

CompTIA Network+

Computer-Netzwerke verständlich erläutert

DAS INHALTS- VERZEICHNIS

» Hier geht's
direkt
zum Buch

Inhaltsverzeichnis

1	Einführung	17
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
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	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
5	Topologie und Verbindungsaufbau	111
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
6	Die Standards der IEEE-802.x-Reihe	123
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
7	Netzwerk ohne Kabel: Drahtlostechnologien	145
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
8	WAN-Datentechniken auf OSI-Layer 1 bis 3	181
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
9	Mein Name ist IP – Internet Protocol	205
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
10	Weitere Protokolle im TCP/IP-Stack	227
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
11	Stets zu Diensten.	247
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
12	Netzwerke betreiben	283
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

13	Sicherheitsverfahren im Netzwerkverkehr	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
14	Verschiedene Angriffsformen im Netzwerk	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
15	Die Verteidigung des Netzwerks	373
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
16	Remote Access Networks	423
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
17	Netzwerkmanagement	439
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
18	Überwachung	463
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
19	Fehlersuche im Netzwerk	495
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
20	Praxis 1: Sie richten ein Netzwerk ein	531
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
21	Praxis 2: Sie richten ein WLAN ein	559
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
22	Praxis 3: Steigern Sie die Netzeffizienz	575
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
23	Die CompTIA-Network+-Prüfung	595
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
A	Antworten und Lösungen	623
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	Abkürzungsverzeichnis	633
	Stichwortverzeichnis	647