

CompTIA Network+

Computer-Netzwerke verständlich erläutert

Vorbereitung auf die Prüfung N10-008

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 8. 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	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	Netzwerkarten	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	Spanning Tree Protocol	93
4.4.3	Shortest Path Bridging und TRILL	95
4.4.4	Managed Switches	96
4.5	Konvertieren und Verbinden	98
4.5.1	Medienkonverter	98
4.5.2	Modems	100
4.5.3	Multiplexer	101
4.5.4	CSU/DSU	103
4.6	Router verbinden diese (Netzwerk-)Welt	103
4.7	Virtuelle Netzwerkkomponenten	105
4.8	Fragen zu diesem Kapitel	107

5	Topologie und Verbindungsaufbau	109
5.1	Physische Topologien	109
5.2	Bandbreitenverwendung	114
5.2.1	Basisbandübertragung	114
5.2.2	Breitbandübertragung	114
5.3	Leitungsvermittelt – paketvermittelt	115
5.3.1	Leitungsvermittelte Netzwerke	115
5.3.2	Paketvermittelte Netzwerke	115
5.3.3	Nachrichtenvermittlung	116
5.4	Verbindungslos – verbindungsorientiert	116
5.5	Unicast, Multicast, Broadcast, Anycast	117
5.6	Fragen zu diesem Kapitel	117
6	Die Standards der IEEE-802.x-Reihe	121
6.1	IEEE 802.2 (LLC Sublayer)	122
6.2	Das Ethernet-Verfahren	122
6.3	Von Fast Ethernet bis 100 Gigabit	126
6.3.1	Fast Ethernet	127
6.3.2	Gigabit-Ethernet	127
6.3.3	Und schon folgen die 10 Gigabit/s	127
6.3.4	Es werde schneller: 40 Gbps und 100 Gbps	129
6.3.5	Power over Ethernet	130
6.4	Dazu dienen VLANs	131
6.5	Weitere Standards in der Übersicht	135
6.6	Strukturierte Verkabelung	136
6.7	Fragen zu diesem Kapitel	139
7	Netzwerk ohne Kabel: Drahtlostechnologien	141
7.1	Wenn sich das LAN plötzlich WLAN nennt	142
7.1.1	Unterschiedliche Übertragungsverfahren	144
7.1.2	Die Verbindungsarten eines WLAN	145
7.1.3	Wie verbinden sich Sender und Empfänger?	148
7.2	Standards für drahtlose lokale Netzwerke	149
7.2.1	Die Standards IEEE 802.11a/b/g	149
7.2.2	Die Gegenwart: IEEE 802.11n, 802.11ac und 802.11ax	150
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	161
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	Kommunikation auf kurze Distanzen	167
7.6.1	Die Bluetooth-Technologie.....	168
7.6.2	Zigbee und Z-Wave	169
7.6.3	RFID	170
7.6.4	NFC	171
7.7	Fragen zu diesem Kapitel	172
8	WAN-Datentechniken auf OSI-Layer 1 bis 3	175
8.1	Von POTS zu ISDN	175
8.2	Breitband-ISDN und seine Nachfolger	177
8.2.1	Synchrone digitale Hierarchie.....	178
8.2.2	Sonet	178
8.2.3	ATM.....	180
8.3	Next Generation Network (NGN)	182
8.4	Die wichtigsten DSL-Varianten.....	185
8.4.1	Die DSL-Technologie	185
8.4.2	DSL-Verfahren	186
8.4.3	Probleme beim DSL-Einsatz	187
8.5	TV-Kabelnetze	188
8.6	Fiber to the Home	189
8.7	Satelliten	190
8.8	LPWAN.....	191
8.9	Mobile Datennetze.....	192
8.10	Fragen zu diesem Kapitel	195
9	Mein Name ist IP – Internet Protocol	199
9.1	Die Geschichte von TCP/IP	199
9.2	Der Aufbau der Adressierung.....	201
9.3	Die Grundlagen der IP-Adressierung.....	203
9.3.1	CIDR statt Adressklassen.....	206
9.3.2	Private Netzwerke unter IPv4	208
9.3.3	Ausnahmen und besondere Adressen	209
9.3.4	Der IPv4-Header.....	209

9.4	IPv6.....	210
9.4.1	Der Header von IPv6	212
9.4.2	Konzepte und spezielle Adressen unter IPv6.....	213
9.5	Fragen zu diesem Kapitel	217
10	Weitere Protokolle im TCP/IP-Stack	221
10.1	ICMP und IGMP	221
10.2	ARP.....	222
10.3	NAT und noch mehr Abkürzungen.....	224
10.3.1	NAT und PAT.....	224
10.3.2	Universal Plug and Play.....	225
10.4	Das TCP-Protokoll.....	226
10.4.1	Verbindungsmanagement.....	227
10.4.2	Datenflusssteuerung	228
10.4.3	Schließen der Verbindung.....	229
10.5	Die Alternative: UDP.....	229
10.6	Die Geschichte mit den Ports.....	230
10.7	Voice over IP und Videokonferenzen	233
10.8	Fragen zu diesem Kapitel	238
11	Stets zu Diensten.....	241
11.1	Routing-Protokolle.....	241
11.1.1	RIP, RIPv2, IGRP.....	244
11.1.2	OSPF und IS-IS	246
11.1.3	BGP	247
11.1.4	CARP und VRRP	248
11.2	Dynamic Host Configuration Protocol	249
11.3	DNS (Domain Name System).....	252
11.3.1	hosts	252
11.3.2	Der Windows Internet Naming Service (WINS)	253
11.3.3	Das Domain Name System	253
11.3.4	Der Aufbau von DNS	254
11.3.5	Das Konzept des dynamischen DNS.....	259
11.4	Web- und Mail-Protokolle.....	259
11.4.1	HTTP.....	259
11.4.2	FTP	261
11.4.3	TFTP	263
11.4.4	NNTP.....	264
11.4.5	SMTP.....	264
11.4.6	POP3 und IMAP4.....	266

11.5	Weitere Dienstprotokolle.....	268
11.5.1	NTP	268
11.5.2	SSH	269
11.5.3	Telnet.....	269
11.6	Fragen zu diesem Kapitel	271
12	Netzwerke betreiben	275
12.1	Grundlagen der Verwaltung	275
12.1.1	Arbeitsgruppen und Domänen	276
12.1.2	Der Client/Server-Ansatz	277
12.1.3	Client/Server-Bausteine	279
12.1.4	Wichtige Fragen zum Einsatz eines NOS.....	279
12.2	Verschiedene Systeme kurz vorgestellt	280
12.2.1	Apple	280
12.2.2	Unix.....	281
12.2.3	Linux	283
12.2.4	Von Windows NT bis Windows 2022.....	284
12.2.5	Citrix und VMWare	286
12.2.6	Die Bedeutung von SMB über Betriebssysteme hinweg....	287
12.3	Die Virtualisierung	288
12.4	Cloud Computing	289
12.4.1	Servicemodelle in der Cloud	290
12.4.2	Betriebsmodelle	292
12.4.3	Angebote aus der Cloud.....	293
12.5	Ein Wort zum Thema Speicher	293
12.6	Sicherheitsfragen zu Cloud-Modellen und Rechenzentren	294
12.7	Die Administration des Netzwerks.....	296
12.8	Ressourcen im Netzwerk teilen	297
12.9	Identifikation und Rechte im Netzwerk.....	298
12.9.1	Benutzer einrichten	300
12.9.2	Das Erstellen von Gruppen	301
12.9.3	Datei- und Ordnerrechte	302
12.9.4	Drucken im Netzwerk	305
12.10	Fragen zu diesem Kapitel	306
13	Sicherheitsverfahren im Netzwerkverkehr	309
13.1	Identifikation und Authentifikation	310
13.1.1	Aller Anfang ist ... das Passwort	311
13.1.2	Das Zero Trust-Konzept.....	312

13.2	Authentifikationsverfahren.	312
13.2.1	Single Sign On und Mehr-Faktor-Authentifizierung	312
13.2.2	PAP und CHAP	314
13.2.3	EAP	314
13.2.4	Kerberos	315
13.2.5	RADIUS	316
13.3	Die Hash-Funktion	317
13.4	Verschlüsselung.	318
13.4.1	Symmetrisch oder asymmetrisch	318
13.4.2	Von DES bis AES	319
13.4.3	RSA	319
13.4.4	Digitale Signatur.	319
13.4.5	PKI – digitale Zertifikate	320
13.5	SSL und TLS	320
13.6	IPSec.	322
13.7	Fragen zu diesem Kapitel	324
14	Verschiedene Angriffsformen im Netzwerk	327
14.1	Viren und andere Krankheiten.	328
14.1.1	Unterscheiden Sie verschiedene Malware-Typen	328
14.1.2	Es gibt verschiedene Viren.	331
14.2	Was tut der Mann in der Mitte?	341
14.2.1	»Sie machen es dem Angreifer ja auch einfach«.	341
14.2.2	Denial-of-Service-Attacken.	342
14.2.3	Pufferüberlauf	345
14.2.4	Man-in-the-Middle-Attacken	346
14.2.5	Spoofing	347
14.3	Angriffe gegen IT-Systeme	348
14.3.1	Exploits und Exploit-Kits	348
14.4	Social Engineering.	351
14.4.1	Die Ziele des Social Engineers	351
14.4.2	Beliebter Ansatz: Phishing-Mails	353
14.4.3	Tailgating und andere Methoden	354
14.5	Angriffspunkt drahtloses Netzwerk.	355
14.6	Der freundliche Mitarbeiter	357
14.7	Fragen zum Kapitel	359
15	Die Verteidigung des Netzwerks	361
15.1	Physikalische Sicherheit	362
15.1.1	Zutrittsregelungen	362

15.1.2	Vom Badge bis zur Biometrie	364
15.1.3	Zutrittsschleusen und Videoüberwachung	365
15.1.4	Schutz gegen Einbruch, Feuer und Wasser	367
15.1.5	Klimatisierung und Kühlung	369
15.1.6	Fachgerechte Inventarisierung und Entfernung	370
15.2	Fehlertoleranter Aufbau	371
15.3	Datensicherung	373
15.4	Virenschutz mit Konzept	374
15.5	Netzwerkhärtung	379
15.6	Firewalls	380
15.6.1	Verschiedene Firewall-Typen	385
15.6.2	Das Konzept der DMZ	388
15.6.3	Erweiterte Funktionen einer Firewall	389
15.6.4	Der Proxyserver	390
15.6.5	IDS und IPS	391
15.7	Aktive Suche nach Schwachstellen	394
15.8	Die Rolle des Risiko-Managements	396
15.9	Verteidigungskonzepte	398
15.9.1	Die Auswertung von Überwachungen	398
15.9.2	Notfallvorsorge	399
15.9.3	Die First Responders	402
15.9.4	Und das alles zusammen?	403
15.10	Fragen zu diesem Kapitel	404
16	Remote Access Networks	409
16.1	Remote Access	409
16.2	Terminaldienste	411
16.2.1	Der Windows Terminal Server	411
16.2.2	Citrix Presentation Server	413
16.2.3	Und die Desktop-Virtualisierung?	413
16.2.4	Ein Wort zum Thema Unterstützung	413
16.3	VPN	414
16.3.1	Der Aufbau der Verbindung	415
16.3.2	Site-to-Site VPN	420
16.3.3	Client-to-Site VPN	422
16.3.4	Dynamisches VPN (Client-to-Site, Site-to-Site)	422
16.4	Fragen zu diesem Kapitel	423

17	Netzwerkmanagement	425
17.1	Wozu brauchen Sie Netzwerkmanagement?	425
17.1.1	Fault Management	428
17.1.2	Configuration Management	429
17.1.3	Performance Management	431
17.1.4	Security Management	431
17.2	Die Netzwerkdokumentation	432
17.2.1	Verkabelungsschema	432
17.2.2	Anschlussdiagramme	433
17.2.3	Logisches Netzwerkdiagramm	433
17.2.4	Inventar- und Konfigurationsdokumentation	435
17.2.5	Erfassungsschemata für die Planung	436
17.2.6	Messdiagramme und Protokolle	439
17.2.7	Änderungsdokumentation	439
17.3	Das Nachführen der Systeme	440
17.4	Der Aufbau von Tests	442
17.5	SNMP-Protokolle	443
17.6	Fragen zu diesem Kapitel	446
18	Überwachung	449
18.1	So funktioniert das Monitoring	450
18.1.1	Was ist ein Monitor?	450
18.1.2	Performancemanagement konzipieren	453
18.1.3	Monitoring als Teil des Quality Management	454
18.1.4	Grundlagen zu Service Level Agreements	456
18.1.5	Weitere wichtige Dokumenttypen	458
18.2	Die Netzwerkanalyse	460
18.3	Netzwerkanalyse-Programme	461
18.3.1	Der Netzwerkmonitor	461
18.3.2	Wireshark	463
18.3.3	MRTG	466
18.3.4	Messung der Netzwerkleistung	467
18.3.5	Was ist ein Portscanner?	471
18.4	Überwachung im industriellen Umfeld	472
18.5	Und nachher?	476
18.6	Fragen zu diesem Kapitel	477

19	Fehlersuche im Netzwerk	481
19.1	Wie arbeiten Sie im Support?	482
19.1.1	Sprechen Sie mit und nicht über den Kunden	482
19.1.2	Vorbereitung für den Supporteinsatz	484
19.1.3	ESD	484
19.1.4	Heben und Tragen	485
19.1.5	MSDS	485
19.1.6	Arbeiten am und mit Racks	486
19.2	Fehlersuche im Netzwerk	487
19.3	Kabelprobleme und Testgeräte	488
19.3.1	Abisolier- und Schneidwerkzeuge	491
19.3.2	Anlege- und Anschlusswerkzeuge	491
19.3.3	Installationswerkzeuge zur Kabelverlegung	492
19.3.4	Prüf- und Analysegeräte	493
19.3.5	Sensoren und Messgeräte	495
19.4	Hilfsmittel bei Routing-Problemen	496
19.4.1	ipconfig/ip	496
19.4.2	ping	497
19.4.3	tracert/traceroute	499
19.4.4	route	500
19.4.5	Looking Glass	501
19.5	Probleme bei der Namensauflösung	502
19.5.1	nbtstat	502
19.5.2	nslookup	503
19.5.3	NET	505
19.6	Arbeiten in der Shell mit netsh	508
19.7	Protokollstatistiken anzeigen mit netstat	510
19.8	Fehlersuche in den Diensten	511
19.9	Fragen zu diesem Kapitel	513
20	Praxis 1: Sie richten ein Netzwerk ein	517
20.1	Die Konzeption	518
20.1.1	Ein Inventar erstellen	518
20.1.2	Netzwerkkonzept erstellen	519
20.1.3	Computer vorbereiten	520
20.2	Das Netzwerk aufbauen	521
20.2.1	Router einrichten	521
20.2.2	Internetzugriff einrichten	523
20.2.3	Das LAN einrichten	524

20.2.4	Abschluss der Router-Konfiguration	525
20.2.5	Test der Internetverbindung	526
20.3	Alternative Konzeption	527
20.3.1	Firewall einrichten	528
20.3.2	Die Schnittstellen einrichten	529
20.3.3	USG hat doch was mit Firewall zu tun	532
20.3.4	Abschluss der Router-Konfiguration	532
20.4	Drucken im Netzwerk	533
20.5	Gemeinsame Nutzung von Daten	538
20.5.1	Vorbereitungsarbeiten	539
20.5.2	Einrichten der Freigabe	539
20.6	Fragen zum Kapitel	541
21	Praxis 2: Sie richten ein WLAN ein	545
21.1	Das Szenario für den Nachbau	545
21.2	Der Beginn Ihrer Installation	546
21.3	Der Aufbau des Netzwerks	547
21.4	Die Konfiguration des WLAN-Geräts	549
21.4.1	WAN-Schnittstelle einrichten	553
21.4.2	Die Konfiguration der LAN-Schnittstellen	554
21.4.3	WLAN einrichten	555
21.4.4	Jetzt kommt die Firewall dran	558
21.5	Fragen zu diesem Kapitel	560
22	Praxis 3: Steigern Sie die Netzeffizienz	563
22.1	Optimierung der physischen Komponenten	563
22.2	Die Optimierung von Ethernet-Netzwerken	564
22.2.1	Reduzieren der Protokolle	566
22.2.2	Drucker	567
22.3	Teilnetze durch Subnettierung	567
22.3.1	Grundlagen zum Subnet Masking	568
22.3.2	Wie eine Subnettierung funktioniert	568
22.4	Weitere Optimierungsmaßnahmen	571
22.4.1	Network Access Control	571
22.4.2	Traffic Shaping	572
22.5	Netzwerke optimieren dank QoS	573
22.5.1	Priorisierung auf OSI-Layer 2: IEEE 802.1q	574
22.5.2	Priorisierung auf OSI-Layer 3: Das DSCP-Verfahren	574
22.5.3	Integrated-Services-Verfahren	575

22.5.4	Class of Service	576
22.5.5	Hardwarebasierte QoS-Verfahren	576
22.6	Optimierungsmöglichkeiten im WLAN	576
22.7	Fragen zu diesem Kapitel	580
23	Die CompTIA-Network+-Prüfung	583
23.1	Was von Ihnen verlangt wird	583
23.2	Wie Sie sich vorbereiten können	584
23.3	Wie eine Prüfung aussieht	585
23.4	Abschlusstest zur Prüfung CompTIA Network+	589
A	Antworten und Lösungen	609
A.1	Antworten zu den Fragen des Eintrittstests	609
A.2	Lösungsbeispiele zu »Jetzt sind Sie dran«	609
A.3	Antworten zu den Kapitelfragen	613
A.4	Antworten zur Musterprüfung	615
A.5	Weiterführende Literatur	616
A.5.1	Nützliche Literatur zum Thema	616
A.5.2	Weiterführende Links zum Thema	617
B	Abkürzungsverzeichnis	619
	Stichwortverzeichnis	631

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.

Wenn meine Mutter mit ihren 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 zum interaktiven internetbasierten Fernsehen, 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 ans Internet oder die Einrichtung einer 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 2018 und aktuell im Jahr 2021 statt. Die Inhalte der Zertifizierung werden anschließend in Lernzieldokumenten auf der Website von CompTIA unter 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 (N10-008) lauten diese Themen wie folgt:

Wissensgebiet	Thematik
Wissensgebiet 1	Netzwerkgrundlagen
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 8. 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 N10-008

Alles in allem wurde die Anzahl Lernziele weiter von 29 auf jetzt noch 25 reduziert und das Gewicht liegt aktuell mehr auf »Wissen und Verstehen« und weniger auf »Analyse«.

Hinweis

Wenn Sie den an dieser Stelle von CompTIA zur Verfügung gestellten Code »Kabera10« nutzen, so erhalten Sie auf den Kauf eines CompTIA Prüfungs-Vouchers 10 % Rabatt.

1.3 Voraussetzungen für CompTIA Network+

Gemäß der Website von CompTIA (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 installieren 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. Details zur Prüfung finden Sie zudem in Kapitel 23 »Die CompTIA-Network+-Prüfung«.

1.4 Danksagung zur 8. 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 geschwächte 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«, in dem 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 8. Auflage herausbringen können. Ein Buch, das viele interessiert und das gelesen wird und mit dem wir in guter Zusammenarbeit gemeinsam Erfolg haben.

1.5 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
 - 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. IEEE 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 802.11ac

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+.

Stichwortverzeichnis

- 1000Base-LX 127
- 1000Base-SX 127
- 1000Base-T 62, 127
- 100Base-T 127
- 100Base-TX 127
- 100GBase 129
- 100GBase-CR10 129
- 10GBase 128
- 10GBase-T 127
- 110-Block 138
- 2,4-GHz-ISM-Band 152
- 3G 193
- 40GBase 129
- 40GBase-KR4 129
- 5G 195
- 5-GHz-ISM-Band 152
- 66-Block 138
- 6in4 216
- 6to4 216
- 802.11a 154, 156
- 802.11ac 151, 547, 555
- 802.11ax 154
- 802.11b 149, 154, 156
- 802.11g 149, 154, 156
- 802.11i 162
- 802.11n 150, 154, 156
- 802.11p 156
- 802.11s. 156
- 802.11aq 95
- A**
- AAA 96
- AAAA 258, 316
- AAA-Protokoll 316
- AAL 181
- Abisolierzange 491
- Absichtserklärung 458
- Access Point 91, 146, 549, 550
- ACK 573
- ACL 299
- ACR 490
- Active Directory 285
- Adernpaare 75
- Ad hoc 159
- Adresse
 - 32 Bit 203
 - Dienstadresse 202
 - IPv4 203
 - IPv6 211
 - Logische Adresse 202
 - Physische Adresse 202
 - Subnetzmaske 205
- Adressschema 519, 546
- ADS 301, 302, 313, 412
- ADSL 185, 186, 523, 546
- Adware 328
- AES 319, 558
- Analoge Datenübertragung 58
- Änderung 477
- Änderungsdokumentation 439
- Änderungsprotokoll 430
- Antenne
 - Fresnelzone 577
 - Omni 578
 - Verbindungskabel 577
 - Wirkungsgrad 577
 - Yagi 578
- Anwendungsschicht 44
- Anycast 117
- APIPA 250
- APON 190
- Application Gateway 383, 386, 387
- APT 338, 340
- Arbitrary Code Execution 349
- ARP 222, 223
 - ARP-Cache 223
 - ARP-Reply 222
 - NDP 223
 - RARP 223
- ARPANet 45, 202
- AS 243, 501
- ASLR 350
- ASP 291
- Asynchrone Datenübertragung 63
- ATM 180
 - ATM-Schichtenmodell 180
- Attacke 341
 - Advanced Persistent Threat 340
 - Bluejacking 357
 - Bluesnarfing 357
 - Carbanak 340
 - Cookie-Diebstahl 347
 - DNS Amplification Attack 343
 - DoS 343
 - FTP Bounce 342
 - Man-in-the-Middle 346
 - MMS-Phishing 339
 - Permanent DoS 344
 - Pharming 340
 - Phishing 339
 - Session-Hijacking 347
 - SMS-Phishing 339
 - Smurf 343
 - Spoofing 347
 - SYN-Flood 344
 - TCP-Hijacking 347
 - Zero hour 339
- Ausbreitungsgeschwindigkeit 54
- Authentifizierung 311, 572
- Autonomes System 243
- Autorisierung 358
- Awareness 376
- AXTLK 490
- B**
- Backbone 113, 137
- Badge 363, 364
- BAKOM 142
- Bandbreite 64
- Banner Grabbing 471

Basisanschluss 176
 Basisbandübertragung 114
 Bastion Host 386
 Baudrate 62
 Bauliche Maßnahme 362
 Beamforming 153
 Benutzer 300
 Benutzerrechte 299
 BGP 247
 Bidirektionale Übertragung 63
 Biometrisches Erkennungssystem 364
 Bitrate 62, 64
 Bitübertragungsschicht 41
 BIX 138
 Bluetooth 168
 BNC 81
 BNetzA 142
 Bonding 371
 BOOTP 249
 Brandfall 403
 Brandschutz 362, 368
 Breitbandübertragung 114
 Bridge 90, 554
 Broadcast 117, 569
 Broadcast Storm 91
 BSS Coloring 153
 Buffer Overflow 348, 350
 Butt Set 493
 Byte 66

C

CARP 248
 CATV 81, 188, 189
 CCMP 162
 CENELEC 73
 Change-Protokoll 477
 CHAP 314, 419
 CIA 309
 CIDR 206, 568, 569
 CIFS 287
 Circuit Level Firewall 387
 Citrix 413
 Client/Server-Architektur 31, 276
 Client-Server 249
 Cloud Computing 288, 290, 472
 IaaS 290
 PaaS 290
 SaaS 290
 XaaS 291

CO₂ 369
 Command and Conquer 488
 Companion-Virus 335
 Connectionless Communication 116
 Connection-oriented Communication 116
 CoS 237
 CRC 64
 Crimeware 329
 Crimpzange 492
 Crosskabel 76
 CSMA/CD 124
 CSU 103
 CVE 351
 CVSS 351
 CWDM 102

D

DAD-Prüfung 215
 Dämpfung 53, 54, 489
 Darstellungsschicht 44
 Daten 32
 Datenbandbreite 114
 Datenintegrität 309
 Datensicherung 373
 Datensignalisierung 63
 Datenübertragung
 Asynchron 63
 Parallel 61
 SCSI 61
 Seriell 62
 Synchron 63
 Datenverfügbarkeit 309
 Datenvertraulichkeit 309
 DCS 473
 DDoS 342
 Dedizierte Firewall 382
 Demarc 136
 Demarkationspunkt 136
 Denial of Service 333, 342, 349
 DEP 350
 DHCP 249, 519, 527, 554
 APIPA 251
 Automatisch 250
 Dynamisch 250
 Scope 251
 Server 554
 Statisch 249
 DHCPv6 251
 Diagramm 519, 546

Diameter 316, 572
 Dienst 511
 Dienstleistungsrahmenvertrag 458
 DiffServ 213, 236
 DLL-Injection 350
 DMZ 381, 388
 Geschlossene 388
 Halboffene 388
 Offene 388
 DNS 253, 384, 422, 502, 523
 CNAME 258
 Missbrauch 343
 Namensraum 254
 Name Server 256
 Resolver 256
 Resource Record 258
 Zonendatei 256
 DOCSIS 188
 DoD-Modell 36, 45, 46, 202
 Drehschleuse 365
 Drucker 533
 Druckerserver 306
 Druckertreiber 306
 DSAP 122
 DSCP 236
 DSL 185
 DSU 103
 Dual-Stack 211
 Duplexverfahren 89
 Auto Sense 89
 DWDM 102, 180, 184

E

EAP 314
 ECN 213
 EDGE 193
 Edge Control 572
 EFS 286
 EGP 244
 EIA/TIA 73
 Norm 569A 137
 TIA-568A 73
 TIA 568B 73
 EIA/TIA-568 73
 EICAR 379
 EICAR-Code 379
 EIGRP 246
 Einbruchsschutz 367
 EIP 350
 EMI 71
 Environmental Monitor 495

- ESD 484
 - Erdung 485
 - ESD-Strip 485
- Etherjack 137
- Ethernet 125
- Ethernet-Frame 123
- Ethernet over HDMI 129
- Ethernet over PowerLine 129
- EUI-64 214
- EuroDOCSIS 189
- Evil Twin 357
- Expertenmodus 552
- Exploit 348, 440
- F**
 - F/FTP 78
 - F/STP 79
 - F/UTP 78
 - Far-End Crosstalk 489
 - Far-End-Fault 99
 - Faser
 - Monomode 82
 - Multimode 82
 - Singlemode 82
 - Fault Management 426
 - FCAPS 426
 - FCC 142
 - F-Connector 81
 - Fehlermanagement 428
 - Fehlersuche 487
 - Lösung 487
 - Symptome 487
 - Ursachen 487
 - Fehlertoleranz 371
 - Ferrule 84
 - APC 85
 - UPC 84
 - Feuerlöschanlage 369
 - Firewall 381, 549, 558
 - Dedizierte 382
 - Hardware 382
 - Personal Firewall 382
 - Firmware 440, 525, 533
 - First Responder 399, 402
 - Fluchtplan 400
 - Fluke 494
 - FQDN 255
 - Frame 66
 - Freigabe 538, 539
 - Freigaberechte 298
 - Frequency Hopping 144
 - Frequenzbereiche 56
 - FRM 402
 - FTP 261
 - FTTH 189
 - F-type 80
 - Fullduplex 63
 - Funkwelle 167
 - Funkzelle 145
 - G**
 - GAN 34
 - Gateway 206, 550
 - GBIC 99
 - GG45 77
 - GigaBIX 138
 - GPL 283
 - GPRS 192, 193
 - Grayware 328
 - Großrechner 30
 - GSM 192
 - H**
 - H2M-Schnittstelle 474
 - H.323 234
 - Halbduplex 63
 - Hardware-Abstraktions-
schicht 285
 - Hardware-Virtualisierung
288
 - Hash 317
 - HDSL 186
 - Header 39
 - IPv4 209
 - IPv6 212
 - Hexadezimalsystem 51
 - Honeynet 390
 - Honeypot 390
 - Host 33, 252
 - Hotline 482
 - HSCSD 192
 - HTTP 259, 384
 - HTTPS 261
 - Hub 90
 - Hub and Spoke 418
 - Hybrid Cloud 292
 - I**
 - IaaS 291
 - IAB 200
 - ICA-Protokoll 413
 - ICMP 221
 - ICS-Server 474
 - ICT-Betriebsdokumentation
435
 - IDS 391, 392, 393, 460
 - IEEE 121
 - IEEE 802.1x 98
 - IEEE 802.2 122
 - IEEE 802.3 122
 - IEEE 802.3-2012 126
 - IEEE-802-Reihe 121
 - IETF 199
 - Ifconfig 496
 - IGMP 222
 - IGP 244
 - IGRP 246
 - IKEv1 418
 - IKEv2 418
 - IMAP4 268
 - Impedanz 53
 - In-band 96
 - Industrie 4.0 472
 - Infrarot 164
 - Integer Overflow 350
 - Internet 30
 - Internet of Things 475
 - IoT 169, 191, 475
 - IP 203
 - IP-Adresse 204
 - Adressklassen 207
 - IPv4 207
 - IPv6 210
 - Private 208
 - Reservierte 208
 - Ipconfig 496
 - Iperf 468
 - IP Helper 252
 - Ip-Kommando 497
 - IPoE 554
 - IPS 460
 - IPSec 322
 - IP-Spoofing 347
 - IP-Telefonie 233
 - IPv4 566
 - Adressklassen 207
 - Adressschema 436
 - Ausnahmeadressen 209
 - CIDR 206
 - IP-Header 209
 - Netz-Bits 207
 - Private Netzwerke 208
 - IPv6 207, 210, 555, 566
 - Adressklassen 212
 - Ausnahmeadressen 213
 - EUI-64 214
 - Header 212
 - Multicast 215
 - Payload 213

Präfix 212
 Reservierte Adresse 213
 Traffic Class 213
 ISAKMP 323, 418
 iSCSI 294
 ISDN 62, 175
 B-ISDN 178
 B-Kanal 176
 Breitband-ISDN 177
 D-Kanal 176
 E1 176
 E3 176
 T1 176
 T3 176
 ISDN-BRI 176
 ISDN-PRI 176
 IS-IS 247
 ISM-Band 142
 ISMS 310, 398, 476
 ISO 27001 398, 402
 ISO/IEC 11801 74
 ITU-R 142

J

Jamming 461
 Jperf 468
 Jumbo Frames 123, 470

K

Ka-Band 191
 Kabel 71
 Adern 75
 AutoSense 76
 Drahtlose 70
 EN 50288 75
 Koaxialkabel 70
 Lichtwellenleiter 70
 Rollover 76
 STP 70
 UTP 70
 Kabeltester 488, 495
 Kabelziehstrumpf 493
 Kamera 365
 Kapazität 53
 Kennwort 522, 528, 551
 Kerberos 315
 Keycard 363
 Klartextübermittlung 341
 Koaxialkabel 80
 Kollisionsdomäne 564
 Kompetenz 482
 Konfigurationsdaten 374
 Kurzschluss 488

L

L2TP 418
 L3-Diagramm 434
 LAN 33
 Latenz 64, 191
 Latenzprobleme 579
 Leistungsbeschreibung 457, 459
 Leitungsunterbrechung 488
 Leitungsvermitteltes Netzwerk 115
 LEO 190
 Letter of Intent 458
 Lichtwellenleiter 81
 Link Aggregation 97
 Link State 246
 Linux 283
 Load Balancing 371
 Logdateien 476
 Looking Glass 501
 Loopback 99
 Loopback Plug 493
 LoRaWAN 192
 LPWAN 191
 LSA-Werkzeug 491
 LTE 194
 LTE+ 194

M

M2M 475
 MAC-Adresse 43, 88, 462
 Mail-Server 264
 Mainframe 59
 Makroviren 332
 Malware 328, 330, 335, 337
 Adware 328
 Antispyware 329
 Crimeware 329
 Grayware 328
 Spam 328
 Spyware 328
 MAN 34
 Managed Switch 96
 Man-in-the-Middle-Attacke 346
 Mannschleuse 365
 Man Trap 365
 Master Service Agreement 458
 Maßnahme
 Bauliche 362
 Medienkonverter 98

Medium

EMI 71
 Installationsaufwand 71
 Kapazität 71
 Kosten 71
 Plenum 71
 MEF-Forum 106
 Mehr-Faktor-Authentifizierung 313
 Mehrpunktverbindung 109
 Memory of Understanding 458
 Messprotokolle 439
 Metrik 243
 Metro Optical 190
 mGRE 419
 MIB 426
 Mikrofilter 547
 MIMO 150, 555
 Mitarbeit
 Aufgabenteilung 358
 Job Rotation 358
 Mandatory Vacations 358
 Segregation of Duty 359
 Modem 100
 Modulation 100
 Modus 1 Siehe Bluetooth
 Monitor 450
 Hardware 451
 Hybrid 452
 Messdaten 451
 Messobjekt 450
 Messpunkt 450
 Messzeit 451
 Schwellwert 451
 Software 451
 Monitoring 450, 454, 476
 MOU 458
 MPLS 184, 237
 MRTG 466
 MSA 458
 MSDS 485
 MTR 500
 MTU 124
 Multicast 117
 Multimeter 493
 Multimode 83
 Multiplexer 59, 101, 178, 185
 CWDM 102
 Demultiplexer 60
 DWDM 102
 FDM 60

- SMX 61
- TDM 60
- WDM 61
- Multiplikator 49
 - Binärsystem 51
 - Dezimalsystem 49
 - Hexadezimalsystem 51
 - Oktalsystem 51
- MUMIMO 152, 153, 555
- N**
 - NAC 390, 571
 - Quarantänebereich 572
 - Server 572
 - Namensauflösung 502
 - Fehlerquellen 502
 - NAS 294
 - NAT 224
 - DNAT 225
 - NAPT 225
 - PAT 225
 - SNAT 225
 - SUA 225
 - Nbtstat 502
 - Nebensprechen 54
 - Negative Rules 384
 - NET-Befehl 297, 505
 - net-Befehl 507
 - NetBIOS 253, 502, 539
 - Netio 468
 - Netsh 508
 - Netstat 510
 - Network+-Zertifizierung 19
 - Eintrittstest 21
 - Prüfungscode 584
 - Wissensgebiete 19
 - Network Interface Unit 493
 - Netzwerk
 - Client/Server 32
 - Definition 31
 - Dienst 32
 - Installation 517
 - Inventar 518, 545
 - Konfiguration 521
 - Konzeption 518
 - Leitungsvermitteltes 115
 - Modell 33
 - Netzwerkelement 31
 - Netzwerkmanagement 31
 - Netzwerkmodell 31
 - Paketvermitteltes 115
 - Peer-to-Peer 32
 - Netzwerkanalyse 460
 - Kenngößen 460
 - Messdaten 460
 - Messkonzept 460
 - Sniffer 460
 - Netzwerkdokumentation 429, 432
 - Änderungsdokumentation 432
 - Anschlussdiagramm 432, 433
 - Konfigurationsdokumentation 432
 - Logbuch 432
 - Messdiagramme 432
 - Messdokumente 439
 - Netzwerkdokumentation 432, 433
 - Verkabelungsschema 432
 - Netzwerkdrucker 305, 519
 - Netzwerkkarte 87
 - Duplexverfahren 89
 - Virtuelle 105
 - Netzwerkmanagement 35, 425
 - Sicherheit 425
 - Skalierbarkeit 425
 - Verfügbarkeit 425
 - Netzwerkmodell 33
 - BAN 33
 - CAN 33
 - GAN 33
 - LAN 33
 - MAN 33
 - WAN 33
 - Netzwerkmonitor 461
 - Netzwerkrichtlinien 355
 - Netzwerküberwachung 461
 - NEXT 489
 - NFC 171
 - NFV 105
 - NGN 182
 - NIDS 392
 - NIPS 392
 - NIU 493
 - NNTP 264
 - NOP 350
 - Notausgänge 400
 - Notfallplan 355
 - Notfallvorsorge 399
 - Novell 30, 31
 - Nslookup 503
 - NTFS 286, 303, 304
 - NTP 268
 - Nutzungsrichtlinien 355
 - O**
 - OC 179
 - OLA 458
 - On Path Attack 346
 - OS-Fingerprinting 471
 - OSI-MF 426
 - OSI-Modell 37, 40, 45, 46, 70, 181, 201
 - Anwendungsschicht 39
 - Bitübertragungsschicht 40
 - Darstellungsschicht 40
 - Sicherungsschicht 40
 - Sieben Schichten 38
 - Sitzungsschicht 40
 - Transportschicht 40
 - Vermittlungsschicht 40
 - OSPF 246
 - OS X 280
 - Aqua 281
 - Darwin 281
 - OUI 89
 - Out-of-band 96
 - P**
 - PaaS 291
 - Paketfilter 383, 385
 - Paketvermitteltes Netzwerk 115
 - PAP 314, 419
 - Passwort 300, 311
 - Patch 440
 - PDCA 456
 - PDOS 344
 - Peer-to-Peer 276
 - Perfect Forward Secrecy 418
 - Performancemanagement 431
 - Personal Firewall 382
 - Piggybacking 354
 - PIMF 78
 - Ping 497
 - ping6 498
 - Pin-zu-Pin-Messung 495
 - PKI 320
 - PLC 474
 - PMTU 124

- PoE 99, 130
 - 802.3at 130
- PoE+ 130
- PON 189
- POP3 266
- Port 230
 - Dienstadresse 230
 - TCP 230
 - UDP 230
- Port Mirroring 98
- Ports 341
 - Dynamisch 230
 - Registered Ports 230
 - Well-known 230
- Portscanner 471
 - Legalität 472
 - Online 471
- Positive Rules 383
- POTS 175
- PowerLAN 87
- Powerline 87
- Powerline Communication
 - 87
- Power over Ethernet 130
- PPP 314, 523, 554
- PPPoE 523, 554
- PPTP 420
- Pre-Shared Key 163, 558
- Primäranschluss 176
- Primärverkabelung 136
- Private Cloud 292
- Profil 300
- Protokoll 32
- Proxy 390, 391
- Prüftelefon 493
- Prüfungsvorbereitung 584
- PSK 558
- PSTN 175
- Public Cloud 292
- Pufferüberlauf 345
- Punch Down Tool 492
- Punkt-zu-Punkt-Verbindung
 - 109
- Q**
- QoS 213, 236, 455
 - Dienstklassen 455
 - Parameter 455
- QSFP 100
- R**
- Rack 486
 - Beschriftung 486
- Kabelkanäle 486
- Monitoring 486
- Säulen 486
- Schienen 486
- Radius 316, 572
- Ransomware 336
- RAS 410
- Rauchabsauganlage 369
- Rauschen 53
- RDP 412
- Reaktionsfähigkeit 482
- Rechte-Matrix 439
- Referenzmodell 35, 36
 - DoD-Modell 35
 - OSI-Modell 36
- Remote Assistance 414
- Remotedesktopverbindung
 - 411
- Repeater 90
- Request for Change 476
- Resource Exhaustion Attack
 - 349
- Rettungsplan 400
- Return Loss 490
- Reverse Proxy 391
- RFC 200, 202
- RFID 170
- RG-58 80
- RG-59 80
- RG-6 80
- RG-8 80
- RIP 104, 244
- RJ45 76
- RJ48 76
- RMON 428, 443
- Rogue Access Point 357
- Rollback 477
- Root Bridge 93
- Round Trip Time 65
- Route
 - Kommando 500
- Router 103, 104, 518
 - Link State 104
 - OSPF 104
 - RIP 104
 - Virtuell 107
- Routing 243
 - BGP 247
 - CARP 248
 - Count-to-Infinity 245
 - DVA 244
 - EIGRP 246
 - Hop-Counts 245
- HRSP 249
- IGRP 246
- IS-IS 247
- Link State 246
- OSPF 246
- RIP 244
- RIPv2 245
- Split Horizon 245
- VRRP 248
- Routing-Protokoll 242
- RRDtool 466
- RSA 319
- RSTP 93, 372
- RSVP 456
- RTP 234
- RTS 148
- RTT 65
- S**
- S/FTP 78
- S/STP 79, 564
- S/UTP 78
- SA 323
- SaaS 291
- Safe 367
- SAN 294
- Sandbox 390
- Satellit 190
 - geostationär 191
 - LEO 191
- Satellitenschüssel 190
- SCADA 474, 475
- Schleuse 365
- Schließsystem 363
- Schlüssel 363
- Schnittstellen 32
- Schulung 377
- Schwachstelle
 - Suche 394
- Score Report 589
- Screened Subnet 388
- SDH 178
- SDN 105, 434
- SDSL 186
- SD-WAN 106
- SD-WAN Edge 106
- SD-WAN Orchestrator 106
- Security-Scanner 394
- Sekundärverkabelung 136
- Sensibilisierung 376
- 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, 355
 - SiBe 398
 - Sicherheitslücke 395, 440
 - Release-Notes 395
 - Sicherheitsmanagement 431
 - Sicherungsschicht 41
 - SIEM 398, 399, 400
 - Sigfox 192
 - Signal
 - Amplitude 58
 - Ausbreitung 54
 - Codierung 59
 - Dämpfung 55, 187
 - Digitale
 - Übertragung 58
 - Frequenz 56, 58
 - Sinus 54
 - Wellenlänge 56
 - Signal-to-Noise 53
 - Simplex 63
 - Singlemode 83
 - Single Sign On 313
 - SIP 234
 - Sitzungsschicht 44
 - SLA 456, 459
 - Fehlerraten 457
 - Leistung 457
 - Reaktionsbereitschaft 457
 - Sanktionen 457
 - Verfügbarkeit 457
 - SLAAC 215
 - Smartjack 137
 - SMB 287, 539
 - SMON 428, 443
 - SMTP 264, 266
 - Smurf 343
 - Amplifier 344
 - Sniffing 460
 - SNMP 426, 427, 443
 - GET 445
 - GETBULK 445
 - RESPONSE 445
 - SET 445
 - TRAP 445
 - WALK 445
 - SNMP-Protokolle 443
 - SNMPv2 445
 - SOA 453
 - Social Engineering 351, 355
 - APT 353
 - Sonet 178
 - SOW 459
 - Spam 328
 - Spanning Tree 93
 - BPDU 93
 - Konvergenz 94
 - Kosten 94
 - Loop-Detection 95
 - Root Bridge 93
 - Spatial Reuse 153
 - SPB 95, 372
 - Speed-Test 526
 - Split Horizon 245
 - Split-Pairs 489
 - Splitter 547
 - Spoofing 347
 - ARP-Spoofing 347
 - DNS-Spoofing 348
 - Web-Spoofing 348
 - Spyware 328
 - SSAP 122
 - SSH 269, 384
 - SSID 148, 159, 549, 555, 556
 - SSL 320
 - Stack 346
 - Stateful Inspection Firewall 383
 - Stateful Packet Inspection 386
 - Stateless 215
 - State of Work 459
 - Stecker
 - GG45 77
 - RJ11 80
 - RJ45 77
 - RJ48 76
 - TERA 77
 - STP 72
 - Strukturierte Verkabelung 136
 - STS 179
 - SUA 224, 225
 - Subnettierung 568
 - Subnetzmaske 568
 - Supernetting 569
 - Supportfall 484
 - Switch 92
 - Content Switch 98
 - Cut through 93
 - Jamming 461
 - Managed 96
 - SAT 92
 - SFP 99
 - stackable 93
 - Store and forward 92
 - Virtuell 105
 - Switching Hub 92, 549
 - Switching-Hub 92
 - SYN 573
 - SynchByte 64
 - Synchrone Datenübertragung 63
 - Systemlog 439
- T**
- TACACS+ 316
 - Tailgating 354
 - Tamper Detection 367
 - TCP 116, 202, 226
 - Abort primitive 229
 - ACK 228
 - FIN-Flag 229
 - Header 227
 - RST-Flag 229
 - Sliding Windows 228
 - SYN 228
 - Verbindungsmanagement 227
 - TCP/IP 46, 60, 115, 202
 - TDM 101
 - TDR 494
 - O-TDR 494
 - Telefonkabel 71
 - Telnet 269
 - Tempest 342, 355
 - Terminaldienst 411
 - Tertiärverkabelung 136
 - Test 442, 526
 - Einzeltest 442
 - Ergebnis 442
 - Integrationstest 443
 - Maßnahmen 442
 - Systemtest 443
 - Testfall 442
 - Testfälle 442
 - Testobjekt 442
 - TFTP 263, 264
 - Thin Client 413

- Time-Division-Multiplexing 60
- TKIP 162
- TLD 254
- TLS 321
- Toner-and-Probe 494
- Tongenerator 495
- Tonsonde 494
- Topologie 109
 - Baum 112
 - Bus 110
 - Doppelring 111
 - Hybrid 113
 - Maschen 112
 - Ring 110
 - Stern 111
 - Zelle 113
- ToS 573
- Traceroute 499
- Tracert 499
- tracert-6 499
- Traffic Shaping 455, 572
- Transportprotokoll 199
- Transportschicht 43
- Transportsteuerung 44
- Triple-Play-Angebote 235
- Trunking 97
- TwinAx 81
- Twinaxial 81
- Twisted Pair 71

- U**
- U/FTP 78
- U/STP 79
- U/UTP 78
- Übertragung
 - Bidirektionale 63
- Überwachung 398, 450
- UC 235
 - Endgerät 235
 - UC-Gateway 235
 - UC-Servers 235
- UC-Kommunikation 234
- UDP 229
- UMTS 193, 194
- Undieren 567
- Unicast 117
- Unix 281
- Update 441
- Upgrade 441
- UPnP 224, 225, 226, 566
- URL 259

- USV 372, 400
- UTP 72

- V**
- VDI 413
- VDSL 186
- VDSL2 187
- Veraltete Systeme 341
- Verantwortungsbewusstsein 482
- Verdrahtungsfehler 489
- Verkabelung 564
 - Arbeitsbereich 136
 - Demarkationspunkt 136
 - Horizontale Leitung 136
 - Lebensdauer 564
 - Permanent Link 138
 - strukturierte 136
 - Vertikale Leitung 136
- Verkabelungsschema 432
- Vermittlungsschicht 43
- Verschlüsselung 318
- VF-45 85
- Videoüberwachung 366
- Viren 376, 378
- Virenverantwortlicher 374
- Virtualisierung 286
- Virtual PBX 107
- Virus 328, 331
 - Makroviren 332
 - Trojanisches Pferd 334
 - Würmer 333
- VLAN 131
 - 802.1Q 131
 - IEEE 802.1X 135
 - MAC-basiert 131
 - Portbasiert 131
 - Protokollbasiert 131
 - Tagging 132
 - Trunking 135
 - Untagged 132
 - VTP 135
- VMWare 286
 - Microkernel 286
- VNC 414
- VoIP 177, 233, 236
- Vollduplex 63
- VPBX 235
- VPN 411, 415
 - 1. Phase 416
 - 2. Phase 417
 - Access VPN 422
 - Client-to-Site 422
 - Dynamisch 422
 - ESP 417
 - Gateway 417, 420
 - GRE 419
 - IPSec 419
 - Konzentrator 422
 - L2TP 419
 - PFS 418
 - Phasen 415
 - SA 418
 - Site-to-Site 420
 - Tunnel 417
- VRRP 248
- vSwitch 105
- Vulnerabilitätsscanner 394

- W**
- W3C 201
- Wachpersonal 363
- WAF 387
- WAN 34
- War Chalking 355
- War Driving 355
- Wartungsfenster 476
- WEP 161, 356
- Widerstand 53
- Wi-Fi 4 155
- Wi-Fi 6 155
- Wi-Fi 6E 155
- Wi-Fi 7 155
- Wi-Fi Alliance 142
- Windows 2000 285
- WINS 253, 502
- Wiremap 495
- WLAN
 - Ad-hoc-Netzwerk 145
 - Antenne 577
 - Aufbau 157
 - Beacon-Frame 148
 - BSS 147
 - CB 148
 - CSMA/CA 148
 - DFS 151
 - DSSS 144
 - ESS 148
 - FHSS 144
 - Gastnetz 572
 - Halbduplex 148
 - Heatmap 159
 - Infrastrukturnetzwerk 146

- ISM-Band 142
 - Kanal 556
 - LWAPP 147
 - MAC-Filter 159
 - OFDM 144
 - Outdoor 151
 - RTS-Frame 148
 - SSID 148
 - Stör- und Dämpfungsfelder 158
 - Strahlungsleistung 142
 - Ticketsystem 572
 - TPC 151
 - Verschlüsselung 159
 - WEP 161
 - WPA 163
 - WPA2 163
 - WPA 162
 - WPA2 163, 356, 555, 557
 - WPA3 163
- X**
- X.25 115
 - XaaS 291
 - xDSL 546
 - X Window 284
- Z**
- Zero Client 413
 - Zero-Day Exploit 349
 - Zero Trust 312
 - Zigbee 169
 - Zutrittsregelung 362
 - Z-Wave 170
 - Zwei-Faktor-Authentifikation 313