

Inhaltsverzeichnis

1	Einführung	17
1.1	Das Ziel dieses Buches	17
1.2	Die CompTIA-Network+-Zertifizierung	18
1.3	Voraussetzungen für CompTIA Network+	20
1.4	Danksagung zur 6. Auflage	20
1.5	Eintrittstest zur Standortbestimmung	21
2	Entwicklungen und Modelle	29
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
3	Grundbegriffe der Telematik	49
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
4	Hardware im lokalen Netzwerk	69
4.1	Die wichtigsten Übertragungsmedien	69
4.1.1	Twisted-Pair-Kabel	71
4.1.2	Unshielded Twisted Pair	73
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	89
4.3.2	Hub	90
4.3.3	Bridge	91
4.4	So funktionieren Switches	91
4.4.1	Methoden der Durchleitung	92
4.4.2	Spanning Tree Protocol	93
4.4.3	Managed Switches	95
4.5	Konvertieren und Verbinden	97
4.5.1	Medienkonverter	97
4.5.2	Modems	99
4.5.3	Multiplexer	100
4.5.4	CSU/DSU	101
4.6	Router verbinden diese (Netzwerk-)Welt	102
4.7	Virtuelle Netzwerkkomponenten	103
4.8	Fragen zu diesem Kapitel	105

5	Topologie und Verbindungsaufbau	107
5.1	Physische Topologien	107
5.2	Bandbreitenverwendung	112
5.2.1	Basisbandübertragung	112
5.2.2	Breitbandübertragung	112
5.3	Paketvermittelt – leitungsvermittelt	113
5.3.1	Leitungsvermittelte Netzwerke	113
5.3.2	Paketvermittelte Netzwerke	113
5.3.3	Nachrichtenvermittlung	114
5.4	Verbindungslos – verbindungsorientiert	114
5.5	Unicast, Multicast, Broadcast, Anycast	115
5.6	Fragen zu diesem Kapitel	115
6	Die Standards der IEEE-802.x-Reihe	119
6.1	IEEE 802.2 (LLC-Sublayer)	120
6.2	Das Ethernet-Verfahren	120
6.3	Von Fast Ethernet bis 100 Gigabit	124
6.3.1	Fast Ethernet	125
6.3.2	Gigabit-Ethernet	125
6.3.3	Und schon folgen die 10 Gigabit/s	125
6.3.4	Es werde schneller: 40 Gbps und 100 Gbps	127
6.3.5	Power over Ethernet	128
6.4	Ältere Verfahren	128
6.4.1	Die 10Base-X-Verfahren	128
6.4.2	IEEE 802.5 (Token Passing)	131
6.4.3	AppleTalk	131
6.4.4	IEEE 802.6	132
6.5	Dazu dienen VLANs	132
6.6	Weitere Standards in der Übersicht	136
6.7	Strukturierte Verkabelung	136
6.8	Fragen zu diesem Kapitel	139
7	Netzwerk ohne Kabel: Drahtlostechnologien	143
7.1	Wenn sich das LAN plötzlich WLAN nennt	144
7.1.1	Unterschiedliche Übertragungsverfahren	146
7.1.2	Die Verbindungsarten eines WLAN	147
7.1.3	Wie verbinden sich Sender und Empfänger?	150
7.2	Standards für drahtlose lokale Netzwerke	151
7.2.1	Die Standards IEEE 802.11a/b/g	151

7.2.2	Die Gegenwart: IEEE 802.11n und 802.11ac	152
7.2.3	Frequenzträger und Kanalbreite	155
7.3	Ein WLAN richtig aufbauen	157
7.3.1	Aufbau der Hardware	157
7.3.2	Konfiguration des drahtlosen Netzwerks	159
7.4	Die Sicherheit im WLAN	161
7.4.1	Wired Equivalent Privacy	162
7.4.2	WPA und 802.11i	162
7.5	Unterschiedliche Sendeverfahren	164
7.5.1	Infrarot	164
7.5.2	Mikrowellen	165
7.5.3	Radiowellen (Funkwellen)	167
7.6	IEEE 802.16 WiMax	167
7.7	Kommunikation auf kurze Distanzen	168
7.7.1	Die Bluetooth-Technologie	168
7.7.2	RFID	169
7.7.3	NFC	170
7.8	Fragen zu diesem Kapitel	171
8	WAN-Datentechniken auf OSI-Layer 1 bis 3	173
8.1	Von POTS zu ISDN	173
8.2	Breitband-ISDN und seine Nachfolger	175
8.2.1	Synchrone digitale Hierarchie	176
8.2.2	Sonet	176
8.2.3	ATM	177
8.3	Next Generation Network (NGN)	180
8.4	Ältere Verfahren	183
8.4.1	FDDI	183
8.4.2	X.25 und Frame Relay	183
8.5	Die wichtigsten DSL-Varianten	184
8.5.1	Die DSL-Technologie	184
8.5.2	DSL-Verfahren	185
8.5.3	Probleme beim DSL-Einsatz	187
8.6	TV-Kabelnetze	187
8.7	Fiber to the Home	188
8.8	Mobile Datennetze	189
8.9	Fragen zu diesem Kapitel	192

9	Meine Name ist IP – Internet Protocol	195
9.1	Die Geschichte von TCP/IP	195
9.2	Der Aufbau der Adressierung	197
9.3	Die Grundlagen der IP-Adressierung	199
9.3.1	CIDR statt Adressklassen	203
9.3.2	Private Netzwerke unter IPv4	204
9.3.3	Ausnahmen und besondere Adressen	205
9.3.4	Der IPv4-Header	206
9.4	IPv6	207
9.4.1	Der Header von IPv6	208
9.4.2	Spezielle Adressen unter IPv6	209
9.5	Zum Schluss: ein Blick in die Geschichte	211
9.5.1	IPX/SPX	212
9.5.2	NetBEUI und NetBIOS	213
9.6	Fragen zu diesem Kapitel	214
10	Weitere Protokolle im TCP/IP-Stack	217
10.1	ICMP und IGMP	217
10.2	ARP	218
10.3	NAT und noch mehr Abkürzungen	220
10.3.1	NAT und PAT	220
10.3.2	Universal Plug and Play	221
10.4	Das TCP-Protokoll	222
10.4.1	Verbindungsmanagement	223
10.4.2	Datenflusssteuerung	224
10.4.3	Schließen der Verbindung	225
10.5	Die Alternative: UDP	225
10.6	Die Geschichte mit den Ports	226
10.7	Voice over IP und Videokonferenzen	228
10.8	Fragen zu diesem Kapitel	233
II	Stets zu Diensten	237
II.1	Routing-Protokolle	237
II.1.1	RIP, RIPv2, IGRP	240
II.1.2	OSPF und IS-IS	242
II.1.3	BGP	243
II.1.4	CARP und VRRP	244
II.2	Dynamic Host Configuration Protocol	245

II.3	DNS (Domain Name System)	248
II.3.1	hosts.	248
II.3.2	Der Windows Internet Naming Service (WINS)	249
II.3.3	Das Domain Name System	249
II.3.4	Der Aufbau von DNS	250
II.3.5	Das Konzept des dynamischen DNS.	255
II.4	Web- und Mail-Protokolle	255
II.4.1	HTTP	255
II.4.2	FTP	257
II.4.3	TFTP	259
II.4.4	NNTP.	260
II.4.5	SMTP.	260
II.4.6	POP3 und IMAP4	262
II.5	Weitere Dienstprotokolle.	264
II.5.1	NTP	264
II.5.2	SSH	265
II.5.3	Telnet.	265
II.6	Fragen zu diesem Kapitel	267
12	Betriebssysteme und ihre Administration	271
12.1	Grundlagen der Verwaltung	271
12.1.1	Arbeitsgruppen und Domänen	272
12.1.2	Der Client/Server-Ansatz	273
12.1.3	Client/Server-Bausteine	275
12.1.4	Wichtige Fragen zum Einsatz eines NOS.	275
12.2	Die Virtualisierung – Cloud Computing	276
12.2.1	Servicemodelle	278
12.2.2	Betriebsmodelle	280
12.2.3	Angebote aus der Cloud	280
12.2.4	Ein Wort zum Thema Speicher	281
12.3	Verschiedene Systeme kurz vorgestellt	282
12.3.1	Apple	282
12.3.2	Unix	283
12.3.3	Linux	285
12.3.4	Novell NetWare.	286
12.3.5	Von Windows NT bis Windows 2012	287
12.3.6	Citrix und VMWare	290

12.4	Anwendungsprotokolle von NOS	290
12.4.1	SMB	291
12.4.2	NCP	291
12.5	Die Administration des Netzwerks	291
12.6	Ressourcen im Netzwerk teilen	292
12.7	Identifikation im Netzwerk	293
12.7.1	Benutzer einrichten	295
12.7.2	Das Erstellen von Gruppen	297
12.7.3	Datei- und Ordnerrechte	298
12.8	Drucken im Netzwerk	301
12.9	Fragen zu diesem Kapitel	302
13	Sicherheitsverfahren im Netzwerkverkehr	305
13.1	Identifikation und Authentifikation	306
13.1.1	Aller Anfang ist ... das Passwort	307
13.2	Authentifikationsverfahren	308
13.2.1	Single Sign On und Mehr-Faktor-Authentifizierung	308
13.2.2	PAP und CHAP	310
13.2.3	EAP	310
13.2.4	Kerberos	311
13.2.5	RADIUS	312
13.3	Die Hash-Funktion	313
13.4	Verschlüsselung	314
13.4.1	Symmetrisch oder asymmetrisch	314
13.4.2	Von DES bis AES	315
13.4.3	RSA	315
13.4.4	Digitale Signatur	315
13.4.5	PKI – digitale Zertifikate	316
13.5	SSL und TLS	316
13.6	IPSec	318
13.7	Forensics	320
13.7.1	Aufgaben und Fragestellungen	320
13.7.2	Sichern von Beweismitteln	321
13.7.3	Schutz und Analyse von Beweismitteln	323
13.7.4	Timeline	325
13.7.5	Programme und Toolkits	325
13.8	Fragen zu diesem Kapitel	326

14	Verschiedene Angriffsformen im Netzwerk	329
14.1	Viren und andere Krankheiten	330
14.1.1	Unterscheiden Sie verschiedene Malware-Typen.	330
14.1.2	Es gibt verschiedene Viren	333
14.2	Was tut der Mann in der Mitte?	340
14.2.1	Sie machen es dem Angreifer ja auch einfach	340
14.2.2	Denial-of-Service-Attacken	342
14.2.3	Pufferüberlauf	345
14.2.4	Man-in-the-Middle-Attacken	345
14.2.5	Spoofing	346
14.3	Social Engineering	347
14.4	Angriffspunkt drahtloses Netzwerk	351
14.5	Der freundliche Mitarbeiter	352
14.6	Fragen zu diesem Kapitel	354
15	Die Verteidigung des Netzwerks	357
15.1	Physikalische Sicherheit	358
15.1.1	Zutrittsregelungen	358
15.1.2	Vom Badge bis zur Biometrie	360
15.1.3	Zutrittsschleusen und Videoüberwachung	361
15.1.4	Schutz gegen Einbruch, Feuer und Wasser	363
15.1.5	Klimatisierung und Kühlung	365
15.2	Fehlertoleranter Aufbau	366
15.3	Datensicherung	369
15.4	Virenschutz mit Konzept	370
15.5	Firewalls	375
15.5.1	Verschiedene Firewall-Typen	380
15.5.2	Das Konzept der DMZ	382
15.5.3	Erweiterte Funktionen einer Firewall	384
15.5.4	Der Proxyserver	385
15.5.5	IDS und IPS	386
15.6	Aktive Suche nach Schwachstellen	388
15.7	Verteidigungskonzepte	390
15.7.1	Die Auswertung von Überwachungen	390
15.7.2	Notfallvorsorge	392
15.7.3	Die First Responders	392
15.7.4	Und das alles zusammen?	394
15.8	Fragen zu diesem Kapitel	395

16	Remote Access Networks	399
16.1	Remote Access	399
16.2	Terminaldienste	401
16.2.1	Der Windows Terminal Server	401
16.2.2	Citrix Presentation Server	403
16.2.3	Und die Desktop-Virtualisierung?	403
16.2.4	Ein Wort zum Thema Unterstützung	403
16.3	VPN	405
16.3.1	Der Aufbau der Verbindung	406
16.3.2	Site-to-Site VPN	409
16.3.3	Client-to-Site VPN	411
16.3.4	Dynamisches VPN (Client-to-Site, Site-to-Site)	412
16.4	Fragen zu diesem Kapitel	412
17	Netzwerkmanagement	415
17.1	Wozu brauchen Sie Netzwerkmanagement?	415
17.1.1	Fehlermanagement	419
17.1.2	Konfigurationsmanagement	419
17.1.3	Performancemanagement	421
17.1.4	Sicherheitsmanagement	421
17.2	Die Netzwerkdokumentation	422
17.2.1	Verkabelungsschema	422
17.2.2	Anschlussdiagramme	423
17.2.3	Logisches Netzwerkdiagramm	423
17.2.4	Inventar- und Konfigurationsdokumentation	426
17.2.5	Erfassungsschemata für die Planung	426
17.2.6	Messdiagramme und Protokolle	429
17.2.7	Änderungsdokumentation	429
17.3	Das Nachführen der Systeme	430
17.4	Der Aufbau von Tests	432
17.5	SNMP-Protokolle	433
17.6	Fragen zu diesem Kapitel	437
18	Überwachung	439
18.1	So funktioniert das Monitoring	440
18.1.1	Was ist ein Monitor?	440
18.1.2	Performancemanagement konzipieren	443
18.1.3	Monitoring als Teil des Quality Management	444

18.1.4	Grundlagen zu Service Level Agreements	446
18.1.5	Weitere wichtige Dokumente	448
18.2	Die Netzwerkanalyse	449
18.3	Netzwerkanalyse-Programme	450
18.3.1	Der Netzwerkmonitor	450
18.3.2	Wireshark	453
18.3.3	MRTG	454
18.3.4	Messung der Netzwerkleistung	456
18.3.5	Was ist ein Portscanner?	459
18.4	Überwachung im industriellen Umfeld	461
18.5	Und nachher?	465
18.6	Fragen zu diesem Kapitel	466
19	Fehlersuche im Netzwerk	469
19.1	Wie arbeiten Sie im Support?	470
19.1.1	Sprechen Sie mit und nicht über den Kunden	470
19.1.2	Vorbereitung für den Supporteinsatz	472
19.1.3	ESD	472
19.1.4	Heben und Tragen	473
19.1.5	MSDS	473
19.1.6	Arbeiten am und mit Racks	474
19.2	Fehlersuche im Netzwerk	475
19.3	Kabelprobleme und Testgeräte	476
19.3.1	Abisolier- und Schneidwerkzeuge	479
19.3.2	Anlege- und Anschlusswerkzeuge	479
19.3.3	Installationswerkzeuge zur Kabelverlegung	480
19.3.4	Prüf- und Analysegeräte	481
19.3.5	Sensoren und Messgeräte	483
19.4	Hilfsmittel bei Routing-Problemen	484
19.4.1	ipconfig/ip	484
19.4.2	ping	485
19.4.3	tracert/traceroute	487
19.4.4	route	488
19.4.5	Looking Glass	489
19.5	Probleme bei der Namensauflösung	490
19.5.1	nbtstat	490
19.5.2	nslookup	491
19.5.3	NET	493
19.6	Arbeiten in der Shell mit netsh	496

19.7	Protokollstatistiken anzeigen mit netstat	498
19.8	Fehlersuche in den Diensten	499
19.9	Fragen zu diesem Kapitel	501
20	Praxis 1: Sie richten ein Netzwerk ein	505
20.1	Die Konzeption	506
20.1.1	Ein Inventar erstellen	506
20.1.2	Netzwerkkonzept erstellen	507
20.1.3	Computer vorbereiten	508
20.2	Das Netzwerk aufbauen	509
20.2.1	Router einrichten	509
20.2.2	Internetzugriff einrichten	511
20.2.3	Das LAN einrichten	512
20.2.4	Abschluss der Router-Konfiguration	513
20.2.5	Test der Internetverbindung	514
20.3	Drucken im Netzwerk	515
20.4	Gemeinsame Nutzung von Daten	520
20.4.1	Vorbereitungsarbeiten	520
20.4.2	Einrichten der Freigabe	521
20.5	Fragen zu diesem Kapitel	523
21	Praxis 2: Sie richten ein WLAN ein	527
21.1	Das Szenario für den Nachbau	527
21.2	Der Beginn Ihrer Installation	528
21.3	Der Aufbau des Netzwerks	529
21.4	Die Konfiguration des WLAN-Geräts	531
21.4.1	WAN-Schnittstelle einrichten	535
21.4.2	Die Konfiguration der LAN-Schnittstellen	536
21.4.3	WLAN einrichten	537
21.4.4	Jetzt kommt die Firewall dran	540
21.5	Fragen zu diesem Kapitel	542
22	Praxis 3: Steigern Sie die Netzeffizienz	545
22.1	Optimierung der physischen Komponenten	545
22.2	Die Optimierung von Ethernet-Netzwerken	546
22.2.1	Reduzieren der Protokolle	548
22.2.2	Drucker	549
22.3	Teilnetze durch Subnettierung	549
22.3.1	Grundlagen zum Subnet Masking	550
22.3.2	Wie eine Subnettierung funktioniert	551

22.4	Weitere Optimierungsmaßnahmen	553
22.4.1	Network Access Control	553
22.4.2	Traffic Shaping	554
22.5	Optimierungsmöglichkeiten im WLAN	555
22.6	Fragen zu diesem Kapitel	559
23	Die CompTIA-Network+-Prüfung	561
23.1	Was von Ihnen verlangt wird	561
23.2	Wie Sie sich vorbereiten können	562
23.3	Wie eine Prüfung aussieht	563
23.4	Abschlusstest zur Prüfung CompTIA Network+	567
A	Anhänge	587
A.1	Hier finden Sie die Prüfungsthemen	587
A.2	Antworten zu den Fragen des Eintrittstest	613
A.3	Lösungsbeispiele zu »Jetzt sind Sie dran«	613
A.4	Antworten zu den Kapitelfragen	617
A.5	Antworten zur Musterprüfung	620
A.6	Weiterführende Literatur	621
A.6.1	Nützliche Literatur zum Thema	621
A.6.2	Weiterführende Links zum Thema	622
B	Abkürzungsverzeichnis	623
	Stichwortverzeichnis	635