatz .....	285
12.1.3	Client/Server-Bausteine .....	287
12.1.4	Wichtige Fragen zum Einsatz eines NOS.....	287
12.2	Verschiedene Systeme kurz vorgestellt .....	288
12.2.1	Apple .....	288
12.2.2	Unix.....	289
12.2.3	Linux .....	291
12.2.4	Von Windows NT bis Windows 2022.....	292
12.2.5	Citrix und VMWare .....	294
12.2.6	Die Bedeutung von SMB über Betriebssysteme hinweg....	295
12.3	Die Virtualisierung .....	296
12.4	Cloud Computing .....	297
12.4.1	Servicemodelle in der Cloud .....	298
12.4.2	Betriebsmodelle .....	300
12.4.3	Angebote aus der Cloud.....	301
12.5	Ein Wort zum Thema Speicher .....	302
12.6	Sicherheitsfragen zu Cloud-Modellen und Rechenzentren .....	303
12.7	Die Administration des Netzwerks.....	305
12.8	Ressourcen im Netzwerk teilen .....	305
12.9	Identifikation und Rechte im Netzwerk.....	306
12.9.1	Benutzer einrichten .....	308
12.9.2	Das Erstellen von Gruppen .....	310
12.9.3	Datei- und Ordnerrechte .....	311
12.9.4	Drucken im Netzwerk .....	314
12.10	Fragen zu diesem Kapitel .....	315

<b>13</b>	<b>Sicherheitsverfahren im Netzwerkverkehr</b> .....	317
13.1	Identifikation und Authentifikation .....	318
13.1.1	Aller Anfang ist ... das Passwort .....	319
13.1.2	Das Zero Trust-Konzept .....	320
13.1.3	SASE .....	321
13.2	Authentifikationsverfahren .....	322
13.2.1	Single Sign On und Mehr-Faktor-Authentifizierung .....	322
13.2.2	Das Identitätsmanagement .....	324
13.2.3	PAP und CHAP .....	325
13.2.4	EAP .....	326
13.2.5	Kerberos .....	326
13.2.6	RADIUS .....	327
13.3	Die Hash-Funktion .....	328
13.4	Verschlüsselung .....	329
13.4.1	Symmetrisch oder asymmetrisch .....	329
13.4.2	Von DES bis AES .....	330
13.4.3	RSA .....	330
13.4.4	Digitale Signatur .....	331
13.5	Die drei Status .....	331
13.5.1	Data-in-transit .....	331
13.5.2	Data-at-rest .....	331
13.5.3	Data-in-use .....	332
13.6	PKI – digitale Zertifikate .....	332
13.7	SSL und TLS .....	332
13.8	IPSec .....	335
13.9	Fragen zu diesem Kapitel .....	336
<b>14</b>	<b>Verschiedene Angriffsformen im Netzwerk</b> .....	339
14.1	Viren und andere Krankheiten .....	340
14.1.1	Unterscheiden Sie verschiedene Malware-Typen .....	340
14.1.2	Es gibt verschiedene Viren .....	343
14.2	Was tut der Mann in der Mitte? .....	353
14.2.1	»Sie machen es dem Angreifer ja auch einfach« .....	353
14.2.2	Denial-of-Service-Attacken .....	354
14.2.3	Pufferüberlauf .....	357
14.2.4	Man-in-the-Middle-Attacken .....	358
14.2.5	Spoofing .....	359
14.3	Angriffe gegen IT-Systeme .....	360
14.3.1	Exploits und Exploit-Kits .....	360

14.4	Social Engineering . . . . .	363
14.4.1	Die Ziele des Social Engineers. . . . .	363
14.4.2	Beliebter Ansatz: Phishing-Mails . . . . .	365
14.4.3	Tailgating und andere Methoden . . . . .	366
14.5	Angriffspunkt drahtloses Netzwerk . . . . .	367
14.6	Der freundliche Mitarbeiter . . . . .	369
14.7	Fragen zum Kapitel . . . . .	371
<b>15</b>	<b>Die Verteidigung des Netzwerks . . . . .</b>	<b>373</b>
15.1	Physikalische Sicherheit . . . . .	374
15.1.1	Zutrittsregelungen . . . . .	374
15.1.2	Vom Badge bis zur Biometrie . . . . .	376
15.1.3	Zutrittsschleusen und Videoüberwachung. . . . .	377
15.1.4	Schutz gegen Einbruch, Feuer und Wasser . . . . .	379
15.1.5	Klimatisierung und Kühlung. . . . .	381
15.1.6	Fachgerechte Inventarisierung und Entfernung . . . . .	382
15.2	Fehlertoleranter Aufbau . . . . .	383
15.3	Datensicherung . . . . .	386
15.4	Malwareschutz mit Konzept . . . . .	387
15.5	Netzwerkhärtung . . . . .	392
15.6	Firewalls . . . . .	393
15.6.1	Verschiedene Firewall-Typen. . . . .	397
15.6.2	Das Konzept der DMZ . . . . .	401
15.6.3	Erweiterte Funktionen einer Firewall . . . . .	402
15.6.4	Der Proxyserver. . . . .	403
15.6.5	IDS und IPS . . . . .	404
15.7	Aktive Suche nach Schwachstellen. . . . .	407
15.8	Die Rolle des Risiko-Managements . . . . .	409
15.9	Verteidigungskonzepte . . . . .	411
15.9.1	Die Auswertung von Überwachungen . . . . .	411
15.9.2	Notfallvorsorge . . . . .	413
15.9.3	Ansätze für das Disaster Recovery. . . . .	415
15.9.4	Die First Responders . . . . .	416
15.9.5	Und das alles zusammen? . . . . .	418
15.10	Fragen zu diesem Kapitel . . . . .	419
<b>16</b>	<b>Remote Access Networks . . . . .</b>	<b>423</b>
16.1	Remote Access . . . . .	423
16.2	Terminaldienste . . . . .	425

16.2.1	Der Windows Terminal Server .....	425
16.2.2	Citrix Presentation Server .....	427
16.2.3	Und die Desktop-Virtualisierung? .....	427
16.2.4	Ein Wort zum Thema Unterstützung. ....	427
16.3	VPN .....	429
16.3.1	Der Aufbau der Verbindung .....	430
16.3.2	Site-to-Site VPN .....	434
16.3.3	Client-to-Site VPN .....	436
16.3.4	Dynamisches VPN (Client-to-Site, Site-to-Site) .....	436
16.4	Fragen zu diesem Kapitel .....	437
<b>17</b>	<b>Netzwerkmanagement</b> .....	<b>439</b>
17.1	Wozu brauchen Sie Netzwerkmanagement? .....	439
17.1.1	Fault Management .....	442
17.1.2	Configuration Management .....	443
17.1.3	Performance Management .....	445
17.1.4	Security Management .....	445
17.2	Die Netzwerkdokumentation .....	446
17.2.1	Verkabelungsschema .....	446
17.2.2	Anschlussdiagramme. ....	447
17.2.3	Logisches Netzwerkdiagramm .....	447
17.2.4	Inventar- und Konfigurationsdokumentation .....	449
17.2.5	Erfassungsschemata für die Planung .....	450
17.2.6	Messdiagramme und Protokolle .....	453
17.2.7	Änderungsdokumentation. ....	453
17.3	Lifecycle Management. ....	454
17.4	Der Aufbau von Tests .....	456
17.5	SNMP-Protokolle .....	458
17.6	Fragen zu diesem Kapitel .....	461
<b>18</b>	<b>Überwachung</b> .....	<b>463</b>
18.1	So funktioniert das Monitoring .....	464
18.1.1	Was ist ein Monitor? .....	464
18.1.2	Performancemanagement konzipieren .....	467
18.1.3	Monitoring als Teil des Quality Management .....	468
18.1.4	Grundlagen zu Service Level Agreements .....	470
18.1.5	Weitere wichtige Dokumententypen. ....	472

18.2	Die Netzwerkanalyse . . . . .	474
18.3	Netzwerkanalyse-Programme . . . . .	475
18.3.1	Der Netzwerkmonitor . . . . .	475
18.3.2	Wireshark . . . . .	477
18.3.3	MRTG . . . . .	480
18.3.4	Messung der Netzwerkleistung . . . . .	481
18.3.5	Was ist ein Portscanner? . . . . .	485
18.4	Überwachung im industriellen Umfeld . . . . .	486
18.5	Die Bedeutung des Change Managements . . . . .	490
18.6	Regulatorische Anforderungen . . . . .	492
18.7	Fragen zu diesem Kapitel . . . . .	493
<b>19</b>	<b>Fehlersuche im Netzwerk . . . . .</b>	<b>495</b>
19.1	Wie arbeiten Sie im Support? . . . . .	496
19.1.1	Sprechen Sie mit und nicht über den Kunden . . . . .	496
19.1.2	Vorbereitung für den Supporteinsatz . . . . .	498
19.1.3	ESD . . . . .	498
19.1.4	Heben und Tragen . . . . .	499
19.1.5	MSDS . . . . .	499
19.1.6	Arbeiten am und mit Racks . . . . .	500
19.2	Fehlersuche im Netzwerk . . . . .	501
19.3	Kabelprobleme und Testgeräte . . . . .	502
19.3.1	Abisolier- und Schneidwerkzeuge . . . . .	505
19.3.2	Anlege- und Anschlusswerkzeuge . . . . .	505
19.3.3	Installationswerkzeuge zur Kabelverlegung . . . . .	506
19.3.4	Prüf- und Analysegeräte . . . . .	507
19.3.5	Sensoren und Messgeräte . . . . .	509
19.4	Hilfsmittel bei Routing-Problemen . . . . .	510
19.4.1	ipconfig/ip . . . . .	510
19.4.2	ping . . . . .	511
19.4.3	tracert/traceroute . . . . .	513
19.4.4	route . . . . .	514
19.4.5	Looking Glass . . . . .	515
19.5	Probleme bei der Namensauflösung . . . . .	516
19.5.1	nbtstat . . . . .	516
19.5.2	nslookup . . . . .	517
19.5.3	NET . . . . .	519
19.6	Arbeiten in der Shell mit netsh . . . . .	522
19.7	Protokollstatistiken anzeigen mit netstat . . . . .	524

19.8	Fehlersuche in den Diensten . . . . .	525
19.9	Fragen zu diesem Kapitel . . . . .	527
<b>20</b>	<b>Praxis 1: Sie richten ein Netzwerk ein . . . . .</b>	<b>531</b>
20.1	Die Konzeption . . . . .	532
	20.1.1 Ein Inventar erstellen . . . . .	532
	20.1.2 Netzwerkkonzept erstellen . . . . .	533
	20.1.3 Computer vorbereiten . . . . .	534
20.2	Das Netzwerk aufbauen . . . . .	535
	20.2.1 Router einrichten . . . . .	535
	20.2.2 Internetzugriff einrichten . . . . .	537
	20.2.3 Das LAN einrichten . . . . .	538
	20.2.4 Abschluss der Router-Konfiguration . . . . .	539
	20.2.5 Test der Internetverbindung . . . . .	540
20.3	Alternative Konzeption . . . . .	541
	20.3.1 Firewall einrichten . . . . .	542
	20.3.2 Die Schnittstellen einrichten . . . . .	543
	20.3.3 USG hat doch was mit Firewall zu tun . . . . .	546
	20.3.4 Abschluss der Router-Konfiguration . . . . .	546
20.4	Drucken im Netzwerk . . . . .	547
20.5	Gemeinsame Nutzung von Daten . . . . .	552
	20.5.1 Vorbereitungsarbeiten . . . . .	553
	20.5.2 Einrichten der Freigabe . . . . .	553
20.6	Fragen zum Kapitel . . . . .	555
<b>21</b>	<b>Praxis 2: Sie richten ein WLAN ein . . . . .</b>	<b>559</b>
21.1	Das Szenario für den Nachbau . . . . .	559
21.2	Der Beginn Ihrer Installation . . . . .	560
21.3	Der Aufbau des Netzwerks . . . . .	561
21.4	Die Konfiguration des WLAN-Geräts . . . . .	562
	21.4.1 WAN-Schnittstelle einrichten . . . . .	565
	21.4.2 Die Konfiguration der LAN-Schnittstellen . . . . .	566
	21.4.3 WLAN einrichten . . . . .	567
	21.4.4 Jetzt kommt die Firewall dran . . . . .	570
21.5	Fragen zu diesem Kapitel . . . . .	571
<b>22</b>	<b>Praxis 3: Steigern Sie die Netzeffizienz . . . . .</b>	<b>575</b>
22.1	Optimierung der physischen Komponenten . . . . .	575
22.2	Die Optimierung von Ethernet-Netzwerken . . . . .	576
	22.2.1 Reduzieren der Protokolle . . . . .	578

22.2.2	Drucker . . . . .	579
22.3	Teilnetze durch Subnettierung . . . . .	579
22.3.1	Grundlagen zum Subnet Masking . . . . .	580
22.3.2	Wie eine Subnettierung funktioniert . . . . .	580
22.4	Weitere Optimierungsmaßnahmen . . . . .	583
22.4.1	Network Access Control . . . . .	583
22.4.2	Traffic Shaping . . . . .	584
22.5	Netzwerke optimieren dank QoS . . . . .	585
22.5.1	Priorisierung auf OSI-Layer 2: IEEE 802.1q . . . . .	586
22.5.2	Priorisierung auf OSI-Layer 3: Das DSCP-Verfahren . . . . .	586
22.5.3	Integrated-Services-Verfahren . . . . .	587
22.5.4	Class of Service . . . . .	588
22.5.5	Hardwarebasierte QoS-Verfahren . . . . .	588
22.6	Optimierungsmöglichkeiten im WLAN . . . . .	588
22.7	Fragen zu diesem Kapitel . . . . .	592
<b>23</b>	<b>Die CompTIA-Network+-Prüfung . . . . .</b>	<b>595</b>
23.1	Was von Ihnen verlangt wird . . . . .	595
23.2	Wie Sie sich vorbereiten können . . . . .	596
23.3	Wie eine Prüfung aussieht . . . . .	597
23.4	Abschlusstest zur Prüfung CompTIA Network+ . . . . .	601
<b>A</b>	<b>Antworten und Lösungen . . . . .</b>	<b>623</b>
A.1	Antworten zu den Fragen des Eintrittstests . . . . .	623
A.2	Lösungsbeispiele zu »Jetzt sind Sie dran« . . . . .	623
A.3	Antworten zu den Kapitelfragen . . . . .	627
A.4	Antworten zur Musterprüfung . . . . .	629
A.5	Weiterführende Literatur . . . . .	630
A.5.1	Nützliche Literatur zum Thema . . . . .	630
A.5.2	Weiterführende Links zum Thema . . . . .	631
<b>B</b>	<b>Abkürzungsverzeichnis . . . . .</b>	<b>633</b>
	<b>Stichwortverzeichnis . . . . .</b>	<b>647</b>

# Einführung

Wenn meine jüngste Tochter unterwegs ist, macht sie mit ihrem Handy Fotos, die sie umgehend im Internet postet. Sie chattet in einem sozialen Netzwerk und auf ihrem PC hat sie Webbrowser und Cloudzugänge installiert, um sich mit der Welt auszutauschen, und speichert so gut wie alle ihre Informationen und Arbeiten digital in ihrer Cloud.

Wenn meine Mutter mit ihren weit über 85 Jahren heute ein Buch lesen möchte, verbindet sie ihr Android-Tablet mit dem WLAN, lädt sich das entsprechende Buch aus dem Internet herunter – genauso selbstverständlich, wie sie früher in eine Buchhandlung gegangen ist – und freut sich, dass sie Farbe, Leuchtkraft und Größe der Buchstaben so einfach an ihre Bedürfnisse anpassen kann.

Mich beeindruckt persönlich, wie tief das Thema »Netzwerke« nicht nur in Unternehmen, sondern auch in den privaten Sprach- und Alltagsgebrauch vorgedrungen ist. Durch die ständig steigende Durchdringung unseres Lebensraums mit vernetzten Geräten und Anwendungen, angefangen beim mobilen Telefon mit Bluetooth-Schnittstelle über Breitbandanschlüsse bis hin zu virtuellen Netzwerken und der doch für viele noch recht neuen Handhabung mit künstlicher Intelligenz, haben sich die Begriffe der Netzwerktechnik bis tief in den allgemeinen Alltagsgebrauch vorgewagt – und es bedarf entsprechend einer ausreichenden Anzahl an Personen, die sich mit dieser Thematik auskennen und in der Lage sind, Netzwerke in verschiedenster Form zu planen, zu installieren und zu warten.

Und was im privaten Umfeld gilt, gilt erst recht in der Unternehmensinformatik. Ob die Nutzung gemeinsamer Ressourcen, die Anbindung der Firma an unterschiedliche Clouddienste oder die Einrichtung einer (virtuellen) Kommunikationsinfrastruktur – ohne Netzwerke ist die Unternehmens-IT von heute nicht mehr denk- und schon gar nicht mehr realisierbar. Und entsprechend braucht es genügend Fachleute, welche die Anwendung dieser Technologie beherrschen und die Kunden unterstützen können.

Darum ist heute ein guter Zeitpunkt, wenn Sie beginnen, sich mit dieser Thematik auseinanderzusetzen und teilzuhaben an den Möglichkeiten, die sich daraus eröffnen, sich mit Netzwerken auszukennen, sie zu planen und zu konfigurieren und damit zu arbeiten.

## 1.1 Das Ziel dieses Buches

Dieses Buch verfolgt zwei Ziele: Ihnen die Welt der Netzwerke zu erklären sowie Sie auf die entsprechende Zertifizierung Ihrer Fähigkeiten als CompTIA-Network+-Techniker/-in vorzubereiten.

Die folgenden Kapitel dieses Buches möchten Ihnen dazu das notwendige Wissen vermitteln und Ihnen eine Orientierung geben, damit Sie sich anschließend in den verschiedenen Themenbereichen von Netzwerken zurechtfinden und in der Lage sind, Netzwerke zu verstehen und entsprechend zu betreuen. Dabei begegnen Sie in diesem Buch Netzwerken in ihren unterschiedlichsten Dimensionen von der Idee der Vernetzung und Modellen von Netzwerken über Stecker, Komponenten und Verbindungen bis hin zu Anwendungen wie dem Teilen von Ressourcen oder dem E-Mail-Verkehr, aber auch den mit Netzwerken verbundenen Risiken.

Zum Inhalt dieses Buches gehört auch, dass Sie in der Lage sein werden, Kunden zu verstehen und deren Anforderungen an einen gewünschten Netzwerksupport umsetzen zu können.

Die Themen dieses Buches und eventuell auch ein dazugehöriges Seminar unterstützen Sie beim Erlernen und beim Aufbau eines eigenen Verständnisses der technischen Begriffe, der Funktionsweise von Netzwerken, Protokollen und Anwendungen sowie der Fehlerdiagnose.

Eine ausreichende eigene Praxis und gegebenenfalls eine ergänzende Ausbildung durch ein Seminar bieten Ihnen zusammen mit diesem Buch die notwendigen Grundlagen, um die Prüfung CompTIA Network+ erfolgreich bestehen zu können. Aus diesem Grund hat CompTIA zusammen mit den Network+-Lernzielen auch eine Liste von nützlichen Komponenten von Hard- und Software veröffentlicht, mit deren Hilfe Sie sich z.B. in einem Training oder Labor praktisch mit der erforderlichen Thematik auseinandersetzen können.

## 1.2 Die CompTIA-Network+-Zertifizierung

Die CompTIA-Network+-Zertifizierung wendet sich an Technikerinnen und Techniker mit vorhandener Berufserfahrung im Informatikbereich und bescheinigt zertifizierten Personen eine breite Kenntnis auf dem Gebiet der Netzwerktechnologie. Das bestandene Examen bedeutet, dass der zertifizierte Absolvent die erforderlichen Kenntnisse und Fähigkeiten besitzt, um eine festgelegte Netzwerkarchitektur mit grundlegenden Sicherheitseinstellungen zu implementieren. Außerdem ist er in der Lage, Netzwerkgeräte mit den geeigneten Netzwerktools zu konfigurieren und instand zu halten sowie auftretende Probleme zu beheben. Des Weiteren kennt er die Eigenschaften und Zielsetzungen von Netzwerktechnologien, kann

grundlegende Lösungen empfehlen und den Netzwerkverkehr analysieren und ist mit den gängigen Protokollen und Medientypen vertraut.

Die CompTIA-Network+-Prüfung eignet sich sehr gut als Vorbereitung auf die IT-Zertifikate diverser im Netzwerktechniksektor aktiver Hersteller.

Damit die Zertifizierung am Markt bestehen bleibt, wird die Prüfung durch die CompTIA regelmäßig aktualisiert und an die aktuellen Anforderungen angepasst. Die letzten beiden Anpassungen fanden 2021 und aktuell im Jahr 2024 statt. Die Inhalte der Zertifizierung werden anschließend in Lernzieldokumenten auf der Website von CompTIA unter [www.comptia.org](http://www.comptia.org) veröffentlicht (sogenannte *Exam Objectives*).

Die Network+-Zertifizierung teilt sich in mehrere Fachgebiete, im CompTIA-Sprachgebrauch *Domain* und in der Übersetzung von CompTIA *Wissensgebiet* genannt. In der aktuellen Fassung der Prüfung (N10-009) lauten diese Themen wie folgt:

Wissensgebiet	Thematik
Wissensgebiet 1	Netzwerk-Konzepte
Wissensgebiet 2	Netzwerk-Implementationen
Wissensgebiet 3	Netzwerkbetrieb
Wissensgebiet 4	Netzwerksicherheit
Wissensgebiet 5	Netzwerk Troubleshooting

Entsprechend lernen Sie in diesem Buch die oben genannten Themenbereiche ausführlich kennen und können sich mit diesem Buch das für die Zertifizierung notwendige Wissen aneignen sowie dazugehörige Praxistipps und Übungen mitnehmen.

Im Zentrum steht dabei weniger die Auflistung aller möglichen und unmöglichen Abkürzungen aus diesem Bereich, sondern die Schaffung eines Verständnisses für die Thematik Netzwerk und die Funktionsweise der einzelnen Elemente.

Für alle relevanten Abkürzungen finden Sie zudem ein ausführliches Abkürzungsverzeichnis im Anhang dieses Buches.

Neu hinzugekommen sind in der vorliegenden 9. Auflage hinsichtlich der aktuellen Prüfung die folgenden Elemente:

- Aktualisierung von Standards und Verfahren (Ethernet, WLAN, IPv6)
- Das Thema Sicherheit wurde aktualisiert
- Eine Beispielprüfung in vollem Umfang des Examens N10-009

## 1.3 Das Weiterbildungsprogramm von CompTIA

Halten Sie Ihre Zertifizierung mit dem Weiterbildungsprogramm (CE) von CompTIA auf dem neuesten Stand. Es ist als kontinuierliche Bestätigung Ihrer Expertise und als Werkzeug zur Erweiterung Ihres Kompetenzspektrums konzipiert.

Durch die Teilnahme am Weiterbildungsprogramm von CompTIA bleiben Sie mit neuen und sich entwickelnden Technologien auf dem Laufenden und können Ihre einmal erworbene Prüfung rezertifizieren.

Ihre CompTIA-Network+-Zertifizierung ist ab dem Tag Ihrer Prüfung drei Jahre lang gültig. Das CE-Programm ermöglicht es Ihnen, Ihre Zertifizierung in dreijährigen Abständen durch Aktivitäten und Schulungen zu verlängern, die sich auf den Inhalt Ihrer Zertifizierung beziehen. Wie Network+ selbst verfügt auch CompTIA Network+ CE über einen weltweit anerkannten ISO/ANSI-Akkreditierungsstatus.

Sie können an unterschiedlichen Aktivitäten und Schulungsprogrammen teilnehmen, darunter auch an höherwertigen Zertifizierungen, um Ihre CompTIA-Network+-Zertifizierung zu erneuern. Schließen Sie CertMaster CE ab, einen Online-CE-Kurs im eigenen Tempo, oder sammeln Sie in drei Jahren mindestens 30 Continuing Education Units (CEUs), laden Sie diese auf Ihr Zertifizierungskonto hoch und Network+ erneuert sich automatisch.

## 1.4 Voraussetzungen für CompTIA Network+

Gemäß der Website von CompTIA ([www.comptia.org/de](http://www.comptia.org/de)) zur CompTIA-Network+-Prüfung sollte ein Teilnehmer für das erfolgreiche Ablegen der Prüfung über folgende Kompetenzen verfügen:

- CompTIA-A+-Zertifizierung oder entsprechende Kenntnisse, auch wenn die CompTIA-A+-Zertifizierung keine zwingende Anforderung ist
- Mindestens neun bis zwölf Monate Berufserfahrung in der ICT-Netzwerktechnik

Diesen Empfehlungen kann ich als Autor nur zustimmen. Zudem kann Ihnen dieses Buch nicht die praktische Erfahrung vermitteln, die im Bereich Netzwerktechnik nötig ist, um im beruflichen Alltag erfolgreich zu sein. Wenn Sie sich also auf die Zertifizierung vorbereiten möchten, lesen Sie dieses Buch, aber installie-

ren Sie auch selbst ein Netzwerk, gehen Sie in ein Training oder bauen Sie mit Kollegen ein Netzwerk auf und üben Sie sich praktisch in der Konzeption, Installation, Konfiguration und Fehlerbehebung bei Netzwerken.

Für weitere Informationen begeben Sie sich bitte auf die Website von CompTIA unter [www.comptia.org/de](http://www.comptia.org/de). Details zur Prüfung finden Sie zudem in Kapitel 23 »Die CompTIA-Network+-Prüfung«.

## 1.5 Danksagung zur 9. Auflage

*»Das Verfassen eines Buches über ein so breit gefasstes und sich ständig entwickelndes Thema wie die Netzwerktechnik ist auch für jemanden mit langjähriger und breiter Erfahrung eine herausfordernde Aufgabe.«* Den Satz schreibe ich mittlerweile schon seit einigen Auflagen immer an dieser Stelle. Und mit jeder Auflage scheint es mir noch mehr an Bedeutung zu gewinnen, was ich danach geschrieben habe: *»Vor mehr als sieben Jahren habe ich mit der 1. Auflage zu diesem Buch begonnen und damals wie heute bin ich allen Lesern und Mitarbeitern dankbar, die mir neue Ideen mitteilen, mich auf Fehler aufmerksam machen oder mit ihren Wünschen dazu beitragen, dass dieses Buch mit jeder Auflage kompletter und vielfältiger werden kann.«*

Als ich selbst die ersten Netzwerke verlegte, waren das freiliegende gelbe Ethernet-Koaxialkabel mit T-Stücken für ein kleines Büronetzwerk und später geschwichte Sternverkabelungen für Server und Clients, dann folgten Umrüstungen auf Gigabit-Verkabelungen sowie der Aufbau von drahtlosen Netzwerken – und heute stehen wir mitten in der Ausbreitung des »Internets der Dinge« und verschiedener KI-basierter Anwendungen, bei denen Maschinen und Komponenten mit Sensoren direkt untereinander kommunizieren. Die Entwicklungen bleiben also keineswegs stehen – und somit bleibt auch mein Bedarf als Autor, nebst eigener Weiterbildung, an Ihren Vorschlägen und Fragen immer noch aktuell.

Mein Dank gilt persönlich all denen, die mir bei verschiedenen Auflagen dieses Buchs immer wieder beim Korrekturlesen sowie mit neuen Ideen oder Anregungen zur Seite stehen, für diese Auflage namentlich meine Studierenden im Bereich Netzwerk mit ihren zahlreichen guten Rückfragen und Anmerkungen. Mein Dank geht aber auch an die vielen Leserinnen und Leser und Teilnehmenden an meinen verschiedenen Seminaren, die immer wieder neue Ideen einbringen.

Bedanken möchte ich mich einmal mehr sehr herzlich bei Katja Völpel und dem mitp-Verlag. Es freut mich immer aufs Neue, dass wir im Zeitalter des Internets zusammen ein Buch aktualisieren und bereits in der 9. Auflage herausbringen können. Ein Buch, das viele interessiert und das gelesen wird und mit dem wir in guter Zusammenarbeit gemeinsam Erfolg haben. Und da dies heute ein aktuelles Thema ist: Dieses Buch wurde auch in der neunten Auflage nicht mit KI-basierten Tools erstellt oder revidiert.

## 1.6 Eintrittstest zur Standortbestimmung

Bevor Sie sich an die eigentlichen Themen von CompTIA Network+ heranwagen, möchte ich Ihnen die Gelegenheit geben, die Erfüllung der Voraussetzungen für den Einstieg zu dieser Zertifizierung in einem Test an sich selbst zu überprüfen.

Sie finden daher im Folgenden 30 Fragen, die sich, basierend auf den von CompTIA definierten Voraussetzungen, vorwiegend mit Systemtechnik- und Netzwerkfragen auf dem Level von CompTIA A+ befassen und Ihnen die Einschätzung erlauben sollen, ob Sie das für die folgenden Themen benötigte Verständnis und Fachwissen mitbringen.

1. Welche Komponente kann verhindern, dass bestimmte Programme während des Bootens durch das Windows-Betriebssystem geladen werden?
  - A. attrib
  - B. snap ins
  - C. msconfig
  - D. bootini.bat
2. Ein Kunde kann zwar zu Hause über den Access Point auf das Internet zugreifen, hat aber Probleme, sich mit einem bestimmten Game-Server zu verbinden. Welche Einstellung wird der Techniker überprüfen?
  - A. Die SSID auf dem Access Point und dem PC
  - B. Die DHCP-Einstellungen auf dem PC
  - C. Die Port-Weiterleitungsregeln
  - D. Die MAC-Filtereinstellungen
3. Durch den Einbau von welchem Gerät kann man einen Rechner mit einem Server mit einem UTP-Kabel verbinden?
  - A. NIC
  - B. USB
  - C. FireWire
  - D. RJ-11
4. Welcher der folgenden Benutzer hat am meisten Autorität auf einem lokalen System, das mit Windows 10 Professional betrieben wird?
  - A. BCM (Basis Custom Master)
  - B. Power User
  - C. Hauptbenutzer
  - D. Administrator

5. Sie haben in Ihrem Rechner eine neue Netzwerkkarte eingebaut und erhalten danach die IP-Adresse 169.254.2.3 zugeordnet. Was ist geschehen?
  - A. Es konnte keine dynamische IP-Adresse zugeordnet werden.
  - B. Der PC hat die Adresse vom Internet bezogen.
  - C. Es besteht keine Verbindung zum Switch.
  - D. Es wurde ein falscher Treiber installiert.
6. Mit welcher Schnittstelle kann eine externe Festplatte üblicherweise an einem PC angeschlossen werden?
  - A. USB-C
  - B. IrDA
  - C. 802.11u
  - D. IEEE 1284
7. Über welche Spezifikation verfügt ein moderner Prozessor?
  - A. Dual ATA
  - B. HyperChannel
  - C. Double Data Clock
  - D. MultiCore
8. Welches Schnittstellenkonzept enthält in einem Notebook PnP-Funktionalität?
  - A. IEE 1283
  - B. USCSI
  - C. P-ATA
  - D. USB-C
9. Woran erkennt man während der POST-Phase ein Problem mit einer Grafikkarte?
  - A. Die `NUM Lock`-Taste blinkt.
  - B. Ein Piepston oder mehrere Piepstöne nacheinander
  - C. Der PC wird heruntergefahren.
  - D. Es erscheint eine Fehleranzeige im Display.
10. Wie nennt sich die Software auf dem Mainboard eines Routers?
  - A. UEFI
  - B. CMOS
  - C. Firmware
  - D. Treiber

11. Wo werden die Hardware-Einstellungen eines PC-Systems gespeichert?
  - A. CMOS
  - B. EPROM
  - C. THERMO
  - D. POST
12. Sie installieren bei einem Kunden zu Hause ein drahtloses Netzwerk. Der Kunde möchte gerne sein Netzwerk nach außen verbergen. Was werden Sie konfigurieren, um dem Kunden diesen Wunsch zu erfüllen?
  - A. Sie schalten das Aussenden der SSID ab.
  - B. Sie schalten das Aussenden der WEP-Verschlüsselung ab.
  - C. Sie deaktivieren die Sendeberechtigung des Access Points.
  - D. Sie deaktivieren die WPA-Verschlüsselung.
13. Mit welchem Befehl kann man über Router vom eigenen System bis zum Zielsystem die Verbindung prüfen?
  - A. ping
  - B. tracert
  - C. route
  - D. ipconfig
14. Wie nennt sich eine Datei, die andere Dateien infiziert und sich selbst replizieren kann?
  - A. Virus
  - B. Trojaner
  - C. Wurm
  - D. Hoax
15. Beim Neustart nach einem Update des Grafikkartentreibers ist der Bildschirm verzerrt, wenn Windows gestartet ist. Der Anwender schaltet den Computer aus und betätigt beim Neustart die Taste **F8**. Das Startmenü wird angezeigt. Welche Option sollte der Anwender auswählen, um das Problem zu lösen?
  - A. Abgesicherter Modus
  - B. Abgesicherter Modus mit Eingabeaufforderung
  - C. Letzte als funktionierend bekannte Konfiguration
  - D. Normaler Modus
16. Beim Verbinden des Notebooks mit dem Netzteil bemerkt der Techniker eine übermäßige Temperatur des Netzteils. Der Techniker sollte ...
  - A. die korrekte Verbindung sicherstellen.
  - B. das Netzteil vom Boden entfernen.
  - C. das Netzteil mit einem Ventilator kühlen.
  - D. das Netzteil ersetzen.

17. Was sollte ein Techniker tun, wenn er zum ersten Mal mit einem neuen Kunden spricht?
  - A. Wenn das Problem nicht sofort gelöst werden kann, dieses eskalieren.
  - B. Fachausdrücke verwenden, damit der Kunde merkt, über welche Fachkenntnisse der Techniker verfügt.
  - C. Dem Kunden seinen Namen und den Namen der Firma nennen.
  - D. Dem Kunden vor Ort Hilfe anbieten.
18. Welches Verfahren sollte ein Techniker im Gespräch mit einem unzufriedenen Kunden anwenden?
  - A. Seinen Vorgesetzten bitten, das Gespräch zu führen, da dies nicht die Aufgabe des Technikers ist.
  - B. Versuchen, alle Fehler zu verheimlichen, die aufgetreten sind.
  - C. Den Kunden ignorieren, weil ein Techniker nicht mit aggressiven Kunden sprechen muss.
  - D. Integrität und Ehrlichkeit bewahren.
19. Welche der Folgenden ist eine drahtlose Lösung für den Anschluss von Netzwerkgeräten?
  - A. IEEE 1284ax
  - B. IEEE 1394b
  - C. IEEE 802.3n
  - D. IEEE 802.11be
20. Sie stellen im Geräte-Manager Ihres Betriebssystems fest, dass ein angeschlossenes Gerät mit einem roten X über dem Icon des Geräts dargestellt wird. Was bedeutet das?
  - A. Das Gerät steht in Konflikt zu einem anderen Gerät.
  - B. Das Gerät benötigt einen aktualisierten Treiber.
  - C. Das Gerät ist deaktiviert.
  - D. Das Gerät wird vom System nicht erkannt.
21. Eine MAC-Adresse finden Sie ...
  - A. in der Festplatte.
  - B. in einer NIC.
  - C. nur in einem Apple-Computer.
  - D. im Prozessor.

22. Was gehört in jedem Fall in ein Werkzeugset? (zwei Antworten)
- A. Ein Akkuladegerät
  - B. Ein Antistatikarmband
  - C. Ein Kreuzschlitzschraubendreher
  - D. Aceton
23. Wie hoch ist die theoretische maximale Geschwindigkeit bei Gigabit-Ethernet?
- A. 10 Mbps
  - B. 100 Mbps
  - C. 1.000 Mbps
  - D. 10.000 Mbps
24. Welches Verzeichnis wird auf einem 64-Bit-Windows-System erstellt, um 32-Bit-Anwendungen zu speichern?
- A. `C:\Programme`
  - B. `C:\Windows`
  - C. `C:\Windows\system32`
  - D. `C:\Programme(x86)`
25. In einer Umgebung mit unzuverlässiger Spannungsversorgung schützt man den Computer am besten durch ...
- A. einen geerdeten Power Strip.
  - B. Aufstellen auf einer antistatischen Unterlage.
  - C. eine unterbrechungsfreie Stromversorgung (USV).
  - D. einen separaten Stromanschluss.
26. Eine Kundin ruft Sie zu Hilfe, weil sich die PCs ihrer Abteilung nicht mehr mit dem Internet verbinden können und auch die Rechner der anderen Abteilung für sie nicht mehr erreichbar sind. Ein `ipconfig`-Aufruf auf einem der betroffenen Abteilungs-PCs ergibt folgende Informationen:
- |                   |             |
|-------------------|-------------|
| IP-Adresse:       | 169.254.2.4 |
| Subnetz:          | 255.255.0.0 |
| Standard-Gateway: |             |
- Was ist die wahrscheinlichste Ursache des Problems?
- A. Die Subnetzmaske ist falsch konfiguriert.
  - B. Der DHCP-Client ist nicht in der Lage, eine Adresse vom DHCP-Server zu beziehen.
  - C. Der DNS-Client ist für diese Computer nicht konfiguriert.
  - D. Das Standard-Gateway ist nicht definiert.

27. Worauf müssen Sie achten, wenn Sie mit Ihrem Notebook von Europa in die USA reisen?
- A. Das lokale Dateisystem
  - B. Die Watt-Einstellungen
  - C. Die regionalen Leistungseinstellungen
  - D. Die Volt-Einstellungen
28. Eine Kundin berichtet, dass sie versucht hat, ein USB-Gerät einzustecken. Dabei hat sie versehentlich einen der Anschlussstecker beschädigt. Seither ist es ihr nicht mehr möglich, den Computer zu betreiben, weil er immer wieder abschaltet. Was ist wahrscheinlich der Grund dafür?
- A. Der beschädigte Anschluss hat Kontakt mit dem Metallkäfig des Gehäuses und verursacht einen Kurzschluss.
  - B. Die Stromversorgung des PC sitzt nicht mehr richtig auf dem Board.
  - C. Der USB-Anschluss verursacht einen Treiberfehler.
  - D. Das Betriebssystem erkennt den USB-Anschluss nicht mehr.
29. Ein Benutzer erhält die Meldung *Zugriff verweigert*, wenn er eine neue Anwendung installieren möchte. Was werden Sie als Erstes überprüfen?
- A. Ob die Datei- und Druckerfreigabe aktiviert ist
  - B. Ob der Benutzer Zugriffsrechte auf das Laufwerk hat
  - C. Ob die Gruppe *Jeder* Zugriffsrechte auf das System hat
  - D. Ob der Benutzer als lokaler Administrator am System angemeldet ist
30. Ein Kunde bereinigt sein System von Malware. Aufgrund der Verseuchung ist es ihm nicht möglich, per Internet Updates der Antivirensoftware zu erhalten. Welche nächsten Schritte sind angebracht? Wählen Sie zwei aus.
- A. Im abgesicherten Modus starten und die Festplatte formatieren
  - B. Einen Pop-up-Blocker installieren und den Internet Explorer starten
  - C. Im abgesicherten Modus mit Netzwerktreibern starten und versuchen, so die Updates zu erhalten
  - D. Von CD starten und einen chkdsk ausführen
  - E. Die Updates manuell einspielen, nachdem sie von einer anderen Maschine aus heruntergeladen worden sind.

Die Antworten zu den Fragen finden Sie in Abschnitt A.1 »Antworten zu den Fragen des Eintrittstests«. Bei einer Quote von 70 % korrekter Antworten oder mehr befinden Sie sich im Bereich des notwendigen Grundwissens für einen Beginn mit CompTIA Network+. Liegen Sie wesentlich darunter, empfehle ich Ihnen gegebenenfalls eine Vorbereitung mit dem Thema Systemtechnik und Support durch die Zertifizierung CompTIA A+.

# Entwicklungen und Modelle

Die Entwicklung der Netzwerktechnologie reicht über einige Jahrzehnte, war anfänglich geprägt von einzelnen großen Systemen und deren Erfindern und wurde immer mehr zu einem industrialisierbaren und damit notwendigerweise zu standardisierenden Thema für die Unternehmen, die in Netzwerke investieren wollten.

Ende der 1970er Jahre wurde mit diesen Bemühungen begonnen. Im Jahr 1983 wurde ein erstes, *OSI* genanntes Modell vorgestellt. Der Begriff steht für *Open Systems Interconnection*. Es wurde anfänglich von der ITU, der Telekommunikationsvereinigung, seit 1984 auch von der ISO veröffentlicht. Das jetzt genormte Schichtenmodell wird seither von der ISO weiterentwickelt und den aktuellen Stand können Sie in ISO/IEC 7498-1:1994 aus dem Jahr 1994 nachlesen.

Dieses theoretische Modell beschreibt allgemeingültig die Kommunikation in Form eines mehrschichtigen Systems mit fest definierten Aufgabenstellungen. Nach diesem Kapitel werden Sie die unterschiedlichen Schichten des OSI-Modells und deren Funktionen benennen können. Das Modell dient Ihnen als Grundlage für die darauf aufbauenden Erläuterungen in den folgenden Kapiteln.

Ebenso in den 1970er Jahren und damit Jahre vor dem OSI-Modell wurde durch das amerikanische Militär (und damit zu Beginn nicht öffentlich!) ebenfalls ein Modell mit Schichten entwickelt, dies im Zusammenhang mit dem Aufbau des ARPANet, der Grundlage des späteren Internets. Dieses – *DoD-Modell* genannt – enthält lediglich vier Schichten und die unterste Schicht wurde nicht durch das Modell, sondern durch Verweise auf bestehende Technologien beschrieben. Beide Modelle sind heute in Verwendung, das OSI-Modell als umfassenderer Ansatz, das DoD-Modell als näher an der Implementation liegendes Modell, das vor allem durch die Verbreitung des Internets nachhaltig an Bedeutung gewonnen hat.

Lernen Sie in diesem Kapitel:

- Die Geschichte der Netzwerke kennen
- Die Aufteilung von Netzen nach verschiedenen Ansätzen durchführen
- Die Bedeutung von Referenzmodellen verstehen
- Entstehung und Aufbau des OSI-Modells verstehen
- Die Schichten und ihre Funktionen auseinanderhalten
- Das DoD-Modell als alternativen Ansatz kennen
- Die Bedeutung der Schichten und der Vergleich zum OSI-Modell erkennen

## 2.1 Es war einmal ein Netzwerk

Die Geschichte der Netzwerke ist nicht ganz so alt wie die Geschichte der Computersysteme. Die 1960er Jahre waren geprägt von der Entdeckung der Kapazität von Großrechnern. Die prägenden Geräte und Nutzer dieser Zeit waren:

- Einzelne Systeme, sogenannte Großrechner
- Lochkartenleser für die Speicherung von Daten
- Programmierer, Operateure, Spezialisten (aber keine Benutzer!)

Ende der 60er Jahre trat mit der Inbetriebnahme der ersten Stufe des Internets (des sogenannten ARPANet) das Thema Vernetzung erstmals in geografisch größerem Ausmaß auf. Es ging dabei darum, bestehende und weit voneinander entfernte Systeme so miteinander zu verbinden, dass Daten hin- und herbewegt werden konnten.

Die 70er Jahre brachten die Entwicklung von Endbenutzergeräten, damals Terminals genannt, welche direkt abhängig von der Kapazität des zentralen Rechners waren und weder über eigene Betriebssysteme noch Anwendungen verfügten. Sie dienten lediglich der Eingabe und Weiterleitung von Daten direkt an den Zentralrechner. Der Begriff *Terminal* hat die Zeit aber überdauert und bezeichnet heute in ähnlicher Funktion eine Software, die mit einem Server Kontakt aufnimmt und die Daten direkt auf dem Server bearbeitet.

Mit der Firma Xerox machte sich ebenfalls in 70er Jahren auch erstmals ein Unternehmen Gedanken über eine mögliche Vernetzung gleichberechtigter Rechner. Die prägenden Stichwörter waren in dieser Zeit:

- Großrechnerlösungen, ergänzt mit Dialog (Terminal) für mehrere Benutzer
- Trennung von Großrechner und eigentlichem Arbeitsplatz
- Palette neuer Produkte in der Datenverarbeitung nahm stark zu

Die 80er Jahre brachten den Einstieg von PCs auf dem EDV-Markt. Im Unterschied zu den Terminals verfügten sie über einen eigenen Prozessor und eigene Speichermöglichkeiten. Damit wurden sie zumindest teilweise unabhängig von den Großrechnern.

Bald schon machten sich mehrere Hersteller auf, um diese PCs miteinander zu verbinden, allen voran die Firma Novell. Es ist aber auch das Jahrzehnt der Firma IBM, deren sogenannte PS/2-Rechner für Jahre den Markt völlig beherrschten.

Die PC-Betriebssysteme der damaligen Zeit waren an sich noch nicht für eine Vernetzung der Geräte geeignet. Prägende Systeme waren etwa DOS und gegen Ende der 80er Jahre die Versionen Windows 1 und Windows 2. Zudem trat Apple mit seinem macOS auf den Markt. Von daher mussten für Netzwerkprojekte spezielle Netzwerkbetriebssysteme eingekauft werden wie etwa Novell NetWare, LANtastic Networks oder auch Banyan Vines.

Die 90er Jahre waren demgegenüber das Jahrzehnt der aufkommenden Client/Server-Architektur. Nachdem Novell über einige Jahre eine marktbeherrschende Stellung im PC-basierten Netzwerkbereich innehatte, betrat mit Microsoft und dem Produkt Windows NT zu Beginn der 90er Jahre ein wichtiger Konkurrent den Markt. Mit der Einführung von Windows 95 und Windows NT 3.5x begann die Dominanz von Novell sich schrittweise aufzulösen, nachhaltig mit der Einführung des Serverbetriebssystems Windows 2000 und dessen Nachfolgern.

Zugleich waren die 90er Jahre geprägt vom Vorhaben, die aufkommenden Netzwerke und ihre Lösungen zu standardisieren.

Das neue Jahrtausend wird bislang von folgenden Bemühungen und Trends geprägt:

- Etablierung von schnellen Verbindungswegen mit 1 Gbps und mehr
- LAN, MAN und WAN verschmelzen technologisch und geografisch.
- Vernetzung unter globalen Gesichtspunkten
- Drahtlose Übertragungen im lokalen Netz (Wireless LAN) mit immer mehr Tempo und mehr Reichweite werden realisiert.
- Das Internet der Dinge schreitet stetig voran.
- Sicherheitsmechanismen greifen immer tiefer in das Netzwerk ein.
- Die Datenverarbeitung wird nicht mehr lokal, sondern in der Cloud durchgeführt, dadurch nimmt die Bedeutung der Virtualisierung stark zu.
- Das moderne Endgerät ist nicht mehr (nur) der PC, sondern Geräte wie das Tablet oder das Smartphone, die Datenbearbeitung wird mobil.

## 2.2 Was ist denn eigentlich ein Netzwerk?

Die aktuelle Definition dazu lautet:

Ein Netzwerk ist eine Anzahl voneinander entfernter, intelligenter Maschinen, die alle über Kommunikationsleitungen miteinander verbunden an denselben Daten und Informationen teilhaben.

*(Markus Kammermann, CompTIA Network+ 1. Auflage 2008)*

Die Welt der Netzwerke kann auf drei Hauptkomponenten reduziert werden:

- Netzwerkelemente: Was gehört ins Netzwerk?
- Netzwerkmodelle: Wie wird das Netzwerk gebaut?
- Netzwerkmanagement: Wie wird das Netzwerk verwaltet?

## 2.2.1 Netzwerkelemente

Sie werden in den folgenden Kapiteln sehen, dass es zahlreiche unterschiedliche Elemente gibt, die Sie für den Aufbau eines Netzwerks benötigen. Die Grundbegriffe der Netzwerktechnik lauten »Daten«, »Schnittstelle« und »Protokoll«.

Als *Daten* bezeichnet man in der Netzwerktechnik Informationen, die über das Netzwerk transportiert werden. Die Übermittlung dieser Informationen von einem zum anderen Ort ist ein Kernanliegen der Vernetzung. Daten werden über verschiedene Geräte und Medien transportiert. Damit dies möglich ist, müssen die Regeln für diese Vermittlung bestimmt werden, dies sind die *Schnittstellen*. Durch die Definition von Schnittstellen wird es möglich, über verschiedene Systeme und Netzwerke hinweg Informationen weiterzugeben.

*Protokolle* sind eigentlich Sprachkonventionen. So wie es Französisch, Deutsch oder Italienisch als Sprache gibt, so gibt es unterschiedliche »Netzwerksprachen«, wobei der Begriff des Protokolls sehr allgemein ist und in vielen unterschiedlichen Zusammenhängen verwendet werden kann. Daher ist es meistens notwendig, dem Begriff die Verwendungsebene oder eine genauere Definition mitzugeben, wie etwa *Transportprotokoll* oder *Anwendungsprotokoll*.

Häufig werden Netzwerke von einem oder mehreren Rechnern aus verwaltet, die zentrale Dienste für das Netzwerk anbieten. Diese speziellen Rechner tragen den Namen *Server*. Die Gegenstellen eines Servers nehmen die Dienste des Servers als Kunden in Anspruch, sie werden daher neudeutsch *Clients* genannt.

Folgende Aufgaben können von einem Server wahrgenommen werden:

- Ressourcen wie Drucker oder Speicher bereitstellen
- Benutzerkonten verwalten (Benutzer erstellen, Rechte und Rollen zuteilen)
- Berechtigungen für Daten und Programme verwalten
- Dienste wie E-Mail oder Telefonie bereitstellen
- Anwendungen ausführen, auf die mittels Clients zugegriffen werden kann

Beim Client/Server-Ansatz ist die Aufgabe der übergeordneten Datenverarbeitung zwischen einem oder mehreren Client-Rechnern und dem Server aufgeteilt. Clients übermitteln Anforderungen an Dienste der Server im Netz. Der Server empfängt die Anforderung und führt eine Aufgabe aus wie etwa das Bereitstellen einer Datei für den Client. Führt ein Server nur einen bestimmten Dienst aus und ist für diesen reserviert, spricht man von einem *dedizierten Server*.

Auf der anderen Seite gibt es auch Netzwerke, die ohne solche zentralen Server funktionieren, denken Sie nur an die Verbindung von mehreren kleinen Geräten wie mobilen Telefonen über Bluetooth. Diese Netzwerke werden ein Netz von Gleichberechtigten, auch *Peer-to-Peer-Netzwerk*, genannt.

Zudem gibt es durchgehend strukturierte Vernetzungen vom kleinsten Rechner bis hin zu Großrechnern, sogenannten *Mainframes*, wo verschiedenste Elemente zusammenwirken.

Dieser letzte Ansatz, der eigentlich aus den 1970er Jahren stammt, gewinnt mit der Verbreitung des sogenannten *Cloud Computing* wieder an Bedeutung. Denn auch hier werden nicht mehr einzelne Dienste für Clients bereitgestellt, sondern die ganze Verarbeitung kann auf dem zentralen Server erfolgen und die Clients greifen über eine internetbasierte Schnittstelle wie einen Browser oder ein Terminalprogramm auf diesen Server zu und arbeiten dann nicht mehr lokal, sondern eben in der Cloud.

Alle diese Ansätze sind in der aktuellen Netzwerktechnik vorhanden und bei allen braucht es eine ganze Reihe von Standards und Spezifikationen, damit die Kommunikation in einem solchen Netzwerk funktioniert.

## 2.2.2 Netzwerkmodelle

Um diese Vielfalt an Möglichkeiten klassifizieren zu können, bedient man sich unterschiedlicher Netzwerkmodelle. Das sind zum einen die sogenannten Schichtenmodelle wie das OSI-Modell oder das DoD-Modell, diesen wenden wir uns im nächsten Kapitel zu. Zum anderen ist ein Modell sehr verbreitet, das sich historisch an der Ausdehnung des Netzwerks orientiert. Die klassischen Begriffe dazu lauten:

- Local-Area Network (LAN)
- Metropolitan-Area Network (MAN)
- Wide-Area Network (WAN)

Dazu sind in den letzten Jahren die Begriffe GAN für globale Netzwerke und PAN (Personal Area Network) bzw. BAN (Body Area Network) für engräumige Netzwerke entstanden. Vereinzelt ist auch der Begriff CAN für Campus Area Network anzutreffen, womit »übergroße« LANs zum Beispiel auf einem Universitätsgelände zu verstehen sind. Der letzte Begriff tritt aber eher selten auf.

Ein PAN bzw. BAN bezeichnet ein Netzwerk im Bereich von wenigen Zentimetern bis einigen Metern, z.B. für das kontaktlose Bezahlen oder die Verbindung eines Headsets mit dem Computer oder Telefon. Auch die »Wearables«, also am Körper tragbare elektronische Geräte wie Smart Watches oder elektronische Armbänder, welche die Bewegung oder den Puls aufzeichnen, gehören in diese Kategorie.

Ein LAN bezieht sich auf eine Kombination von Computer-Hardware und Übertragungsmedien von relativ geringem Umfang. LANs befinden sich üblicherweise innerhalb eines Gebäudes und benutzen meist nur eine Art der Verkabelung. Sie sind selten größer als 10 km und laufen ausschließlich über privaten Grund. LANs bilden heute das Rückgrat der Informatik in vielen Unternehmen, sie verbinden

die verschiedenen Mitarbeiter untereinander und versorgen mit lokalen Daten, bieten aber auch eine Schnittstelle zu MAN oder WAN an, z.B. dem Internet.

Ein MAN ist größer als ein LAN. Es wird »Metropolitan« genannt, weil es normalerweise die Ausdehnung einer Stadt erreicht. Oft werden verschiedene Typen von Hardware und Übertragungsmedien benutzt, um die Entfernungen effizient zu überbrücken. MANs verbinden typischerweise unterschiedliche Systeme mit verschiedenen Funktionen. Sie dienen daher eher als Transportnetzwerke, sind also nicht unbedingt direkt mit Clients verbunden, sondern stehen als Rückgrat zur Verbindung von verschiedenen lokalen Netzwerken zur Verfügung.

Ein WAN ist das klassische Verbindungsnetzwerk über größere Distanzen für LANs oder MANs. Auch hier handelt es sich um ein Transport- und Verbindungsnetzwerk. Von einer WAN-Anbindung spricht man, wenn das eigene LAN über eine größere Distanz Verbindung zu einem anderen LAN aufnehmen möchte oder wenn Sie Ihr lokales Netzwerk ans Internet anbinden wollen. Ein WAN wird nicht privat betrieben, sondern von einem Provider, bei dem man sich für dessen Benutzung anmelden und dann eine Leitung oder Kapazitäten mieten kann. Technologisch betrachtet, sind MAN und WAN heute weitgehend identisch, nicht aber in ihrer Ausdehnung. Und während WANs in der Regel von größeren Telekom-Providern betrieben werden, gibt es für ein MAN durchaus auch regionale Anbieter.

Der Begriff des GAN ist der am wenigsten spezifizierte in dieser Liste. Er bezeichnet weniger ein Netz als die Technologien, die dann eingesetzt werden, wenn eine Verbindung über sehr große Distanzen oder in Gebieten ohne WAN-Anschlüsse realisiert werden soll.

Die folgende Tabelle zeigt Ihnen den aktuellen Stand der Begriffe und Modelle.

	Geschwindigkeit	Ausdehnung	Bemerkungen
GAN	9,6 Kbps bis > 2 Mbps	Weltweit	Häufig Satellitenverbindung. Sehr heterogene Technologien im Einsatz, erst wenig Glasfaser.
WAN	2 Mbps bis 100'000 Mbps	... 1'000 km	Zunehmend reine Glasfasernetze, vor allem in Europa. Für Kontinentalverbindungen immer noch Kupferkabel, z.B. Seekabel. Neuere Seekabel bestehen ebenfalls aus Glasfaser.
MAN	100 bis 100'000 Mbps	... 100 km	Technisch heute keine eigene Domäne mehr, da WAN und MAN zusammengedrückt sind.
LAN	100 bis 100'000 Mbps	< 10 km	Heute 1 Gbps als aktueller Standard, Multi-Gigabit ist zunehmend weitverbreitet, 10 Gbps im Zunehmen, 40/100 Gbps ebenso.
PAN/ BAN	1 bis 300 Mbps	< 100 m	Klassische Wireless-Zone für Bluetooth, Mobile Devices, Wearables und Smart Devices untereinander oder als Verbindung zu größeren Geräten (z.B. Headset zu Smartphone).

Tabelle 2.1: Netzwerkmodelle

# Stichwortverzeichnis

- 1000Base-LX 129
  - 1000Base-SX 129
  - 1000Base-T 62, 129
  - 100Base-T 129
  - 100Base-TX 129
  - 100GBase 131
  - 100GBase-CR10 131
  - 10GBase 130
  - 10GBase-T 129
  - 110-Block 141
  - 2,4-GHz-ISM-Band 157
  - 2FA 323
  - 3G 200
  - 3-Tier Architecture 116
  - 40GBase 131
  - 40GBase-KR4 131
  - 5G 202
  - 5-GHz-ISM-Band 157
  - 66-Block 141
  - 6in4 223
  - 6to4 223
  - 802.11a 159
  - 802.11ac 156
  - 802.11ax 158
  - 802.11b 154, 159
  - 802.11g 154, 159
  - 802.11i 167
  - 802.11n 155, 159
  - 802.11p 162
  - 802.11s. 162
  - 802.11aq 96
  - 802.3bt 132
  - A**
  - AAA 97
  - AAAA 265, 328
  - AAA-Protokoll 328
  - AAL 187
  - Abisolierzange 505
  - Absichtserklärung 472
  - Access Point 91, 150, 562, 563
  - ACK 585
  - ACL 307
  - ACR 504
  - Active Directory 293
  - Adernpaare 75
  - Ad hoc 165
  - Adresse
    - 32 Bit 209
    - Dienstadresse 208
    - IPv4 209
    - IPv6 217
    - Logische Adresse 208
    - Physische Adresse 208
    - Subnetzmaske 211
  - Adressschema 533, 560
  - ADS 309, 310, 323, 426
  - ADSL 191, 537, 560
  - Adware 340
  - AES 330, 569
  - Analoge Datenübertragung
    - 58
  - Änderungsdokumentation
    - 453
  - Änderungsprotokoll 444
  - Antenne
    - Fresnelzone 589
    - Omni 590
    - Verbindungskabel 589
    - Wirkungsgrad 589
    - Yagi 590
  - Anwendungsschicht 44
  - Anycast 120
  - APIPA 257
  - APON 196
  - Application Gateway 396,  
399, 400
  - APT 350, 352
  - Arbitrary Code Execution 361
  - ARP 228, 229
    - ARP-Cache 229
    - ARP-Reply 228
    - NDP 229
    - RARP 229
  - ARPANet 45, 208
  - AS 249, 515
  - ASLR 362
  - ASP 299
  - Asynchrone Datenübertragung 63
  - ATM 186
    - ATM-Schichtenmodell 186
  - Attacke 353
    - Advanced Persistent Threat 352
  - Bluejacking 369
  - Bluesnarfing 369
  - Carbanak 352
  - Cookie-Diebstahl 359
  - DNS Amplification Attack 355
  - DoS 355
  - FTP Bounce 354
  - Man-in-the-Middle 358
  - MMS-Phishing 351
  - Permanent DoS 356
  - Pharming 352
  - Phishing 351
  - Session-Hijacking 359
  - SMS-Phishing 351
  - Smurf 355
  - Spoofing 359
  - SYN-Flood 356
  - TCP-Hijacking 359
  - Zero hour 351
- Ausbreitungsgeschwindigkeit 54
  - Authentifizierung 319, 584
  - Autonomes System 249
  - Autorisierung 370
  - Awareness 389
  - AXTLK 504
  - B**
  - Backbone 115, 139
  - Badge 375, 376
  - BAKOM 146
  - Bandbreite 64

- Banner Grabbing 485  
 Basisanschluss 182  
 Basisbandübertragung 118  
 Bastion Host 399  
 Baudrate 62  
 Bauliche Maßnahme 374  
 Beamforming 157  
 Benutzer 308  
 Benutzerrechte 307  
 BGP 253  
 Bidirektionale Übertragung 63  
 Biometrisches Erkennungssystem 376  
 Bitrate 62, 64  
 Bitübertragungsschicht 41  
 BIX 141  
 Bluetooth 173  
 BNC 81  
 BNetzA 146  
 Bonding 383  
 BOOTP 255  
 Brandfall 417  
 Brandschutz 374, 380  
 Breitbandübertragung 118  
 Bridge 90, 566  
 Broadcast 120, 581  
 Broadcast Storm 91  
 BSS Coloring 157  
 Buffer Overflow 360, 362  
 Butt Set 507  
 Byte 66
- C**
- CAM 92  
 CARP 254  
 CATV 81, 195  
 CCMP 168  
 CENELEC 73  
 Change-Protokoll 492  
 CHAP 325, 433  
 CIA 317  
 CIDR 212, 580, 581  
 CIFS 295  
 Circuit Level Firewall 400  
 Citrix 427  
 Client/Server-Architektur 31, 284  
 Client-Server 255  
 Cloud Computing 296, 298, 486  
   IaaS 298  
   PaaS 298
- SaaS 298  
 XaaS 299
- CO<sub>2</sub> 381  
 Collapsed core 116  
 Command and Conquer 502  
 Companion-Virus 347  
 Connectionless Communication 120  
 Connection-oriented Communication 119  
 Consumption Budget 133  
 CoS 243  
 CRC 64  
 Crimeware 341  
 Crimpzange 506  
 Crosskabel 76  
 CSMA/CD 126  
 CSU 103  
 CVE 363  
 CVSS 363  
 CWDM 103
- D**
- DAD-Prüfung 221  
 Dämpfung 53, 54, 503  
 Darstellungsschicht 44  
 Data-at-rest 331  
 Data-in-transit 331  
 Data-in-use 331  
 Daten 32  
 Datenbandbreite 117  
 Datenintegrität 317  
 Datensicherung 386  
 Datensignalisierung 63  
 Datenübertragung  
   Asynchron 63  
   Parallel 61  
   SCSI 61  
   Seriell 62  
   Synchron 63  
 Datenverfügbarkeit 317  
 Datenvertraulichkeit 317  
 DCS 487  
 DDoS 354  
 Dedizierte Firewall 395  
 Demarc 139  
 Demarkationspunkt 139  
 Denial of Service 345, 354, 361  
 DEP 362  
 DHCP 255, 533, 541, 566  
   APIPA 257  
   Automatisch 256  
   Dynamisch 256  
   Scope 257  
   Server 566  
   Statisch 256  
 DHCPv6 257  
 Diagramm 533, 560  
 Diameter 327, 584  
 Dienst 525  
 Dienstleistungsrahmenvertrag 472  
 DiffServ 218, 243  
 DLL-Injection 362  
 DMZ 394, 401  
   Geschlossene 401  
   Halboffene 401  
   Offene 401  
 DNS 259, 397, 436, 516, 537  
   CNAME 265  
   Missbrauch 355  
   Namensraum 260  
   Name Server 262  
   Resolver 263  
   Resource Record 264  
   Zonendatei 262  
 DNSSEC 266  
 DOCSIS 195  
 DoD-Modell 36, 45, 46, 208  
 DoH 266  
 DoT 266  
 Drehschleuse 377  
 Drucker 547  
 Druckerserver 314  
 Druckertreiber 314  
 DSAP 124  
 DSCP 243  
 DSL 191  
 DSU 103  
 Dual-Stack 217  
 Duplexverfahren 89  
   Auto Sense 89  
 DWDM 103, 185, 190
- E**
- EAP 326  
 ECN 219  
 EDGE 200  
 Edge Control 584  
 EFS 294  
 EGP 250  
 EIA/TIA 73  
   Norm 569A 139  
   TIA-568A 73  
   TIA 568B 73

- EIA/TIA-568 73  
 EICAR 391  
 EICAR-Code 392  
 EIGRP 252  
 Einbruchsschutz 379  
 EIP 362  
 EMI 71  
 end-of-life 454  
 end-of-support 454  
 Endspan 133  
 Environmental Monitor 509  
 ESD 498  
   Erdung 499  
   ESD-Strip 499  
 Etherjack 139  
 Ethernet 127  
 Ethernet-Frame 125  
 Ethernet over HDMI 131  
 Ethernet over PowerLine 131  
 EUI-64 220  
 EuroDOCSIS 195  
 Evil Twin 369  
 EVPN 116  
 Expertenmodus 564  
 Exploit 360
- F**  
 F/FTP 78  
 F/STP 79  
 F/UTP 78  
 Far-End Crosstalk 503  
 Far-End-Fault 100  
 Faser  
   Monomode 82  
   Multimode 82  
   Singlemode 82  
 Fault Management 440  
 FCAPS 440  
 FCC 146  
 F-Connector 81  
 Fehlermanagement 442  
 Fehlersuche 501  
   Lösung 501  
   Symptome 501  
   Ursachen 501  
 Fehlertoleranz 383  
 Ferrule 84  
   APC 85  
   UPC 84  
 Feuerlöschanlage 381  
 Firewall 394, 561, 570  
   Dedizierte 395  
   Hardware 395  
   Personal Firewall 394  
   Firmware 454, 539, 547  
   First Responder 412, 416  
   Fluchtplan 413  
   Fluke 508  
   FQDN 261  
   Frame 66  
   Freigabe 552, 553  
   Freigaberechte 307  
   Frequency Hopping 148  
   Frequenzbereiche 56  
   FRM 417  
   FTP 270  
   FTTH 196  
   F-type 80  
   Fullduplex 63  
   Funkwelle 173  
   Funkzelle 149
- G**  
 GAN 34  
 Gateway 212, 563  
 GBIC 100  
 GG45 77  
 GigaBIX 141  
 GPL 291  
 GPRS 199  
 Grayware 340  
 Großrechner 30  
 GSM 199
- H**  
 H2M-Schnittstelle 488  
 H.323 240  
 Halbduplex 63  
 Hardware-Abstraktionsschicht 293  
 Hardware-Virtualisierung 296  
 Hash 328  
 HDSL 192  
 Header 39  
   IPv4 216  
   IPv6 218  
 Hexadezimalsystem 51  
 Honeynet 403  
 Honeypot 403  
 Host 33, 258  
 Hotline 496  
 Hot Site 415  
 HSCSD 199  
 HTTP 267, 397  
 HTTPS 268
- Hub 90  
 Hub and Spoke 432  
 Hybrid Cloud 300
- I**  
 IaaS 299  
 IAB 206  
 ICA-Protokoll 427  
 ICMP 227  
 ICS-Server 488  
 ICT-Betriebsdokumentation 449  
 IDS 404, 405, 406, 474  
 IEEE 123  
 IEEE 802.1x 98  
 IEEE 802.2 124  
 IEEE 802.3 124  
 IEEE 802.3-2012 128  
 IEEE-802-Reihe 123  
 IETF 205  
 Ifconfig 510  
 IGMP 228  
 IGP 250  
 IGRP 252  
 IKEv1 432  
 IKEv2 432  
 IMAP4 276  
 Impedanz 53  
 In-band 97  
 Industrie 4.0 486  
 Infrarot 170  
 Integer Overflow 362  
 Internet 30  
 Internet of Things 489  
 IoT 175, 198, 489  
 IP 209  
 IP-Adresse 210  
   Adressklassen 213  
   IPv4 213  
   IPv6 217  
   Private 214  
   Reservierte 214  
 Ipconfig 510  
 Iperf 482  
 IP Helper 258  
 Ip-Kommando 511  
 IPoE 566  
 IPS 474  
 IPsec 335  
 IP-Spoofing 359  
 IP-Telefonie 240  
 IPv4 578  
   Adressklassen 213

- Adressschema 450
  - Ausnahmeadressen 215
  - CIDR 212
  - IP-Header 215
  - Netz-Bits 214
  - Private Netzwerke 214
  - IPv6 213, 217, 567, 578
    - Adressklassen 218
    - Ausnahmeadressen 220
    - EUI-64 220
    - Header 218
    - Multicast 222
    - Payload 219
    - Präfix 218
    - Reservierte Adresse 220
    - Traffic Class 218
  - ISAKMP 335, 432
  - iSCSI 302
  - ISDN 62, 182
    - B-ISDN 183
    - B-Kanal 182
    - Breitband-ISDN 183
    - D-Kanal 182
    - E1 182
    - E3 182
    - T1 182
    - T3 182
  - ISDN-BRI 182
  - ISDN-PRI 182
  - IS-IS 253
  - ISM-Band 146
  - ISMS 318, 411, 490
  - ISO 27001 411, 417
  - ISO/IEC 11801 74
  - ITU-R 146
- J**
- Jamming 475
  - Jperf 482
  - Jumbo Frames 125, 484
- K**
- Ka-Band 198
  - Kabel 71
    - Adern 75
    - AutoSense 76
    - Drahtlose 70
    - EN 50288 75
    - Koaxialkabel 70
    - Lichtwellenleiter 70
    - Rollover 76
    - STP 70
    - UTP 70
  - Kabeltester 502, 509
  - Kabelziehstrumpf 507
  - Kamera 377
  - Kapazität 53
  - Kennwort 536, 542, 564
  - Kerberos 326
  - Keycard 375
  - Klartextübermittlung 353
  - Koaxialkabel 80
  - Kollisionsdomäne 576
  - Kompetenz 496
  - Konfigurationsdaten 386
  - Kurzschluss 502
- L**
- L2TP 432
  - L3-Diagramm 448
  - LAN 33
  - Latenz 64, 198
  - Latenzprobleme 591
  - LCAP 384
  - Leistungsbeschreibung 471, 473
  - Leitungsunterbrechung 502
  - Leitungsvermitteltes Netzwerk 118
  - LEO 197
  - Letter of Intent 472
  - Lichtwellenleiter 81
  - Link Aggregation 98
  - Link State 252
  - Linux 291
  - Load Balancing 383
  - Logdateien 490
  - Looking Glass 515
  - Loopback 99
  - Loopback Plug 507
  - LoRaWAN 198
  - LPWAN 198
  - LSA-Werkzeug 505
  - LTE 201
  - LTE+ 201
- M**
- M2M 489
  - MAC-Adresse 43, 88, 476
  - Mail-Server 272
  - Mainframe 59
  - Makroviren 344
  - Malware 340, 342, 346, 349, 390
    - Adware 340
    - Antispyware 341
    - Crimeware 341
    - Grayware 340
    - Spam 340
    - Spyware 340
  - MAN 34
  - Managed Switch 97
  - Man-in-the-Middle-Attacke 358
  - Mannschleuse 377
  - Man Trap 377
  - Master Service Agreement 472
  - Maßnahme
    - Bauliche 374
  - Medienkonverter 99
  - Medium
    - EMI 71
    - Installationsaufwand 71
    - Kapazität 71
    - Kosten 71
    - Plenum 71
  - MEF-Forum 107
  - Mehr-Faktor-Authentifizierung 323
  - Mehrpunktverbindung 111
  - Memory of Understanding 472
  - Messprotokolle 453
  - Metrik 249
  - Metro Optical 197
  - MFA 323
  - mGRE 433
  - MIB 440
  - Midspan 133
  - MIMO 155, 567
  - Mitarbeit
    - Aufgabenteilung 370
    - Job Rotation 370
    - Mandatory Vacations 370
    - Segregation of Duty 371
  - Modem 101
  - Modulation 101
  - Modus 1 Siehe Bluetooth
  - Monitor 464
    - Hardware 465
    - Hybrid 466
    - Messdaten 465
    - Messobjekt 464
    - Messpunkt 464
    - Messzeit 465
    - Schwellwert 465
    - Software 465

- Monitoring 464, 468
- MOU 472
- MPLS 190, 243
- MRTG 480
- MSA 472
- MSDS 499
- MTR 514
- MTU 125
- Multicast 120
- Multimeter 507
- Multimode 83
- Multiplexer 59, 102, 184, 191
  - CWDM 103
  - Demultiplexer 60
  - DWDM 103
  - FDM 60
  - SMX 61
  - TDM 60
  - WDM 61
- Multiplikator 49
  - Binärsystem 51
  - Dezimalsystem 49
  - Hexadezimalsystem 51
  - Oktalsystem 51
- MUMIMO 156, 157, 567
  
- N**
- NAC 403, 583
  - Quarantänebereich 584
  - Server 584
- Namensauflösung 516
  - Fehlerquellen 516
- NAS 302
- NAT 230
  - DNAT 231
  - NAPT 231
  - PAT 231
  - SNAT 231
  - SUA 231
- Nbtstat 516
- Nebensprechen 54
- Negative Rules 396
- NET-Befehl 305, 519
- net-Befehl 521
- NetBIOS 259, 516, 553
- Netio 482
- Netsh 522
- Netstat 524
- Network+-Zertifizierung 19
  - Eintrittstest 22
  - Prüfungscodes 596
  - Wissensgebiete 19
- Network Interface Unit 507
  
- Netzwerk
  - Client/Server 32
  - Definition 31
  - Dienst 32
  - Installation 531
  - Inventar 532, 559
  - Konfiguration 535
  - Konzeption 532
  - Leitungsvermitteltes 118
  - Modell 33
  - Netzwerkelement 31
  - Netzwerkmanagement
    - 31
    - Netzwerkmodell 31
    - Paketvermitteltes 119
    - Peer-to-Peer 32
- Netzwerkanalyse 474
  - Kenngrößen 474
  - Messdaten 474
  - Messkonzept 474
  - Sniffer 474
- Netzwerkdigramm 444
- Netzwerkdokumentation
  - 443, 446
  - Änderungsdokumentation 446
  - Anschlussdiagramm
    - 446, 447
  - Konfigurationsdokumentation 446
  - Logbuch 446
  - Messdiagramme 446
  - Messdokumente 453
  - Netzwerkdigramm
    - 446, 447
  - Verkabelungsschema
    - 446
- Netzwerkdrucker 314, 533
- Netzwerkkarte 87
  - Duplexverfahren 89
  - Virtuelle 106
- Netzwerkmanagement 35, 439
  - Sicherheit 439
  - Skalierbarkeit 439
  - Verfügbarkeit 439
- Netzwerkmodell 33
  - BAN 33
  - CAN 33
  - GAN 33
  - LAN 33
  - MAN 33
  - WAN 33
- Netzwerkmonitor 475
- Netzwerkrichtlinien 367
- Netzwerküberwachung 475
- NEXT 503
- NFC 177
- NFV 105
- NGN 188
- NIDS 405
- NIPS 405
- NIU 507
- NNTP 272
- NOP 362
- Notausgänge 413
- Notfallplan 367
- Notfallvorsorge 413
- Novell 30, 31
- Nslookup 517
- NTFS 294, 311, 312
- NTP 276
- NTS 277
- Nutzungsrichtlinien 367
  
- O**
- OC 185
- OLA 472
- On Path Attack 358
- OS-Fingerprinting 485
- OSI-MF 440
- OSI-Modell 37, 40, 45, 46, 70, 187, 207
  - Anwendungsschicht 39
  - Bitübertragungsschicht 40
  - Darstellungsschicht 40
  - Sicherungsschicht 40
  - Sieben Schichten 38
  - Sitzungsschicht 40
  - Transportschicht 40
  - Vermittlungsschicht 40
- OSPF 252
- Ost-West-Verkehr 116
- OS X 288
  - Aqua 289
  - Darwin 289
- OUI 89
- Out-of-band 97
  
- P**
- PaaS 299
- Paketfilter 396, 397
- Paketvermitteltes Netzwerk
  - 119
- PAP 325, 433

- Passwort 308, 319
- Patch 454
- PDCA 470
- PDoS 356
- Peer-to-Peer 284
- Perfect Forward Secrecy 432
- Performancemanagement 445
- Personal Firewall 394
- Piggybacking 366
- PIMF 78
- Ping 511
- ping6 512
- Pin-zu-Pin-Messung 509
- PKI 332
- PLC 488
- PMTU 125
- PoE 99, 132
  - 802.3at 132
- PoE+ 132
- PON 196
- POP3 274
- Port 236
  - Dienstadresse 236
  - TCP 237
  - UDP 237
- Port Mirroring 98
- Ports 353
  - Dynamisch 237
  - Registered Ports 237
  - Well-known 237
- Portscanner 485
  - Legalität 486
  - Online 485
- Positive Rules 396
- POTS 181
- PowerLAN 87
- Powerline 87
- Powerline Communication 87
- Power over Ethernet 132
- PPP 325, 537, 566
- PPPoE 537, 566
- PPTP 434
- Pre-Shared Key 169, 569
- Primäranschluss 182
- Primärverkabelung 138
- Private Cloud 300
- Profil 309
- Protokoll 32
- Proxy 403, 404
- Prüftelefon 507
- Prüfungsvorbereitung 596
- PSK 569
- PSTN 181
- Public Cloud 300
- Pufferüberlauf 357
- Punch Down Tool 506
- Punkt-zu-Punkt-Verbindung 111
- Q**
- QoS 218, 243, 469
  - Dienstklassen 469
  - Parameter 469
- QSFP 100
- R**
- Rack 500
  - Beschriftung 500
  - Kabelkanäle 500
  - Monitoring 500
  - Säulen 500
  - Schienen 500
- Radius 327, 584
- Ransomware 347
- RAS 424
- Rauchabsauganlage 381
- Rauschen 53
- RDP 426
- Reaktionsfähigkeit 496
- Rechte-Matrix 453
- Redundanz 415
- Referenzmodell 35, 36
  - DoD-Modell 35
  - OSI-Modell 36
- Remote Assistance 428
- Remotedesktopverbindung 425
- Repeater 90
- Resource Exhaustion Attack 361
- Rettungsplan 413
- Return Loss 504
- Reverse Proxy 404
- RFC 206, 208
- RFID 175
- RG-58 80
- RG-59 80
- RG-6 80
- RG-8 80
- RIP 105, 250
- RJ45 76
- RJ48 76
- RMON 442, 458
- Rogue Access Point 369
- Root Bridge 94
- Round Trip Time 65
- Route
  - Kommando 514
- Router 104, 105, 532
  - Link State 105
  - OSPF 105
  - RIP 105
  - Virtuell 107
- Routing 249
  - BGP 253
  - CARP 254
  - Count-to-Infinity 251
  - DVA 250
  - EIGRP 252
  - Hop-Counts 251
  - HRSP 255
  - IGRP 252
  - IS-IS 253
  - Link State 252
  - OSPF 252
  - RIP 250
  - RIPv2 251
  - Split Horizon 251
  - RRRP 254
- Routing-Protokoll 248
- RRDtool 480
- RSA 330
- RSTP 93, 385
- RSVP 470
- RTP 241
- RTS 152
- RTT 65
- S**
- S/FTP 78
- S/STP 79, 576
- S/UTP 78
- SA 335
- SaaS 299
- Safe 379
- SAN 302
- Sandbox 403
- Satellit 197
  - geostationär 198
  - LEO 198
- Satellitenschüssel 197
- SCADA 488, 489
- Schleuse 377
- Schließsystem 375
- Schlüssel 375
- Schnittstellen 32
- Schulung 390

- Schwachstelle  
Suche 407
- Score Report 601
- Screened Subnet 401
- SDH 184
- SDN 105, 448
- SDSL 192
- SD-WAN 106
- SD-WAN Edge 107
- SD-WAN Orchestrator 107
- Security-Scanner 407
- Sekundärverkabelung 138
- Sensibilisierung 389
- Seriell  
DB-25 62  
EIA-RS232 62  
USB 62  
V.24 62
- SF/FTP 78
- SF/STP 79
- SF/UTP 78
- SFP+ 100
- Shielded Twisted Pair 78
- Shoulder Surfing, 367
- SiBe 411
- Sicherheitslücke 408, 454  
Release-Notes 408
- Sicherheitsmanagement 445
- Sicherungsschicht 41
- SIEM 411, 412, 413
- Sigfox 198
- Signal  
Amplitude 58  
Ausbreitung 54  
Codierung 59  
Dämpfung 55, 194  
Digitale  
Übertragung 58  
Frequenz 56, 58  
Sinus 54  
Wellenlänge 56
- Signal-to-Noise 53
- Simplex 63
- Singlemode 83
- Single Sign On 323
- SIP 241
- Sitzungsschicht 44
- SLA 470, 473  
Fehlerraten 471  
Leistung 471  
Reaktionsbereitschaft 471  
Sanktionen 471
- Verfügbarkeit 471
- SLAAC 221
- Smartjack 139
- SMB 295, 553
- SMON 442, 458
- SMTP 273, 274
- Smurf 355  
Amplifier 356
- Sniffing 474
- SNMP 440, 441, 458  
GET 460  
GETBULK 460  
RESPONSE 460  
SET 460  
TRAP 460  
WALK 460
- SNMP-Protokolle 458
- SNMPv2 460
- SOA 467
- Social Engineering 363, 367  
APT 365
- Sonet 184
- SOW 473
- Spam 340
- Spanning Tree 93  
BPDU 94  
Konvergenz 95  
Kosten 94  
Loop-Detection 95  
Root Bridge 94
- Spatial Reuse 157
- SPB 95, 385
- Speed-Test 540
- Spine-Leaf 116
- Split Horizon 251
- Split-Pairs 503
- Spoofing 359  
ARP-Spoofing 359  
DNS-Spoofing 360  
Web-Spoofing 360
- Spyware 340
- SSAP 124
- SSH 278, 397
- SSID 152, 164, 562, 567
- SSL 332
- Stack 358
- Stateful Inspection Firewall 396
- Stateful Packet Inspection 399
- Stateless 221
- State of Work 473
- Stecker
- GG45 77  
RJ11 80  
RJ45 77  
RJ48 76  
TERA 77
- STP 72
- Strukturierte Verkabelung 139
- STS 185
- SUA 230, 231
- Subnettierung 580
- Subnetzmaske 580
- Supernetting 581
- Supportfall 498
- SVI 136
- Switch 92  
Content Switch 98  
Cut through 93  
Jamming 475  
Managed 97  
SAT 92  
SFP 100  
stackable 93  
Store and forward 92  
Virtuell 106
- Switching Hub 92, 562
- Switching-Hub 92
- SYN 585
- SynchByte 64
- Synchrone Datenübertragung 63
- Systemlog 453
- T**
- TACACS+ 327
- Tailgating 366
- Tamper Detection 379
- TCP 120, 208, 232  
Abort primitive 235  
ACK 234  
FIN-Flag 235  
Header 233  
RST-Flag 235  
Sliding Windows 234  
SYN 234  
Verbindungsmanagement 233
- TCP/IP 46, 60, 119, 208
- TDM 102
- TDR 508  
O-TDR 508
- Telefonkabel 71
- Telnet 278

- Tempest 354, 367
  - Terminaldienst 425
  - Tertiärverkabelung 138
  - Test 456, 540
    - Einzeltest 457
    - Ergebnis 456
    - Integrationstest 457
    - Maßnahmen 457
    - Systemtest 457
    - Testfall 456
    - Testfälle 456
    - Testobjekt 456
  - TFTP 272
  - Thin Client 427
  - Time-Division-Multiplexing 60
  - TKIP 168
  - TLD 260
  - TLS 333
  - Toner-and-Probe 508
  - Tongenerator 509
  - Tonsonde 508
  - Topologie 111
    - Baum 114
    - Bus 112
    - Doppelring 113
    - Hybrid 115
    - Maschen 114
    - Ring 112
    - Stern 113
    - Zelle 115
  - ToS 585
  - Traceroute 513
  - Tracert 513
  - tracert-6 513
  - Traffic Shaping 469, 584
  - Transportprotokoll 205
  - Transportschicht 43
  - Transportsteuerung 44
  - Triple-Play-Angebote 241
  - Trunking 98
  - TwinAx 81
  - Twinaxial 81
  - Twisted Pair 71
- U**
- U/FTP 78
  - U/STP 79
  - U/UTP 78
  - Übertragung
    - Bidirektionale 63
  - Überwachung 411, 464
  - UC 242
    - Endgerät 242
    - UC-Gateway 242
    - UC-Servers 242
  - UC-Kommunikation 240
  - UDP 235
  - UMTS 200
  - Undieren 579
  - Unicast 120
  - Unix 289
  - Update 456
  - Upgrade 456
  - UPnP 230, 231, 232, 578
  - URL 267
  - USV 384, 413
  - UTP 72
- V**
- VDI 427
  - VDSL 192
  - VDSL2 192
  - Veraltete Systeme 353
  - Verantwortungsbewusstsein 496
  - Verdrahtungsfehler 503
  - Verkabelung 576
    - Arbeitsbereich 139
    - Demarkationspunkt 139
    - Horizontale Leitung 139
    - Lebensdauer 576
    - Permanent Link 140
    - strukturierte 139
    - Vertikale Leitung 139
  - Verkabelungsschema 446
  - Vermittlungsschicht 43
  - Verschlüsselung 329, 330
  - VF-45 85
  - Videüberwachung 378
  - Viren 388
  - Virenverantwortlicher 387
  - Virtualisierung 294
  - Virtual PBX 107
  - Virtual Private Cloud 300
  - Virus 340, 343
    - Makroviren 344
    - Trojanisches Pferd 346
    - Würmer 345
  - VLAN 133
    - 802.1Q 133
    - IEEE 802.1X 138
    - MAC-basiert 134
    - Portbasiert 134
  - Protokollbasiert 134
  - Tagging 135
  - Trunking 137
  - Untagged 135
  - VTP 137
  - VLISM 213
  - VMWare 294
    - Microkernel 294
  - VNC 428
  - VoIP 239, 242
  - Vollduplex 63
  - VPBX 242
  - VPN 425, 429
    1. Phase 430
    2. Phase 431
    - Access VPN 436
    - Client-to-Site 436
    - Dynamisch 436
    - ESP 431
    - Gateway 431, 434
    - GRE 433
    - IPSec 433
    - Konzentrator 436
    - L2TP 433
    - PFS 432
    - Phasen 430
    - SA 432
    - Site-to-Site 434
    - Tunnel 431
  - RRRP 254
  - vSwitch 105
  - Vulnerabilitätsscanner 407
  - VXLAN 116
- W**
- W3C 207
  - Wachpersonal 375
  - WAF 400
  - WAN 34
  - War Chalking 367
  - War Driving 367
  - Warm Site 416
  - WEP 167, 368
  - Widerstand 53
  - Wi-Fi 4 160
  - Wi-Fi 6 160
  - Wi-Fi 6E 160
  - Wi-Fi 7 160
  - Wi-Fi 8 160
  - Wi-Fi Alliance 146
  - Windows 2000 293
  - WINS 259, 516

- Wiremap 509
  - WLAN
    - Ad-hoc-Netzwerk 149
    - Antenne 589
    - Aufbau 162
    - Beacon-Frame 152
    - BSS 151
    - CB 152
    - CSMA/CA 152
    - DFS 156
    - DSSS 148
    - ESS 152
    - FHSS 148
    - Gastnetz 584
    - Halbduplex 152
    - Heatmap 163
    - Infrastrukturnetzwerk 150
    - ISM-Band 146
    - Kanal 568
  - LWAPP 151
  - MAC-Filter 165
  - OFDM 148
  - Outdoor 155
  - RTS-Frame 152
  - SSID 152
  - Stör- und Dämpfungsfelder 163
  - Strahlungsleistung 146
  - Ticketsystem 584
  - TPC 156
  - Verschlüsselung 165
  - WEP 166
  - WPA 168
  - WPA2 168
  - WPA 168, 567
  - WPA2 168, 368, 567
  - WPA3 169, 567
  - WPS 153
- X**
- X.25 119
  - XaaS 299
  - xDSL 560
  - X Window 292
- Z**
- Zero Client 427
  - Zero-Day Exploit 361
  - Zero Trust 320
  - Zigbee 175
  - Zutrittsregelung 374
  - Z-Wave 175
  - Zwei-Faktor-Authentifikation 323