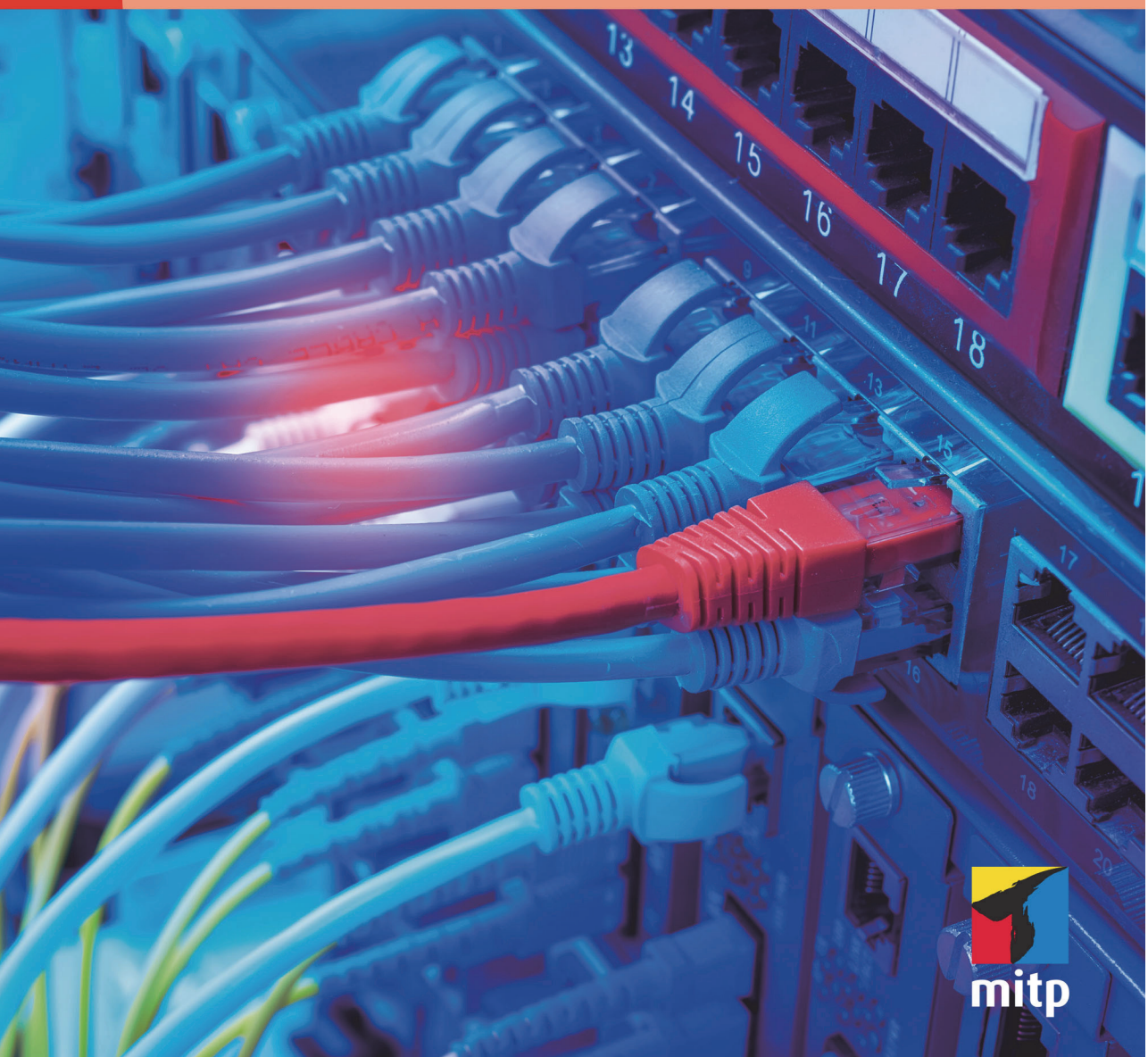


Eric Amberg | Daniel Schmid

Netzwerke

Verstehen, Einrichten, Administrieren

Mit umfassendem Praxisteil und
vielen Schritt-für-Schritt-Anleitungen



Inhaltsverzeichnis

	Einleitung.....	19
Teil I	Grundlagen	23
1	Grundlagen moderner Computernetzwerke.....	25
1.1	Die Entstehung der Computernetzwerke	25
1.1.1	UNIX und C	26
1.1.2	TCP/IP.....	27
1.1.3	Ethernet	28
1.1.4	Computernetzwerke heute.....	28
1.2	Normen und Standards.....	30
1.2.1	Internet-Standardisierungsorganisationen.....	30
1.2.2	IEEE-Standardisierung für lokale Netze	32
1.3	Komponenten eines Computernetzwerks.....	32
1.3.1	Räumliche Abgrenzung von Netzwerken	33
1.3.2	Physische Komponenten	34
1.3.3	Netzwerkanwendungen	35
1.4	Netzwerktopologien.....	36
1.4.1	Bus	37
1.4.2	Stern.....	37
1.4.3	Ring	38
1.4.4	Punkt-zu-Punkt.....	38
1.4.5	Gemischte Topologien	39
1.5	Überblick über die TCP/IP-Protokollsuite	40
1.5.1	Netzwerkebene	40
1.5.2	Anwendungsebene	40
1.6	Die Netzwerk-Referenzmodelle	41
1.6.1	Das ISO-OSI-Referenzmodell	41
1.6.2	Das TCP/IP-Modell	45
1.6.3	Vergleich OSI- und TCP/IP-Modell	46
1.7	Zahlensysteme.....	47
1.7.1	Bits und Bytes – das Binärsystem	47
1.7.2	Größenordnungen	48
1.7.3	Das Hexadezimalsystem	49
2	Kabelgebundene Übertragungstechnologien	51
2.1	Kabel und Stecker	51
2.1.1	Koaxialkabel-Standards.....	51

2.1.2	Twisted-Pair-Standards	52
2.1.3	Glasfaser-Standards	57
2.2	Ethernet-Grundlagen	61
2.2.1	Von der Bus- zur Stern-Topologie	61
2.2.2	CSMA/CD	62
2.2.3	Bridges	62
2.2.4	Switches	63
2.3	LAN-Switching	64
2.3.1	Grundsätzliche Funktionsweise des Switches	64
2.3.2	Half Duplex und Full Duplex	66
2.3.3	Kollisionsdomänen vs. Broadcast-Domänen	66
2.3.4	Multilayer-Switches	67
2.3.5	VLANs und VLAN-Tagging	67
2.3.6	Spanning Tree Protocol (STP)	69
2.3.7	Power over Ethernet	71
2.4	WAN-Technologien	72
2.4.1	Digital Subscriber Line (DSL)	72
2.4.2	Kabelanschlüsse	73
2.4.3	Fibre to the Home (FTTH)	73
2.4.4	Metro Ethernet	74
2.4.5	Multi Protocol Label Switching (MPLS)	75
2.4.6	SD-WAN (SDN)	76
2.4.7	CWDM und DWDM	76
3	Das Internet Protocol und die IPv4-Adressen	79
3.1	Der IPv4-Header	79
3.1.1	Überblick	79
3.1.2	Die einzelnen Felder des IPv4-Headers	80
3.2	Die IPv4-Adressen	81
3.2.1	Aufbau von IPv4-Adressen	81
3.2.2	Die Subnetzmaske	82
3.2.3	Subnetzadresse und Broadcast-Adresse	84
3.2.4	Wozu Subnetze?	86
3.3	Netzklassen	86
3.3.1	Herleitung der Netzklassen	86
3.3.2	So entstanden die Subnetzmasken	89
3.4	Die privaten IPv4-Adressbereiche	90
3.5	Network Address Translation (NAT)	91
3.5.1	Die NAT-Tabelle	91
3.5.2	Source NAT und Destination NAT	91
3.5.3	NAT-Kategorien	93
3.5.4	NAT Traversal	94
3.6	Spezielle IP-Adressen	95
3.6.1	Die Loopback-Adresse	95

3.6.2	APIPA und ZeroConf	96
3.6.3	Sonstige Adressen	97
4	Subnetting und CIDR	99
4.1	Einführung in das Subnetting	99
4.1.1	Herleitung des Subnettings	99
4.1.2	Binärdarstellung von IPv4-Adressen	101
4.1.3	Die Funktion der Subnetzmaske	101
4.1.4	Einführung in die Subnetz-Berechnung	102
4.1.5	Wenn Subnetze übrig bleiben	106
4.1.6	Die Magic Number	107
4.2	Fortgeschrittenes Subnetting nach RFC 950	108
4.2.1	Subnetting von größeren Ausgangsnetzen	108
4.2.2	Überlegungen zu statischem Subnetting (SLSM)	111
4.3	CIDR und VLSM – die Evolution des Subnettings	112
4.3.1	Die Variable Length Subnet Mask (VLSM)	114
4.3.2	Routen-Zusammenfassung	115
4.3.3	VLSM-Praxisbeispiel	115
4.4	Tabellenzusammenfassung	120
5	ARP und ICMP	123
5.1	Das Szenario	123
5.2	ARP – die Wahrheit über die Netzwerkkommunikation	124
5.2.1	Einführung in das Address Resolution Protocol (ARP)	124
5.2.2	Was ist nun eigentlich eine MAC-Adresse?	127
5.2.3	Der ARP-Cache	129
5.2.4	ARP bei subnetzübergreifender Kommunikation	130
5.2.5	Spezielle ARP-Nachrichten	132
5.3	ICMP – der TCP/IP-Götterbote	133
5.3.1	Einführung in ICMP	133
5.3.2	ICMP-Typen und -Codes	134
6	Routing	141
6.1	Routing-Grundlagen	141
6.1.1	Das Standardgateway	141
6.1.2	Interface-Routen	143
6.1.3	Statische Routen	144
6.1.4	Host-Routen	146
6.1.5	Die Internetanbindung	146
6.2	Dynamisches Routing mit Routing-Protokollen	148
6.2.1	Statisches versus dynamisches Routing	148
6.2.2	Grundlagen der Routing-Protokolle	148
6.2.3	Gängige Routing-Protokolle	149
6.2.4	Beispiel: Routing-Szenario mit OSPF	153

6.3	Weitere Aspekte des Routings	156
6.3.1	Die Metrik und die administrative Distanz	157
6.3.2	Die Routing-Logik	157
6.3.3	Fragmentierung und MTU	158
7	Das Internet Protocol Version 6 (IPv6)	161
7.1	Einführung in IPv6	161
7.1.1	Gründe für IPv6	162
7.1.2	Migration auf IPv6	163
7.1.3	IPv6-Support	163
7.1.4	Der IPv6-Header	163
7.1.5	Die Extension Header	164
7.1.6	Der IPv6-Adressraum	166
7.1.7	IPv6-Adressierungsgrundlagen	167
7.1.8	Global-Unicast-Adressen	169
7.1.9	Link-Local-Adressen	170
7.1.10	Spezielle Adressen	171
7.1.11	Unique-Local-Adressen	171
7.1.12	Multicast-Adressen	173
7.1.13	Anycast-Adressen	174
7.1.14	Die IPv6-Adresstypen in der Übersicht	174
7.1.15	Das Adressierungskonzept	175
7.1.16	Die Interface-ID	178
7.1.17	Berechnung der Subnet-ID	180
7.2	ICMPv6	182
7.2.1	Neighbor Discovery	184
7.2.2	Die Adressenauflösung mit ND	184
7.2.3	Der Neighbor-Cache	186
7.2.4	Die Stateless Address Autoconfiguration (SLAAC)	187
7.2.5	DHCPv6	189
7.2.6	Manuelle IPv6-Konfiguration	190
7.2.7	Path MTU Discovery	192
7.3	Weitere IPv6-Technologien und -Aspekte	194
7.3.1	IPv6-Routing	194
7.3.2	IPv6-Migrationstechnologien	194
8	Die Transportprotokolle TCP und UDP	199
8.1	TCP – das wichtigste Transportprotokoll	199
8.1.1	Der TCP-Header	200
8.1.2	Der TCP-Three-Way-Handshake	201
8.1.3	Abbau von TCP-Verbindungen	202
8.1.4	Weitere Flags im TCP-Header	203
8.1.5	Die Portnummern	203
8.1.6	Sequence und Acknowledgement Numbers	207
8.1.7	Die MSS und das TCP Receive Window	208

8.2	UDP – die schnelle Alternative	210
8.2.1	Der UDP-Header	210
8.2.2	Eigenschaften und Verwendung von UDP	211
8.3	Der Übergang zwischen den Protokollen	212
9	Die Infrastrukturdienste DHCP und DNS	215
9.1	DHCP – das Dynamic Host Configuration Protocol	215
9.1.1	Die DHCP-Kommunikation	215
9.1.2	Erweiterte DHCP-Konfiguration	218
9.1.3	DHCPv6	219
9.2	DNS – das Domain Name System	220
9.2.1	Einführung in DNS	220
9.2.2	Die DNS-Zonenverwaltung	223
9.2.3	Die Ressource Records (RR)	223
9.2.4	Die DNS-Namensauflösung	224
9.2.5	Forward und Reverse Lookup	226
9.2.6	Namensauflösung mit Resolver-Tools	226
10	Wichtige Netzerkanwendungen	229
10.1	HTTP und das World Wide Web (WWW)	229
10.1.1	Grundlagen der HTTP-Kommunikation	230
10.1.2	URL – Uniform Ressource Locator	231
10.1.3	Die HTTP-Methoden	232
10.1.4	HTTP-Request und -Response	232
10.1.5	Die HTTP-Statuscodes	234
10.1.6	Cookies – Statusinformationen im Browser	235
10.1.7	Gängige Webtechnologien	236
10.1.8	Strukturierte Daten – XML, JSON und YAML	237
10.1.9	HTTPS – die sichere Variante	239
10.2	FTP – das File Transfer Protocol	240
10.2.1	Grundlagen	240
10.2.2	Wie funktioniert FTP?	240
10.2.3	Anonymous FTP	242
10.2.4	TFTP	242
10.3	Netzwerkmanagement mit SNMP	243
10.3.1	Arbeitsweise von SNMP	243
10.3.2	SNMP-Sicherheit	246
10.4	SMTP – das E-Mail-Protokoll	246
10.4.1	Einführung	246
10.4.2	Funktionsweise von SMTP	247
10.4.3	Die SMTP-Befehle	247
10.4.4	E-Mail-Sicherheit	249
10.5	Telnet und SSH	250
10.5.1	Telnet	250

10.5.2	SSH – die Secure Shell	251
10.6	Windows-Serverdienste	253
10.6.1	Datei- und Druckerfreigabe	253
10.6.2	Active Directory	253
10.6.3	Sonstige Windows-Serverdienste	257
10.7	Voice over IP (VoIP)	258
10.7.1	Einführung	258
10.7.2	Vor- und Nachteile von VoIP	258
10.7.3	Technische Grundlagen von VoIP	259
10.7.4	Die VoIP-Infrastruktur	261
10.7.5	VoIP-Kommunikation mit SIP	262
Teil II	Praxis: Aufbau eines Netzwerks	265
11	Aufbau der virtuellen Laborumgebung	267
11.1	Bereitstellung einer virtuellen Umgebung mit VirtualBox	267
11.1.1	Download und Installation von VirtualBox	267
11.1.2	Konfiguration der virtuellen Netzwerkinfrastruktur in VirtualBox	269
11.2	Installation der virtuellen Maschinen	271
11.2.1	Installation von Windows 11	271
11.2.2	Installation von Windows Server 2022	274
11.2.3	Installation von Debian Linux	277
11.2.4	Das Laborszenario	281
12	IP-Grundkonfiguration von Windows und Linux	283
12.1	Netzwerkkonfiguration von Windows-Systemen	283
12.1.1	Ermitteln der Netzwerkkonfiguration	283
12.1.2	Anpassen der IPv4-Netzwerkkonfiguration	287
12.1.3	Testen der IPv4-Netzwerkkommunikation	290
12.1.4	Anpassen der IPv6-Netzwerkkonfiguration	292
12.1.5	Testen der IPv6-Netzwerkkonfiguration	293
12.2	Netzwerkkonfiguration von Linux-Systemen	295
12.2.1	Ermitteln der Netzwerkkonfiguration	295
12.2.2	Anpassen der IP-Netzwerkkonfiguration	297
12.2.3	Testen der Netzwerkkommunikation	300
13	Switches und Router einrichten	301
13.1	Unterschiede zwischen Home-Office- und professionellen Geräten	301
13.1.1	Home-Office-Geräte	301
13.1.2	Professionelle Switches und Router	302
13.1.3	Eigene Router-Plattformen	303
13.2	Konfiguration von Cisco-Switches	303
13.2.1	Das Cisco CLI	304

13.2.2	Grundkonfiguration des Switches	305
13.2.3	Wichtige Show-Befehle für Cisco-Switches	308
13.2.4	VLANs und VLAN-Trunking konfigurieren	309
13.3	Konfiguration eines Cisco-Routers	312
13.3.1	Die Laborumgebung	312
13.3.2	Grundkonfiguration eines Cisco-Routers	313
13.3.3	Statisches Routing konfigurieren	317
13.3.4	Dynamisches Routing mit OSPF	319
14	Bereitstellen von DHCP und DNS	321
14.1	Konfiguration eines DHCP-Servers	321
14.1.1	Installation der DHCP-Serverrolle	321
14.1.2	Erstellen eines DHCP-Bereichs	323
14.1.3	Den DHCP-Server testen	326
14.1.4	Weitere Aspekte der DHCP-Konfiguration	328
14.2	Konfiguration eines DNS-Servers	330
14.2.1	Installation von BIND9	330
14.2.2	Konfiguration einer Forward-Lookup-Zone	331
14.2.3	Den DNS-Server testen	333
14.2.4	Rekursive DNS-Anfragen	335
14.2.5	Konfiguration einer Reverse-Lookup-Zone	336
14.2.6	DNS-Replikation	338
15	Gängige Serverdienste konfigurieren	341
15.1	SSH-Server mit OpenSSH	341
15.1.1	Installation von OpenSSH	341
15.1.2	Authentifizierung mit Public Key	343
15.2	FTP-Server mit ProFTPD	346
15.2.1	Installation und Konfiguration von ProFTPD	346
15.2.2	Verbindung mit dem FTP-Server herstellen	347
15.2.3	Anonymous FTP	347
15.3	Webserver mit Apache	349
15.3.1	Installation von Apache 2.4	349
15.3.2	Übersicht über die Apache-Konfiguration	349
15.3.3	Konfiguration einer Website	350
15.3.4	HTTPS mit TLS-Zertifikat bereitstellen	354
15.4	Mail-Server mit Postfix	357
15.4.1	Postfix installieren	357
15.4.2	Postfix konfigurieren	358
15.4.3	Den Mail-Server testen	360
15.4.4	E-Mail-Sicherheit mit TLS	361
16	Eine Active-Directory-Domäne einrichten	365
16.1	Active Directory installieren	365
16.1.1	Installieren der Active-Directory-Domänendienste (AD DS)	365

16.1.2	Einen Domänencontroller erstellen	366
16.1.3	DNS überprüfen	370
16.2	Objekte und Ressourcen in AD verwalten	372
16.2.1	Benutzer erstellen und verwalten	372
16.2.2	Gruppen erstellen und verwalten	375
16.2.3	Organisationseinheiten (OUs) erstellen und verwalten	378
16.2.4	Einen Computer in die Domäne integrieren	378
16.2.5	Standorte und Dienste	381
16.3	Zugriffsberechtigungen in AD	381
16.3.1	Grundlagen der Rechte und Berechtigungen	382
16.3.2	Zugriffsrechte auf ein Objekt festlegen	382
16.4	Gruppenrichtlinien konfigurieren und zuweisen	386
16.4.1	Verwalten der Gruppenrichtlinien	386
16.4.2	Struktur einer Gruppenrichtlinie	387
16.4.3	Zuweisung und Auswirkung von Gruppenrichtlinien	389
17	Einrichtung eines Heimnetzwerks mit einem SoHo-Router	391
17.1	Die Router-Grundkonfiguration	391
17.1.1	Verbindung mit dem Router herstellen	392
17.1.2	Erste Sicherheitseinstellungen	392
17.1.3	Internetanbindung bereitstellen	394
17.2	Firmware-Update und Sicherung	396
17.2.1	Sicherung erstellen	396
17.2.2	Firmware-Update durchführen	397
17.3	Grundlegende Netzwerkeinstellungen	398
17.3.1	Switchports konfigurieren	398
17.3.2	DHCP- und IP-Adressverwaltung	400
17.3.3	DNS-Server-Einstellungen	402
17.4	Erweiterte Einstellungen und Optimierungen	403
17.4.1	Bandbreitenoptimierung durch Priorisierung	403
17.4.2	Firewall-Einstellungen	404
17.4.3	Kindersicherung und Filter	405
17.4.4	Fernzugriff und Netzwerkdienste	407
18	Netzwerk-Troubleshooting	415
18.1	Troubleshooting-Strategien	415
18.1.1	Unverzichtbar: die Intuition	416
18.1.2	Die Strategien im Detail	416
18.2	Netzwerktools richtig einsetzen	419
18.2.1	ipconfig und ip – die IP-Konfiguration	419
18.2.2	Verbindungstest mit Ping	421
18.2.3	ARP- und Neighbor-Cache prüfen	423
18.2.4	Die eigene Routing-Tabelle prüfen mit netstat und ip route show	424
18.2.5	Routenverfolgung mit tracertracert/traceroute	425
18.2.6	IP-Adressen und MAC-Adressen im Subnetz anzeigen	426

18.3	DNS prüfen	427
18.3.1	nslookup	427
18.3.2	dig und host.	428
18.4	Der Netzwerkstatus von Anwendungen	429
18.4.1	Den Portstatus und die gebundenen Ports prüfen.	429
18.4.2	Portscanning mit Nmap	432
18.5	Netzwerkanalyse mit Wireshark.	433
18.5.1	Installation und Grundlagen von Wireshark	433
18.5.2	Mitschnittfilter	434
18.5.3	Tipps zur optimalen Nutzung von Wireshark	436
Teil III	WLAN & Co. – Drahtlosnetzwerke	437
19	Einführung in Drahtlosnetzwerke	439
19.1	Grundlagen drahtloser Kommunikation	439
19.1.1	Arten drahtloser Netzwerke	439
19.1.2	Kabelgebunden versus kabellos	440
19.1.3	Entwicklung der drahtlosen Netzwerke	440
19.1.4	Technologien hinter drahtlosen Netzwerken	441
19.2	WLAN-Grundlagen	441
19.2.1	Überblick über die Hardware.	442
19.2.2	Frequenzen und Kanäle	445
19.2.3	Der IEEE 802.11 Standard	446
19.2.4	WLAN-Infrastrukturen.	447
19.2.5	Der Verbindungsaufbau.	450
19.2.6	WLAN-Sicherheit	452
20	Praktische Konfiguration eines WLAN-Netzwerks	457
20.1	WLAN-Funktionen in der Übersicht	457
20.2	Reichweiten- und Geschwindigkeitsoptimierung.	458
20.2.1	Kanaleinstellungen und Frequenzbänder.	458
20.2.2	Mesh-Funktion	461
20.2.3	Sendeleistung anpassen	462
20.3	Sicherheitskonfigurationen	463
20.3.1	SSID anpassen	463
20.3.2	Sichere Passwörter festlegen	464
20.3.3	Verschlüsselungsmethode festlegen	465
20.3.4	WPS deaktivieren	466
20.3.5	MAC-Filterung	467
20.3.6	Gastnetzwerke einrichten und verwalten	468
20.3.7	SSID verbergen.	470
20.4	WLAN-Troubleshooting	471
20.4.1	Häufige WLAN-Probleme und deren Ursachen	471
20.4.2	WLAN-Analyse durchführen und Störquellen erkennen	472

20.4.3	Geräteliste regelmäßig überprüfen	472
20.4.4	Ereignisprotokolle überwachen	473
20.4.5	Interferenzen und Störungen minimieren	473
21	Weitere Drahtlosnetzwerke	475
21.1	Drahtlose Netzwerke für Kommunikation und Internetzugang	475
21.1.1	Mobilfunknetze	476
21.1.2	Satellitenkommunikation	481
21.2	Drahtlose Netzwerke für IoT	485
21.2.1	Low Power Wide Area Networks	485
21.2.2	Kurzstrecken-IoT-Netzwerke	488
21.3	Drahtlose Technologien für persönliche Netzwerke und Nahbereichs- kommunikation	490
21.3.1	Bluetooth	490
21.3.2	NFC und RFID	493
Teil IV	Netzwerksicherheit	495
22	Grundlagen der Netzwerksicherheit	497
22.1	Ziele der IT-Sicherheit	497
22.1.1	Vertraulichkeit (Confidentiality)	497
22.1.2	Integrität (Integrity)	498
22.1.3	Verfügbarkeit (Availability)	498
22.1.4	Authentizität (Authenticity)	499
22.1.5	Verbindlichkeit / Nicht-Abstreitbarkeit (Non-Repudiation)	500
22.1.6	Zurechenbarkeit (Accountability)	500
22.2	Grundlagen der Kryptografie	501
22.2.1	Symmetrische Verschlüsselung	501
22.2.2	Asymmetrische Verschlüsselung	502
22.2.3	Hashwerte und Prüfsummen	503
22.2.4	Public Key Infrastructure (PKI)	504
22.3	Die Top-Ten-Angriffsvektoren	506
22.3.1	Schwachstellen und Exploits	506
22.3.2	Angriffe auf Webanwendungen	506
22.3.3	Malware	507
22.3.4	Social Engineering	508
22.3.5	Phishing, Spear Phishing und Whaling	509
22.3.6	Passwort-Angriffe	510
22.3.7	Man-in-the-Middle (MITM)	511
22.3.8	DoS- und DDoS-Angriffe	512
22.3.9	Angriffe auf die Cloud	513
22.3.10	Insider-Angriffe	514

22.4	Wichtige Sicherheitssysteme	514
22.4.1	Organisatorische Maßnahmen und rechtliche Vorgaben	515
22.4.2	Firewalls	516
22.4.3	Virenschutz	516
22.4.4	Intrusion Detection und Prevention Systeme	517
22.4.5	Proxys und Gateways	518
22.4.6	Maßnahmen auf Netzwerkgeräten	518
22.4.7	Externe Dienstleister	519
22.5	Systeme härten	520
22.5.1	Windows absichern	520
22.5.2	Linux absichern	521
22.5.3	Anwendungen absichern	522
23	Firewalls in der Praxis	523
23.1	Firewall-Grundlagen	523
23.1.1	Netzwerk-Firewall vs. Personal Firewall	523
23.1.2	Firewall-Architekturen	524
23.1.3	Paketfilter-Firewalls	525
23.1.4	Stateful Inspection Firewalls	527
23.1.5	Application Level Firewalls	529
23.1.6	Weitere Firewall-Features und NGFWs	529
23.2	Netzwerk-Firewalls in der Praxis	531
23.2.1	Die Laborumgebung einrichten	531
23.2.2	Übersicht über das Frontend	534
23.2.3	Grundlegende Regelkonfiguration	536
23.2.4	Erweiterte Features	543
24	VPNs mit IPsec und SSL/TLS	545
24.1	Einführung in VPNs	545
24.1.1	Was ist ein VPN	545
24.1.2	Tunnelprotokolle	546
24.1.3	VPN-Arten	546
24.1.4	IPsec und IKE	547
24.1.5	SSL/TLS-VPNs mit OpenVPN	549
24.2	VPNs mit IPsec in der Praxis	550
24.2.1	Konfiguration des Standorts Berlin	551
24.2.2	Konfiguration des Standorts Stuttgart	555
24.3	VPNs mit SSL/TLS und OpenVPN in der Praxis	559
24.3.1	Das CA-Zertifikat erstellen	559
24.3.2	Das Server-Zertifikat erstellen	560
24.3.3	Den OpenVPN-Server erstellen	561
24.3.4	Den Client-Zugriff vorbereiten	563
24.3.5	Die OpenVPN-Verbindung testen	566

Teil V	Netzwerkkonzeption und Cloud Computing	569
25	Netzwerkplanung	571
25.1	Einführung in die Netzwerkplanung	571
25.1.1	Anforderungen an das Netzwerk	572
25.1.2	Netzwerktopologien und Architekturmodelle	573
25.1.3	Redundanz und Hochverfügbarkeit	574
25.1.4	Skalierungsmöglichkeiten	576
25.2	Netzwerkarchitekturen für Campus-Netzwerke	576
25.2.1	Hierarchische LAN-Infrastrukturen	577
25.2.2	Strukturierte Verkabelung	581
25.2.3	Routing in Campus-Netzwerken	583
25.2.4	Standortvernetzung und SD-WAN	586
25.2.5	Remote Access und VPN-Strategien	587
25.3	Virtuelle Maschinen vs. Hardware	589
25.3.1	Physische Server vs. Virtualisierte Umgebungen	589
25.3.2	Cloud-Netzwerke und Hybrid-Architekturen	591
25.3.3	Container-Technologien und Microservices	591
25.3.4	Edge Computing und verteilte Architekturen	592
25.3.5	Software-defined Networking (SDN)	592
25.4	Sicherheitsstrategien	593
25.4.1	Zero-Trust-Ansatz	593
25.4.2	Netzsegmentierung	594
26	Grundlagen des Cloud Computings	595
26.1	Einführung in das Cloud Computing	595
26.2	Cloud-Service-Modelle	596
26.2.1	Infrastructure as a Service (IaaS)	597
26.2.2	Platform as a Service (PaaS)	597
26.2.3	Software as a Service (SaaS)	597
26.2.4	Weitere Service-Modelle	598
26.3	Deployment-Modelle für die Cloud	598
26.3.1	Public Cloud	599
26.3.2	Private Cloud	599
26.3.3	Community Cloud	599
26.3.4	Hybrid Cloud	600
26.3.5	Virtualisierung	600
26.4	Integration der Cloud in bestehende Netzwerke	601
26.4.1	Cloud-Dienste lokal betreiben	602
26.4.2	Anbindung an Cloud-Dienste	603
26.4.3	Einheitliches Identitätsmanagement	603
26.4.4	Container-Orchestrierung	604
26.4.5	Daten- und Applikationsmigration	605
26.4.6	Management, Monitoring und Sicherheitsrichtlinien	606

27	AWS – Cloud Computing in der Praxis	607
27.1	AWS und andere Cloud-Anbieter	607
27.2	Anmeldung und Einrichtung – erste Schritte mit AWS	608
27.2.1	Amazon Free Tier	608
27.2.2	AWS-Konto erstellen	609
27.2.3	Die AWS Management Console	609
27.3	Virtuelle Maschinen mit EC2 in der Praxis	610
27.3.1	EC2-Instanzen und AMIs	611
27.3.2	SSH-Zugriff auf eine EC2-Instanz	615
27.3.3	EC2 stoppen, beenden, sichern und wiederherstellen	617
27.3.4	EBS-Volumes	620
27.3.5	Amazon S3	621
27.3.6	Sicherheitsgruppen (Security Groups)	621
27.3.7	VPC (Virtual Private Cloud)	622
27.4	Weitere Dienste und Funktionen	625
	Stichwortverzeichnis	627

Einleitung

Netzwerke sind das Fundament unserer digitalen Welt – sie verbinden Menschen, Maschinen und Systeme rund um den Globus. Egal ob E-Mail, Cloud-Dienste, Videostreaming oder IoT-Anwendungen: Ohne funktionierende Netzwerk-Infrastruktur läuft heute nichts mehr. Dieses Buch führt Sie fundiert und praxisnah in die faszinierende Welt der Computernetzwerke ein.

Sie lernen, wie Netzwerke aufgebaut sind, wie sie kommunizieren und welche Protokolle und Technologien dabei zum Einsatz kommen. Angefangen bei den Grundlagen der Datenübertragung und Netzwerkschichten über IP-Adressierung, Routing und Switching bis hin zu modernen Themen wie WLAN, VPN, Netzwerkvirtualisierung und Netzwerksicherheit – alle Inhalte sind systematisch aufbereitet, praxisorientiert und mit vielen Beispielen und Abbildungen verständlich erklärt.

Dieses Buch richtet sich an alle, die ein solides Verständnis für moderne IT-Netzwerke aufbauen möchten – sei es für die Ausbildung, Studium, berufliche Weiterbildung oder als Vorbereitung auf Zertifizierungen wie CompTIA Network+ oder Cisco CCNA. Der Fokus liegt dabei nicht nur auf theoretischem Wissen, sondern auch auf der praktischen Umsetzung: Zahlreiche Übungen und Konfigurationsbeispiele helfen Ihnen dabei, das Gelernte direkt anzuwenden.

Tauchen Sie ein in die Welt der Netzwerke – klar strukturiert und praxisorientiert.

Für wen ist dieses Buch geeignet?

Dieses Buch ist für Sie geeignet, wenn Sie sich praxisnah und umfassend mit dem Thema »Computernetzwerke« beschäftigen möchten – ganz gleich, ob Sie Einsteiger sind oder bereits über erste Vorkenntnisse verfügen. Die Zielgruppe umfasst insbesondere:

- Studierende und Auszubildende in IT-nahen Fachrichtungen
- Netzwerk- und Systemadministratoren
- IT-Fachkräfte, die ihr Netzwerkverständnis vertiefen möchten
- Quereinsteiger mit technischem Interesse
- Vorbereitungskandidaten für Zertifizierungen wie CompTIA Network+ oder Cisco CCNA

Das Buch eignet sich sowohl zum systematischen Einstieg als auch zur gezielten Vertiefung einzelner Themenbereiche. Die Inhalte sind so aufgebaut, dass sie ein solides praxisorientiertes Fundament für den Aufbau, Betrieb und die Analyse von Netzwerken schaffen.

Auch wenn das Lesen allein bereits einen guten Überblick vermittelt, profitieren Sie am meisten von diesem Buch, wenn Sie aktiv mitarbeiten – etwa durch das Nachvollziehen von Beispielkonfigurationen oder das eigenständige Umsetzen kleiner Netzwerkaufbauten. Viele Kapitel bauen inhaltlich aufeinander auf, gleichzeitig kann das Buch aber auch als Nachschlagewerk dienen: Verweise innerhalb des Buchs helfen Ihnen, schnell die für ein Thema relevanten Grundlagen zu finden.

Inhaltsübersicht

Das Buch ist in fünf Teile gegliedert. Nachfolgend stellen wir Ihnen die Inhalte kurz vor, damit Sie sich ein Bild vom Aufbau und der Struktur machen können.

Teil I – Grundlagen

In diesem ersten Teil lernen Sie die technischen Grundlagen moderner Computernetzwerke kennen. Kapitel 1 »Grundlagen moderner Computernetzwerke« gibt Ihnen einen Überblick über die Funktionsweise und Prinzipien von IT-Netzwerken. In Kapitel 2 widmen wir uns den kabelgebundenen Übertragungstechnologien, also der physischen Basis jeder Netzwerkkommunikation. Kapitel 3 bis 7 beschäftigen sich mit dem Internet Protocol (IPv4 und IPv6), der IP-Adressierung, Subnetting, ARP, ICMP und den grundlegenden Routing-Mechanismen. Hier lernen Sie, wie Datenpakete ihren Weg durch Netzwerke finden. Kapitel 8 behandelt die zentralen Transportprotokolle TCP und UDP. In Kapitel 9 lernen Sie wichtige Infrastrukturdienste wie DHCP und DNS kennen. Den Abschluss dieses Teils bildet Kapitel 10 »Wichtige Netzwerkanwendungen«, in dem wir zentrale Netzwerkanwendungen wie SSH, Mailserver, Webserver und weitere Netzwerkdienste betrachten.

Teil II – Praxis: Aufbau eines Netzwerks

In diesem Teil setzen Sie das erlernte Wissen praktisch um. Kapitel 11 zeigt, wie Sie eine virtuelle Laborumgebung mit VirtualBox aufbauen – eine ideale Testumgebung für Experimente und Übungen. Kapitel 12 erklärt die IP-Grundkonfiguration unter Windows und Linux. Im weiteren Verlauf erfahren Sie in Kapitel 13, wie Switches und Router eingerichtet werden. Kapitel 14 und 15 widmen sich der Konfiguration typischer Serverdienste wie DHCP, DNS, Webserver, Mailserver und andere. Kapitel 16 geht einen Schritt weiter und zeigt die Einrichtung einer Active-Directory-Domäne. In Kapitel 17 »Einrichtung eines Heimnetzwerks mit einem SoHo-Router« lernen Sie, wie Sie ein einfaches Heimnetzwerk mit einem SoHo-Router aufbauen können. Kapitel 18 befasst sich mit typischen Problemen und deren systematischer Behebung – dem Troubleshooting.

Teil III – WLAN & Co – Drahtlose Netzwerke

Teil III widmet sich der drahtlosen Kommunikation. In Kapitel 19 erhalten Sie eine Einführung in WLAN und die Funktionsweise drahtloser Netzwerke. Kapitel 20 führt Sie Schritt für Schritt durch die praktische Einrichtung eines WLANs, einschließlich typischer Konfigurationsoptionen und Sicherheitsaspekten. Kapitel 21 erweitert den Blick auf weitere drahtlose Technologien, die heute ebenfalls im Netzwerkbereich relevant sind – etwa Mobilfunk, Satellitenkommunikation, Bluetooth und andere.

Teil IV – Netzwerksicherheit

Dieser Teil führt Sie in die Grundlagen der Netzwerksicherheit ein. Kapitel 22 behandelt die zentralen Bedrohungen für Netzwerke und zeigt, wie Sie Risiken durch gezielte Schutzmaßnahmen minimieren können. In Kapitel 23 richten wir Firewalls ein und betrachten deren Rolle in modernen Sicherheitskonzepten. Kapitel 24 behandelt VPN-Technologien – sowohl IPsec-basierte als auch SSL/TLS-gestützte VPNs – und erklärt, wie sichere Tunnel für die Datenübertragung aufgebaut werden. Kapitel 25 zeigt, welche sicheren Protokolle und Dienste (z.B. HTTPS, SFTP) in der Praxis eingesetzt werden und wie Sie diese implementieren.

Teil V – Netzwerkkonzeption und Cloud Computing

Im letzten Teil dieses Buchs geht es um die Planung und den Aufbau von Netzwerk-Infrastrukturen. Kapitel 25 vermittelt Grundlagen der Netzwerkplanung: Sie lernen, wie man Anforderungen analysiert, Netze strukturiert plant und Aspekte wie Skalierung, Redundanz und Segmentierung berücksichtigt. Kapitel 26 führt Sie in die Welt des Cloud Computings ein und vermittelt grundlegende Konzepte wie IaaS, PaaS und SaaS. Im abschließenden Kapitel 27 setzen Sie das Gelernte praktisch um und lernen anhand konkreter Beispiele, wie Sie eine Netzwerk-Infrastruktur in der Cloud – speziell bei AWS – entwerfen und konfigurieren.

Aktualität der Inhalte

Die Welt der IT entwickelt sich ständig weiter. Neue Tools kommen hinzu, bestehende Anwendungen erhalten Updates, grafische Oberflächen verändern sich und Konfigurationsschritte können sich von einer Softwareversion zur nächsten unterscheiden. Dieses Buch wurde mit größter Sorgfalt erstellt, alle Anleitungen wurden in funktionierenden Testumgebungen nachvollzogen und mit aktuellen Software-Versionen getestet. Dennoch möchten wir Sie darauf hinweisen, dass sich manche Darstellungen – etwa Benutzeroberflächen, Befehle oder Menüstrukturen – im Laufe der Zeit ändern können. Es ist daher möglich, dass bestimmte Abbildungen nicht mehr exakt mit dem aktuellen Stand der Software übereinstimmen oder einzelne Arbeitsschritte in einer neueren Version leicht anders funktionieren.

Lassen Sie sich davon nicht entmutigen. Die technischen Prinzipien, Protokolle und Konzepte, die diesem Buch zugrunde liegen – von IP-Adressierung über Routing bis hin zur Netzwerksicherheit –, sind weitaus langlebiger als einzelne Tools oder Konfigurationsmasken. Dieses Grundlagenwissen bleibt in der Regel über viele Jahre hinweg gültig und übertragbar – auch wenn sich eine Administrierungsfläche, das Verhalten eines Kommandos oder die Position eines Menüpunktes verändert.

Sollten Sie beim Nachvollziehen von Anleitungen auf Unterschiede stoßen, nehmen Sie dies als Gelegenheit, eigenständig weiterzudenken, nachzulesen oder Alternativen auszuprobieren. Genau diese Fähigkeit – sich selbstständig durch neue oder veränderte Netzwerkumgebungen zu bewegen – ist eine der wichtigsten Kompetenzen, die Sie als Netzwerkprofi oder Administrator entwickeln können.

Über die Autoren

Eric Amberg ist selbstständiger Experte für IT-Netzwerke und -Sicherheit und hat in den letzten 25 Jahren zahlreiche Projekte aller Größenordnungen durchgeführt. Seine große Leidenschaft ist die Wissensvermittlung, die er in Büchern, Magazinen, Seminaren und Videotrainings stets praxisnah und lebendig präsentiert.

Daniel Schmid ist bei einem großen Energiekonzern im Bereich Netzwerke und Security tätig. Als Projektleiter für diverse große, teils internationale Projekte hat er in 20 Jahren viel Erfahrung in der Planung und Implementation sicherheitskritischer Infrastruktur gesammelt.

Eric und Daniel haben bereits viele gemeinsame Projekte erfolgreich umgesetzt und sind die Gründer der Hacking-Akademie (hacking-akademie.de).

Danksagung

Ein Buch wie dieses entsteht nicht im luftleeren Raum – es ist das Ergebnis intensiver Arbeit, Diskussionen, Recherchen, Rückmeldungen und Durchhaltevermögen. Ohne die Unterstützung zahlreicher Menschen hätte dieses Buchprojekt nicht zu dem werden können, was Sie nun in den Händen halten. Dafür möchten wir – Eric und Daniel – von Herzen Danke sagen.

Ein herzliches Dankeschön geht an Sabine Schulz und Nicole Winkel vom mitp-Verlag, die dieses Projekt mit großem Vertrauen begleitet haben. Vielen Dank für eure Unterstützung und den guten Austausch während der gesamten Entstehungsphase.

Der größte Dank gilt natürlich unseren geliebten Ehefrauen Kati und Rocío. Ihr habt uns über die gesamte Dauer hinweg den Rücken freigehalten, mit viel Geduld und Verständnis die zahlreichen Abende und Wochenenden toleriert, an denen wir tief in Netzwerkthemen versunken waren. Ohne eure Unterstützung wäre dieses Buch schlicht nicht möglich gewesen.

Und Daniel möchte an dieser Stelle noch eine ganz besondere Person würdigen: Dieses Buch ist auch dir gewidmet, Noelia. Wenn Papa oft im Büro saß, hast du ihn immer »arbeiten lassen« – mit erstaunlich viel Geduld und Verständnis für dein Alter. Danke, dass du nach getaner Arbeit immer mit deinem Lachen für den nötigen Ausgleich gesorgt hast.

Vielen Dank euch allen!

Berlin und Stuttgart, August 2025

Eric und Daniel

Grundlagen moderner Computernetzwerke

Betrachten wir die rasante Entwicklung der EDV, so ist die Entstehung und Verbreitung von Computernetzwerken noch gar nicht so lange her – andererseits sehen wir auf rund 70 Jahre zurück, seit die ersten nennenswerten Computer das Licht der Welt erblickten. Zwar wurde das Internet in seinen Grundzügen bereits in den 1960er-Jahren entwickelt, jedoch wurden Computernetzwerke in Unternehmen erst in den 1980er-Jahren eingeführt. Nun, das ist inzwischen auch schon wieder rund 40 Jahre her – und angesichts der unglaublich schnellen Entwicklung in der Computertechnik kann man hier schon von Steinzeit sprechen.

In diesem ersten Kapitel sprechen wir über die Grundlagen heutiger IT-Netzwerke. Dabei fassen wir uns kurz, um den Umfang dieses Buchs nicht zu sprengen. Nach Abschluss dieses Kapitels haben Sie eine solide Übersicht und ein Grundwissen über folgende Themen:

- Die Historie von Computernetzwerken
- Normen und Standards
- Die wichtigsten Begriffe und Komponenten eines Netzwerks
- Räumliche Abgrenzung von Netzwerken (LAN, WAN etc.)
- Netzwerktopologien
- Die TCP/IP-Protokollfamilie
- Die Netzwerk-Referenzmodelle (OSI und TCP/IP)
- Zahlensysteme (Binär und Hexadezimal)

Damit legen wir die Grundlagen für die weiteren Kapitel dieses Buchs. Wir gehen nicht davon aus, dass Sie Vorwissen im Bereich der Netzwerktechnik mitbringen, von daher beginnen wir von Anfang an.

1.1 Die Entstehung der Computernetzwerke

Ende der 1960er-Jahre beauftragte das amerikanische Verteidigungsministerium (genauer die Abteilung *Advanced Research Project Agency* oder kurz: ARPA) verschiedene Universitäten und Computerhersteller damit, ein Datennetz zu konzipieren, das redundante (also mehrfach vorhandene) Datenwege ermöglichte, um beim Ausfall eines Knotens keinen *Single Point of Failure* zu haben, der das gesamte Netzwerk lahmlegen würde.

Ein *Single Point of Failure* ist eine einzelne notwendige Komponente in einem System, deren Ausfall den Ausfall des gesamten Systems zur Folge hat.

1969 wurde ein Testlauf mit einem halben Dutzend von vernetzten Systemen gestartet und unter dem Projektnamen ARPANET in Betrieb genommen. Es hatte zum Ziel, verschiedene Universitäts-

ten und das Verteidigungsministerium dezentral miteinander zu verbinden, um Forschungsergebnisse untereinander auszutauschen. Die Verbindungen wurden über Telefonleitungen aufgebaut. Im Laufe der Jahre erweiterte sich das ARPANET und wurde mit neuen Technologien versehen. Eine Übersicht über das ARPANET 1977 zeigt Abbildung 1.1.

ARPANET LOGICAL MAP, MARCH 1977

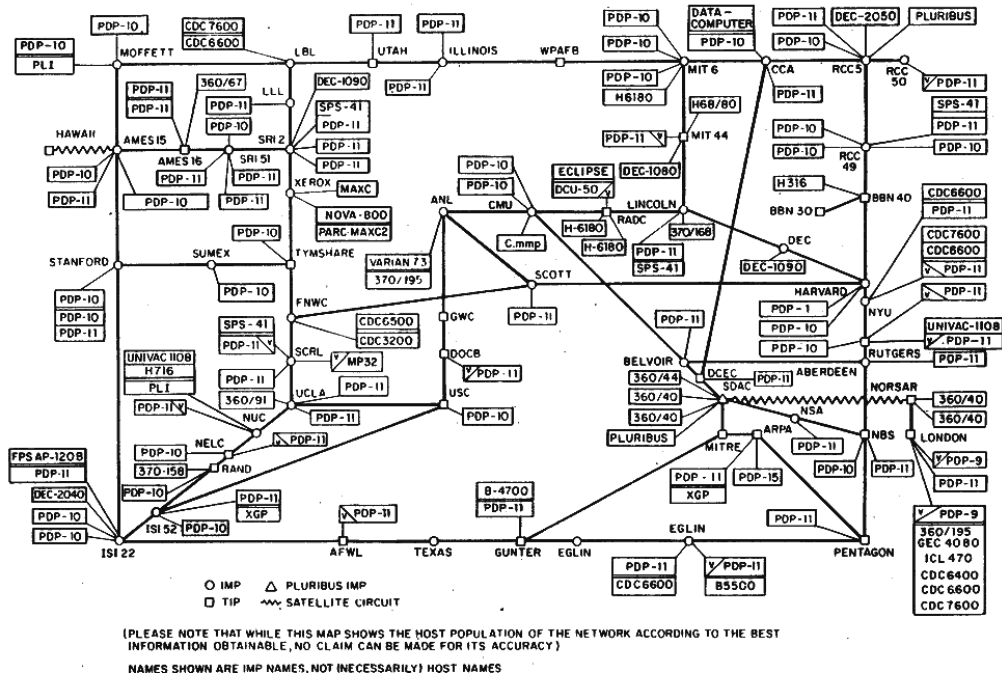


Abb. 1.1: Das ARPANET 1977 (Quelle: Wikipedia)

Die Verbindung über das Telefonnetz wurde durch sogenannte *Packet-Switching*-Technologien verdrängt, die die Datenübermittlung über Pakete ermöglichte, statt einen kontinuierlichen Datenstrom zu erzeugen. Damit konnten Verbindungen von mehreren Systemen gleichzeitig verwendet werden, da es keine dediziert geschalteten Leitungen zwischen den Kommunikationspartnern gab, sondern ein Netzwerk, das von allen Teilnehmern nach Bedarf genutzt werden konnte. Immer mehr Institutionen wurden an dieses neue Netzwerk angeschlossen. Schließlich wurde das Netzwerk auch von Unternehmen genutzt.

Beim Aufbau von dedizierten Verbindungen, wie es beim Telefon der Fall ist, spricht man dagegen von *Circuit Switching*. Hierbei werden immer zwei Systeme direkt zusammengeschaltet.

1.1.1 UNIX und C

Die weitere Entwicklung wurde durch zwei zentrale Komponenten ermöglicht: zum einen durch das Betriebssystem *UNIX* und zum anderen durch die Programmiersprache *C*, die von 1971 bis 1973 von *Dennis Ritchie* entwickelt wurde – übrigens, um genau dieses UNIX zu programmieren!

Kennen Sie den Spruch: »UNIX ist das Betriebssystem der Zukunft – schon seit 40 Jahren!«? Diese ironische Aussage entstammt einer interessanten Tatsache: Durch die Entwicklung von UNIX auf Basis der Programmiersprache C wurde eine einheitliche Betriebssystem-Plattform auf vielen verschiedenen Maschinenplattformen verfügbar und erleichterte so die Entwicklung von Netzwerkprotokollen und -anwendungen, da man nun endlich einen Quasistandard hatte. Dadurch wurde eine plattformübergreifende Kommunikation ermöglicht – das *Internet* war geboren!

UNIX schien eine goldene Zukunft bevorzustehen. Wie sich jedoch später herausstellte, sollte UNIX zwar die Zeit überdauern, jedoch diverse andere Betriebssysteme bezüglich der Bedeutung an sich vorbeiziehen lassen müssen.

1.1.2 TCP/IP

TCP/IP ist das »Protokoll« des Internets. Ein Protokoll ist ein Satz von Regeln und Prozessen, auf die sich die kommunizierenden Partner einigen. Da es verschiedene Ebenen und unterschiedliche Anwendungen innerhalb der Netzwerkkommunikation gibt, existiert eine große Anzahl von zusammenhängenden Protokollen, die als *Protokollfamilie* bezeichnet wird. TCP/IP ist daher eigentlich kein Protokoll, sondern eine ganze Protokollfamilie, wobei die beiden wichtigsten Protokolle, nämlich TCP (Transmission Control Protocol) und IP (Internet Protocol), lediglich die Namensgeber sind. Dennoch spricht man umgangssprachlich von *dem* TCP/IP-Protokoll.

Anfangs gab es im Internet (bzw. ARPANET) eine Reihe von konkurrierenden Protokollen – insbesondere die ISO (International Organization for Standardization) entwickelte einen umfassenden Protokollstapel namens OSI (Open Systems Interconnect).

Kommt Ihnen das bekannt vor? Schon mal vom *OSI-Modell* gehört? Vielleicht! Aber wussten Sie auch, dass OSI ursprünglich auch als eigenes Protokoll konzipiert wurde? In einigen sehr eingeschränkten Bereichen (z.B. beim Routing-Protokoll *IS-IS*) findet es auch heute noch tatsächlich Anwendung, jedoch konnte sich OSI gegenüber TCP/IP als Protokoll nicht durchsetzen – es war einfach zu überladen. Man entschied sich dafür, das einfachere und leichter zu implementierende Protokoll TCP/IP für das Internet zu nutzen.

Im März 1982 entschied das US-Verteidigungsministerium, dass TCP/IP *der* Standard für das ARPANET (und damit das zukünftige Internet) sein soll. Am 1. Januar 1983 erfolgte die komplette Umschaltung auf TCP/IP. Dieser Tag wurde *Flag Day* genannt.

TCP/IP wurde übrigens schon Anfang der 1970er-Jahre konzipiert – hätten Sie gedacht, dass dieses Protokoll schon so alt ist? *IPv4*, das bis heute gängige Standard-Netzwerkprotokoll, wurde 1978 vorgestellt und 1981 in **RFC 791** standardisiert. Ursprünglich wurde es im Rahmen von TCP entwickelt, doch 1978 wurde TCP in TCP und IP aufgeteilt, wodurch IP als eigenständiges Protokoll entstand. Verbunden sind die beiden jedoch bis heute. TCP ist in **RFC 793**, ebenfalls aus dem Jahr 1981, definiert.

Die *RFCs* (Request for Comment) sind die Dokumente, in denen die Komponenten des Internets inhaltlich und formal definiert werden. Mehr zu den RFCs Abschnitt 1.2.1.

TCP/IP besteht aus diversen Protokollen, die auf unterschiedlichen Netzwerkebenen arbeiten und aufeinander aufbauen. Zu diesem Thema kann man ganze Bücher füllen, und auch Sie werden im Rahmen dieses Buchs immer wieder mit einzelnen Protokollen des TCP/IP-*Stacks* (die englische

Fachbezeichnung für »Protokollfamilie«) konfrontiert werden. Wir kommen in Abschnitt 1.5 noch einmal darauf zurück. Wie auch immer: Das Internet hatte nun eine einheitliche Sprache – was die Verbreitung des größten Netzwerks dieses Planeten natürlich weiter förderte.

1.1.3 Ethernet

Ebenfalls Anfang der 1970er-Jahre begannen verschiedenen Unternehmen, wie z.B. IBM und Xerox, an lokalen Netzwerksystemen zu arbeiten, die die Computer innerhalb eines Standorts miteinander vernetzen sollten. Daraus entstand 1973 das ursprüngliche *Ethernet*. Es übertrug mit einer Geschwindigkeit von bis zu 3 Mbit/s.

Die Funktionsweise des ursprünglichen Ethernets könnte man als »koordiniertes Chaos« beschreiben. In Kapitel 2 »Kabelgebundene Übertragungstechnologien« erfahren Sie mehr Details.

Ethernet wurde ab 1980 vom *IEEE* (Institute of Electrical and Electronics Engineers) in der Arbeitsgruppe 802 weiterentwickelt und als *IEEE 802.3* standardisiert. Doch war Ethernet nicht der einzige Ansatz, den das IEEE verfolgte: Neben *Token Bus* (IEEE 802.4) wurde auch *Token Ring* (IEEE 802.5) als lokale Netzwerktechnologie entwickelt. Allerdings konnte sich langfristig nur *Ethernet* durchsetzen. Token Bus und Token Ring sind heutzutage de facto ausgestorben bzw. fristen nur noch ein Nischendasein in industriellen Produktionsnetzwerken und anderen, speziellen Netzwerken.

Im Zusammenhang mit der Einführung von Personal Computern wurde nun die Vernetzung von Arbeitsplatz-Computern möglich. Dies läutete eine neue Ära in der Unternehmenskommunikation ein – das LAN (Local Area Network) hielt Einzug in die Unternehmen.

1.1.4 Computernetzwerke heute

Es gab eine Zeit, da haben führende Computerexperten behauptet, dass niemals der Zeitpunkt kommen würde, an dem einzelne Mitarbeiter, geschweige denn Privatpersonen, einen eigenen Computer benötigen oder besitzen werden. Sie haben sich gründlich geirrt. Mittlerweile ist es ganz normal, dass jedes Familienmitglied (vielleicht mit Ausnahme des Hundes) über seinen eigenen PC, Laptop oder sein Tablet verfügt.

Ebenso selbstverständlich ist die Vernetzung der Computer untereinander geworden. Konnten sich früher nur Unternehmen den Aufbau eines lokalen Netzwerks mit Internetanbindung leisten, ist dies inzwischen für jeden »Otto-Normal-Haushalt« zur Selbstverständlichkeit geworden. Schließlich wollen mittlerweile nicht nur PC und Laptop ins Internet, sondern auch Smartphones, Tablets und der Fernseher sowie der Blu-ray-Player, smarte Assistenten wie Alexa etc. – und alle Daten müssen untereinander synchronisiert werden.

In fast allen Unternehmen existieren heutzutage Computernetzwerke. Fällt die EDV aus, liegt nicht selten der komplette Betrieb lahm. Viele Unternehmen, besonders größere, sind komplett abhängig von ihrer EDV und verlieren viel Geld, wenn vitale Systeme ausfallen.

Die meisten Menschen beschäftigen sich allerdings nur so weit mit der Materie, wie es notwendig ist, um mit dem Computer möglichst effektiv arbeiten zu können. Mit anderen Worten: Anwender von Computernetzwerken möchten einfach nur, »dass es funktioniert«. Alles andere ist nicht von Bedeutung.

Jedoch existieren hochkomplexe Prozesse hinter simplen Aktionen wie z.B. dem Aufrufen einer Website. Verschiedenste Komponenten sind beteiligt und arbeiten perfekt über eindeutig definierte Schnittstellen zusammen. Der Anwender vor dem PC macht sich keine Gedanken darüber, dass die

Daten zunächst über sein lokales Netzwerk in das Netzwerk seines Internetproviders gesendet werden. Auf der Seite des Anwenders steht vielleicht ein DSL-Router oder ein Kabelmodem, der (bzw. das) die Daten irgendwohin weiterleitet. Punkt! Dahinter steckt für den Anwender einfach eine Blackbox – irgendetwas, das funktioniert, dessen Funktionsweise er aber nicht verstehen muss (vgl. Abbildung 1.2).

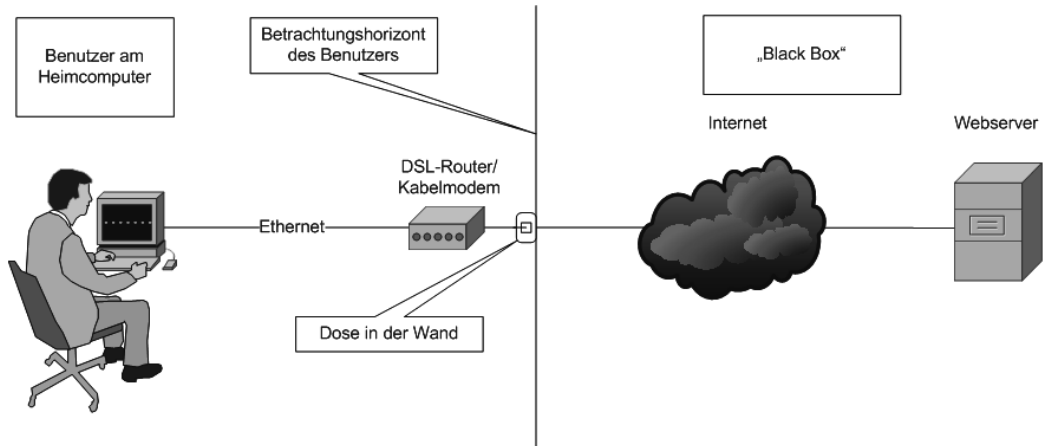


Abb. 1.2: Die Sicht des Benutzers auf das Netzwerk

Der Provider seinerseits nimmt das Datenpaket vom DSL-Router/Kabelmodem über die Punkt-zu-Punkt-Verbindung entgegen und leitet es durch sein eigenes Netzwerk hindurch entweder zum Ziel-Netzwerk oder zu einem angebundenen Provider. Dort endet sein Zuständigkeitsbereich, über den weiteren Verlauf macht er sich keine Gedanken.

Eine kurze Begriffsklärung: Ein *Provider* ist ein Anbieter von Telekommunikationsdiensten. Dies betrifft in unserem Fall in der Regel die Internetanbindung, kann aber auch Hostingdienste und Ähnliches umfassen.

Der Administrator des Unternehmens, das den aufgerufenen Webserver bereitstellt, ist dafür verantwortlich, dass das Datenpaket mit der Anfrage des Browsers zum Zielservers geleitet wird. Dieser steht aller Wahrscheinlichkeit nach auch wieder in einem lokalen Netz, das von diesem Unternehmen betrieben wird.

Merken Sie was? Jeder hat seine eigene Perspektive, seinen eigenen Blickwinkel. Wir unterscheiden im Businesskontext vier Hauptbereiche:

- **Heimnetzwerke:** Es gibt viele Menschen, die per Homeoffice von zu Hause arbeiten und darauf angewiesen sind, dass das Computernetzwerk und die Internetanbindung funktionieren. Hierbei liegt das Hauptaugenmerk auf der Anbindung der (vergleichsweise wenigen) lokalen Computer an das Internet bzw. genauer gesagt an den Provider.
- **Mobiler Benutzer:** Viele Mitarbeiter eines Unternehmens benötigen von überall Zugriff auf Ressourcen des Unternehmens. Vertriebsmitarbeiter z.B. benötigen aktuelle Präsentationen oder Daten, die auf den Servern des Unternehmens gespeichert sind, wie z.B. E-Mail. Hierzu wird ein Fernzugriff (Remote Access) bereitgestellt, in der Regel über VPN-Technologien (VPN = Virtual

Private Network). Dies sind gesicherte Verbindungen zum Unternehmens-Netzwerk. Im Grunde ist der Zugriff durch den mobilen Benutzer ein Sonderfall des Homeoffices, da in beiden Fällen dieselben Technologien zum Einsatz kommen.

- **Provider-Netzwerke:** Sie stellen die Internetwolke dar. Provider sind die Verbindungsglieder zwischen den lokalen Netzwerken. Hier geht es primär um die Bereitstellung von Schnittstellen für die lokalen Netzwerke und das Routing im Internet. Weiterhin kommt es aufgrund der hohen Datenlast auf effektive und leistungsstarke Systeme an. Die Optimierung der Datenübertragung ist hier ein wichtiges Thema.
- **Unternehmens-Netzwerke:** Fast jedes Unternehmen benötigt ein funktionierendes Computernetzwerk, um effektiv arbeiten zu können. E-Mail, Datenbanken, Datei- und Druckdienste, Webserver und viele andere Netzwerkanwendungen sind unverzichtbarer Bestandteil der Unternehmensprozesse. Fällt das Netzwerk aus, sind viele Unternehmen komplett handlungsunfähig. Hier gilt es, eine sichere, stabile und robuste Netzwerkinfrastruktur aufzubauen und zu administrieren.

Ein Unternehmens-Netzwerk kann und wird in vielen Fällen aus mehreren Standorten bestehen. Oftmals gibt es eine *Zentrale* (engl. headquarter) und eine oder mehrere *Filialen* (engl. branch offices). Während in den einzelnen Standorten LANs implementiert werden, werden die Standorte untereinander mittels WAN-Technologien miteinander verbunden. Entweder wird hierzu das Internet verwendet oder das Unternehmen nutzt einen dedizierten Anschluss, der vom Provider bereitgestellt wird. Zu den Begriffen LAN und WAN siehe Abschnitt 1.3.1.

1.2 Normen und Standards

In den Anfangszeiten der Computer und Computernetzwerke entwickelte jedes Unternehmen seine eigenen Lösungen. Diese Lösungen waren nur auf die eigenen Systeme ausgelegt und somit *proprietär*. Das bedeutet, dass es keine Interoperabilität zwischen den Systemen verschiedener Hersteller gab. Das war ein großes Problem, da somit die Skalierbarkeit und Flexibilität fehlte.

Durch die Normierung und Standardisierung von Technologien und Prozessen wird es möglich, dass Systeme verschiedener Hersteller miteinander vernetzt werden und kommunizieren können. Dies ist eine Grundvoraussetzung für die globale Vernetzung und das Internet. Es werden Anforderungen definiert, die jeder Hersteller erfüllen muss, wenn er eine bestimmte Komponente entwickelt und anbieten möchte. In diesem Abschnitt werfen wir daher einen Blick auf Institutionen, die im Rahmen der Netzwerkkommunikation Normen und Standards definieren oder bestimmte Aspekte zentral verwalten.

1.2.1 Internet-Standardisierungsorganisationen

Für die Weiterentwicklung und Standardisierung der Internet-Technologien existiert eine Reihe von wichtigen Institutionen, die wir Ihnen nachfolgend kurz vorstellen.

Internet Society

Die Dachorganisation des Internets heißt *Internet Society* (ISOC) und wurde 1992 gegründet. Sie ist eine Nichtregierungsorganisation und hat die Aufgabe, die Internetstruktur zu pflegen und weiterzuentwickeln. Sie besteht aus 150 Organisationen in über 170 Ländern und hat ihren Hauptsitz in den USA. Unter der ISOC sind verschiedene andere Organisationen und Gremien vereint, die jeweils spezifische Aufgaben wahrnehmen. Eine Übersicht über die wichtigsten Gremien finden Sie in Abbildung 1.3.

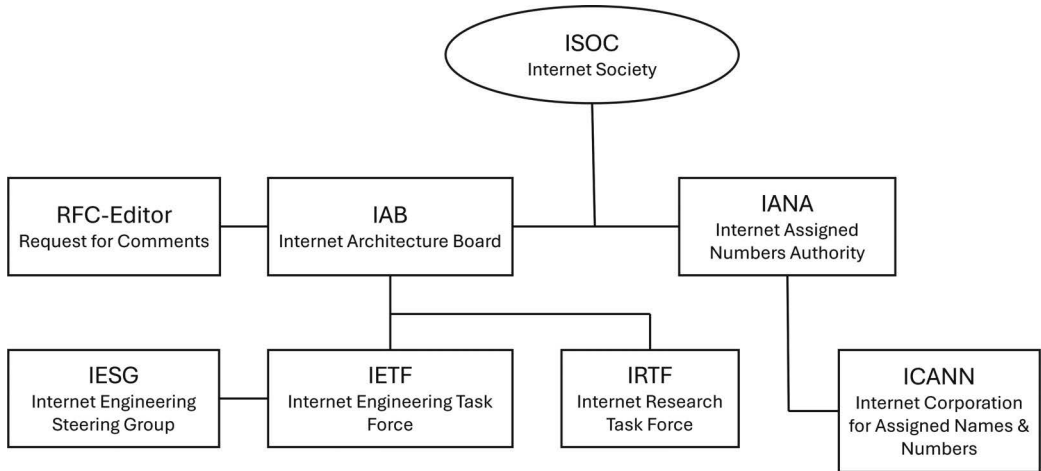


Abb. 1.3: Die ISOC und ihre untergeordneten Institutionen

Diese Institutionen haben die folgenden Aufgaben:

- **IAB (Internet Architecture Board):** Dieses Komitee unterstützt die ISOC beratend und wahrt den Überblick über die Architektur und die Standardisierungsaktivitäten der IETF.
- **RF-Editor:** Diese Institution ist der Herausgeber der RFCs (Request for Comments). Früher hatte diese Funktion eine einzige Person inne, nämlich *Jonathan Postel*. Er verstarb jedoch 1998. Die RFCs sind die wichtigsten Standardisierungsdokumente für Technologien und Prozesse, die im Internet und auch in lokalen Netzwerken verwendet werden. In diesem Buch verweisen wir immer wieder auf die entsprechenden RFCs. Diese haben verschiedene Zustände, z.B. *Draft* (Entwurf), *Proposed Standard* (vorgeschlagener Standard) oder *Internet Standard*. Letzterer ist verpflichtend und muss von allen Herstellern eingehalten werden. Viele *Proposed Standards* sind allerdings auch bereits de facto Standards geworden, die in der Praxis fast immer so umgesetzt werden. RFCs können einen anderen Status erhalten, werden aber im Nachhinein nicht verändert. Für Updates werden neue RFCs erstellt.
- **IANA (Internet Assigned Numbers Authority):** Sie ist eine der ältesten Institutionen des Internets und wurde ursprünglich ebenfalls durch *Jonathan Postel* repräsentiert. Die IANA verwaltet zentrale technische Ressourcen des Internets, darunter die IP-Adressblöcke, Protokollnummern und die Root-Zone des *Domain Name Systems* (DNS). Die IPv4- und IPv6-Adressblöcke werden an sogenannte *Regional Internet Registries* (RIR) vergeben. Für jeden Kontinent gibt es eine: *ARIN* (Nordamerika), *RIPE* (Europa), *APNIC* (Asien und Pazifik), *LACNIC* (Lateinamerika und Karibik) und *AfriNIC* (Afrika). Die RIRs vergeben ihrerseits Teile dieser Adressblöcke an regionale Internetprovider.
- **ICANN (Internet Corporation for Assigned Names and Numbers):** Diese Institution wurde 1998 gegründet, um die globale Verwaltung des Internets zu koordinieren. Ihr wurde die IANA organisatorisch unterstellt. Dies wird jedoch vertraglich regelmäßig neu ausgehandelt. Die ICANN ist für die Vergabe von Top-Level-Domains (TLDs) und andere organisatorische Aufgaben wie die Akkreditierung von Domain-Registren zuständig.
- **IETF (Internet Engineering Task Force):** Sie stellt eine Arbeitsgruppe des IAB dar und ist eine der wichtigsten Organisationen, da sie sich mit der technischen Weiterentwicklung des Internets befasst. Das Ziel sind neue Internetstandards und Best Practices, um die Funktionalität, Stabilität und Sicherheit des Internets zu verbessern. Die IETF ist offen für freiwillige Mitarbeit von

Herstellern, Netzbetreibern, Forschern oder Netzwerktechnikern aus der ganzen Welt. Es existiert keine förmliche Mitgliedschaft oder Mitgliedsvoraussetzung.

- **IESG (Internet Engineering Steering Group):** Sie ist für die Leitung der IETF zuständig und an den Standardisierungsverfahren und der Genehmigung von Standards beteiligt.
- **IRTF (Internet Research Task Force):** Ist ebenfalls eine Arbeitsgruppe des IAB und besteht aus Forschern im Bereich Netzwerktechnik mit dem Schwerpunkt Internet. Ihre Ziele sind die Erforschung und Entwicklung neuer Technologien. Die IRTF ist inhaltlich und personell eng mit der IETF vernetzt.

1.2.2 IEEE-Standardisierung für lokale Netze

Es gibt viele Technologien und Prozesse, die auch in lokalen Netzwerken zum Einsatz kommen. Somit spielt die Arbeit der oben genannten Institutionen auch in Unternehmens-Netzwerken eine große Rolle. Jedoch gibt es auch insbesondere eine Institution, die diverse Standards für Technologien in lokalen bzw. nicht globalen Netzwerken festgelegt hat. Dabei handelt es sich um das *Institute of Electrical and Electronics Engineers*, kurz: IEEE.

Hierbei handelt es sich um einen weltweiten Berufsverband von Ingenieuren der Bereiche Elektrotechnik und Elektronik sowie Informatik. Seine mehr als 400.000 Mitglieder in über 150 Ländern der Erde machen das IEEE zum größten technischen Berufsverband der Welt.

Das IEEE standardisiert Kommunikationstechnologien, Hardware und Software und ist im Gegensatz zur ISOC nicht auf das Internet spezialisiert.

Die Arbeitsgruppe 802 beschäftigt sich mit Netzwerk- und Übertragungsstandards. Die jeweiligen Standards beginnen alle mit 802 und erhalten durch Punkt getrennt eine laufende Nummer, optional gefolgt von einem oder mehreren Buchstaben, um Weiterentwicklungen und Versionsstände zu kennzeichnen. Einige dieser Standards kennen Sie vielleicht oder haben zumindest schon einmal davon gehört:

- *IEEE 802.3* – der ursprüngliche Ethernet-Standard
- *IEEE 802.3u* – Fast Ethernet (100 Mbps)
- *IEEE 802.5* – Token Ring
- *IEEE 802.11* – der ursprüngliche Wireless-LAN-Standard
- *IEEE 802.11b/g* – Übertragungsstandard mit 11 bzw. 54 Mbps
- *IEEE 802.11ax* – einer der neueren WLAN-Standards mit bis zu 9600 Mbps
- *IEEE 802.1X* – Standard zur Authentifizierung in Rechnernetzen

Vermutlich werden Sie im Laufe Ihrer Netzwerk-Karriere immer wieder über Spezifikationen der IEEE-802-Reihe stolpern. Eine Übersicht enthält der Wikipedia-Artikel unter de.wikipedia.org/wiki/IEEE_802.

1.3 Komponenten eines Computernetzwerks

Woraus besteht nun also solch ein Computernetzwerk? Was sind typische Komponenten und Begriffe, denen Sie aller Wahrscheinlichkeit nach immer wieder begegnen werden? Welche Ebenen, Strukturen und Abgrenzungen werden unterschieden? Das schauen wir uns in diesem Abschnitt näher an.

1.3.1 Räumliche Abgrenzung von Netzwerken

Bevor wir uns die physischen Komponenten ansehen, müssen wir zunächst eine grundsätzliche Unterscheidung bezüglich der Art des Netzwerks machen. Die Frage ist: Wo befindet sich unser Netzwerk, was umfasst es und welche Funktion hat es?

LAN

Die grundlegenden Netzwerke werden als *LAN* (Local Area Network) bezeichnet. LANs umfassen klassischerweise die Vernetzung innerhalb von Gebäuden. Befinden sich zwei miteinander vernetzte Gebäude in räumlicher Nähe, also z.B. auf demselben Gelände, so spricht man auch noch von einem *LAN*, wobei hier oft der Terminus *Campus-Netzwerk* verwendet wird. LANs werden hauptsächlich über Ethernet und WLAN-Technologien implementiert.

Wichtig

LANs sind *nicht* dadurch gekennzeichnet, wie viele Geräte in dem jeweiligen Netzwerk angeschlossen sind. Es kann sich um zwei Geräte in einem Home-Office-Netzwerk handeln oder um Tausende Geräte in einem Campus-Netzwerk.

PAN

Ein *PAN* (Personal Area Network) ist für die Vernetzung von Kleingeräten innerhalb eines Raums gedacht und ist eine Sonderform der lokalen Netzwerke. Zur Datenübertragung wird oft eine Drahtlos-Technologie wie WLAN, Bluetooth oder IrDA verwendet.

WAN

Wenn Standorte untereinander verbunden werden sollen, stellt sich die Wahl, ob wir eine direkte Verbindung zwischen den Standorten wünschen oder ob wir das Internet nutzen möchten. Grundsätzlich bezeichnen wir aber alle Netzwerkverbindungen, die über den Einzugsbereich eines LANs hinausreichen, als *WAN* (Wide Area Network). Ein typisches Beispiel ist die Anbindung einer Filiale an den Hauptsitz über eine Standleitung.

MAN

Eine Sonderform des WANs ist das *MAN* (Metropolitan Area Network). Es wird für die Verbindung zwischen Standorten innerhalb eines Stadtgebiets verwendet. Hierfür wird in der Regel ein sogenannter *Backbone* aufgebaut, also eine Übertragungsinfrastruktur, an die sich einzelne Standorte (LANs) anschließen können. MANs können eine Ausdehnung von bis zu 100 Kilometern haben.

GAN

Als *GAN* (Global Area Network) bezeichnen wir weltumspannende Netzwerke. Das größte GAN ist das Internet. Große Unternehmen und bestimmte Provider betreiben ihre eigenen GANs. Die Verwendung des Internets ist jedoch für die weltumspannende Vernetzung mittlerweile der Häufigkeitsfall, da die Anbindung günstig und – ggf. unter Berücksichtigung entsprechender Redundanz – auch ausreichend zuverlässig ist.

Das Internet

Typisch für LANs und WANs ist, dass sie klare und eindeutige Grenzen haben. LANs gehören einem Unternehmen, WANs werden über Provider realisiert, die dedizierte Standleitungen oder Technologien bereitstellen, für deren einzelne Anschlüsse die Unternehmen Geld zahlen müssen. GANs und MANs sind Sonderformen, die keine grundsätzlich neuen Regeln einbringen.

Das Internet jedoch ist der Zusammenschluss aller Provider und (theoretisch) all deren Kunden. Im Grunde könnten Sie jedes System auf der ganzen Welt erreichen, das an das Internet angebunden ist.

Diese Schnittstellen zwischen einzelnen Providern werden übrigens über die Internet-Knotenpunkte (*IX* für *Internet Exchange* genannt) bereitgestellt. Diese auch als *Peering Points* bezeichneten Knotenpunkte dienen den Providern als Übergangspunkte zwischen zwei Provider-Netzen. Es existieren ca. 340 Internet-Knoten weltweit. Der größte Knotenpunkt in Deutschland ist der *DE-CIX* in Frankfurt am Main, wobei *CIX* für *Commercial Internet Exchange* steht.

Im Internet ist es egal, ob Sie einen Server ansprechen möchten, der im Nebenhaus steht oder auf der anderen Seite der Welt. Aus finanzieller Sicht ist die Distanz zwischen den Kommunikationspartnern – im Gegensatz zu Standleitungen – im Internet ohne Bedeutung! Es fallen grundsätzlich nur die Kosten an, die durch die Anbindung des jeweiligen Standorts an das Internet entstehen.

1.3.2 Physische Komponenten

Bisher ging es nur um abstrakte Begriffe und es wurde allerlei Terminologie in den Raum geworfen. Nun werden wir konkret: Wie ist denn nun ein solches Computernetzwerk physisch aufgebaut? Betrachten Sie Abbildung 1.4.

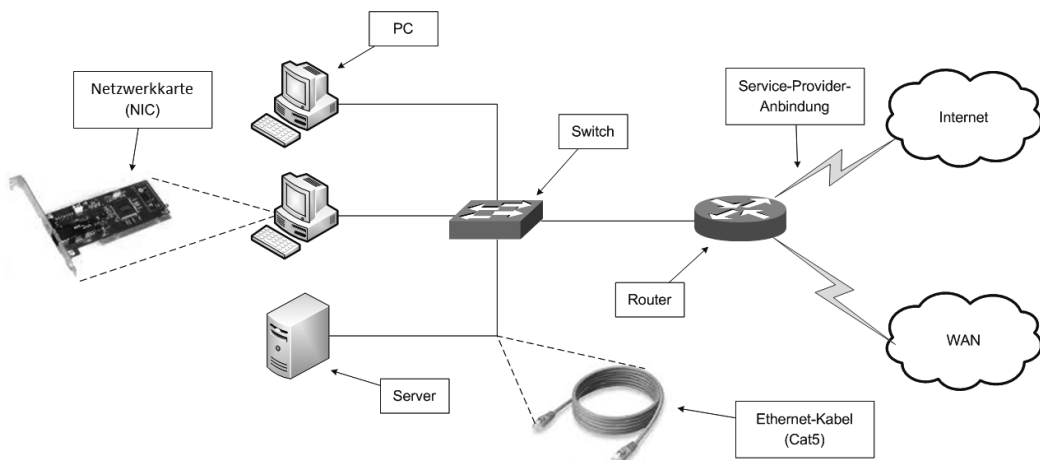


Abb. 1.4: Physische Netzwerkkomponenten

Natürlich ist dies nur ein sehr einfaches Modell – aber es reicht völlig aus, um einige grundlegende Komponenten eines Computernetzwerks vorzustellen:

- **Computer der Endanwender:** Sie stellen die Schnittstelle der Benutzer zum Netzwerk dar und bestehen in der Regel aus PCs, Laptops oder Ähnlichem. Auf ihnen werden verschiedene Arten

von Anwendungen ausgeführt: *Betriebssysteme* sind die Schnittstellen zwischen dem Benutzer, den Anwendungsprogrammen und der Hardware. *Lokale Programme* laufen nur lokal auf dem Computer und interagieren nicht mit anderen Systemen oder Programmen im Netzwerk. *Netzwerkprogramme* sind auf Endgeräten der Anwender in der Regel Client-Anwendungen, die vornehmlich keine eigenen Daten bereitstellen, sondern auf den Datenbestand von anderen Systemen (Servern) zugreifen.

- **Server:** Sie bieten bestimmte Netzwerkdienste an. Die PCs greifen auf den oder die Server zu, um z.B. Informationen aus einer Datenbank zu erhalten, eine Datei zu öffnen oder zu speichern, ein Dokument auszudrucken, eine Website anzeigen zu lassen etc. Daher nennt man diese Art der Kommunikation auch *Client-Serveranwendungen*. Sprechen Endgeräte auf gleicher Ebene untereinander, sprechen wir von *Peer-to-Peer-Kommunikation*.
- **Netzwerkkarte:** Um mit dem Netzwerk zu kommunizieren, benötigen die PCs und Server Netzwerkkarten, auch *NICs* (Network Interface Cards) genannt. Sie stellen die Schnittstelle für die Anbindung ans Netzwerk bereit. Nach außen hin enthält eine NIC lediglich eine Ethernet-Buchse und eine oder mehrere Leuchtdioden, die den Status anzeigen. Oftmals sind die Netzwerkschnittstellen heutzutage direkt auf dem Mainboard implementiert und nicht mehr eigenständige Karten, die in das Mainboard in entsprechende Slots eingesteckt werden.
- **Ethernet-Kabel:** In den meisten Fällen wird der Computer über ein Ethernet-Kabel an einen Switch angeschlossen. In der Praxis geschieht dies oft über sogenannte *Patch-Panel*. Das sind Verbindungselemente für die Gebäudeverkabelung, da diese Kabel häufig unter dem Boden verlegt werden, und am Arbeitsplatz lediglich eine Ethernet-Buchse bereitstellen. Am Patch-Panel enden diese Kabel und münden in eine weitere Ethernet-Buchse, an der ein Kabel angeschlossen wird, das z.B. zu einem Switch führt. Mehr über die verschiedenen Kabelvarianten lernen Sie in Kapitel 2.
- **Switch:** Der Switch ist ein sogenannter *Sternverteiler*. Im Switch treffen sich die Systeme und werden physisch miteinander verbunden. Früher wurden hierfür *Hubs* verwendet, aber diese Geräte sind heutzutage kaum noch anzutreffen – im Unternehmensumfeld sind sie praktisch ausgestorben. Switches werden fast ausschließlich für Ethernet-Verkabelung und damit nur im LAN verwendet. Im Gegensatz zu Hubs verfügen sie über eine gewisse Intelligenz.
- **Router:** Switches sind in der Regel an Router angebunden. Router sind die Bindeglieder zwischen einzelnen Netzwerken. Entweder verbinden Router verschiedene LAN-Subnetze (z.B. verschiedene Etagen oder Nachbargebäude) miteinander oder sie realisieren die Anbindung von lokalen Netzwerken an andere Standorte (per WAN) bzw. an das Internet. Router können zudem noch zahlreiche andere Funktionen bereitstellen, insbesondere NAT (Network Address Translation), VPN-Tunnel (Virtual Private Network) und Firewall-Funktionalität.

Hinweis

Auf WLAN und seine Komponenten gehen wir gesondert in Kapitel 19 ff. ein. Daher lassen wir das Thema zunächst außen vor und beschränken unsere Betrachtung auf die kabelgebundenen Technologien, die nach wie vor die Basis moderner Netzwerke sind.

1.3.3 Netzerkanwendungen

Die verschiedenen Netzwerkkomponenten dienen der Verbindung von Computern in einem Netzwerk und deren Kommunikation untereinander. Dies wird softwareseitig durch die Netzerkanwendungen realisiert. Es gibt hauptsächlich zwei Arten von Netzwerkkommunikation: *Client-Server* und *Peer-to-Peer*. Bei einer Client-Server-Architektur greift eine Client-Anwendung (z.B. ein Brow-

ser) auf eine Serveranwendung (z.B. einen Webserver) zu. Das ist die wichtigste Architektur in der Netzwerkkommunikation. Peer-to-Peer-Netzwerke werden eher in besonderen Situationen genutzt, z.B. im *Darknet*, wenn Daten auf verschiedene Systeme verteilt sind. In diesem Fall sind die Computer gleichzeitig Clients und Server.

Schauen wir auf einige gängige Client-Serveranwendungen:

- **World Wide Web (WWW):** Server stellen Webseiten mit Informationen und Downloads bereit, auf die mit Web-Clients, meistens Browsern, mittels HTTP(S) zugegriffen werden kann. WWW ist die wohl wichtigste Anwendung im Internet.
- **File Transfer Protocol (FTP):** Bietet die Möglichkeit, Dateien herunterzuladen oder hochzuladen. Wird heutzutage oft durch HTTP(S) ersetzt.
- **Datei- und Druckdienste:** Sowohl UNIX/Linux als auch Windows stellen Netzwerkzugriffsmöglichkeiten auf Datenspeicher bereit, die auf einzelnen Systemen liegen. Der Dateiserver speichert die Dateien und der Client greift via SMB (Microsoft Windows) oder NFS (Linux) darauf zu. Auch Drucker können in dieser Form im Netzwerk bereitgestellt werden.
- **Zentrale Objekt- und Zugriffsverwaltung:** Über Netzwerkdienste wie *Active Directory* können Domänen erstellt werden, die von Domänencontrollern gesteuert werden. In der Domänenstruktur können verschiedene Ressourcen und der Zugriff darauf zentral verwaltet werden.
- **Datenbankanwendungen:** Die strukturierte Datenspeicherung in Datenbanken ist eine der Grundlagen für die Bereitstellung von Daten im Rahmen vieler Anwendungen. Auf die Daten kann gezielt zugegriffen werden. Die Datenspeicherung geschieht auf verschiedene Arten. Es gibt auf SQL basierende Datenbanken, sogenannte NoSQL-Datenbanken und Verzeichnisse, wie z.B. LDAP. Der Datenbankserver stellt eine Schnittstelle bereit, über die durch eine Client-Anwendung auf die Daten zugegriffen werden kann. Meistens sind diese Clients direkt in die Anwendungen integriert. Dem Anwender wird eine Oberfläche angeboten, über die er die Daten abrufen, erstellen oder ändern kann.
- **E-Mail:** Als eine der ältesten Anwendungen des Internets überhaupt ist E-Mail auch heute noch sehr wichtig und überall präsent. Mailclients sind die Schnittstelle des Benutzers. Dieser kann damit Mails versenden und empfangen. Die Mails werden über den eigenen Mailserver an den Mailserver des Empfängers gesendet. Dort kann der Empfänger seine Mail einsehen bzw. durch seinen eigenen Mailclient in sein lokales Postfach herunterladen.
- **Instant Messaging:** Live Chats erfreuen sich großer Beliebtheit und werden sowohl im privaten als auch im beruflichen Umfeld genutzt. Sie sind ein guter Mittelweg zwischen einer E-Mail und einem Telefonat.
- **Voice-und Video-over-IP:** Eine der neueren Entwicklungen im Netzwerkbereich ist die Überführung bereits vorhandener Technologien in Datennetze, wie Telefonie und Video. Das bringt viele Vorteile mit sich: Wegfall eines separaten Fernsprechnetzes, Integration in die vorhandene Infrastruktur, Redundanz, zusätzliche Features und Kostenersparnis.

Natürlich gibt es noch viele weitere Netzwerkanwendungen. Dies soll zunächst eine erste Übersicht sein, um sich zu orientieren. Im Laufe des Buchs werden wir noch auf viele Aspekte der oben genannten Anwendungen detaillierter eingehen.

1.4 Netzwerktopologien

Netzwerktopologien sind ein Thema, das seit der Urzeit der Computernetzwerke eine Rolle spielt: In welcher Form werden die Systeme miteinander vernetzt? Wie Sie gleich sehen werden, müssen wir dabei in physische und logische Topologien unterscheiden.

Hinweis

Kurz zur Begriffsbestimmung: Aktive Systeme im Netzwerk werden auch als *Knoten* bezeichnet. Dabei kann es sich um ein Endgerät oder eine aktive Netzwerkkomponente wie z.B. einen Router handeln. Endgeräte werden darüber hinaus als *Host* bezeichnet. Diesen Begriffen werden Sie in diesem Buch häufig begegnen.

1.4.1 Bus

Die ersten Ethernet-Netzwerke wurden als Bus-Topologie implementiert. Jeder Computer war »in Reihe« mit dem jeweiligen Nachbarn physisch verbunden. Dies wurde über Koaxialkabel mit *BNC-Stecker* (British Naval Connector) mittels T-Stück realisiert (vgl. Abbildung 1.5).



Abb. 1.5: Koaxialkabel mit BNC-Stecker und T-Stück

Die Bus-Topologie stellt sich schematisch wie in Abbildung 1.6 dar.

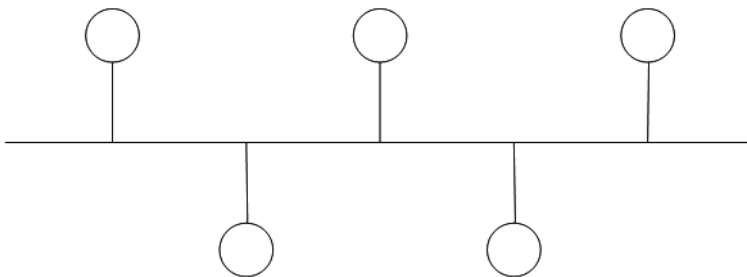


Abb. 1.6: Busverkabelung: Die Kreise stellen die Netzwerkknöten dar.

Der große Nachteil von physischen Bus-Topologien ist, dass alle Knoten an einem Kabelstrang hängen, der einen *Single Point of Failure* darstellt. Ist eine Stelle im Netzwerk defekt, wirkt sich das unter Umständen auf das gesamte Netzwerk aus. Mittlerweile werden Ethernet-Netzwerke nicht mehr in dieser Form implementiert.

1.4.2 Stern

Bei einer Stern-Topologie werden die Knoten an einem zentralen Verteiler angeschlossen, der zwischen den Knoten vermittelt. In lokalen Netzwerken ist das heute regelmäßig ein Switch, früher ein Hub. Die Stern-Topologie stellt sich schematisch dar, wie in Abbildung 1.7 gezeigt.

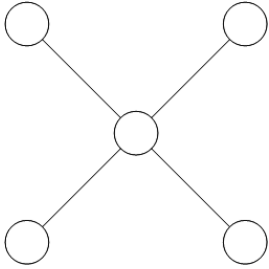


Abb. 1.7: Stern-Topologie

Im Falle eines Hubs oder Switches liegt physisch eine Stern-Topologie vor, logisch ist die Kommunikationsverbindung jedoch als Bus implementiert. Näheres dazu im nächsten Kapitel.

Stern-Topologien haben den Vorteil, dass sie relativ einfach zu implementieren sind und dass die Fehlersuche ebenfalls vereinfacht wird. Andererseits haben wir hier erneut einen *Single Point of Failure*. Fällt der zentrale Punkt – im LAN der Switch – aus, bedeutet das den Ausfall der gesamten Netzwerkkommunikation aller Knoten, die an diesem zentralen Punkt angeschlossen sind. Im Umkehrschluss führt der Ausfall eines Endpunkts oder einer Filiale nicht wie beim Bus zum Ausfall des gesamten Netzwerks.

1.4.3 Ring

Ring-Topologien spielten früher auch im LAN eine Rolle. Namentlich in Token-Ring-Netzwerken nach IEEE 802.5. Hier wurde ein physischer Ring aufgebaut, an dem alle Knoten angeschlossen waren. Der schematische Aufbau stellt sich dar, wie in Abbildung 1.8 gezeigt.

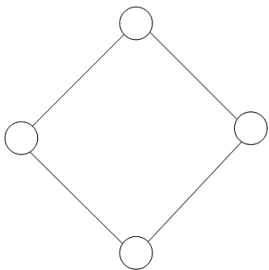


Abb. 1.8: Schematische Darstellung einer Ring-Topologie

Mittlerweile ist Token Ring jedoch nur noch in wenigen Produktionsnetzwerken anzutreffen. Heute werden Ring-Topologien jedoch noch immer in Backbone-Netzwerken z.B. in MANs eingesetzt. Auch in LAN-Umgebungen kommen sie noch vor in Form ringförmig verbundener Switches, um Redundanz zu gewährleisten.

1.4.4 Punkt-zu-Punkt

Obwohl eigentlich keine echte Topologie, sind Punkt-zu-Punkt-Verbindungen jedoch häufig bei WAN-Anbindungen anzutreffen. Punkt-zu-Punkt-Verbindungen bestehen schlicht aus zwei Endpunkten, zwischen denen sich meistens nichts außer der Leitung befindet (vgl. Abbildung 1.9).



Abb. 1.9: Schematische Darstellung einer Punkt-zu-Punkt-Verbindung

Oftmals sind Router in dieser Form miteinander verbunden, jedoch kann die Punkt-zu-Punkt-Topologie auch als Bestandteil anderer Topologien auftreten. Auf höheren Ebenen der Netzwerkkommunikation sind auch virtuelle Punkt-zu-Punkt-Verbindungen möglich.

1.4.5 Gemischte Topologien

Topologien können auch miteinander kombiniert werden (vgl. Abbildung 1.10).

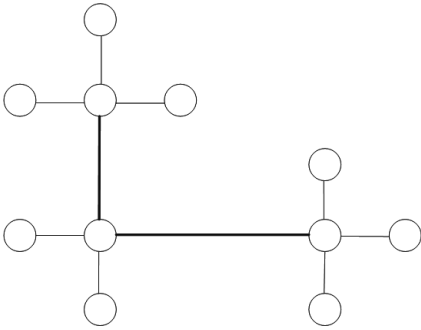


Abb. 1.10: Stern-Bus-Topologie

Im Beispiel in der Abbildung sind die Knoten über eine Stern-Topologie miteinander angebunden, aber die Sternverteiler sind als Bus verbunden. Werden Systeme, z.B. Router, über diverse Wege miteinander verbunden, sprechen wir auch von *teilvermascht* (engl. partial meshed) oder *vollvermascht* (engl. full meshed), je nachdem, ob nur ein Teil der Knoten redundant angebunden ist oder ob alle Knoten mit allen verbunden sind (vgl. Abbildung 1.11).

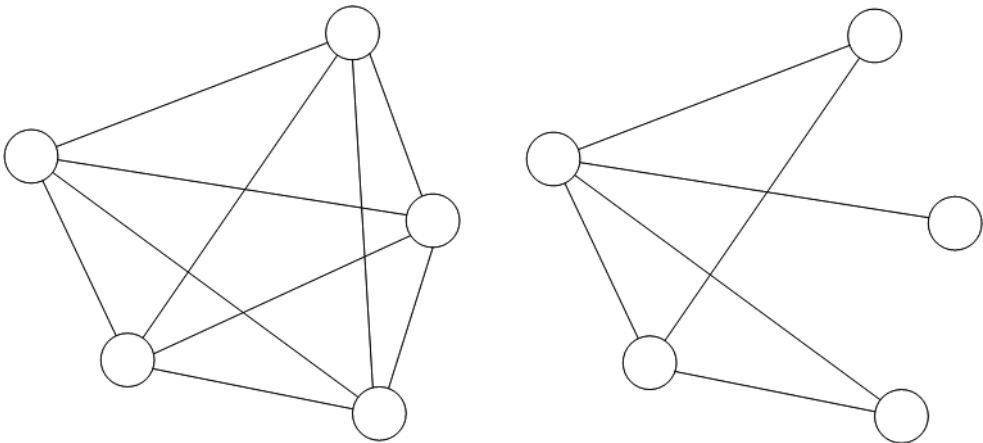


Abb. 1.11: Links ein vollvermaschtes (full meshed) und rechts teilvermaschtes (partial meshed) Netzwerk

Denken Sie daran, dass sich Topologien auf die physische und logische Ebene sowie Standortverbindungen beziehen können. Sie müssen also die Netzwerktopologie im jeweiligen Kontext betrachten. Über VPN und andere Tunneltechnologien können Systeme wie Router logisch direkt miteinander verbunden sein, wobei der physische Weg über viele Router führt.

1.5 Überblick über die TCP/IP-Protokollsuite

Sie haben bereits in Abschnitt 1.1.2 einen ersten Kontakt mit der TCP/IP-Protokollfamilie gehabt. Weitere Bezeichnungen sind:

- TCP/IP-Protokollsuite
- TCP/IP-Protokoll-Stack (bzw. engl. TCP/IP Protocol stack)
- TCP/IP (als Synonym für die gesamte Protokollfamilie)

Wie bereits erwähnt, besteht TCP/IP aus diversen Einzelprotokollen, die aber auch miteinander in Verbindung stehen.

1.5.1 Netzwerkebene

Wir können grob zwischen der Netzwerkebene und der Anwendungsebene unterscheiden. Auf der Netzwerkebene arbeiten generische Protokolle, die für alle Anwendungen gleichermaßen nutzbar sind und allgemeine Aufgaben der Netzwerkkommunikation übernehmen. Zu den TCP/IP-Protokollen der Netzwerkebene gehören die folgenden. Sie sind in aufsteigender Reihenfolge gemäß der Netzwerk-Referenzmodelle geordnet:

- **ARP** – das *Address Resolution Protocol*: Es löst logische IP-Adressen in Hardware-Adressen (MAC-Adressen) auf.
- **IP** – das *Internet Protocol*: Es ist das zentrale Protokoll der Suite und regelt die logische Adressierung sowie die Wegfindung. Es existiert als IPv4 und IPv6.
- **ICMP** – das *Internet Control Message Protocol*: Ist ein wichtiges Protokoll zur Übertragung von Status- und Fehlerinformationen im Netzwerk.
- **TCP** – das *Transmission Control Protocol*: Dies ist das am häufigsten verwendete Transportprotokoll für Anwendungsdaten im Internet.
- **UDP** – das *User Datagram Protocol*: Eine Alternative für TCP mit weniger »Overhead«, also weniger Features, dafür einfacher und schneller.

1.5.2 Anwendungsebene

Die Anwendungsebene kann weiter unterteilt werden, jedoch finden wir hier im Allgemeinen spezifische Protokolle für bestimmte Anwendungen. Dazu gehören z.B. die folgenden:

- **HTTP** (Hypertext Transfer Protocol) – Anwendung: WWW
- **FTP** (File Transfer Protocol) – Anwendung: Dateiübertragung
- **Telnet/SSH** – Anwendung: Remotezugriff via Kommandozeile
- **SMTP** (Simple Mail Transfer Protocol) – Anwendung: E-Mail
- **DNS** (Domain Name System) – Anwendung: Namensauflösung
- **DHCP** (Dynamic Host Configuration Protocol) – Anwendung: IP-Konfigurationszuweisung
- **NTP** (Network Time Protocol) – Anwendung: Zeitsynchronisation
- **SIP** (Session Initiation Protocol) – Anwendung: VoIP-Management

Stichwortverzeichnis

10BASE2 (RG 58) 51
10BASE5 (RG-8) 52
1Password 510
2FA Authentifizierung 522
2G (Mobilfunk) 476
2-Tier-Design 577
3DES-Verschlüsselung 502
3G (Mobilfunk) 478
3rd Generation Partnership Project (3GPP) 487
3-Tier-Design 579
464XLAT 196
4G (Mobilfunk) 478
5G (Mobilfunk) 479
5G Campus-Netze 481
5G Private-Netze 481
6to4 195
802.1Q-Tag 314
802.1X 519

A

a2enmod 354
Access Control List (ACL) 498, 518
Access Layer 577, 580
Access Point (AP) 443
Access-Port 69
Access Switche 577
Access Token 513
Accounting 513
Acknowledgement Numbers 207
Acknowledgment Number (TCP-Header) 200
Active-Active 574
Active Directory 253
Active-Directory-Domänendienste (AD DS) 365
Active-Directory-integrierte Zonen (DNS) 372
Active-Directory-Schema 254
Active Directory-Standorte und -Dienste 381
Active FTP 241
Active Member Address (AMA) 490
Active-Passive 574
AD CS 257
Address Resolution Protocol (ARP) 123, 124
Address Space Layout Randomization (ASLR) 521
AD DS 257
AD FS 257
Ad-hoc-Netzwerk 448
Adjacency 150
AD LDS 257

Administrative Distanz (AD) 157
AD RMS 257
ADSL 72
Advanced Distance Vector Protocol 151
Adware 507
A-Eintrag 224
AES (Advanced Encryption Standard) 502
AGDLP-Prinzip (AD) 375
AH 547
AIDE 522
Alibaba Cloud 608
Amazon CloudFront 625
Amazon CloudWatch 625
Amazon DynamoDB 625
Amazon Free Tier 608
Amazon Machine Image (AMI) 611
Amazon RDS (Relational Database Service) 625
Amazon S3 (Simple Storage Service) 621
Amazon SNS (Simple Notification Service) 625
Amazon Web Services (AWS) 607
Anomaly Detection 593
Anonymous FTP 242, 347
Antenne 442
Antivirenprogramm 508, 516
Anycast 167
Anycast-Adressen 174
Anycast Routing 513
Anzeigefilter (Wireshark) 435
Apache 349
API 237
API-Key 513
APIPA-Adresse 96
AppArmor 522
Application-Layer-Gateway 173
Application-Level-Firewall 529
Application-Level-Gateway (ALG) 529
Architekturmodelle 573
Area Border Router (ABR) 151
Argon2 511
ARP 423
ARPA 25
ARP-Cache 125, 129, 423
ARP-Reply 125
ARP-Request 125
ARP-Spoof-Detection 512
ARP-Tabelle 129
ASP.net 237

Asymmetrische Verschlüsselung 502
 Auditing 522
 Authentication Frame (WLAN) 451
 Authentication Header 165
 Authenticator-App 393
 Authentizität (Authenticity) 499
 authorized_keys-Datei 345
 Autoconfiguration 189
 Auto MDI-X 56
 Autonomes System 149, 152
 Autoritative Nameserver 223
 AV-Programm 516
 AWS CloudFormation 625
 AWS IAM (Identity and Access Management) 625
 AWS Lambda 625
 AWS Management Console 609
 AWS Outposts 602
 AWS Step Functions 625
 AXFR (Authoritative Transfer) 338
 Azure AD Connect 603

B

Backbone-Area 150
 Backdoor 507
 Backhaul-Dienste 484
 Backplane 64
 Backup Designated Router (BDR) 151
 Baiting 509
 Bajonettverschluss 52
 Bandbreite 49
 Bandwidth 157
 Bare-Metal-Server 589
 Base Station Controller (BSC) 477
 Base Station Subsystem (BSS) 477
 Base Transceiver Station (BTS) 477
 Basisbandübertragung 51
 bcrypt 504, 511
 Beamforming 480
 Benutzer (AD) 372
 Bereichsoptionen (DHCP) 328
 Binärsystem 48
 BIND9 330
 Biometrische Merkmale 499
 Bit 48
 Blacklist 405
 Blacklisting 525
 Blowfish 502
 Bluetooth 441, 490
 Bluetooth 4.0 492
 Bluetooth Low Energy (BLE) 490
 Bluetooth Mesh 492
 Bluetooth Special Interest Group (SIG) 490
 BNC 52
 Bootstrap Protocol (BOOTP) 215
 Border Gateway Protocol (BGP) 112, 152
 Bot 512
 Botnet 508
 Bottom-up (Troubleshooting) 417

BPDU 70
 BPDU Guard 519
 branch offices 30
 Breitbandübertragung 51
 Bridge 62
 Bridge-Mode-Firewall 523
 Broadcast 85, 167
 Broadcast-Adresse 84
 Broadcast Control 519
 Broadcast-Domäne 66
 Broken Access Control 506
 Brute-Force-Angriff 510
 BSS 448
 BSSID 451
 Burned-In Address (BIA) 127
 Bus-Topologie 37, 573
 BYOD 441
 Byte 48

C

Campus-Netzwerke 576
 Canonical-Name-Eintrag (CNAME) 224
 Carrier 74
 Carrier Ethernet 74
 CCMP 453
 Certificate Authorities (CA) 504
 CGI 237
 ChaCha20-Algorithmus 502
 Changemanagement 516
 Checksum (TCP-Header) 200
 CI/CD 604
 CIDR (Classless Inter Domain Routing) 112
 Circuit Switched Fallback 479
 Circuit Switching 26
 Cisco Packet Tracer 303
 Classful Network 88
 Classful Routing 149
 Classless Routing 149
 Client-Server-Architektur 35, 573
 Cloud 595
 Cloud-Anbieter 607
 Cloud API 513
 Cloudbasierte Infrastrukturen 574
 Cloud Computing 595
 Cloud-Dienste 603
 Cloud-Netzwerke 591
 Cloud-Service-Modelle 596
 Cloud Storage 595
 Clustering 575
 CMTS 73
 Collapsed Core 579, 581
 Command and Control Server 512
 Common Name (CN) 355
 Community Cloud 599
 Computerverwaltung 380
 Connection Tracking 528
 Connectivity Standards Alliance (CSA) 489
 Container 513

Container (AD) 373
 Container-Orchestrierung 604
 Container-Technologien 591
 Control Bits (TCP-Header) 200
 Control Plane 76
 Cookies 231
 Core-Design 581
 Core Layer 579, 581
 Core-Switches 580
 costs 150
 Country-Code-TLD (ccTLD) 222
 Crossover-Kabel 55
 CRUD-Operationen 237
 Cryptographic Failures 506
 CSS 236
 CTI 261
 CWDM 77

D

Database as a Service (DBaaS) 598
 Data Execution Prevention (DEP) 521
 Datagram Length 211
 Datagramme 46
 Data Offset (TCP-Header) 200
 Data Plane 76
 Datenschutz-Grundverordnung (DSGVO) 515
 Dead Peer Detection (DPD) 549
 Debian Linux in VirtualBox 277
 DE-CIX 34
 Deep Packet Inspection 525
 Default Address Selection 173, 176
 Default-Gateway 141
 Default-Route 141, 317
 Denial of Service (DoS) 512
 DES (Data Encryption Standard) 502
 Designated Port 70
 Designated Router (DR) 151
 Desktop as a Service (DaaS) 598
 Desktop-Firewall 523
 Destination NAT (DNAT) 91, 93
 Destination Options Header 164
 Device-Management 593
 Device Provisioning Protocol (DPP) 466
 DevOP 604
 Dezimalsystem 47
 DHCPACK 216
 DHCP-Agent 217
 DHCPDISCOVER 216
 DHCP-Einstellungen FRITZ!Box 400
 DHCP-Lease 321
 DHCP NACK 217
 DHCPOFFER 216
 DHCP-Optionen 218, 325
 DHCP Relay Agent 218
 DHCPREQUEST 216
 DHCP-Reservierung 328
 DHCP-Server Konfiguration 321
 DHCP-Serverrolle 321

DHCP-Snooping 519
 DHCPv6 189, 219, 329
 Dictionary Attack 510
 Diffie-Hellman (DH) 503
 Diffusing Update Algorithm (DUAL) 151
 dig 228, 333, 428
 Digitale Signatur 498, 500, 503
 Disaster Recovery 499
 Discontiguous Networks 112
 Distance-Vector-Protokolle 149
 Distributed DoS 499, 512
 Distribution Layer 577, 581
 Divide and Conquer (Troubleshooting) 417
 DMZ 524, 542
 DN (Distinguished Name) 256
 DNS 256, 292, 307, 370, 427, 539
 DNS-Cache 225
 DNS-Replikation 338
 DNS-Request 225
 DNS-Resolver 224
 DNS-Server 330
 DNS-Server-Einstellungen FRITZ!Box 402
 DNS-Suffix 290
 DNS-Zonen 223
 Docker 591, 604
 DOCSIS 73
 DoD-Modell 45
 Domaincontroller (DC) 256
 Domänen-Admins (Gruppe) 380
 Domänenbaum (AD) 253
 Domänenbenutzer (Gruppe) 380
 Domänencontroller (DC) 366
 Domänenlokale Gruppen 375
 Dovecot 362
 Drahtloses Netzwerk 439
 DSA (Digital Signature Algorithm) 503
 DSCP 80
 DSL 72
 DSLAM 72
 DS-Lite 196
 DSL-Modem 72
 DSRM-Kennwort 367
 Dual-Band-Antenne 443
 dual homed 144
 Dual-Stack 195
 DWDM 77
 Dynamic ARP Inspection (DAI) 519
 Dynamic Host Configuration Protocol (DHCP) 215
 Dynamisches Routing 148
 DynDNS 409

E

EAP 453, 454
 EBGp (Exterior BGP) 152
 EBS-Snapshot 620
 EBS-Volume (Elastic Block Store) 620
 EC2 (Elastic Compute Cloud) 597
 EC2 Instance Connect 615

Echo Reply 133
 Echo Request 133
 EDGE (Enhanced Data rates for GSM Evolution) 476
 Edge Computing 592
 EIA/TIA-568 54
 EIGRP(v6) 194
 Einstellungen (Windows) 283
 Elastic Compute Cloud (EC2) 610
 Elastic Kubernetes Services 604
 Elastic Load Balancing (ELB) 625
 ElGamal 503
 E-Mail-Sicherheit 361
 Encapsulation Security Payload 165
 Ende-zu-Ende-Adressierung 81
 Ende-zu-Ende-Kommunikation 131
 Enhanced Interior Gateway Routing Protocol (EIGRP) 151
 eNode-B 478
 Enterprise-Mode 454
 ESP 547
 ESS 449
 ESSID 451
 Etherchannel 575
 Ethernet 28
 Ethernet-ID 127
 Ethernet-Kabel 35
 EU1-64 178
 Evil Twin 511
 Evolved Packet Core (EPC) 478
 Evolved Packet System (EPS) 478
 Evolved UMTS Terrestrial Radio Access Network (E-UTRAN) 478
 Exim 357
 Exploit 506
 Extension Header 162, 164
 Exterior Gateway Protocol (EGP) 149

F

F/STP 54
 Failover 574
 False Negative 517
 False Positive 517
 Fernzugriff FRITZ!Box 407
 Fingerprint 252
 Firewall-as-a-Service (FWaaS) 516
 Firewall Einstellungen FRITZ!Box 404
 Firewalls 516
 Firmware-Update FRITZ!Box 396, 397
 Flag 201
 Flag-Day 27, 163
 Flags (IPv4-Header) 80
 Flapping 153
 Flooding 65
 Flow Label 164
 Follow the Path (Troubleshooting) 418
 Forwarder (DNS) 335
 Forward Lookup 226
 Forward-Lookup-Zone 331

Fragment Header 165
 Fragmentierung 158, 209
 Fragment Offset 80
 Frame 46, 212
 Frequenz-Hopping (Bluetooth) 491
 FRITZ!Box 457
 FRITZ!Box Einrichtung 393
 FRITZ!Fernzugang 408
 FSMO 257
 FTP 54, 240
 FTP-Datenkanal 240
 FTP-Server 346
 FTP-Verwaltungskanal 240
 FTTH 73
 Full Cone NAT (Port Forwarding) 94
 Full Duplex 66
 Full Tunneling 588
 Fully Qualified Domain Name (FQDN) 221
 Function as a Service (FaaS) 598
 Funktionsebenen (AD) 367
 Funkzelle 476

G

G.fast 72
 GAN (Global Area Network) 33
 Gastnetz FRITZ!Box 398
 Gast-WLAN 468
 Gateway of last resort 319
 Gateways 518
 Geo-Blocking 513
 Geostationary Earth Orbit (GEO) 482
 Gesamtstruktur (AD) 253
 Gibibyte 48
 Gigabyte 49
 Glasfaser-Kabel 57
 Global Configuration Mode (Cisco) 305
 Globale Gruppen 375
 Globaler Katalog (DC) 256, 367
 Global-Routing-Präfix 169
 Global-Unicast-Adressen 169
 Google Cloud Platform (GCP) 607
 GPRS (General Packet Radio Service) 476
 GPS-Tracker 477
 gpupdate 390
 Gratuitous ARP 133
 GRUB-Bootloader 279
 Gruppen (AD) 375
 Gruppenrichtlinien (GPOs) 255, 386
 Gruppenrichtlinienverwaltung 389
 GSM (Global System for Mobile Communications) 476
 GUID 256

H

H.323 259
 Half Duplex 66
 Hardware Address 127
 Hashcat 510

- Hashwert 498, 503
- Header Checksum (IPv4-Header) 81
- headquarter 30
- Health Insurance Portability and Accountability Act (HIPAA) 515
- Heim-Netzwerk 29
- Hello-Protokoll 150
- Heuristische Analyse 517
- Hexadezimalsystem 49
- Hide-NAT 524
- Hierarchische LAN-Infrastrukturen 577
- High Availability (HA) 574
- High-Availability-Protokolle 575
- High Ports 204
- High-Throughput IoT (H-T IoT) 485
- Hochverfügbarkeit 574
- Home Location Register (HLR) 477
- Home-Office-Geräte (Merkmale) 301
- Hop-by-Hop Options Header 164
- Hop Count 149, 157
- Hop Limit 164
- Horizontale Skalierung 576
- host 334
- Hostanteil (Subnetting) 82
- Host-based IDS (HIDS) 517
- Host-Header-Wert 233
- Host-Routen 146
- Hosts-Datei 220, 225
- Hot Standby Router Protocol (HSRP) 575
- HTML 229
- HTTP 229
- HTTP-Cookies 235
- HTTP-Methoden 232
- HTTP Request 232
- HTTP-Response 233
- HTTPS 239, 354, 539
- HTTP-Statuscode 234
- HTTP Strict Transport Security (HSTS) 512
- Hub 61
- Human Hacking 508
- Hybrid-Architekturen 591
- Hybride Netzwerk-Infrastrukturen 574
- Hybrid-Topologie 573
- Hypervisor 589
- Hypervisor (Typ-1) 589
- Hypervisor (Typ-2) 589
- I**
- IAB (Internet Architecture Board) 31
- IANA (Internet Assigned Numbers Authority) 31, 175
- IBM Cloud 607
- IBPG (Interior BGP) 152
- IBSS 448
- ICANN (Internet Corporation for Assigned Names and Numbers) 31
- ICE 262
- ICMP 123
- ICMP-Codes 134
- ICMP-Typen 134
- ICMPv6 182
- Identification and Authentication Failures 507
- Identitäts-Management 603
- Identity and Access Management (IAM) 513
- IEEE 28, 32
- IEEE 802.11 441, 446
- IESG (Internet Engineering Steering Group) 32
- IETF (Internet Engineering Task Force) 31
- IKE 548
- IKEv1/IPsec 546
- IKEv2/IPsec 546
- IMAP4 247
- Incident Response 515
- Infrastructure as a Service (IaaS) 597
- Infrastruktur-Modus (WLAN) 448
- Initialisierungsvektor (IV) 453
- Initial Sequence Numbers (ISN) 207
- Injection 506
- Insecure Design 506
- Insider-Angriffe 514
- Instanz-Familien 612
- Instanz-Typ 612
- Integrität (Integrity) 498
- Interesting Octet 109
- Interface Configuration Mode (Cisco) 305
- Interface-ID 178
- Interface-Routen 143
- Interferenzen 459
- Interior Gateway Protocol (IGP) 149, 151
- Intermediate CA 504
- Internet 34
- Internet Control Message Protocol (ICMP) 133
- Internet der Dinge (IoT) 592
- Internet Information Services (IIS) 257, 349
- Internet of Things (IoT) 484
- Internet Protocol 79
- Internet Society (ISOC) 30
- Inter-Satelliten-Kommunikation 483
- Intrusion Detection-Systeme (IDS) 512, 517
- Intrusion Prevention Systeme (IPS) 512, 517
- IoT-Netzwerke 440, 485
- IP-Blocking 513
- ipconfig 286, 290, 370, 419
- IP-Paket 46
- IP-Range (DHCP) 323
- IPsec 547, 587
- iptables 303, 522, 526
- IPv4 79
- IPv4-Adressen 81, 101
- IPv4-Header 79
- IPv6-Header 163
- IPv6-Routing 194
- IRTF (Internet Research Task Force) 32
- ISAKMP 548
- ISATAP 195
- ISC DHCP-Server 329

ISM-Band (Industrial, Scientific, and Medical Band) 486
 IT-Sicherheitsgesetz 515
 IXFR (Incremental Zone Transfer) 338

J

Java 237
 JavaScript 236
 John the Ripper 510
 JSON 238
 Jumbogram 164

K

Kabelmodem 73
 Kanaleinstellungen (WLAN) 459
 KeePass2 510
 Kerberos 256
 Kernnetz (Mobilfunk) 476
 Keylogger 507
 Kibibyte 48
 Kilobyte 49
 Kindersicherung FRITZ!Box 405
 Kollisionsdomäne 63, 66
 Kosten 150
 Kryptografie 501
 Kubernetes 513, 591
 Kurzstrecken-IoT-Netzwerke 485

L

L2TP/IPsec 546
 Label Edge Router (LER) 75
 Label Popping 75
 Label Switched Path (LSP) 75
 Label Switch Router (LSR) 75
 LAN (Local Area Network) 33
 LAN-Routing 585
 Layer-3-Switch 67
 LDAP 256
 Lease 215
 Leasedauer 324
 Least Connections 575
 Least Privilege 514, 593
 Least Significant Bit (LSB) 127
 Let's Encrypt 354
 Lightweight Access Points 449
 Link-Local-Adresse 170, 287
 Link State Advertisement (LSA) 150
 Link-State-Protokolle 150
 Load Balancing 499, 513, 575
 Local Exploit 506
 localhost 95
 Locally Administered Address 128
 Logging 500, 521, 522, 543, 588
 Long Range Wide Area Network (LoRaWAN) 486
 Long Term Evolution for Machines (LTE-M) 487
 Loopback-Adresse 95, 171
 Loop Guard 519

LoRa-Gateways 486
 LoRaWAN-Server 486
 Low Earth Orbit (LEO) 482
 Low Power Wide Area Networks (LPWAN) 485
 Low-Throughput IoT (L-T IoT) 484
 LTE (Long Term Evolution) 478
 LTE-Netz 478

M

M2M-Kommunikation 477, 484
 MAC-Adresse 127
 MAC-Filter (WLAN) 467
 Magic Number (Subnetting) 107, 118
 Maildir-Verfahren 359
 Mail-Exchanger-Eintrag (MX) 224
 Mailserver 357
 Mail Transfer Agents (MTA) 357
 Mail User Agents (MUAs) 362
 Malware 507
 MAN (Metropolitan Area Network) 33
 Management Mobility Entity (MME) 478
 Man-in-the-Middle (MITM) 511
 Man-in-the-Middle-Angriffe (MITM) 498
 Masquerading (Hide NAT, NAT Overload) 92
 Maximum Segment Size (MSS) 209
 Maximum Transmission Unit (MTU) 158, 209
 mbox 360
 MD5 (Message Digest) 504
 Mebibyte 48
 Media Gateway (MGW) 477
 Medium Earth Orbit (MEO) 482
 Megabyte 49
 Mesh-WLAN 458, 461
 Metrik 157
 Metro Ethernet 74
 M-Flag (DHCPv6) 220
 MGCP 259
 MIB (SNMP) 244
 Microsegmentation 593
 Microservices 591
 Microsoft Azure 607
 Microsoft Exchange 357
 Microsoft Management Console (MMC) 323
 Millimeterwellen 480
 MIME 233
 MIMO-Antenne 443, 447
 Mitschnittfilter (Wireshark) 434
 Mobiler Benutzer 29
 Mobile Switching Center (MSC) 477
 Mobilfunknetz 441, 476
 Mobil Station (MS) 477
 ModSecurity 529
 Monitoring 588, 593
 Monitoring (Cloud) 606
 MOS-Wert 260
 Mountpoints 522
 MP-BGP-4 194
 MPLS 75

MTA (Mail Transfer Agent) 247
 MUA (Mail User Agent) 247
 Multicast 85, 167
 Multicast-Adressen (IPv6) 173
 Multifaktor-Authentifizierung (MFA) 500, 593
 Multilayer-Switch 67, 578, 585
 Multimode-Glasfaser 58
 Multiprotocol Label Switching (MPLS) 587
 Multi-Tier-Architektur 525

N

Nameserver 223
 Narrowband IoT (NB-IoT) 487
 NAT64/DNS64 196
 National Institute of Standards and Technology (NIST) 596
 NAT-PT 196
 NAT-Tabelle 91
 NAT Traversal 94, 548
 Near Field Communication (NFC) 493
 Neighbor Advertisement 184
 Neighbor Cache 186, 294
 Neighbor Discovery 184
 Neighbor Solicitation 184
 NETCONF 593
 netdiscover 426
 netstat 142, 205, 425, 429
 Network Access Control (NAC) 588
 Network Address Translation (NAT) 91, 404, 518
 Network and Switching Subsystem (NSS) 477
 Network as a Service (NaaS) 598
 Network Attached Storage (NAS) 410
 Network-based IDS (NIDS) 517
 Network Functions Virtualization (NFV) 574
 Network Manager 145, 295
 Network Slicing 480
 Netzanteil (Subnetting) 82
 Netzklasse 86
 Netzlaufwerk einbinden 412
 Netzsegmentierung 594
 Netzwerkeinstellungen FRITZ!Box 398
 Netzwerk-Firewall 523
 Netzwerkkarte 35
 Netzwerkkonfiguration (Windows) 283
 Netzwerkrichtlinien- und Zugriffsdienste 257
 Netzwerksicherheit 497
 Netzwerkspiegel (Debian Linux) 279
 Netzwerktopologien 573
 Next-Generation-Firewall 530
 Next Header 163
 Next Hop 144
 nftables 522
 nginx 349
 Nicht-Abstreitbarkeit 500
 Nicht autoritative Nameserver 223
 Nmap 432
 NO_PROPOSAL_CHOSEN 558
 NodeB 478
 Northbound-API 76
 Notfallmanagement 515
 nslookup 227, 292, 334, 427
 NTP 307

O

Öffentlicher Schlüssel 502
 Offline-Angriff 510
 O-Flag (DHCPv6) 220
 OID (SNMP) 245
 One-Time-Password (OTP) 499
 OneWeb 481, 483
 Online-Angriff 510
 ONT (Optical Network Terminal) 74
 OpenFlow 593
 Open Relay 249, 359
 Open Shortest Path First (OSPF) 150
 OpenSSH 341
 OpenSSL 354
 OpenVPN 546, 549, 559, 588
 OpenWrt 303
 Options (TCP-Header) 200
 Oracle Cloud 608
 Orbit 482
 Organisationseinheit (AD) 253, 373, 378
 Organizationally Unique Identifier 128
 OSI-Modell 27
 OSI-Referenzmodell 41
 OSPF (Cisco) 319
 OSPFv3 194
 OWASP (Open Web Application Security Project) 506
 OWE 454

P

Packet Data Unit, PDU 62
 Packet-Switching 26
 Pairing (Bluetooth) 491
 Paketfilter-Firewall 525
 PAN (Personal Area Network) 33
 Panel-Antenne 443
 Parabolspiegelantenne 443
 Parsen 212
 Passive FTP 242
 Passive Member Address (PMA) 491
 Password Guessing 510
 Passwort-Angriff 510
 Patchmanagement 516
 Path MTU Discovery 192
 Payload Length 164
 Payment Card Industry Data Security Standard (PCI DSS) 515
 PBX 261
 PDU 44
 Peering Points 34
 Peer-to-Peer-Architektur (P2P) 573
 Peer-to-Peer-Netzwerke 36
 Perfect Forward Secrecy (PFS) 549

Personal-Firewall 523
 Personal Mode 454
 PFS 454
 pfSense 531
 Phased-Array-Antenne 483
 Phishing 249, 509
 PHP 237
 Physikalische Adresse 127
 Piconet 490
 Ping 133, 291, 421, 536
 Platform as a Service (PaaS) 597
 Pluggable Authentication Modules (PAM) 521
 Podman 591
 Pointer-Eintrag (PTR) 224
 Policy and Charging Rules Function (PCRF) 479
 POP3 247
 POP (Point of Presence) 74
 Port Address Translation (PAT) 93
 Portchannel 575
 Port Forwarding 408, 542
 Portfreigabe 404
 Portnummern 203
 Port Restricted Cone NAT 94
 Port Security 519
 Portweiterleitung 404
 Postfix 357
 Powerline 71
 Power over Ethernet (PoE) 71
 PTP 546
 Primärbereich 581
 Primäre Nameserver 223
 Privacy Extensions 179
 Private Cloud 591, 599
 Private Key 343, 502
 Private Ports 204
 Privater Schlüssel 502
 Privileged EXEC Mode (Cisco) 305
 Privilege Escalation 506
 Probe Requests (WLAN) 451
 Professionelle Router (Merkmale) 302
 Professionelle Switches (Merkmale) 302
 ProFTPD 346
 Proposal (VPN) 549
 Protokollfamilie 27
 Protokollierung 500
 Provider 29
 Provider-Netzwerk 30
 Proxy 593
 Proxy ARP 132
 Proxy-Server 518
 Prüfsumme 503
 Pseudo-Header 211
 PSK 453
 Public Cloud 591, 599
 Public Key 343, 502
 Public-Key-Authentifizierung 343
 Public Key Infrastructure (PKI) 500, 504
 Punkt-zu-Punkt-Verbindungen 38

PuTTY 251

Q

Qmail 357
 Quad-A-Eintrag 224
 Quagga 303
 Quality of Service (QoS) 259, 403
 Quid pro quo 509

R

Radio Frequency Identification (RFID) 493
 Radio Network Controller (RNC) 478
 RADIUS 454
 Rahmen 46
 Ransomware 507
 Rapid STP (RSTP) 71
 Rate-Limiting 512
 RC4-Algorithmus 502
 Realtime-Schutz 516
 Redundanz 574
 Regional Internet Registry (RIR) 31, 113
 Registered Ports 204
 Registration Authorities (RA) 89, 504
 Registrierungsstellen 504
 Rekursiver DNS-Request 335
 Relayhost 359
 Remote-Access 587
 Remote-Access-VPN 546
 Remote-Desktopdienste 257
 Remote Exploit 506
 Repeater 61
 Ressource Record (RR) 223
 Restricted Cone NAT 94
 Reverse ARP (RARP) 133
 Reverse Lookup 226
 Reverse-Lookup-Zone 336
 Reverse Proxies 518
 RFC 27
 RFC-Editor 31
 Richtantenne 443
 Ring-Topologie 38, 573
 RIPng 194
 RJ-45-Stecker 54
 RNDC-Verfahren 339
 Road-Warrior 546
 Roaming 461
 Rogue Access Point 511
 Rogue-DHCP-Server 321, 519
 Role-Based Access Control (RBAC) 588
 Rollen- und Rechtekonzepte 515
 Root-Bridge 70
 Root-CA 504
 Root Guard 519
 Rootkit 507
 Root Port 70
 Round Robin 575
 Round Trip Time (RTT) 134

Routen-Zusammenfassung 115
 Router 35
 Router Advertisements 187
 Router Solicitation 187
 Routing 141
 Routing Domain 149
 Routing Header 164
 Routing Information Protocol (RIP) 149
 Routing-Protokolle 148
 RSA (Rivest, Shamir, Adelman) 503
 RTCP 259
 RTP 259

S

S3 (Simple Storage Service) 597
 S3-Bucket 621
 S3 Glacier 621
 S/STP 54
 Salt-Wert 511
 Sandbox 517
 Satellitenkommunikation 440, 481
 Scatternetz 491
 Schlüsselaustausch 503
 Schreibgeschützter Domänencontroller (RODC) 367
 Schwachstelle 506
 Scope-ID (IPv6) 171
 SCP (Secure Copy) 252
 script 504, 511
 SDN-Controller 592
 SDSL 72
 SD-WAN 76, 586
 Second-Level-Domain 222
 SecureCRT 251
 Security as a Service (SECaaS) 598
 Security Association (SA) 548
 Security Groups (AWS) 621
 Security Logging and Monitoring Failures 507
 Security Misconfiguration 506
 Segmente 46
 Sekundärbereich 581
 Sekundäre Nameserver 223
 Self-Signed-Zertifikat 355
 SELinux 522
 Sendeleistung (WLAN) 462
 Sendmail 357
 Sequence Number (TCP-Header) 200, 207
 Server 35
 Server-Manager 321, 365
 Serveroptionen (DHCP) 328
 Server-Side Request Forgery (SSRF) 507
 Service-Eintragstyp (SRV) 224
 Services-Datei 220
 Serving-Gateway (SGW) 478
 Session-ID 235
 SFTP (Secure FTP) 252
 SHA-1 (Secure Hash Algorithm) 504
 SHA-2 (Secure Hash Algorithm) 504

SHA-3 (Secure Hash Algorithm) 504
 Shell 250
 Sicherheitseinstellungen FRITZ!Box 392
 Sicherheitsrichtlinien 515
 Sicherheitsrichtlinien (Cloud) 606
 Sicherung FRITZ!Box 396
 SID 256
 SIEM-Systeme 514
 Sigfox 486
 SIM-Karte 476
 Singlemode-Glasfaser 58
 Single Point of Failure 25, 37
 Single-Sign-On (SSO) 385, 588
 SIP 259, 262
 Site-to-Site-VPN 546
 Sliding Window 209
 Slowloris 512
 Small Cells 480
 Small Formfactor Pluggable (SFP) 60, 583
 Smart Meter 477
 SMB 256
 Smishing 509
 SMTP 246
 Snapshot 601
 SNMP 243
 SNMP-Agents 243
 SNMP-Kommandos 245
 SNMP-Managementkonsole 243
 SOA-Eintrag (DNS) 331
 Social Engineering 508
 Softphone 261
 Software and Data Integrity Failures 507
 Software as a Service (SaaS) 597
 Software-defined Networking (SDN) 76, 574, 592
 Software-defined Wide Area Network (SD-WAN) 587
 SoHo-Router 449
 SoHo-Router Einrichtung 391
 Source NAT 91
 Southbound-API 76
 SpaceX 483
 Spam 249
 Spanning Tree Protocol (STP) 69, 575
 Spear Phishing 509
 Splitter 72
 Split Tunneling 562, 588
 Spoofing 467, 528
 Spot the Differences (Troubleshooting) 418
 Spyware 507
 SQL-Injection 506
 SRD-Band (Short Range Device Band) 486
 SRV-Einträge 371
 ss 431
 SSH (Secure Shell) 251, 307
 ssh-keygen 343
 SSH-Server 341
 SSID 451, 463, 470
 SSL 239, 549

SSLplus 354
 Stabantenne 443
 StackWise 574
 Stammdomäne (AD) 366
 Standard-Gateway 141, 317
 Starlink 481, 483
 Start-of-Authority-Eintrag (SOA) 224
 STARTTLS 249, 364
 Stateful Inspection Firewall 527
 Stateful Packet Inspection (SPI) 519, 527
 Stateless Address Autoconfiguration (SLAAC) 187
 Static Length Subnet Mask (SLMS) 111
 Static SNAT 92
 Statische Routen 144
 statische Subnetzmasken 106
 Stern-Topologie 37, 573
 Storm Control 519
 STP 54
 Straight-Through-Kabel 55
 Strukturierte Verkabelung 581
 Stub-Resolver 225
 STUN 93, 261
 Subinterfaces (Cisco) 314
 Subnet-ID 169, 180
 Subnetting 99
 Subnetz 83
 Subnetzadresse 84
 Subnetzmaske 82, 100, 101
 Summary Routes 151
 Switch 35, 63
 Switched Virtual Interfaces (SVIs) 585
 Switch-Stacking 63
 Switch Virtual Interface (Cisco) 306
 Symmetric NAT 94
 Symmetrische Verschlüsselung 501
 System Configuration Dialog (Cisco) 313
 System Ports 204

T

TAE-Dose 72
 Tagged Port 68
 Tailgating 509
 TAP (OpenVPN) 550
 TCP/IP 79
 TCP/IP-Referenzmodell 45
 TCP-Header 200
 TCP Receive Window 208
 Tebibyte 48
 teilvermascht 39
 Teilvermaschte Topologie 578
 Telekommunikations- und Telemediengesetz (TKG/ TMG) 515
 Telnet 250
 Teredo 195
 Terminal 250
 Tertiärbereich 581
 TFTP 242
 Thickenet 52

Thinnenet 51
 Thread 489
 Three-Legged Firewall 524
 Three-Way-Handshake 201
 Timestamps 500
 Time to Live (IPv4-Header) 80
 Time to Live (TTL) 134
 TKIP 453
 TLS (Transport Layer Security) 239, 361, 549
 TLS-Zertifikat 354
 Token Bus 28
 Token Ring 28, 38
 Top-down (Troubleshooting) 416
 Toplevel-Domain 221
 Topology Table 151
 Traceroute 137, 425
 Tracert 137
 Traffic Class 163
 Transitives Vertrauen 504
 Transmission Control Protocol (TCP) 199
 Transparente Firewall 523
 Transportbereich (Mobilfunk) 476
 Transport Mode 547, 548
 Tripwire 522
 Trojaner 507
 Trunk Port 68
 TUN (OpenVPN) 550
 Tunnel-Broker 196
 Tunnel Mode 547, 549
 TURN 262
 Twisted-Pair-Kabel 52
 Twisted-Pair-Medientypen 56

U

UDP-Datagram 211
 UDP-Header 210
 Ultra-Narrowband-Modulation (UNB) 487
 UMTS-Netz 478
 Unicast 85, 167
 Unique-Local-Adressen 171
 Universally Administered Address 128
 Universelle Gruppen 375
 Unmanaged Switches 301
 Unspezifizierte Adresse 143, 171
 Unternehmens-Netzwerk 30
 Urgent Pointer (TCP-Header) 200
 URL 231
 User Datagram Protocol (UDP) 210
 User Equipment (UE) 478
 User EXEC Mode (Cisco) 305
 User Ports 204
 UTP 54

V

Variable Length Subnet Mask (VLSM) 112, 114
 VDSL 72
 Vendor Extension 218

Verbindungsorientiert 199
 Vererbung der Berechtigungen (Windows) 382
 Verhaltensanalyse 517
 Vermaschte Topologie (Mesh) 573
 Verteilte Architekturen 592
 Vertikale Skalierung 576
 Vertraulichkeit (Confidentiality) 497
 Viren 507
 Virenschutz 516
 VirtualBox 267
 VirtualBox Extension Pack 269
 Virtualisierte Netzwerke 574
 Virtualisierung 600
 Virtual Machine (VM) 600
 Virtual Private Network (VPN) 407, 519, 545, 586
 Virtual Router Redundancy Protocol (VRRP) 575
 Virtual Switching System (VSS) 574
 Virtuelle LANs (VLANs) 583
 Virtuelle Maschinen (VMs) 589
 Virtuelle Routing-Instanzen 519
 Vishing 509
 Visitor Location Register (VLR) 477
 VLAN 67, 309, 519
 VLAN-Tagging 68
 VLAN-Trunking 310
 Voice over IP (VoIP) 258
 Voice over LTE (VoLTE) 479
 VoIP-Codecs 260
 Vollvermaschte Topologie 39, 578
 VPC (Virtual Private Cloud) 622
 VPN-Protokolle 587
 VTY-Lines (Cisco) 308
 Vulnerable and Outdated Components 507

W

WAN (Wide Area Network) 33
 WCDMA (Wideband Code Division Multiple Access) 478
 WDS 450
 Web Application Firewall (WAF) 518, 529
 Webserver 349
 Website 230
 Well Known Ports 204
 WEP 452, 465
 Whaling 509
 Whitelist 405, 525
 Wi-Fi 441, 447
 Wi-Fi Alliance 447
 Wi-Fi Easy Connect 466
 Wildcard Mask (Cisco) 319
 Window (TCP-Header) 200
 Windows 11 in VirtualBox 271
 Windows Defender Firewall 293, 521

Windows Rechte und Berechtigungen 382
 Windows-Server 2022 in VirtualBox 274
 WINS 290
 WireGuard 546, 588
 Wireless Network 439
 Wireless Personal Area Network (WPAN) 490
 Wireshark 433
 WLAN 439
 WLAN-Controller 449
 WLAN-Frequenzen 445
 WLAN-Hotspot 469
 WLAN-Konfiguration (Fritz!Box) 457
 WLAN-Netzwerkkarte 442
 WLAN-Netzwerkschlüssel 464
 WLAN-Router 444
 WLAN-Troubleshooting 471
 Wörterbuch-Angriff 510
 WPA 453, 465
 WPA2 453, 465
 WPA3 454, 465
 WPAN 439
 WPS 455, 458, 466
 WSUS 257, 521
 Würmer 507
 WWAN 440
 WWW 229

X

XML 237

Y

Yagi-Antenne 443
 YAML 238

Z

Zeitstempel 500
 ZeroConf 96
 Zero Day Exploit 517
 Zero-Trust 593
 Zertifikat (OpenVPN) 559
 Zertifikate 499
 Zertifizierungsstellen 504
 Zigbee 488
 Zone-ID (IPv6) 171
 Zonendatei (DNS) 223, 331
 Zugangsnetz (Mobilfunk) 476
 Zugriffskontrollen 516
 Zurechenbarkeit (Accountability) 500
 Z-Wave 489
 Zwei-Faktor-Authentifizierung (2FA) 499, 588
 Zwischenzertifizierungsstellen 504