

# HANSER



## Leseprobe

zu

## Technik der IP-Netze

von Anatol Badach und Erwin Hoffmann

Print-ISBN: 978-3-446-47371-3  
E-Book-ISBN: 978-3-446-47426-0

Weitere Informationen und Bestellungen unter  
<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446473713>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Inhaltsverzeichnis

<b>I</b>	<b>'Klassisches' IPv4/UDP/TCP</b>	<b>1</b>
<b>1</b>	<b>Grundlagen der IP-Netze</b>	<b>3</b>
1.1	Entwicklung des Internet . . . . .	4
1.1.1	Internet vor der Nutzung des WWW . . . . .	4
1.1.2	Die Schaffung des WWW . . . . .	6
1.1.3	Internet nach der Etablierung des WWW . . . . .	9
1.1.4	Meilensteine der Internet-Entwicklung und Trends . . . . .	10
1.2	Funktionen der Kommunikationsprotokolle . . . . .	17
1.2.1	Prinzipien der Fehlerkontrolle . . . . .	18
1.2.2	Realisierung der Flusskontrolle . . . . .	20
1.2.3	Überlastkontrolle . . . . .	22
1.3	Schichtenmodell der Kommunikation . . . . .	23
1.3.1	Konzept des OSI-Referenzmodells . . . . .	24
1.3.2	Schichtenmodell der Protokollfamilie TCP/IP . . . . .	27
1.4	Allgemeine Prinzipien der IP-Kommunikation . . . . .	29
1.4.1	Bildung von IP-Paketen . . . . .	30
1.4.2	Netzwerkschicht in IP-Netzen . . . . .	31
1.4.3	Verbindungslose IP-Kommunikation im Internet . . . . .	33
1.4.4	Transportschicht in IP-Netzen . . . . .	34
1.4.5	Multiplexmodell der Protokollfamilie TCP/IP . . . . .	37
1.5	Komponenten der Protokollfamilie TCP/IP . . . . .	38
1.5.1	Protokolle der Netzwerkschicht . . . . .	38
1.5.2	Protokolle der Transportschicht . . . . .	39
1.5.3	Protokolle der Supportschicht und für Echtzeitkommunikation . . . . .	40
1.5.4	Komponenten der Anwendungsschicht . . . . .	42
1.6	IETF und Internet-Standards . . . . .	44
1.7	Schlussbemerkungen . . . . .	46
1.8	Verständnisfragen . . . . .	48
<b>2</b>	<b>Sicherheit in der IP-Kommunikation</b>	<b>49</b>
2.1	Grundlagen und Entwicklung der IT-Sicherheit . . . . .	50
2.1.1	Daten und ihre Nutzung . . . . .	51
2.1.2	Rolle der IT-Security . . . . .	53
2.1.3	Akteure und Identitäten bei der Datenverarbeitung . . . . .	55
2.1.4	Entwicklung der Internet-Kryptographie . . . . .	58
2.1.5	Schichtenspezifische IT-Security-Protokolle . . . . .	60
2.2	Prinzipien und Primitive der Kryptographie . . . . .	62
2.2.1	Verschlüsselungs-Primitiv $C$ . . . . .	63
2.2.2	Schlüsseltausch-Primitiv $\kappa$ . . . . .	63
2.2.3	Hash-Primitiv $h$ . . . . .	65
2.2.4	Signatur-Primitiv $\sigma$ . . . . .	67
2.2.5	Zusammenspiel der Krypto-Primitive . . . . .	68

2.3	Hashfunktionen und ihr Einsatz	70
2.3.1	Hashfunktionen zur Nachrichtensicherung	70
2.3.2	Message Authentication Codes	71
2.3.3	Hashfunktionen für Passwörter	73
2.4	Symmetrische Verschlüsselung	75
2.4.1	Stromchiffren	77
2.4.2	Blockchiffren	79
2.4.3	Klassische Betriebsarten	80
2.4.4	Counter Mode und AEAD	82
2.5	Schlüsseltauschverfahren	84
2.5.1	Ablauf des RSA-Schlüsseltauschs	86
2.5.2	Ablauf des DH-Verfahrens	87
2.5.3	ElGamal-Schlüsseltausch-Protokoll	89
2.6	Kryptographie auf Elliptischen Kurven	90
2.6.1	Schlüsseltausch mit ECC	92
2.6.2	Digitale Signaturen mit ECC	93
2.7	Identitäten und Authentisierung	97
2.7.1	Authentisierung mit MS-ChapV2	99
2.7.2	Digitale Identitäten mit X.509-Zertifikaten	101
2.7.3	Der X.509-Datencontainer	102
2.7.4	X.509-Einsatzgebiete	103
2.7.5	Öffentliche und private Zertifikate	105
2.7.6	Verifikation und Validierung von Zertifikaten	106
2.8	Gesicherte und vertrauliche Datenübertragung	108
2.9	Schlussbemerkungen	113
2.10	Verständnisfragen	114
<b>3</b>	<b>Internet-Netzwerkprotokolle IPv4, ARP, ICMP und IGMP</b>	<b>115</b>
3.1	Aufgaben von IPv4	116
3.2	Aufbau von IPv4-Paketen	117
3.2.1	Differentiated Services	119
3.2.2	Fragmentierung der IPv4-Pakete	122
3.2.3	Optionen in IP-Paketen	124
3.3	IPv4-Adressen	127
3.3.1	Darstellung von IP-Adressen	129
3.3.2	Standard-Subnetzmaske	130
3.3.3	Vergabe von IP-Adressen	131
3.4	Bildung von Subnetzen	134
3.4.1	Bestimmen von Subnetz-IDs und Host-IDs	135
3.4.2	Zielbestimmung eines IP-Pakets beim Quellrechner	138
3.4.3	Adressierungsaspekte in IP-Netzen	139
3.5	Klassenlose IP-Adressierung (VLSM, CIDR)	142
3.5.1	Konzept der klassenlosen IP-Adressierung	143
3.5.2	VLSM-Nutzung	147
3.5.3	CIDR-Einsatz	151

3.6	Protokolle ARP und RARP	155
3.6.1	Protokoll ARP	156
3.6.2	Proxy-ARP	159
3.6.3	Protokoll RARP	162
3.7	Protokoll ICMP	163
3.7.1	ICMP-Nachrichten	164
3.7.2	ICMP-Fehlermeldungen	165
3.7.3	ICMP-Anfragen	167
3.7.4	Pfad-MTU Ermittlung	168
3.8	IP-Multicasting	169
3.8.1	Multicast-Adressen	170
3.8.2	Internet Group Management Protocol	171
3.9	Schlussbemerkungen	175
3.10	Verständnisfragen	178
<b>4</b>	<b>Transportprotokolle TCP, UDP, SCTP und QUIC</b>	<b>179</b>
4.1	Grundlagen der Transportprotokolle	180
4.2	Konzept und Einsatz von UDP	182
4.2.1	Aufbau von UDP-Paketen	183
4.2.2	Protokoll UDP-Lite	184
4.3	Funktion des Protokolls TCP	186
4.3.1	Aufbau von TCP-Paketen	187
4.3.2	Konzept der TCP-Verbindungen	191
4.3.3	Auf- und Abbau von TCP-Verbindungen	192
4.3.4	Flusskontrolle bei TCP	195
4.3.5	TCP Sliding-Window-Prinzip	197
4.4	Implementierungsaspekte von TCP	201
4.4.1	Klassische TCP-Implementierungen	201
4.4.2	Abschätzung der Round Trip Time	203
4.4.3	Verbesserung der Effizienz von TCP	204
4.4.4	Datendurchsatz beim TCP	206
4.4.5	TCP Socket-Interface	209
4.4.6	Angriffe gegen den TCP-Stack	211
4.4.7	Socket Cloning und TCP-Handoff	213
4.4.8	MSS Clamping	213
4.5	Explicit Congestion Notification	214
4.5.1	Anforderungen an ECN-fähige Netzknoten	215
4.5.2	Überlastkontrolle mit ECN	216
4.5.3	Signalisierung von ECN in IP- und TCP-Headern	218
4.5.4	Ablauf des ECN-Verfahrens	220
4.6	Multipath TCP	223
4.6.1	Typischer Einsatz von MPTCP	224
4.6.2	Transportschicht mit MPTCP	226
4.6.3	Multipath-Kommunikation mit MPTCP	229
4.6.4	MPTCP-Angaben im TCP-Header	233
4.6.5	Aufbau einer MPTCP-Verbindung	235

4.6.6	Anpassung des TCP-Headers für MPTCP	237
4.6.7	Abbau einer MPTCP-Verbindung	238
4.6.8	Middleboxen als Störfaktoren bei MPTCP	239
4.7	Konzept und Einsatz von SCTP	240
4.7.1	SCTP versus UDP und TCP	241
4.7.2	SCTP-Assoziationen	241
4.7.3	Struktur der SCTP-Pakete	243
4.7.4	Aufbau und Abbau einer SCTP-Assoziation	244
4.7.5	Daten- und Nachrichtenübermittlung nach SCTP	245
4.8	Das QUIC-Protokoll	249
4.8.1	Ziele von QUIC	250
4.8.2	QUIC-Pakete in UDP und Transport über IP-Netze	251
4.8.3	Aufbau von QUIC-Nachrichten und der Payload	252
4.8.4	QUIC-Verbindungen und Datenströme	256
4.8.5	Verbindungsmanagement bei QUIC	259
4.9	Schlussbemerkungen	261
4.10	Verständnisfragen	262
<b>5</b>	<b>Domain Name System (DNS)</b>	<b>263</b>
5.1	Aufgaben des DNS	264
5.1.1	Namen als Schlüssel zu Internet-Ressourcen	265
5.1.2	Organisation des DNS-Namensraums	266
5.1.3	Internet Root-Server	269
5.1.4	Architektur und Komponenten des DNS-Dienstes	270
5.1.5	Abfrage von IP-Adressen	273
5.1.6	Ermittlung des FQDN für eine IP-Adresse	275
5.1.7	Direkte Abfrage von Resource Records	277
5.2	Resource Records	277
5.2.1	Taxonomie der Resource Records	279
5.2.2	Resource Records für IPv6	281
5.2.3	Internationalisierung des DNS (IDN)	283
5.3	Zonen und Zonentransfer	284
5.3.1	Zonendatei	285
5.3.2	Zonentransfer	287
5.4	DNS-Nachrichten	289
5.4.1	DNS-Nachrichtenformate	289
5.4.2	DNS-Nachrichten mit EDNS(0)	292
5.5	DNS Security mit DNSSEC	294
5.5.1	Typische Bedrohungen bei DNS	295
5.5.2	Sicherung des Zonentransfers	296
5.5.3	Konzept von DNSSEC	297
5.5.4	Funktionale DNS-Erweiterung bei DNSSEC	299
5.5.5	Ablauf des DNSSEC-Verfahrens	300
5.6	Vertrauliche DNS-Nachrichten mit CurveDNS	305
5.6.1	Kryptographisches Konzept von CurveDNS	307
5.6.2	CurveDNS-Nachrichtenformate	308

5.7	DNS und Internetdienste	311
5.7.1	DNS und E-Mail nach SMTP	311
5.7.2	DNS und die ENUM-Domain	313
5.7.3	DNS und VoIP mit SIP	315
5.8	Autoritative Records in der DNS-Zone	317
5.8.1	DNS-Based Authentication of Named Entities: DANE	318
5.8.2	DomainKeys Identified Mail Signatures	321
5.8.3	Certification Authority Authorization	324
5.9	Internetanbindung und DNS	325
5.9.1	Domain Name Registrare	328
5.9.2	Dynamisches DNS	329
5.10	Multicast-DNS-Dienste	330
5.10.1	Multicast-DNS	331
5.10.2	Dienstleistungsprotokolle LLMNR und UPnP	334
5.11	Schlussbemerkungen	336
5.12	Verständnisfragen	338
<b>6</b>	<b>IP-Support-Protokolle</b>	<b>339</b>
6.1	IPv4-Autoconfiguration	340
6.1.1	Einrichten von IP-Adressen	342
6.1.2	Stateless Autoconfiguration für IPv4 – APIPA	342
6.2	Vergabe von IP-Adressen mit DHCP	344
6.2.1	Aufbau von DHCP-Nachrichten	346
6.2.2	Ablauf beim Protokoll DHCP	347
6.2.3	Aufgabe von DHCP-Relay-Agents	350
6.2.4	DHCP im Einsatz	351
6.2.5	DHCP und PXE	352
6.3	Network Address Translation (NAT)	352
6.3.1	Klassisches NAT	353
6.3.2	Konzept von NAT	355
6.3.3	Prinzip von Full Cone NAT	356
6.3.4	Prinzip von Restricted Cone NAT	357
6.3.5	NAT und Echtzeitkommunikationsprotokolle	358
6.3.6	Session Traversal bei NAT	360
6.3.7	Carrier-Grade NAT	365
6.4	IP Security Protocol (IPsec)	367
6.4.1	Ziele von IPsec	367
6.4.2	Erweiterung der IP-Pakete mit IPsec-Angaben	369
6.4.3	Aufbau einer IPsec-Sicherheitsvereinbarung	370
6.4.4	IPsec im Authentication Mode	375
6.4.5	Encapsulating Security Payload (ESP)	376
6.4.6	IPsec-basierte Virtuelle Private Netze	378
6.4.7	NAT-Traversal bei IPsec	382
6.5	Extensible Authentication Protocol	383
6.5.1	EAP-Funktionskomponenten	384
6.5.2	EAP-Nachrichten	386

6.5.3	Ablauf der EAP-Authentisierung	387
6.6	Einsatz des Protokolls RADIUS	390
6.6.1	Remote Access Services und RADIUS	390
6.6.2	Konzept von RADIUS	392
6.6.3	RADIUS-Nachrichten	395
6.7	Lightweight Directory Access Protocol	397
6.7.1	Directory Information Tree	398
6.7.2	LDAP-Server	400
6.7.3	LDAP-Client-Zugriff	401
6.8	Schlussbemerkungen	403
6.9	Verständnisfragen	405
<b>7</b>	<b>Protokolle der Supportschiicht und für Echtzeitkommunikation</b>	<b>407</b>
7.1	Konzept und Einsatz von SOCKS	408
7.1.1	SOCKS-Ablauf	409
7.1.2	Gesicherte Verbindungen mit SOCKS	411
7.2	Transport Layer Security (TLS)	412
7.2.1	TLS-Dienste im Schichtenmodell	415
7.2.2	Ablauf des TLS-Verfahrens – bis TLS 1.2	416
7.2.3	Ablauf der Verbindungsaufnahme bei TLS 1.3	418
7.2.4	Record Layer Protocol	422
7.2.5	Cipher Suites	424
7.2.6	Erzeugung der TLS-Schlüssel	425
7.2.7	Verzögerte TLS-Verbindung mittels STARTTLS	428
7.2.8	Datagram TLS	429
7.3	Protokolle für die Echtzeitkommunikation	431
7.3.1	RTP/RTCP und Transportprotokolle in IP-Netzen	432
7.3.2	Real-time Transport Protocol (RTP)	434
7.3.3	Das Protokoll RTCP im Überblick	445
7.4	Das Protokoll SIP	449
7.4.1	SIP und Transportprotokolle	449
7.4.2	Eigenschaften des Protokolls SDP	451
7.4.3	Aufbau von SIP-Adressen	452
7.4.4	Funktion eines SIP-Proxy bei der IP-Videotelefonie	453
7.4.5	Trapezoid-Modell von SIP	454
7.4.6	Unterstützung der Benutzermobilität bei SIP	456
7.4.7	Beschreibung von Sessions mittels SDP	459
7.5	Zeitprotokolle und Zeitsynchronisation	462
7.5.1	Von Kalendern, Uhren und Zeitzonen	463
7.5.2	Temps Atomic International	466
7.5.3	Network Time Protocol	467
7.5.4	Precision Time Protocol	474
7.6	Schlussbemerkungen	481
7.7	Verständnisfragen	483

<b>II</b>	<b>Internet Protocol Version 6</b>	<b>485</b>
<b>8</b>	<b>Das Protokoll IPv6</b>	<b>487</b>
8.1	Neuerungen bei IPv6 gegenüber IPv4	488
8.2	Header-Struktur bei IPv6	490
8.3	Erweiterungs-Header	492
8.4	IPv6-Flexibilität mit Options-Headern	495
8.4.1	Aufbau von Options-Headern	496
8.4.2	Belegung des Option-Feldes	497
8.5	Einsatz von Jumbo Payload	498
8.6	Source Routing bei IPv6	499
8.7	Fragmentierung langer IPv6-Pakete	501
8.8	Aufbau von IPv6-Adressen	502
8.8.1	Darstellung von IPv6-Adressen	503
8.8.2	IPv6-Adressensystematik und -Gültigkeitsbereiche	506
8.8.3	Interface-Identifer in IPv6-Adressen	507
8.8.4	Interface-Index bei Link-Local IPv6-Adressen	509
8.9	Unicast-Adressen bei IPv6	510
8.9.1	Globale Unicast-Adressen	511
8.9.2	Vergabe globaler IPv6-Adressen	514
8.9.3	Unicast-Adressen von lokaler Bedeutung	515
8.9.4	IPv4-Kompatibilitätsadressen	516
8.10	Multicast- und Anycast-Adressen bei IPv6	518
8.10.1	Automatische Multicast-Adressen	520
8.10.2	Anycast-Adressen	522
8.11	Zuweisung von IPv6-Unicast-Adressen	523
8.11.1	Privacy Extensions	524
8.11.2	Auswahl der 'richtigen' IPv6-Quelladresse	526
8.12	Schlussbemerkungen	527
8.13	Verständnisfragen	528
<b>9</b>	<b>IPv6-Support-Protokolle ICMPv6, NDP und DHCPv6</b>	<b>529</b>
9.1	Nachrichten des Protokolls ICMPv6	530
9.2	Das Neighbor Discovery Protokoll	532
9.2.1	Bestimmen des Ziels eines IPv6-Pakets	535
9.2.2	Ermittlung von Linkadressen	537
9.2.3	Router Advertisement/Solicitation	539
9.2.4	Unsolicited Router Advertisements	541
9.2.5	IPv6-Paket-Umleitung	542
9.3	Stateless Address Autoconfiguration (SLAAC)	543
9.3.1	SLAAC und Router Advertisements	545
9.3.2	SeND – Secure Neighbor Discovery	546
9.4	Konzept und Einsatz von DHCPv6	549
9.4.1	Client/Relay/Server-Architektur bei DHCPv6	550
9.4.2	Aufbau von DHCPv6-Nachrichten	552
9.4.3	Ablauf von DHCPv6 im stateful Mode	554



9.4.4	Verlängerung der Ausleihe einer IPv6-Adresse . . . . .	556
9.4.5	Schnelle Umadressierung mit DHCPv6 . . . . .	557
9.4.6	Ablauf von DHCPv6 im stateless Mode . . . . .	558
9.4.7	Einsatz von DHCPv6-Relays . . . . .	559
9.5	Schlussbemerkungen . . . . .	561
9.6	Verständnisfragen . . . . .	562
<b>10</b>	<b>Migration zum IPv6-Einsatz</b>	<b>563</b>
10.1	Arten der Koexistenz von IPv6 und IPv4 . . . . .	564
10.1.1	IPv6-Kommunikation über IPv4-Netze . . . . .	568
10.1.2	IPv4-Kommunikation über IPv6-Netze . . . . .	570
10.1.3	IP-Kommunikation durch Translation IPv4 ↔ IPv6 . . . . .	570
10.2	Dual-Stack-Verfahren . . . . .	571
10.2.1	Dual-Stack-Rechner in einem LAN-Segment . . . . .	571
10.2.2	Betrieb von Dual-Stack-Rechnern in IPv4-Netzen . . . . .	571
10.2.3	Dual-Stack Lite . . . . .	572
10.3	Tunneling-Protokolle: IPv6 über X . . . . .	574
10.3.1	Erweiterung eines IPv4-Netzes um ein IPv6-Netz . . . . .	574
10.3.2	Kopplung der IPv6-Netze über ein IPv4-Netz . . . . .	576
10.3.3	Zugang zum IPv6-Internet über Tunnel-Broker . . . . .	576
10.4	Von 6to4 nach 6rd . . . . .	578
10.4.1	Bedeutung von 6to4 . . . . .	578
10.4.2	Aufbau von 6to4-Adressen . . . . .	578
10.4.3	IPv6-Kommunikation über IPv4-Netz . . . . .	579
10.4.4	Probleme bei 6to4 mit NAT . . . . .	581
10.4.5	IPv6 Rapid Deployment – 6rd . . . . .	582
10.5	IPv6 over IPv4 mit ISATAP . . . . .	584
10.5.1	Kommunikation mit ISATAP . . . . .	584
10.5.2	Struktur und Bedeutung von ISATAP-Adressen . . . . .	585
10.5.3	Funktionsweise von ISATAP . . . . .	587
10.6	IPv6 in IPv4-Netzen mit NAT (Teredo) . . . . .	589
10.6.1	Teredo-Adresse und -Pakete . . . . .	590
10.6.2	Bestimmung der Art von NAT . . . . .	593
10.7	Protokoll-Translation: IPv4 ↔ IPv6 . . . . .	595
10.7.1	Stateless IPv4/IPv4 Translation (SIIT) . . . . .	596
10.7.2	Adressierung bei SIIT . . . . .	596
10.7.3	Translation IPv4 ↔ IPv6 . . . . .	598
10.7.4	Translation ICMPv4 ↔ ICMPv6 . . . . .	601
10.8	NAT64 und DNS64 . . . . .	602
10.8.1	NAT64-Arbeitsmodell . . . . .	603
10.8.2	NAT64-IPv6-Adressen . . . . .	604
10.8.3	NAT64 Stateful Translation . . . . .	605
10.8.4	DNS-Integration bei NAT64 . . . . .	606
10.9	Schlussbemerkungen . . . . .	607
10.10	Verständnisfragen . . . . .	608

<b>III Internet-Routing-Architektur</b>	<b>609</b>
<b>11 Routing in IP-Netzen</b>	<b>611</b>
11.1 Routing-Grundlagen	612
11.1.1 Grundlegende Aufgaben von Routern	612
11.1.2 Adressierung beim Router-Einsatz	614
11.1.3 Routing-Tabelle	617
11.1.4 Routing-Verfahren	620
11.1.5 Inter-/Intra-Domain-Protokolle	624
11.2 Routing Information Protocol (RIP)	624
11.2.1 Erlernen von Routing-Tabellen beim RIP	625
11.2.2 Besonderheiten des RIP-1	631
11.2.3 Routing-Protokoll RIP-2	635
11.2.4 RIP für das Protokoll IPv6 (RIPng)	638
11.3 Open Shortest Path First (OSPF)	640
11.3.1 Funktionsweise von OSPF	640
11.3.2 Nachbarschaften zwischen Routern	643
11.3.3 OSPF-Einsatz in großen Netzwerken	647
11.3.4 OSPF-Nachrichten	654
11.3.5 Besonderheiten von OSPFv2	661
11.3.6 OSPF für IPv6 (OSPFv3)	661
11.4 Border Gateway Protocol (BGP-4)	662
11.4.1 Grundlagen des BGP-4	662
11.4.2 Funktionsweise des BGP-4	664
11.4.3 BGP-4-Nachrichten	664
11.4.4 Multiprotocol Extensions for BGP-4 (MP-BGP)	670
11.4.5 Sicherung des BGP-Nachrichtenaustauschs	674
11.4.6 BGP Blackholing	678
11.5 Redundante Auslegung von Routern	679
11.5.1 Konzept des virtuellen Routers	679
11.5.2 Funktionsweise von VRRP	682
11.5.3 Idee und Einsatz des HSRP	685
11.6 Multicast Routing-Protokolle	688
11.6.1 Einige Aspekte von MC-Routing	689
11.6.2 Aufgaben von MC-Routing	691
11.6.3 Intra-Domain-MC-Routing mit PIM-SM	695
11.6.4 Inter-Domain-MC-Routing mit MSDP	701
11.7 Schlussbemerkungen	705
11.8 Verständnisfragen	708
<b>12 Verbindungsorientierte IP-Netze mit MPLS und GMPLS</b>	<b>709</b>
12.1 Weg zu neuer Generation der IP-Netze	710
12.1.1 Notwendigkeit von (G)MPLS	710
12.1.2 Bedeutung von Traffic Engineering in IP-Netzen	711
12.1.3 Multiplane-Architekturen moderner IP-Netze	713
12.1.4 Schritte zu einem Label Switched Path (LSP)	714

12.2	Multi-Protocol Label Switching (MPLS)	715
12.2.1	Multiplane-Architektur der MPLS-Netze	716
12.2.2	MPLS als Integration von Routing und Switching	717
12.2.3	Logisches Modell des MPLS	718
12.2.4	Prinzip des Label-Switching	720
12.2.5	Logische Struktur der MPLS-Netze	721
12.2.6	Bildung der Klassen von IP-Paketen und MPLS-Einsatz	722
12.2.7	MPLS und die Hierarchie von Netzen	724
12.2.8	MPLS und verschiedene Übermittlungsnetze	726
12.2.9	Virtual Private Networks mit MPLS	727
12.3	Konzept von GMPLS	728
12.3.1	Vom MPLS über MPAS zum GMPLS	729
12.3.2	Struktur optischer Switches bei GMPLS	730
12.3.3	Interpretation der Label	731
12.3.4	Interpretation des Transportpfads	732
12.3.5	Bedeutung des LMP in GMPLS-Netzen	733
12.4	Traffic Engineering in (G)MPLS-Netzen	736
12.4.1	Traffic Trunks und LSPs	736
12.4.2	Aufgaben und Schritte beim MPLS-TE	738
12.4.3	Routing beim Traffic Engineering	739
12.4.4	Attribute von Traffic Trunks	739
12.4.5	Constraint-based Routing	741
12.4.6	Re-Routing und Preemption	743
12.5	Signalisierung in (G)MPLS-Netzen	743
12.5.1	Einsatz des RSVP-TE	744
12.5.2	Einsatz des GMPLS RSVP-TE	749
12.5.3	Einsatz des CR-LDP	751
12.6	Schlussbemerkungen	754
12.7	Verständnisfragen	755

## IV Virtuelle Netzstrukturen 757

<b>13</b>	<b>IP over X und virtuelle IP-Netze</b>	<b>759</b>
13.1	IP über LANs	760
13.1.1	Übermittlung der IP-Pakete in MAC-Frames	762
13.1.2	Multiprotokollfähigkeit der LANs	763
13.2	Punkt-zu-Punkt-Verbindungen mit PPP	765
13.2.1	PPP-Dateneinheiten	766
13.2.2	PPP-Zustände	768
13.2.3	LCP als Hilfsprotokoll von PPP	769
13.2.4	IPv4 Control Protocol (IPCP) bei PPP	770
13.2.5	Protokollablauf beim PPP	771
13.2.6	Benutzerauthentisierung beim PPP	772
13.3	Grundlagen der WLAN	773
13.3.1	WLAN-Betriebsarten	775

13.3.2	Beitritt zum WLAN	776
13.3.3	WLAN MAC-Frame: MSDU	777
13.3.4	Kommunikation zwischen WLAN und Ethernet	781
13.3.5	Robust Security Network	782
13.4	Virtual Private Networks (VPN)	783
13.4.1	Tunneling als Basis für VPNs	784
13.4.2	VPN-Taxonomie	786
13.4.3	Von Providern bereitgestellte VPNs	788
13.4.4	Layer-2-Tunneling über IP-Netze	799
13.5	Schlussbemerkungen	804
13.6	Verständnisfragen	806
<b>14</b>	<b>IP-Netzwerke und Virtual Networking</b>	<b>807</b>
14.1	Moderne Netzstrukturen	808
14.1.1	Funktionsbereiche in Netzwerken	808
14.1.2	Strukturierter Aufbau von Netzwerken	809
14.2	Virtual Networking in LANs	811
14.2.1	Arten und Einsatz von VLANs	811
14.2.2	Layer-2-Switching	812
14.2.3	Layer-3-Switching	814
14.2.4	Bedeutung von VLAN Tagging	816
14.3	Bildung von VLANs im Client-LAN	819
14.3.1	Intra- und Inter-VLAN-Kommunikation	819
14.3.2	Modell der Bildung von VLANs im Client-LAN	821
14.4	Bildung von VLANs im Server-LAN	822
14.4.1	Multilayer-Struktur im Server-LAN	822
14.4.2	Anbindung virtueller Server an Access Switches	823
14.4.3	Modelle der Bildung von VLANs im Server-LAN	824
14.5	Abgesicherte VPNs mit MACsec	826
14.5.1	MACsec-Schlüsselhierarchien	828
14.5.2	Trusted MAC Frame Format	830
14.5.3	MACsec-Implementierungsaspekte	832
14.5.4	MACsec Key Agreement Protocol & Security Association	834
14.6	Virtual Networking mit TRILL und SPB	835
14.6.1	Konzept und Bedeutung von TRILL	836
14.6.2	Idee und Einsatz von Shortest Path Bridging	838
14.7	VXLAN – VLAN mit VM	844
14.7.1	Vom VLAN zum VXLAN	845
14.7.2	VXLANs oberhalb Layer-3-Netzwerke	846
14.8	Mobilität von Virtual Networks	848
14.8.1	Konzept und Bedeutung von ILNP	849
14.8.2	LISP – Idee und Bedeutung	858
14.9	Schlussbemerkungen	864
14.10	Verständnisfragen	868

<b>15 Distributed Layer-2/3-Switching</b>	<b>869</b>
15.1 Genesis der Idee von VPLS und EVPN	870
15.2 Konzept und Einsatz von VPLS	873
15.2.1 Grundlegende Idee von VPLS	873
15.2.2 Ethernet over MPLS	875
15.2.3 VPLS als Vollvermaschung von VSIs	877
15.2.4 Grundlegende Funktionen von VSIs	878
15.2.5 VPLS-Modell für die Vernetzung von VSIs	879
15.2.6 Information in PEs über bereitgestellte VPLSs	881
15.2.7 PE Forwarding Table – Learning und Forwarding	882
15.2.8 Learning von MAC-Adressen aus Broadcast-Frames	884
15.2.9 Learning von MAC-Adressen aus Unicast-Frames	885
15.2.10 Skalierbarkeit von VPLSs	886
15.2.11 Auto-Discovery and VPLS Signaling	887
15.2.12 Bekanntgabe von Informationen über PW Labels	888
15.2.13 Hierarchical VPLS (H-VPLS) – Multi-Tenant-VPLS	889
15.2.14 H-VPLS und VLAN-Stacking	890
15.3 Ethernet Virtual Private Networks	891
15.3.1 Grundlegende Architektur von EVPN	892
15.3.2 Datacenter und grundlegende EVPN-Topologie	894
15.3.3 Allgemeines EVPN-Konzept im Überblick	897
15.3.4 EVI als emulierter L2-Switch – Basisfunktionen	899
15.3.5 EVIs als emulierter L2-Switch – spezielle Funktionen	900
15.3.6 EVI als emulierter L3-Switch – Basisfunktionen	902
15.3.7 Arten von EVI Service Interfaces	904
15.3.8 Control Plane in EVPNs	906
15.4 Schlussbemerkungen	907
15.5 Verständnisfragen	908
<b>V Mobilität und Internet of Things</b>	<b>909</b>
<b>16 Unterstützung der Mobilität in IP-Netzen</b>	<b>911</b>
16.1 Ansätze zur Unterstützung der Mobilität	912
16.1.1 Bedeutung von WLAN- und Hotspot-Roaming	912
16.1.2 Hauptproblem der Mobilität in IP-Netzen	914
16.1.3 Die grundlegende Idee des Mobile IP	915
16.1.4 Idee des Mobile IPv4	916
16.1.5 Idee des Mobile IPv6	918
16.2 Roaming zwischen Hotspots	918
16.2.1 Hotspot-Roaming zwischen mehreren WISPs	919
16.2.2 Ablauf des Hotspot-Roaming	920
16.3 Funktionsweise des MIPv4	921
16.3.1 Beispiel für einen Ablauf des MIP	922
16.3.2 Agent Discovery	924
16.3.3 Erkennen des Verlassens des Heimatsubnetzes	925

16.3.4	Erkennen des Wechsels eines Fremdsubnetzes	926
16.3.5	Erkennen einer Rückkehr in das Heimatsubnetz	928
16.3.6	Registrierung beim Heimatagenten	928
16.3.7	Mobiles IP-Routing	933
16.4	Konzept des MIPv6	936
16.4.1	MN hat sein Heimatsubnetz verlassen	936
16.4.2	MN hat das Fremdsubnetz gewechselt	938
16.4.3	MN ist in sein Heimatsubnetz zurückgekehrt	939
16.4.4	MIPv6-Nachrichten	940
16.4.5	Kommunikation zwischen MN und CN	941
16.4.6	Home Agent Binding	943
16.4.7	Correspondent Node Binding	944
16.4.8	Entdeckung eines Subnetzwechsels	944
16.4.9	Entdeckung der Home-Agent-Adresse	945
16.5	Hierarchical MIPv6	946
16.5.1	Unterstützung der Mobilität mit dem HMIPv6	946
16.5.2	Finden eines MAP	948
16.5.3	Unterstützung der Mikromobilität	949
16.5.4	Unterstützung der Makromobilität	950
16.5.5	Datentransfer zwischen MN und CN	951
16.6	Schlussbemerkungen	953
16.7	Verständnisfragen	956
<b>17</b>	<b>Internet of Things – Technische Grundlagen und Protokolle</b>	<b>957</b>
17.1	Herkömmliches Internet und IoT	958
17.1.1	Allgemeine Definition von IoT	958
17.1.2	IoT aus funktionaler Sicht	960
17.1.3	Grundlegendes technisches Konzept von IoT	962
17.1.4	Cloud Computing und Fog Computing im IoT	964
17.1.5	Near Real-Time IoT Services mit Fog Computing	966
17.1.6	Funktionales Multilayer-Modell von IoT	968
17.1.7	Bedeutung von SDN im IoT	971
17.1.8	Protokollarchitektur von Devices im IoT	973
17.1.9	Protokollarchitektur von IoT Access Gateways	975
17.1.10	Struktur von MAC-Frames in Low Rate WPANs	976
17.2	6LoWPAN – IPv6-Adaption für das IoT	978
17.2.1	Grundlegende Topologien von LR-WPANs	979
17.2.2	Adressierung von Instanzen in Rechnern mit IPv6	980
17.2.3	Adressierung von Instanzen bei 6LoWPAN Devices	982
17.2.4	LoWPAN als IPv6-Adaptation-Layer-Struktur	984
17.2.5	Redundante Angaben im IPv6- und im UDP-Header	986
17.2.6	Dispatch Header und seine Nutzung bei 6LoWPAN	987
17.2.7	Komprimierung der IPv6- und UDP-Header	990
17.2.8	Multi-hop Communication in WPANs	992
17.2.9	Fragmentierung langer IPv6-Pakete in WPANs	994

17.3	RPL – Routing-Protokoll im IoT	997
17.3.1	Funktionales Modell von RPL	998
17.3.2	Hauptfunktion von RPL	999
17.3.3	RPL-Begriffe: Objective Function, Metric und Rank	1001
17.3.4	Logische Strukturierung von LLNs	1003
17.3.5	Besonderheiten von Routing mit RPL	1005
17.3.6	Traffic Patterns in LLNs	1007
17.3.7	Routing Metrics und Constraints	1009
17.3.8	Nutzung von Metric Container in Nachrichten DIO	1011
17.3.9	RPL-Nachrichten – Struktur und Typen	1013
17.3.10	Bildung von Virtual Root Nodes	1015
17.3.11	Nutzung der RPL-Nachricht DIO	1016
17.4	CoAP – Applikationsprotokoll im IoT	1019
17.4.1	CoAP im Protokollschichtenmodell von IoT	1019
17.4.2	Proxying zwischen HTTP und CoAP	1021
17.4.3	CoAP Messages und Timeout-Mechanismus	1024
17.4.4	Requests und Responses von CoAP	1026
17.4.5	Adressierung von Ressourcen bei CoAP	1029
17.4.6	Struktur und Typen von CoAP Messages	1031
17.4.7	Mapping zwischen HTTP und CoAP	1034
17.5	Schlussbemerkungen	1036
17.6	Verständnisfragen	1038
<b>18</b>	<b>Networking-Trends</b>	<b>1039</b>
18.1	Internet of Things (IoT)	1040
18.1.1	Industrial Internet of Things (IIoT)	1041
18.1.2	Internet of Robotic Things	1042
18.1.3	Internet of Vehicles	1043
18.1.4	Internet of Drones	1044
18.1.5	Mobility in IoT	1045
18.1.6	IoT Security	1045
18.2	Software-Defined Networking (SDN)	1047
18.2.1	Software-Defined WANs (SD-WANs)	1049
18.2.2	Software-Defined Optical Networking (SDON)	1050
18.2.3	Software-Defined Data Centers (SDDCs)	1051
18.2.4	Software-Defined IoT (SD-IoT)	1051
18.2.5	Wireless Software-Defined Networking	1052
18.2.6	Software-Defined Internet of Vehicles (SD-IoV)	1054
18.3	Network Function Virtualization (NFV)	1055
18.3.1	Software-Defined VNFs Networking	1056
18.3.2	Service Function Chaining (SFC)	1057
18.3.3	VNFs Management and Orchestration	1058
18.3.4	Network Slicing	1059
18.4	(Docker) Container Networking	1060
18.4.1	Container-based Network Services	1062
18.4.2	Cloud Computing Containerization	1062

18.4.3	Mobile VNFs Networking	1063
18.4.4	Containerized IoT Services	1064
18.5	Cloud Computing Services	1064
18.5.1	Infrastructure-as-a-Service (IaaS)	1065
18.5.2	Software-Defined Cloud Computing Networking	1066
18.5.3	Cloud-Native Microservices	1067
18.5.4	Mobile Cloud Computing in 5G	1068
18.6	Fog Computing und Artificial Intelligence	1069
18.6.1	Time-Sensitive IoT/5G Applications	1071
18.6.2	Intelligent IoT, Cognitive IoT	1072
18.6.3	Ambient Intelligence in IoT	1074
18.6.4	IoT Service Orchestration	1075
18.7	Next 5G und 6G (Generation) Mobile Networks	1076
18.7.1	5G-enabled Mobile IoT Applications	1077
18.7.2	Vehicle-to-Everything (V2X) Services	1078
18.7.3	SDN and NFV for 5G Mobile Networks	1079
18.7.4	5G Network Slicing	1080
18.7.5	5G Network Security	1082
18.7.6	6G als zukünftige Vision der Mobilfunknetze	1083
18.8	Information-Centric Networking and Services	1084
18.8.1	Software-Defined ICN (SD ICN)	1086
18.8.2	Information-Centric IoT (IC IoT)	1088
18.8.3	Information-Centric Services für Smart Cities	1090
18.8.4	ICN Security	1091
18.9	Time-Sensitive and Deterministic Networking	1092
18.9.1	Time-Sensitive Networking	1093
18.9.2	Deterministic Networking	1095
18.9.3	6TiSCH Wireless Industrial Networks	1096
18.9.4	Time-Sensitive SDN	1097
18.10	AI-based Networking	1099
18.10.1	AI-enabled SDN	1101
18.10.2	Data-Driven Networking	1101
18.10.3	Cognitive Networks	1103
18.10.4	Intent-based Networking	1104
18.10.5	Autonomic Networking	1105
18.10.6	AI, IoT and 5G Convergence	1106
18.11	Abschließende Bemerkungen	1107
18.11.1	Vom IoT zum Intelligent IoT	1108
18.11.2	Rückblick auf 50 Jahre Rechnerkommunikation	1109
	<b>Abkürzungsverzeichnis</b>	<b>1117</b>
	<b>Literaturverzeichnis</b>	<b>1129</b>
	<b>Stichwortverzeichnis</b>	<b>1137</b>





# Vorwort

Das Internet ist inzwischen zum unabdingbaren Kommunikationsmedium geworden, über das jeder zu jeder Zeit Information über fast alles abrufen sowie Nachrichten senden und empfangen kann. Unsere heutige Gesellschaft kann man sich ohne Internet kaum noch vorstellen. Voraussetzung zur Kommunikation zwischen Rechnern sind bestimmte Regeln, die vor allem die Datenformate und die Prinzipien der Datenübermittlung festlegen. Diese Regeln werden als Kommunikationsprotokolle bezeichnet. TCP/IP (*Transmission Control Protocol / Internet Protocol*) stellt eine derartige Protokollfamilie dar, sie wird im weltweiten Internet, in privaten Intranets und in anderen Netzen verwendet. Netze, die auf dieser Protokollfamilie aufbauen, bezeichnet man als *IP-Netze*.

Begriff: IP-Netze

Ein IP-Netz – und insbesondere das Internet – besteht nicht nur aus mehreren Rechnern und IP/TCP dazwischen, sondern dahinter verbergen sich sehr komplexe Vorgänge. Das Internet stellt einen weltweiten Dienst zur Übermittlung nicht nur von Daten, sondern auch von audiovisuellen Informationen, also von Audio und Video, in Form von IP-Paketen dar. Vergleicht man diesen Dienst mit dem Briefdienst der Post, so entspricht ein IP-Paket einem Brief und die sogenannte IP-Adresse einer postalischen Adresse. Das massive Wachstum des Internet und die dabei entstehenden Probleme und neuen Anforderungen haben die Entwicklung sowohl eines neuen Internetprotokolls, des IPv6, als auch von Techniken MPLS und GMPLS für die Übermittlung der IP-Pakete über Hochgeschwindigkeitsnetze, insbesondere über optische Netze, vorangetrieben. Noch in der ersten Dekade dieses Jahrhunderts hat man von *Next Generation IP Networks* gesprochen und sie sind bereits Realität geworden.

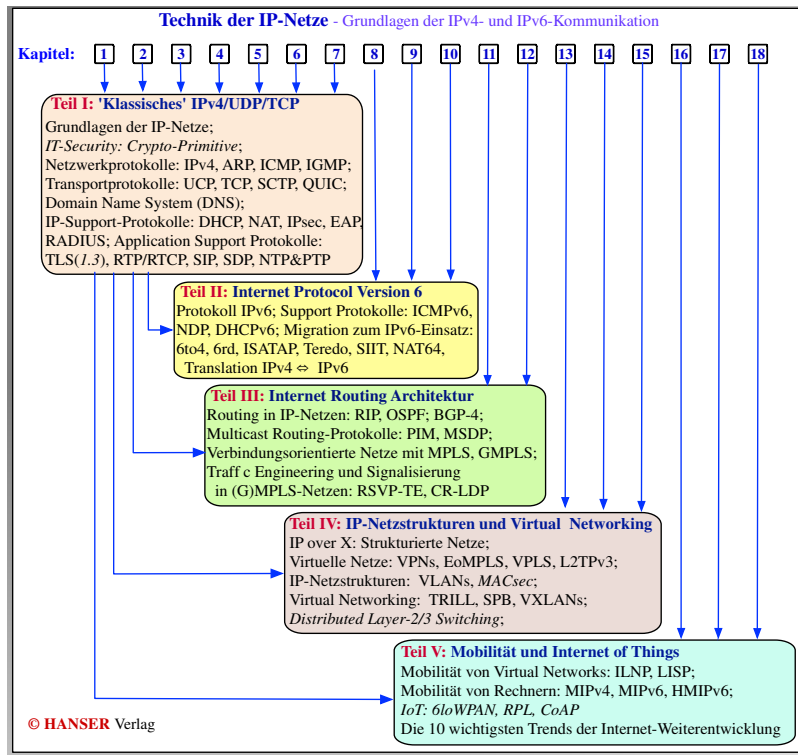
Komplexität und Weiterentwicklung

Dieses Buch gibt eine fundierte Darstellung zentraler Komponenten der TCP/IP-Protokollfamilie, wie z.B. IP, TCP, UDP, DNS und DHCP, sowie von Routing sowohl beim klassischen IP, IPv4 genannt, als auch beim IPv6. Das Buch erläutert die Strategien für die Migration zum Einsatz von IPv6, präsentiert die Konzepte zum Aufbau der IP-Netze auf Basis verschiedener Netztechnologien, wie LANs, WLANs, SDH und WDM, und geht auch auf die IP-Weitverkehrsnetze mit (G)MPLS ein. Die Themen wie die Realisierung von VPNs, *Virtual Networking* in LANs durch die Bildung von VLANs und VXLANs, Konzepte und Einsatz von TRILL und *Shortest Path Bridging* werden ebenso präsentiert. Die Darstellung der Protokolle MIPv4, MIPv6 und HMIPv6 zur Unterstützung der Mobilität von Rechnern wie auch der Protokolle ILNP und LISP, mit denen man die Mobilität virtueller Netzwerke erreichen kann, rundet den Inhalt dieses Buches ab.

Ziel des Buches

Das Buch ist so aufgebaut, dass sowohl die notwendigen technischen Grundlagen fundiert dargestellt als auch verschiedene Aspekte bei der Planung und Verwaltung der IP-Netze diskutiert werden. Damit eignet es sich nicht nur als Lehrbuch für Studenten und Neueinsteiger, sondern auch als Nachschlagewerk für alle Interessenten, die für die

An wen richtet sich das Buch?



Planung, Realisierung, Verwaltung und Nutzung des Internet, von privaten Intranets und anderen IP-Netzen verantwortlich sind.

#### Aufbau des Buches

Zurzeit ist kein Buch verfügbar, in dem die Technik der IP-Netze so breit dargestellt wäre. Daher kann dieses Buch als ein Handbuch für alle Netzwerk-Verantwortlichen dienen. Durch die fundierte und praxisorientierte Darstellung der Inhalte eignet sich gut dieses Buch auch für alle 'Internet-Fans' zum Selbststudium. Dieses Buch präsentiert in 17 Kapiteln, die auf fünf Teile verteilt sind, alle wichtigen Aspekte der IP-Netze und kann nicht wie ein spannender Roman in einem Schlag durchgelesen werden. Das vorliegende Bild zeigt dessen logische Struktur und Abhängigkeiten zwischen Inhalten einzelner Teile, um den Lesern eine Orientierung zu geben, aus welchen Teilen man Kenntnisse benötigt, um beim Lesen verschiedene, voneinander abhängige Themenbereiche besser zu verstehen.

#### Inhalte der Kapitel

Betrachtet man die einzelnen Kapitel dieses Buches etwas detaillierter, so lassen sie sich wie folgt kurz charakterisieren:

#### Kapitel 1

Kapitel 1 präsentiert die Entwicklung des Internet sowie die notwendigen Grundlagen der Rechnerkommunikation und der *Kommunikationsprotokolle* und geht u.a. daher auf die folgenden Probleme ein: Welche Funktionen liegen den Kommunikationsprotokollen zugrunde und wie kann die Kommunikation in IP-Netzen mittels eines Schichtenmodells anschaulich dargestellt werden? Wie können die verbindungslo-

se und die verbindungsorientierte Kommunikation in IP-Netzen interpretiert werden und welche Bedeutung hat die Transportschicht? Welche Sicherheitsziele werden in IP-Netzen verfolgt und wie können diese technisch umgesetzt werden? Wie koordiniert die IETF die technologische Entwicklung des Internet und wie können wir diese verfolgen?

Kapitel 2 führt den Leser in die Problematik der IT-Security ein: Netze sind *Vermittlungsnetze*, die Nachrichten *zuverlässig* und *unveränderlich* von A nach B transportieren sollen. Heute besteht der Bedarf aber auch darin, dass der Nachrichtentransport *vertraulich* erfolgt. Wie das zu bewerkstelligen ist, versucht Kapitel 2 zu vermitteln, indem vier Krypto-Primitive eingeführt und erklärt werden. Moderne Kryptographie (Pre-Quantum) kommt nicht ohne Elliptische Kurven aus, deren Bedeutung und Einsatz hier erläutert wird. Auch die Frage der Benutzer- und Rechnerauthentifizierung als 'Digitale Identitäten' mit und ohne *X.509 Zertifikate* wird beleuchtet. Kapitel 2

Kapitel 3 stellt sowohl IPv4 als auch dessen Hilfsprotokolle ARP und ICMP umfassend dar und erläutert u.a. folgende Fragestellungen: Wie sind IPv4-Pakete aufgebaut und welche Steuerungsangaben kann der Header eines IPv4-Pakets enthalten? Welche Arten von IPv4-Adressen gibt es und wie werden sie aufgebaut? Wie erfolgt die *Adressierung* in IP-Netzen und wie werden Subnetze gebildet? Welche Bedeutung haben die Protokolle ARP und ICMP und wie funktionieren sie? Wie realisiert man *Multicasting* in IP-Netzen mit dem Protokoll IGMP? Kapitel 3

Von großer Bedeutung in IP-Netzen ist die sogenannte *Transportschicht* mit den klassischen Protokollen TCP und UDP; hierzu kommen noch die neuen Protokolle SCTP und UDP-Lite. Weil das IP keine zuverlässige Übermittlung der Pakete garantiert, verwendet man hauptsächlich das TCP und in einigen Fällen das SCTP, um die zuverlässige Übermittlung der IP-Pakete zu gewährleisten. Kapitel 4 präsentiert die Aufgaben der Transportschicht. Diese können einfach gestaltet sein, wie bei UDP, das verbindungslos fungiert; aber auch komplex, wie bei TCP. Hier werden *Sessions* aufgebaut und unterhalten und sich um den Datenfluss gekümmert. Aufbauend hierauf wurde das Protokoll SCTP entwickelt. Einen anderen Ansatz stellt QUIC dar, das auf UDP aufsetzt, intern aber über umfangreiche Mechanismen zur Steuerung und vor allem Datenverschlüsselung entsprechend TLS verfügt. Deren prinzipielle Arbeitsweise wird hier dargestellt und speziell betrachtet: Wie funktioniert der gemeinsame Datenfluss über ggf. mehrere Übertragungsmedien? Kapitel 4

Die Rechner in IP-Netzen werden zwar durch ihre IP-Adressen lokalisiert, aber es ist sinnvoll, statt einer IP-Adresse einen Rechner über seinen Namen anzusprechen – wie es auch unter Menschen üblich ist. Dies ist mit dem *Domain Name System* (DNS) möglich. Kapitel 5 liefert eine fundierte Darstellung von DNS, geht auf verschiedene Möglichkeiten des DNS-Einsatzes ein und erörtert u.a. die folgenden Probleme: Wie funktioniert DNS und welche Aufgaben kann DNS wahrnehmen? Wie erfolgt die Ermittlung der IP-Adresse aufgrund des Hostnamens und umgekehrt? Welche Informationen als Resource Records enthält DNS und wie werden diese strukturiert? Welche Ziele werden mit ENUM, DynDNS und DNSSEC und DNSCurve verfolgt? Kapitel 5

Kapitel 6 stellt, als *IP-Support-Protokolle* bezeichnete, ergänzende Lösungen für das IPv4-Protokoll dar und erläutert hierbei u.a. die folgenden Aspekte: Wie können sich Kapitel 6

Rechner mittels DHCP automatisch eine gültige IPv4-Adresse zuweisen? Welche Lösungen für die Nutzung von privaten IPv4-Adressen mithilfe von NAT (*Network Address Translation*) gibt es und welche Probleme entstehen dabei – insbesondere bei der audiovisuellen Kommunikation? Wie kann *IPsec* zum verschlüsselten und authentisierten Austausch von IP-Paketen genutzt werden? Welche Probleme verursacht NAT bei IPsec und wie können diese bewältigt werden? Welche Probleme ergeben sich bei der Überprüfung von 'Digitalen Identitäten' unter Einsatz von EAP, RADIUS und LDAP?

#### Kapitel 7

Mehrere ergänzende Lösungen sind nicht nur für das IPv4 nötig, sondern in Form spezieller Protokolle auch für Applikationen, sodass wir von *Application Support Protokollen* sprechen. Kapitel 7 präsentiert diese, erläutert deren Aufgaben und geht u.a. auf folgende Fragestellungen ein: Wie kann der Datentransport zwischen Applikationen mittels TLS (1.3) gesichert realisiert werden und welche Voraussetzungen sind hierfür nötig? Welche Protokolle zur Realisierung der Echtzeitkommunikation in IP-Netzen benötigt werden, welche Aufgaben haben sie und wie werden sie konzipiert? Gerade diese Protokolle benötigen eine Zeitsynchronisation zwischen den Teilnehmern. Wie wird dies mittels NTP und PTP ermöglicht, und welche Zeitformate und -referenzen werden hierbei genutzt?

#### Kapitel 8

Um den steigenden Anforderungen an IP-Netze gerecht zu werden, wurde das IPv6 als '*IP der nächsten Generation*' entwickelt und die Ära von IPv6 hat bereits begonnen. IPv6 bringt neue Möglichkeiten und diese reichen von Sicherheitsfunktionen über mehr Flexibilität bis hin zur Unterstützung von neuartigen Anwendungen. Das IPv6 ermöglicht die automatische Konfiguration von Rechnern, sodass man sogar von *Plug&Play-Konfiguration* spricht. Kapitel 8 stellt das IPv6 ausführlich dar und geht u.a. auf die folgenden Probleme ein: Welche Ziele wurden bei der Entwicklung von IPv6 verfolgt? Welche neuen Funktionen bringt IPv6 mit sich? Welche Arten von IPv6-Adressen gibt es und wie können sie den Rechnern zugewiesen werden?

#### Kapitel 9

Ein wichtiges Ziel bei der Entwicklung von IPv6 war die Unterstützung der automatischen Konfiguration von Rechnern. Hierfür stehen die Protokolle ICMPv6, NDP und DHCPv6 zur Verfügung. Diese *IPv6 Support Protokolle* stellt Kapitel 9 dar und geht hierbei u.a. auf folgende Aspekte ein: Wie wurde ICMPv6 konzipiert und welche Aufgaben hat es? Welche Funktionen liefert NDP, um die automatische Konfiguration von Rechnern mit IPv6 zu unterstützen? Wie bekommt ein IPv6-Rechner seine Netzkonfiguration automatisch zugewiesen?

#### Kapitel 10

Da die Umstellung von allen Rechnern, in denen das klassische IPv4 verwendet wird, auf das IPv6 nicht auf einen Schlag geschehen kann, benötigt man geeignete Systemlösungen für die Migration zum IPv6-Einsatz. Kapitel 10 präsentiert verschiedene Ansätze und Systemlösungen für die Koexistenz von IPv4 und IPv6 – vor allem die Konzepte *IPv6 over IPv4* und *IPv4 over IPv6*. Die Integration der IPv4- und der IPv6-Netze dank der Translation  $IPv4 \leftrightarrow IPv6$  wird ebenso präsentiert. Hier werden u.a. folgende Probleme erörtert: Wie kann man sich die Koexistenz von IPv4 und IPv6 in einem Rechner vorstellen, wann ist diese Koexistenz möglich und welche Bedeutung hat sie? Wie kann die IPv6-Kommunikation über IPv4-Netze erfolgen? Wie lassen sich IPv6-Netzsegmente über IPv4-Netze verbinden? Wie können die Rechner aus

IPv6-Netzen auf das IPv4-Internet zugreifen? Wie erfolgt die Translation IPv4  $\leftrightarrow$  IPv6 und was ermöglicht sie?

Router fungieren in IP-Netzen als Knoten, ermitteln optimale Übermittlungswege, die sogenannten *Routen*, für die empfangenen IP-Pakete und leiten sie weiter. Kapitel 11 vermittelt eine kompakte Darstellung von Routing-Grundlagen und -Protokollen. Es werden hier die *Routing-Protokolle* RIP-1, RIP-2 und OSPF sowie BGP-4 erläutert. Dieses Kapitel zeigt auch, wie eine redundante Router-Auslegung mithilfe der Protokolle HSRP und VRRP erfolgen kann, und stellt die Protokolle PIM-SM und MSDP für das *Multicast-Routing* dar. Hierbei werden u.a. folgende Fragen beantwortet: Welche Aufgabe haben die Router und wie funktionieren sie? Welche Prinzipien liegen den Routing-Protokollen zugrunde? Wie verlaufen die Routing-Protokolle RIP und OSPF? Welche Erweiterungen dieser Protokolle sind für IPv6 notwendig? Wie funktioniert BGP-4, für welche Zwecke und wie kann es eingesetzt werden? Wie können die Router am Internetzugang redundant ausgelegt werden? Wie realisiert man Multicast-Routing in IP-Netzen?

Kapitel 11

Die IP-Netze im Weitverkehrsbereich basieren überwiegend auf dem MPLS-Konzept und auf der, als GMPLS (*Generalized MPLS*) bezeichneten, dessen Erweiterung. Die Techniken MPLS und GMPLS ermöglichen die Konvergenz von Ethernet u.a. mit SDH- und WDM-Netzen. Dank dieser Konvergenz können Ethernet heutzutage nicht nur als LAN eingerichtet werden, sondern *Ethernet-Services* können sogar weltweit verfügbar gemacht werden. Kapitel 12 stellt die Konzepte und Protokolle zum Aufbau der IP-Netze mit dem MPLS und dem GMPLS vor und geht u.a. auf die folgenden Probleme ein: Worin bestehen die Konzepte MPLS und GMPLS und welche Möglichkeiten entstehen durch deren Einsatz? Welche Services werden durch *Traffic Engineering* in IP-Netzen erbracht? Wie werden (G)MPLS-Netze aufgebaut und wie wird die IP-Kommunikation über sie realisiert? Wie erfolgt die IP-Kommunikation über optische Netze? Wie können Datenpfade über (G)MPLS-Netze dynamisch eingerichtet werden?

Kapitel 12

In vielen Unternehmen können gleichzeitig unterschiedliche Netztechnologien eingesetzt und entsprechend integriert werden. Sie lassen sich mithilfe von *Tunneling-Techniken* so einsetzen, dass virtuelle Standleitungen für den Transport von Daten über öffentliche IP-Netze aufgebaut werden können. Diese Idee hat zur Entstehung von VPNs geführt. Somit erläutert Kapitel 13 einerseits die Konzepte für den IP-Einsatz in Netzen mit klassischen LANs (Ethernet), Punkt-zu-Punkt-Verbindungen (z.B. physikalischen Standleitungen, Satellitenverbindungen) und WLANs. Andererseits präsentiert dieses Kapitel auch die Lösungen und Protokolle für den Aufbau von VPNs auf Basis sowohl klassischer IP-Netze mittels des IPsec als auch der IP-Netze mit den Techniken MPLS bzw. GMPLS, die auch als *Provider Provisioned VPNs* bezeichnet werden. Hierbei geht dieses Kapitel u.a. auf folgende Fragestellungen ein: Wie kann man sich ein logisches LAN-Modell vorstellen und wie kann die *Multiprotokollfähigkeit in LANs* erreicht werden? Welche Ideen liegen den WLANs nach IEEE 802.11 zugrunde und wie werden WLANs mit einem Ethernet gekoppelt? Welche Typen von virtuellen Netzen gibt es, wie werden sie aufgebaut und wie können sie genutzt werden? Wie lassen sich sichere, virtuelle IP-Netze aufbauen?

Kapitel 13

- Kapitel 14** In den letzten Jahren haben sich einige Megatrends auf der 'Netzwerkwelt' herauskristallisiert. In privaten Netzwerken spricht man heute von *Layer-3-Switching* und von VLANs (*Virtual LANs*). Dabei stellt die Virtualisierung von Rechnern neue Anforderungen an IP-Netze. Die Unterstützung der Mobilität virtueller Rechner und virtueller Netzwerke sowie der Wunsch nach flexibler Möglichkeit, einen Rechner bzw. ein Netzwerk an das Internet parallel anbinden zu können, sind nur die wichtigsten von ihnen. Diese Probleme erläutert Kapitel 14 und präsentiert neue Konzepte und Protokolle hierfür, um diesen Anforderungen gerecht zu werden. Hervorgehoben sei hier *Shortest Path Bridging* (SPB), TRILL, VXLANs, ILNP und LISP. Dieses Kapitel geht u.a. auf folgende Fragen ein: Wie werden moderne IP-Netzwerke physikalisch und logisch strukturiert? Wie funktionieren Layer-2- und Layer-3-Switches, wo und wie werden sie eingesetzt? Wie können komplexe, auch virtuelle Rechner enthaltene VLANs gebildet werden und welche Bedeutung dabei hat VLAN Tagging? Worin bestehen die Ideen von TRILL, SPB, VXLAN, ILNP und LISP? Welche Möglichkeiten der Integration von IPv4 und IPv6 liefert LISP?
- Kapitel 15** Der Gedanke der Virtuellen Netze kann aber von einer IP-basierten Infrastruktur gelöst werden und sehr effizient auf dem Layer 2 umgesetzt werden. Hiermit ergeben sich Konvergenzen von Layer 2 und Layer 3 Verfahren, die unter dem Stichwort 'Distributed Layer-2/3 Switching in Kapitel 15 vorgestellt werden, die bis zu auf Ethernet basierten virtuellen Netzen reicht, sowie so wie sie heute im Provider-Umfeld angeboten werden.
- Kapitel 16** Um die Mobilität in IP-Netzen zu ermöglichen, wurden die Protokolle MIP (*Mobile IP*), MIPv6 (*Mobile IPv6*) und HMIPv6 (*Hierarchical MIPv6*) entwickelt. Kapitel 16 zeigt, wie diese Protokolle funktionieren und was gemacht werden muss, damit ein mobiler Rechner während bestehender Verbindungen ein Subnetz verlassen und in ein neues hinein bewegen kann, ohne die bestehenden Verbindungen abbrechen zu müssen. Auch die Integration von Hotspots mit dem Internet und die Möglichkeiten von Roaming zwischen Hotspots werden präsentiert. Darüber hinaus werden u.a. die folgenden Aspekte erörtert: Welche Ansätze und Protokolle zur Unterstützung der Mobilität in IP-Netzen gibt es? Wie kann *Roaming* zwischen Hotspots realisiert werden? Wie verläuft die Kommunikation beim Einsatz von MIP bzw. von MIPv6?
- Kapitel 17** Ein in der Tat neues 'Kapitel' haben wir mit der Diskussion um das 'Internet of Things' IoT Kapitel 17 aufgeschlagen. Hier stellen wir die wesentlichen Konzepte des 'Internet der Dings', die Adaption von IPv6 für IoT – 6LoWAPN – die nun notwendigen Routingverfahren, sowie das Applikationsprotokoll CoAP vor.
- Kapitel 18** Der Zukunft des Internet und seine möglichen Anwendungen und Perspektiven ist Kapitel 18 gewidmet. Wir wissen ja: "Schwer zu sehen, in ständiger Bewegung die Zukunft ist." (Meister Joda). Trotzdem ist hier der Versuch gewagt, die beherrschenden Tendenzen in systematischer Weise zu betrachten und die aktuelle Diskussion in den Internet-Gremien zu referenzieren.
- Verständnisfragen** Zu jedem einzelnen Kapitel gibt es ergänzend 'Verständnisfragen', durch die der geneigte Leser sein Wissen um zentrale Punkte der einzelnen Kapiteln überprüfen

und ggf. vertiefen kann. Die Antworten auf diesen Fragen finden sich Online auf der Webseite des Buchs.

## Vorwort zur vierten Auflage

Geschuldet der schnellen Entwicklung der Internet-Technologien und der guten Akzeptanz unserer 'Technik der IP-Netze' haben wir unsern 'siebenjährigen' Updatezyklus (erste, zweite und dritte Auflage) etwas beschleunigt und stellen nun mit der vierten Auflage eine aktualisierte Version zur Verfügung. Neben obligatorischen Verbesserungen und Richtigstellungen in einigen Details, sind folgende Aspekte neu hinzugekommen:

- Die heutzutage als unentbehrliche IT-Security bei der Internetnutzung wird auf dem aktuellen Stand umfangreich diskutiert und in Kapitel 2 an zentraler Stelle untergebracht. Wir führen hier die vier zentralen *kryptographischen Primitiven* vor, die eine hervorgehobene Rolle einnehmen.
- Die Switching-Technologien für IP-Netze umfassen nun Layer-2 und Layer-3 Eigenschaften, deren Würdigung in Kapitel 16 zu finden ist.
- Ein wichtiger neuer Aspekt stellt das *Internet of Things* (IoT) dar. Dies würdigen wir in den Kapiteln 17 und 18. Während zunächst Lösungen für Komponenten mit Ressourcen-beschränkter und im Besonderen geringer elektrischer Leistung (6LoWAPN) und die hieraus erwachsenden Konsequenzen, die sich für das Routing und für Applikationen, wie dem *Constrained Application Protocol* (CoAP) ergeben, beschrieben werden, spannen wir in Kapitel 18 dieses neue Umfeld mit seinen vielfältigen Facetten in Gänze auf.

Die vierte Auflage wurde auch typographisch aufgefrischt:

- Das Layout wurde über die vielen Kapitel vereinheitlicht und die Tabellen mit einem modernen Design versehen.
- Beispiele im Buch werden – wie in diesem Fall – mit einem links-seitigen Balken hervorgehoben.

Layout-  
Anpassungen und  
Beispiele

## Vorwort zur fünften Auflage

Diese Auflage beinhaltet im wesentlichen redaktionelle Änderungen und Anpassungen, die der Entwicklung des Internets und seiner Protokolle geschuldet sind. Allerdings verweist diese Auflage bereits auf das nächste Projekt der Autoren, das virtuellen Netzstrukturen gewidmet sein wird.

- *Redaktionelle* Änderungen betreffen die Verlinkung der Inhalte und die Verbesserung der Nutzung des Buchs als PDF-Dokument. Somit kann man im PDF nun zwischen Kapiteln und Abschnitten navigieren. Alle Links zu den IETF-Quellen wurden von *http* auf *https* umgestellt; das trägt zum Komfort bei, da dort keine 'Umleitung' gesetzt wurde. Wir wurden gelegentlich gefragt: *Warum gibt es das Buch nicht als eBook?* Die Antwort ist einfach: 'Technik der IP-Netze' wurde im

Redaktionelles



aktuellen Format mittels  $\text{\LaTeX}$  gesetzt. Darstellung, Seitenumbruch und Lesbarkeit sind darauf abgestimmt. Bei einem eBook-Format gingen dies verloren.

Bei den Abbildungen, wo wir Bitstrukturen erklären, halten wir es nun mit *Edsger Dijkstra* (siehe Vorspann zum Thema 'Internet-Routing-Architektur') und fangen bei '0' zu zählen an: Das erste Bit wird mit '0' nummeriert. Das ist auch die übliche Schreibweise in der Literatur.

Wurde das Manuskript bislang unter MacOS erstellt, findet nun Linux Anwendung. Die neuen Abbildungen wurden mit *InkScape* erstellt, an dessen Nutzung sich der Autor noch gewöhnen muss ;-)

#### Inhaltliches

- *Inhaltliche* Änderungen sind überschaubar, und es mussten lediglich einige wenige Fehler korrigiert werden. In Kapitel 2 wurde die ECC-Kryptographie endlich entsprechend ihrer Bedeutung nach eingeführt. Trotzdem ist 'Technik der IP-Netze' weder ein Lehrbuch der Kryptographie noch der 'IT-Security'. Allerdings ist die Literatur zu diesen Themen relativ überschaubar, sodass wir einen aktuellen Abriss hierzu als notwendig betrachtet haben.

Das Kapitel 4 integriert nun endlich auch Multipath-TCP an der richtigen Stelle, und es wurde dem QUIC-Protokoll ein eigener Abschnitt gewidmet, der versucht, dieses doch recht komplexe Protokoll zumindest in seinen Grundzügen zu erklären. In verteilten System spielt die Zeitsynchronisation von IT-Systemen eine wichtige Rolle (auch weil man Eindringlinge erkennen will). Daher haben wir in Kapitel 7 sowohl die Protokolle NTP als auch PTP beschrieben; nicht immer zur Zufriedenheit des Autors.

Die fünfte Auflage ist dem Internet-Aktivisten *Sven Guckes* gewidmet.

## Technik der IP-Netze – Homepage

Die Homepage des Buches ist unter <https://www.fehcom.de/pub/tipn.html> erreichbar, wo sich auch Korrekturen einfinden werden. Ihre Kritik, Verbesserungsvorschläge und eventuell Ihre Korrekturen sind willkommen und wir nehmen sie gerne entgegen. Für Lehr- und Ausbildungszwecke stellen wir die Abbildungen auf Anfrage zur Verfügung.

## Danksagung

Ein so umfangreiches Buch kann ohne Anregungen von außen und einen entsprechenden Erfahrungsaustausch nicht geschrieben werden.

Ein besonderer Dank gilt Herrn Dipl. math. Jürgen Müller (Darmstadt) und Herrn Dirk Müller (Koblenz) für die notwendige Sorgfalt, die dritte Auflage des Buches intensiv durchzuarbeiten und uns Korrekturen vorzuschlagen. Ebenso möchten wir Frau Hasselbach als primäre Ansprechpartnerin sowie Frau Irene Weihart und Frau Kristin Rothe und nicht zu vergessen Herrn Jürgen Dubau für das sorgfältige Lektorat auch in dieser Auflage danken. Bei einem so umfangreichen Projekt ergeben sich immer Inkonsistenzen, auf die die aufmerksame Leserschaft stößt.

## Die Autoren

### Prof. Dr.-Ing. Anatol Badach

Über 30 Jahre war er auf den Gebieten Informatik und Telekommunikation beruflich tätig; Promotion (1975), Habilitation (1983). Von Dezember 1985 bis August 2012 war er Professor im Fachbereich Angewandte Informatik an der Hochschule Fulda. Seine Schwerpunkte in Lehre und Forschung waren: Rechnerkommunikation, Netzwerktechnologien und Multiservice Networking. Er hat u.a. auf den Gebieten: Netzwerktechnologien und Protokolle, VoIP und Next Generation Networking geforscht und verfolgt mit Engagement einige wichtige Entwicklungen weiter.



Prof. Badach ist Autor zahlreicher Veröffentlichungen und u.a. zahlreicher anderer Fachbücher, darunter *Voice over IP – Die Technik, Netzwerkprojekte* (Mitautor), *Web-Technologien* (Mitautor), *Integrierte Unternehmensnetze*, *Datenkommunikation mit ISDN*, *High Speed Internetworking* (Mitautor), *ISDN im Einsatz*. Seine Erfahrung vermittelt er weiter als Leiter/Referent bei Fachkongressen und -seminaren, Berater bei innovativen Projekten und Entwicklungen, Autor von Fachbeiträgen.

<https://www.competence-site.de/Anatol-Badach>

### Prof. Dr. Erwin Hoffmann

Jahrgang 1958, Studium der Physik und Astrophysik an der Universität Bonn und 1989 Promotion an der TU München (Max-Planck-Institut für Physik und Astrophysik). Durch seine Tätigkeit in der experimentellen Teilchenphysik am CERN und Fermilab verschaffte er sich Kenntnisse über unterschiedlichste Rechnerbetriebssysteme. Beruflich war er zunächst im Bereich Hochgeschwindigkeitsnetze (FDDI) engagiert sowie mit der Implementierung von TCP/IP auf IBM-Großrechnern.



Seit 1998 ist er an der Weiterentwicklung der Software von D.J. Bernstein involviert und veröffentlicht diese als *Public Domain*. Heute ist er Professor an der Frankfurt University of Applied Sciences mit den Schwerpunkten Rechnernetze, Betriebssysteme, IT-Security, Software Engineering sowie Verteilten Systeme.

<https://www.fehcom.de>

*Dieses Buch möchten wir all jenen widmen, die dank ihrer technischen Schöpfungen zur Entstehung des Internet beigetragen haben, und ebenso denen, die sich dafür engagieren das Internet weiterzuentwickeln, es offen und aufrecht zu erhalten.*

*Prof. Anatol Badach (Fulda/Petersberg)*

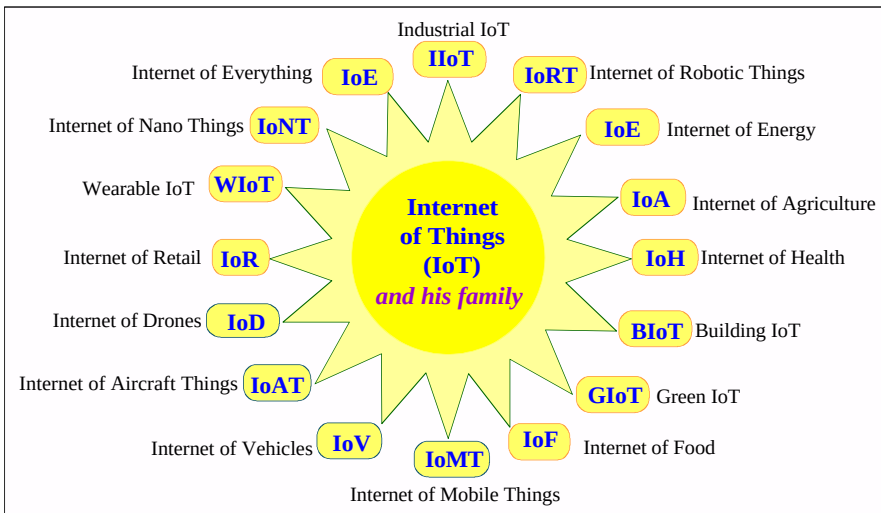
*Prof. Erwin Hoffmann (Höhn-Schönberg) – im September 2022*



# 18 Networking-Trends

Die wichtigsten Meilensteine der Internet-Entwicklung bis Ende 2014, d.h. bis zum Zeitpunkt der Erstellung der 3. Auflage dieses Buches, präsentiert der damals verfasste Abschnitt 1.1.4. In darauffolgenden vier Jahren haben sich bedeutende Entwicklungstrends auf dem Gebiet Networking, auf dem das Protokoll IP in beiden Versionen 4 und 6 eine fundamentale Rolle spielt, herauskristallisiert. Das Ziel dieses Abschnittes ist es, die aktuellen, in Abb. 18.0-1 dargestellten 'Top 10 Networking Trends' näher zu erläutern.

[Networking Trends 2022 im Überblick](#)



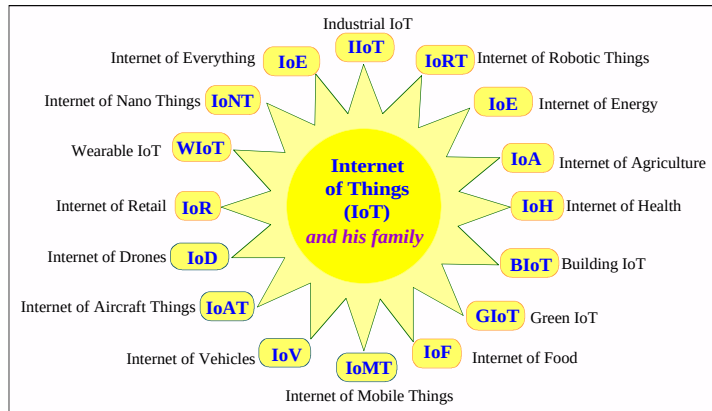
**Abb. 18.0-1:** Internet, Internet of Things und andere IP-Netze; Top 10 Networking Trends

Die aktuellen 'Top 10 Networking Trends' wollen wir nun abschließend kurz beleuchten. Da diese Entwicklungen sich derzeit im Fluss befinden, können die Resultate daher nicht in der notwendigen fachlichen Durchdringung dargestellt werden. Allerdings kann sich jeder Leser mittels der angegebenen Quellen ein Bild des aktuellen Standes bilden, wobei natürlich auch dann im Verborgenen bleibt, welche der aufgezeigten Tendenzen tatsächlich eingesetzt werden.

## 18.1 Internet of Things (IoT)

### IoT-Familie

Das Spektrum von Einsatzmöglichkeiten des IoT ist so groß, dass zwischen diversen Arten des IoT zu unterscheiden ist. Es kann in diesem Zusammenhang sogar von einer IoT-Familie gesprochen werden. Abb. 18.1-1 präsentiert die Mitglieder dieser Familie mit teilweise überlappenden Nutzungsmöglichkeiten.



**Abb. 18.1-1:** Spezialisierte IoT-Varianten als Mitglieder der IoT-Familie

### IoT-betreffende Networking Trends

Die Integration verschiedener allgegenwärtiger, zu unserem Alltag gehörender Dinge (*Things*) in das Internet führt zur Entstehung einer besonderen Internet-Erweiterung. Diese wird als *Internet of Things* (IoT) bzw. als *Internet der Dinge* bezeichnet. Das Konzept von IoT und seine Protokolle präsentiert Kapitel 17. An dieser Stelle sei aber darauf hingewiesen, und dies geht aus Abb. 1.1-6 hervor, dass diverse Networking Trends auf eine Art mit dem IoT zusammenhängen und folglich auch seine weiteren Entwicklungen im gewissen Grade beeinflussen. Die folgenden Trends in der Weiterentwicklung von IoT sind hervorzuheben: *Industrial IoT* (IIoT), *Internet of Robotic Things* (IoRT), *Internet of Vehicles* (IoV), *Internet of Drones* (IoD), *Mobility in IoT* und *IoT Security*. Für Näheres darüber siehe:

- 1.a i-SCOOP: [The Internet of Things \(IoT\) – essential IoT business guide](#)
- 1.b i-SCOOP: [Blockchain and the Internet of Things: the IoT blockchain opportunity and challenge](#)
- 1.c Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva: [Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues](#); IEEE Communications Surveys & Tutorials, Vol. 17(3), Jul 2015; DOI: 10.1109/COMST.2015.2388550
- 1.c Misty Blowers, Jose Iribarne, Edward Colbert, Alexander Kott: [The Future Internet of Things and Security of its Control Systems](#); arXiv:1610.01953v1; Oct 2016
- 1.d P.P. Ray: [A survey on Internet of Things architectures](#); Journal of King Saud University - Computer and Information Sciences; Vol. 30 (3), Jul 2018, DOI: 10.1016/j.jksuci.2016.10.003

- 1.e Onoriode Uviase, Gerald Kotonya: [IoT Architectural Framework: Connection and Integration Framework for IoT Systems](#); arXiv:1803.04780v1, 2018, DOI: 10.4204/EPTCS.264.1
- 1.f Alem Čolaković, Mesud Hadžialić: [Internet of Things \(IoT\): A Review of Enabling Technologies, Challenges, and Open Research Issues](#); Computer Networks, Vol. 144, Oct 2018; DOI: 10.1016/j.comnet.2018.07.017

### 18.1.1 Industrial Internet of Things (IIoT)

Das IoT hat eine enorme Bedeutung für die Industrie, denn Dank ihm – insbesondere der Nutzung von Sensordaten und der M2M-Kommunikation (M2M: *Machine to Machine*) –, kann die Effizienz von Maschinen und Automaten verbessert werden. Die M2M-Kommunikation stellt hohe QoS-Anforderungen (QoS: *Quality of Service*) an die industriellen Netzwerke und folglich an das IoT. Zu ihrer Erfüllung ist eine besondere Realisierung des IoT erforderlich. Diese an die industriellen Anforderungen angepasste Art von IoT wird als IIoT (*Industrial IoT*) bezeichnet. Für Näheres über IIoT siehe: [1.1.a], [1.1.c] und [1.1.h].

IoT als Basis für  
M2M-  
Kommunikation

Um hohe QoS-Anforderungen erfüllen zu können, müssen für das IIoT spezielle Netzwerke eingerichtet werden. Zu deren Aufbau wurde das Verfahren TSCH (*Time-Slotted Channel Hopping*) konzipiert. Es stellt eine spezielle zeitsynchrone Realisierung des MAC-Protokolls (*Media Access Control*) zum Aufbau drahtloser industrieller Netzwerke dar. Bei TSCH handelt sich um eine Kombination des Frequenzmultiplexes und des synchronen Zeitmultiplexes, also um eine Variante des Frequenz- und Zeitmultiplexverfahrens FTDM (*Frequency-Time Division Multiplexing*). Die auf TSCH basierenden Netzwerke ermöglichen es im industriellen Bereich, das *Deterministic Networking* zu realisieren. Für weitere Informationen über IIoT und TSCH sei verwiesen auf:

IIoT und TSCH

- 1.1.a i-SCOOP: [The Industrial Internet of Things \(IIoT\): the business guide to Industrial IoT](#)
- 1.1.b i-SCOOP: [IT and OT convergence – two worlds converging in Industrial IoT](#)
- 1.1.c Li Da Xu, Wu He, Shancang Li: [Internet of Things in Industries: A Survey](#); IEEE Transactions on Industrial Informatics“, Vol. 10(4), Nov 2014; DOI: 10.1109/TII.2014.2300753
- 1.1.c Martin Wollschlaeger, Thilo Sauter, Jürgen Jasperneite: [The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0](#); IEEE Electronics Magazine, Mar 2017
- 1.1.d Anatol Badach: [TSCH – Time-Slotted Channel Hopping](#); In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Jan 2018
- 1.1.f Jiangfeng Cheng, Weihai Chen, Fei Tao, Chun-Liang Lin: [Industrial IoT in 5G environment towards smart manufacturing](#); Journal of Industrial Information Integration, Vol. 10, Jun 2018, DOI: 10.1016/j.jii.2018.04.001

- 1.1.g Emiliano Sisinni, Abusayeed Saifullah, Song Han, Ulf Jennehag, Mikael Gidlund: [Industrial Internet of Things: Challenges, Opportunities, and Directions](#); IEEE Transactions on Industrial Informatics (Early Access), Jul 2018; DOI: 10.1109/TII.2018.2852491
- 1.1.h Hugh Boyes, Bil Hallaq, Joe Cunningham, Tim Watson: [The industrial internet of things \(IIoT\): An analysis framework](#); Computers in Industry, Vol. 101, Oct 2018; DOI: 10.1016/j.compind.2018.04.015
- 1.1.i Cristina Paniagua, Jerker Delsing: [Industrial Frameworks for Internet of Things: A Survey](#); IEEE Systems Journal, Vol. 15, Issue 1, Mar 2021; DOI: 10.1109/JSYST.2020.2993323
- 1.1.j Yulei Wu, Hong-Ning Dai, Haozhe Wang, Zehui Xiong, Song Guo: [A Survey of Intelligent Network Slicing Management for Industrial IoT: Integrated Approaches for Smart Transportation, Smart Energy, and Smart Factory](#); IEEE Communications Surveys & Tutorials, Vol. 24, Issue 2, Mar 2022; DOI: 10.1109/COMST.2022.3158270

## 18.1.2 Internet of Robotic Things

### Verteilte Robotersysteme

Dank der modernsten Technologien werden vor allem in der Industrie und auch anderswo, immer mehr Roboter eingesetzt. Sie werden auch auf eine spezielle Art und Weise in das IoT integriert, und dies führt zur Entstehung einer besonderen IoT-Art, die als *Internet of Robotic Things* (IoRT) bezeichnet wird. Mit dem IoRT wird das Ziel verfolgt, sowohl diverse Roboter untereinander als auch weit im IoT verbreitete Sensoren und als Aktuatoren bezeichnete intelligente Antriebs Elemente mit autonomen Robotern zu vernetzen. Diese Vernetzung bedeutet eine Verschmelzung von Robotik- und IoT-Technologien und ermöglicht, die IoT-Services um die Fähigkeiten intelligenter Robotersysteme zu erweitern. Dadurch kann ein neues breites Spektrum von IoRT-basierten Services angeboten werden. Für Näheres über IoRT siehe:

- 1.2.a Partha Pratim Ray: [Internet of Robotic Things: Concept, Technologies, and Challenges](#); IEEE Access, Vol. 4, 2016; DOI: 10.1109/ACCESS.2017.2647747
- 1.2.b Cristanel Razafimandimby, Valeria Loscri, Anna Maria Veg: [Towards Efficient Deployment in Internet of Robotic Things](#); In book: Gravina R., et al. (Eds) 'Integration, Interconnection, and Interoperability of IoT Systems. Internet of Things (Technology, Communications and Computing)'. Springer, Jul 2017; DOI: 10.1007/978-3-319-61300-0\_2
- 1.2.c Pieter Simoens, Mauro Dragone, Alessandro Saffiotti: [The Internet of Robotic Things: A review of concept, added value and applications](#); International Journal of Advanced Robotic Systems, Vol. 15(1), Jan - Feb 2018; DOI: 10.1177/1729881418759424
- 1.2.d Ovidiu Vermesan, Roy Bahr, Marco Ottella, Martin Serrano, at al: [Internet of Robotic Things Intelligent Connectivity and Platforms](#); Frontiers in Robotics and AI, Sep 2020; DOI: 10.3389/frobt.2020.00104

- 1.2.e Davide Villa, Xinchao Song, Matthew Heim, Liangshe Li: [Internet of Robotic Things: Current Technologies, Applications, Challenges and Future Directions](#); arXiv:2101.06256v1, Jan 2021; DOI: 10.48550/arXiv.2101.06256
- 1.2.f Aqsa Sayeed, Chaman Verma, Neerendra Kumar, Neha Koul, Zoltán Illés: [Approaches and Challenges in Internet of Robotic Things](#); Future Internet, Vol. 14. Issue 9, Sep 2022; DOI:10.3390/fi14090265

### 18.1.3 Internet of Vehicles

Zur Unterstützung autonom fahrender Fahrzeuge mithilfe von IoT müssen im IoT verschiedene zeitkritische Services realisiert werden. Die Unterstützung des autonomen Fahrens führt daher zur Entstehung einer besonderen, als *Internet of Vehicles* (IoV) bezeichneten Variante von IoT. Dabei kann Fog Computing [Abschnitt 17.1] als Basis für das IoV angesehen werden. Im IoV sollen verschiedene Arten der drahtlosen Vernetzung von autonom fahrenden Fahrzeugen realisiert werden, insbesondere:

Voraussetzung  
des autonomen  
Fahrens

- *Vehicle-to-Vehicle*: Fahrzeug-zu-Fahrzeug-Kommunikation ermöglicht, dass autonom fahrende, benachbarte Fahrzeuge untereinander kommunizieren und sich damit z.B. über den Straßenzustand informieren können. V2V
- *Vehicle-to-Infrastructure*: Mittels Fahrzeug-zu-Infrastruktur-Kommunikation können autonom fahrende Fahrzeuge auf straßenseitige Infrastrukturelemente (z.B. entlang von Straßen installierte Verkehrsleitsysteme) wie z.B. Ampeln und andere Verkehrszeichen aufmerksam gemacht werden. Hiermit kann die Verkehrssicherheit verbessert werden. V2I
- *Vehicle-to-Pedestrian*: Fahrzeug-zu-Fußgänger-Kommunikation kann als präventive Maßnahme betrachtet werden, dank dieser ein autonom fahrendes Fahrzeug Fußgänger und Radfahrer erkennen kann, um folglich eine potenzielle Kollision zu verhindern und Schaden von den Verkehrsteilnehmern abzuwenden. V2P
- *Vehicle-to-Network*: Fahrzeug-zu-Netzwerk-Kommunikation erlaubt z.B. über Mobilfunk Verbindungen mit großer Reichweite zwischen Fahrzeug und Netzwerk, um z.B. einen Cloud-Zugang aufbauen zu können. V2N

Für weitere Informationen über IoV siehe:

- 1.3.a Yang Fangchun, Wang Shangguang, Li Jinglin, Liu Zhihan, Sun Qibo: [An Overview of Internet of Vehicles](#); China Communications, Oct 2014
- 1.3.b Kang Kai, Wang Cong and Luo Tao: [Fog Computing for Vehicular AdHoc Networks: Paradigms, Scenarios, and Issues](#); The Journal of China Universities of Posts and Telecommunications, Vol. 23(2), Apr 2016; DOI 10.1016/S1005-8885(16)60021-3
- 1.3.c Omprakash Kaiwartya, et al.: [Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects](#); IEEE Access, Vol. 4, Sep 2016; DOI: 10.1109/ACCESS.2016.2603219
- 1.3.f Juan Contreras, Sherali Zeadally, Juan Antonio Guerrero-Ibanez: [Internet of Vehicles: Architecture, Protocols and Security](#); IEEE Internet of Things Journal (Early Access), Apr 2017; DOI: 10.1109/JIOT.2017.2690902



- 1.3.g Fangchun Yang, Jinglin Li, Tao Lei, Shangguang Wang: [Architecture and key technologies for Internet of Vehicles: a survey](#); Networks, Vol. 2(2), Jun 2017; DOI: 10.1007/s41650-017-0018-6
- 1.3.h Eugen Borcoci, Serban Obreja, Marius Vochin: [Internet of Vehicles Functional Architectures-Comparative Critical Study](#), The Ninth International Conference on Advances in Future Internet AFIN, Sep 2017
- 1.3.i Min Chen, Yuanwen Tian, Giancarlo Fortino, Jing Zhang, Iztok Humar: [Cognitive Internet of Vehicles, Computer Communications](#); Vol. 120, May 2018; DOI: 10.1016/j.comcom.2018.02.006

### 18.1.4 Internet of Drones

#### Kommunikation der UAVs

Die Drohnen, unbemannte und kurz als UAVs (*Unmanned Aerial Vehicle*) bezeichnete Luftfahrzeuge, gewinnen immer mehr an Bedeutung. Sie können ohne eine an Bord befindliche menschliche Besatzung selbständig durch einen Computer oder vom Boden über eine Fernsteuerung navigiert und für verschiedene Zwecke eingesetzt werden. Aus diesem Grund werden Drohnen als mobile Objekte in das Internet, insbesondere in das IoT, integriert. Dadurch entsteht eine besondere Art von IoT, und man nennt diese *Internet of Drones* (IoD). Als Literatur über IoD siehe:

- 1.4.a Ilker Bekmezci, Ozgur Koray Sahingoz, Samil Temel: [Flying Ad-Hoc Networks \(FANETs\): A Survey](#); Vol. 11(3), May 2013; DOI: 10.1016/j.adhoc.2012.12.004
- 1.4.b Ozgur Koray Sahingoz: [Networking Models in Flying Ad-Hoc Networks \(FANETs\): Concepts and Challenges](#); J. Intelligent & Robotic Systems, Vol. 74 (1), Apr 2014; DOI 10.1007/s10846-013-9959-7
- 1.4.c Naser Hossein Motlagh, Tarik Taleb, Osama Arouk: [Low-Altitude Un-manned Aerial Vehicles-Based Internet of Things Services: Comprehensive Survey and Future Perspectives](#); IEEE Internet of Things Journal, Vol. 3(6), Dec 2016; DOI: 10.1109/JIOT.2016.2612119
- 1.4.d Armir Bujari, et al.: [Flying ad-hoc network application scenarios and mobility models](#); International Journal of Distributed Sensor Networks; Vol. 13(10), 2017; DOI: 10.1177/1550147717738192
- 1.4.e Mariana Rodrigues, et al.: [UAV Integration Into IoIT: Opportunities and Challenges](#); ICAS 2017: The Thirteenth International Conference on Autonomic and Autonomous Systems, May 2017
- 1.4.f Muhammad Asghar Khan, Ijaz Mansoor Qureshi, Engr Alamgir Safi, Inam Ullah Khan: [Flying Ad-Hoc Networks \(FANETs\): A Review of Communication architectures, and Routing protocols](#); First International Conference on Latest trends in Electrical Engineering and Computing Technologies (Intellect 2017); Nov 2017; DOI: 10.1109/INTELLECT.2017.8277614
- 1.4.g Weisen Shi, et al.: [Drone Assisted Vehicular Networks: Architecture, Challenges and Opportunities](#); IEEE Network, Vol.32(3), May/June 2018; DOI: 10.1109/MNET.2017.1700206

- 1.4.h Gaurav Choudhary, Vishal Sharma, Takshi Gupta, Jiyoung Kim, Ilseun You: [Internet of Drones \(IoD\): Threats, Vulnerability, and Security Perspectives](#); arXiv:1808.00203v2, Aug 2018
- 1.4.i Mohammad Wazid, Ashok Kumar Das, Jong Hyouk Lee: [Authentication protocols for the internet of drones: taxonomy, analysis and future directions](#); Journal of Ambient Intelligence and Humanized Computing; Aug 2018; DOI: 10.1007/s12652-018-1006-x

### 18.1.5 Mobility in IoT

An das IoT wird u.a. eine breite Palette von mobilen *Sensoren*, *Aktuatoren* und mobile virtualisierte Rechner in Form von VMs (*Virtual Machines*) angebunden. Diese können z.B. in selbstfahrenden Autos, in Drohnen bzw. in anderen UAVs installiert sein. Mit mobilen VMs am IoT-Rande (IoT Edge) werden verschiedene mobile Services erbracht, sodass man von *Mobile Edge Computing* (MEC) spricht. Mobile VMs können aber auch als mobile Fog Nodes fungieren [Abschnitt 17.1]. Dies deutet darauf hin, dass die Unterstützung der Mobilität im IoT (Mobility in IoT) von enorm großer Bedeutung ist. Für Näheres über Mobilität im IoT sei verwiesen auf:

Mobile Edge  
Computing

- 1.5.a Rodrigo Roman, Javier Lopez, Masahiro Mambo: [Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges](#); arXiv:1602.00484v2, Nov 2016; DOI: 10.1016/j.future.2016.11.009
- 1.5.b Safwan M. Ghaleb, et al.: [Mobility management for IoT: a survey](#); EURASIP Journal on Wireless Communications and Networking, Dec 2016; DOI 10.1186/s13638-016-0659-4
- 1.5.c Jabiry M. Mohammed, Bi-Lynn Ong, R. Badlishan Ahmad, Mohammed Hakawati: [Internet of Things \(IoT\) Mobility Support based on distributed Sensor Proxy MIPv6](#); Journal of Theoretical and Applied Information Technology, Vol. 95(17), Sept. 2017
- 1.5.d Tuan Nguyen gia, et al.: [Fog Computing Approach for Mobility Support in Internet-of-Things Systems](#); IEEE Access PP(99):1-1; Jun 2018, DOI:10.1109/ACCESS.2018.2848119

### 18.1.6 IoT Security

Mit IoT soll die Vision verwirklicht werden, unsere Alltagseinrichtungen unterschiedlicher Art und mit unterschiedlichen Fähigkeiten sowohl untereinander als auch mit Rechnern am Internet so zu vernetzen, dass sie alle Internet-Services nutzen können. Mit der Verwirklichung dieser Vision entstehen verschiedene potenzielle Sicherheitsbedrohungen, dabei aber auch solche, die wir heute noch nicht kennen.

Um die IoT-Sicherheit möglichst auf einem hohen Niveau zu gewährleisten, sind klassische Ansätze nicht mehr ausreichend. Hierfür ist zurzeit noch ein breites Spektrum von Forschungs- und Entwicklungsaktivitäten erforderlich. Vor allem müssen unsere

Klassische  
IT-Security  
reicht nicht aus

Alltagseinrichtungen am IoT eine besondere sicherheitsrelevante Intelligenz besitzen, also sicherheitsbewusst (*security aware*) sein. Für Näheres über IoT-Sicherheit siehe:

- 1.6.a T. Heer, et al.: [Security Challenges in the IP-based Internet of Things](#), *Wireless Personal Communications*; Vol. 61(3), Dec 2011; DOI: 10.1007/s11277-011-0385-5
- 1.6.b Sabrina Sicari, et al.: [Security, Privacy & Trust in Internet of Things: The road ahead](#); *Computer Networks* Vol. 76, Jan 2015; DOI: 10.1016/j.comnet.2014.11.008
- 1.6.c Jorge Granjal, Edmundo Monteiro, Jorge Sá Silva: [Security for the Internet of Things: A Survey of Existing Protocols and Open Research Issues](#); *IEEE Communications Surveys & Tutorials*, Vol. 17(3), Jul 2015; DOI: 10.1109/COMST.2015.2388550
- 1.6.e M. A. Ferrag, L. A. Maglaras, H. Janicke, J. Jiang: [Authentication Protocols for Internet of Things: A Comprehensive Survey](#), arXiv, Dec 2016
- 1.6.e Rodrigo Roman, Javier Lopez, Masahiro Mambo: [Mobile edge computing, Fog et al.: A survey and analysis of security threats and challenges](#); arXiv:1602.00484v2, Nov 2016; DOI: 10.1016/j.future.2016.11.009
- 1.6.e Shancang Li, Li Da Xu, Imed Romdhani (Contributor): [Securing the Internet of Things](#): 2017 Elsevier Inc.; ISBN: 978-0-12-804458-2
- 1.6.f Xiruo Liu, Meiyuan Zhao, Sugang Li, Feixiong Zhang, Wade Trappe: [A Security Framework for the Internet of Things in the Future Internet Architecture](#); *Future Internet*, Vol. 9(3), 2017; DOI: 10.3390/fi9030027
- 1.6.g B. B. Zarpelão, R. S. Miani, C. T. Kawakani and S. C. de Alvarenga: [A Survey of Intrusion Detection in Internet of Things](#), *Journal of Network and Computer Applications*; Vol. 84, Apr 2017; DOI: 10.1016/j.jnca.2017.02.009
- 1.6.h Pooja, Dr. R. K. Chauhan: [Review on Security Attacks and Countermeasures in Wireless Sensor Networks](#); *International Journal of Advanced Research in Computer Science*, Vol. 8(5), May-Jun 2017
- 1.6.i Chao Lin, et al.: [Security and Privacy for the Internet of Drones: Challenges and Solutions](#); *IEEE Communications Magazine*, Vol. 56(1), Jan 2018; DOI: 10.1109/MCOM.2017.1700390
- 1.6.j Djedjig Nabil, D. Tandjaoui, Imed Romdhani, Faiza Medjek: [Trust Management in Internet of Things](#); In book: *Security and Privacy in Smart Sensor Networks*; May 2018; DOI: 10.4018/978-1-5225-5736-4.ch007
- 1.6.k Francesco Restuccia, Salvatore D'Oro, Tommaso Melodia: [Securing the Internet of Things in the Age of Machine Learning and Software-defined Networking](#); *IEEE Internet of Things Journal (Early Access)*, Jun 2018; DOI: 10.1109/JIOT.2018.2846040
- 1.6.l Djamel Eddine Kouicem, Abdelmadjid Bouabdallah, Hicham Lakhlef: [Internet of things security: A top-down survey](#); *Computer Networks*, Vol. 141, Aug 2018; DOI: 10.1016/j.comnet.2018.03.012
- 1.6.m Shui Yu, Guojun Wang, Xiting Liu, Jianwei Niu: [Security and Privacy in the Age of the Smart Internet of Things: An Overview from a Networking](#)

- [Perspective](#); IEEE Communications Magazine, Vol. 56(9), Sep 2018; DOI: 10.1109/MCOM.2018.1701204
- 1.6.n RFC 8576: [Internet of Things \(IoT\) Security: State of the Art and Challenges](#); Apr 2019
- 1.6.o Jian Zhang, Huaijian Chen, Liangyi Gong, Jing Cao, Zhaojun Gu: [The Current Research of IoT Security](#), IEEE Fourth International Conference on Data Science in Cyberspace, Jun 2019; DOI: 10.1109/DSC.2019.00059
- 1.6.p Vikas Hassija, Vinay Chamola, Vikas Saxena, Divyansh Jain, Pranav Goyal, Biplob Sikdar: [A Survey on IoT Security: Application Areas, Security Threats, and Solution Architectures](#); IEEE Access, Vol. 7, Jun 2019; DOI: 10.1109/ACCESS.2019.2924045
- 1.6.q Hui Wu, Haiting Han, Xiao Wang, Shengli Sun: [Research on Artificial Intelligence Enhancing Internet of Things Security: A Survey](#); IEEE Access, Vol. 8, Aug 2020; DOI: 10.1109/ACCESS.2020.3018170

## 18.2 Software-Defined Networking (SDN)

Die grundlegende Idee von SDN besteht darin [Abschnitt 17.1], die Software in zur Übermittlung von Daten bestimmten Netzwerkkomponenten möglichst von ihrer Hardware zu trennen und diese dann auf eine bzw. mehrere zentrale, als Controller bezeichnete Steuerungskomponente/n auszulagern. Dies führt zu neuen Möglichkeiten der Entwicklung, de facto Programmierung, diverser Network Services. SDN ermöglicht auf diese Weise eine dem Bedarf entsprechende, schnelle Einrichtung verschiedener SD Networks und SD Network Services. Folglich kann sogar von *Programmable Network Services* bzw. von *Network Programmability* gesprochen werden. Die Idee von SDN liegt insbesondere den Networking Trends zugrunde – hervorgehoben seien insbesondere *SD WANs*, *SD Optical Networking*, *SD Data Centers*, *SD IoT*, *Wireless SD Networking* und *SD Internet of Vehicles*. Für Näheres über SDN siehe:

[Programmable Network Services](#)

- 2.a Anatol Badach: [SDN – Software Defined Networking](#); In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Dec 2012, DOI 10.13140/RG.2.1.4963.4001
- 2.b Sandra Scott-Hayward, Gemma O’Callaghan, Sakir Sezer: [SDN Security: A Survey](#); IEEE SDN for Future Networks and Services (SDN4FNS), Nov 2013; DOI: 10.1109/SDN4FNS.2013.6702553
- 2.c Yosr Jarraya, Taous Madi, Mourad Debbabi: [A Survey and a Layered Taxonomy of Software-Defined Networking](#); IEEE Communications Surveys & Tutorials, Vol. 16(4), 2014; DOI: 10.1109/COMST.2014.2320094
- 2.d RFC 7426: [Software-Defined Networking \(SDN\): Layers and Architecture Terminology](#); Jan 2015
- 2.e Hamid Farhady, HyunYong Lee, Akihiro Nakao: [Software-Defined Networking: A survey](#); Computer Networks, Vol. 81, Apr 2015; DOI: 10.1016/j.comnet.2015.02.014

- 2.f Akram Hakiri, et al.: [Software-Defined Networking: Challenges and research opportunities for Future Internet](#); Computer Networks, Vol. 75, Part A, Dec 2014; DOI: 10.1016/j.comnet.2014.10.015
- 2.g Bruno Astuto A. Nunes, et al.: [A Survey of Software-Defined Networking: Past, Present, and Future of Programmable Networks](#); IEEE Communications Surveys & Tutorials, Vol. 16(3), 2014; DOI: 10.1109/SURV.2014.012214.00180
- 2.h Diego Kreutz, et al.: [Software-Defined Networking: A Comprehensive Survey](#); Proceedings of the IEEE, Vol. 103(1), Jan 2015; DOI: 10.1109/JPROC.2014.2371999
- 2.i Junjie Xie, Deke Guo, Zhiyao Hu, Ting Qu, Pin Lv: [Control plane of software defined networks: A survey](#); Computer Communications, Vol. 67, Aug 2015, DOI: 10.1016/j.comcom.2015.06.004
- 2.j Izzat Alsmadi, Dianxiang Xu: [Security of Software Defined Networks: A survey](#); Computers & Security, Vol. 53, Sep 2015; DOI: 10.1016/j.cose.2015.05.006
- 2.k ONF TR-521: [SDN Architecture](#); Issue 1.1; 2016
- 2.l Rahim Masoudi, AliGhaffari: [Software defined networks: A survey](#); Journal of Network and Computer Applications, Vol. 67, May 2016; DOI: 10.1016/j.jnca.2016.03.016
- 2.m Taimur Bakhshi: [State of the Art and Recent Research Advances in Software Defined Networking](#); Wireless Communications and Mobile Computing, Vol. 2017, Article ID 7191647; Jan 2017; DOI: 10.1155/2017/7191647
- 2.n Murat Karakus, Arjan Durrezi: [Quality of Service \(QoS\) in Software Defined Networking \(SDN\): A survey](#); Journal of Network and Computer Applications, Vol. 80, Feb 2017; DOI: 10.1016/j.jnca.2016.12.019
- 2.o Mehmet Fatih Tuysuz, Zekiye Kubra Ankarali, Didem Gözüpek: [A survey on energy efficiency in software defined networks](#); Computer Networks, Vol. 113, Feb 2017; DOI: 10.1016/j.comnet.2016.12.012
- 2.p Sanjev Singh, Rakesh Kumar Jha: [A Survey on Software Defined Networking: Architecture for Next Generation Network](#), Journal of Network and Systems Management, 2017, Vol. 25, DOI 10.1007/s10922-016-9393-9
- 2.q Fetia Bannour, Sami Souihi, Abdelhamid Mellouk: [Distributed SDN Control: Survey, Taxonomy and Challenges](#); IEEE Communications Surveys and Tutorials, 2017, DOI 10.1109/COMST.2017.2782482
- 2.r Yustus Eko Oktian, SangGon Lee, HoonJae Lee, JunHuy Lam: [Distributed SDN controller system: A survey on design choice](#); Computer Networks, Vol. 121, Jul 2017; DOI: 10.1016/j.comnet.2017.04.038
- 2.s Sibylle Schallera, Dave Hoodb: [Software defined networking architecture standardization](#); Computer Standards & Interfaces, Vol. 54, 2017; DOI: 10.1016/j.csi.2017.01.005
- 2.t Michel S. Bonfim, Kelvin L. Dias, Stenio F. L. Fernandes: [Integrated NFV/SDN Architectures: A Systematic Literature Review](#); Jan 2018; arXiv:1801.01516v1

- 2.u Rashid Amin, Martin Reisslein, Nadir Shah: [Hybrid SDN Networks: A Survey of Existing Approaches](#); IEEE Communications Surveys & Tutorials, Vol. 20(4), May 2108; DOI: 10.1109/COMST.2018.2837161
- 2.v Anatol Badach: [SDN – Software Defined Networking](#), In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Mai 2020
- 2.w Roaa Shubbar, Mohammad Alhisnawi, Aladdin Abdulhassan, Mahmood Ahmadi: [A Comprehensive Survey on Software-Defined Network Controllers](#); in Book: Next Generation of Internet of Things; Jan 2021; DOI: 10.1007/978-981-16-0666-3\_18
- 2.x Ozgur Yurekten, Mehmet Demirci: [SDN-based cyber defense: A survey](#); Future Generation Computer Systems, Vol. 115, Feb 2021; DOI: 10.1016/j.future.2020.09.006

### 18.2.1 Software-Defined WANs (SD-WANs)

Das Konzept von SDN kann zur flexiblen Gestaltung und zum Management privater WANs eingesetzt werden, um diese schnell an aktuelle Anforderungen, z.B. im Hinblick auf die Erfüllung von QoS (*Quality of Service*) und Garantie der Sicherheit, anpassen zu können. In diesem Zusammenhang spricht man von *Software-Defined WANs* (SD-WANs). Ein SD-WAN kann vereinfacht als Software-basierte Lösung für WANs angesehen werden. Zum Einrichten eines SD-WAN für den Transport von IP-Datenpaketen können unterschiedliche Netzwerktechnologien eingesetzt werden. Dabei erfolgt die Konfiguration und Steuerung der Funktionen und Leistungsmerkmale über eine oder mehrere Software-Instanzen innerhalb einer speziellen, den Hardware-Komponenten übergeordneten SD-WAN Control Plane. Für weitere Information über SD-WANs siehe:

Intelligent  
Integration von  
WANs

- 2.1.a Happiest Minds Technologies Pvt. Ltd.; Author: Purnendu: [SDWAN: Re-architecting WAN with Software Defined Networking](#)
- 2.1.b CATO-Networks: [MPLS, SD-WAN, Internet, and Cloud Network; Understanding the Trade-offs for Your Next Generation WAN](#)
- 2.1.c pwc: [SD-WAN for service providers; Threat or opportunity?](#)
- 2.1.d ONUG-SD-WAN-WG-Whitepaper: [Software-Defined WAN Use Case](#); Oct 2014
- 2.1.d Sanjay Uppal, Steve Woo, Dan Pitt, Lee Doyle (Special Foreword): [Software Defined WAN For Dummies](#); John Wiley & Sons, 2015, ISBN: 978-1-119-101482
- 2.1.e MEF Forum: [Understanding SD-WAN Managed Services: Service Components, MEF LSO Reference Architecture and Use Cases](#), Jul 2017
- 2.1.f Fan Gu: [SD-WAN Strategy to Address Key Trends and Scalability](#); IEEE Softwarization, Sep 2017
- 2.1.g Juniper Networks [Contrail SD-WAN Design & Architecture Guide](#); 2018

- 2.1.h Rodolfo Alvizu, et al.: [Comprehensive Survey on T-SDN: Software-Defined Networking for Transport Networks](#); IEEE Communications Surveys & Tutorials, Vol. 19(4), Jun 2017; DOI: 10.1109/COMST.2017.2715220

## 18.2.2 Software-Defined Optical Networking (SDON)

SDON als Ersatz für Signalisierungsprotokolle

Ein wichtiges Merkmal von SDN ist die logische Trennung der *Data Plane* mit diversen Systemkomponenten zur Datenübermittlung von der *Control Plane* mit Systemkomponenten zur Ansteuerung von Systemkomponenten innerhalb der Data Plane. Diese Besonderheit von SDN ist insbesondere in optischen Netzen anzutreffen, in denen optische Switches und optische Multiplexer eine Data Plane bilden, zu deren Ansteuerung ein separates 'nicht-optisches' IP-Netz mit einem speziellen *Signalisierungsprotokoll* zwecks Auf- und Abbau optischer Verbindungen erforderlich ist. Dieses Merkmal prädestiniert optische Netze in besonderer Weise für die Anwendung der SDN-Technologie. Kommt SDN beim Aufbau optischer Netze zum Einsatz, wird von *Software-Defined Optical Networking* (SDON) gesprochen.

Die grundlegende Idee von SDON illustriert Bild 9545 in [2.2.f]. Für Näheres über SDON sei verwiesen auf:

- 2.2.a Akhilesh Thyagaturu, Anu Mercian, Michael P. McGarry, Martin Reisslein, Wolfgang Kellerer: [Software Defined Optical Networks \(SDONs\): A Comprehensive Survey](#); IEEE Communications Surveys & Tutorials, Vol. 18, Issue 4, Fourthquarter 2016
- 2.2.b Yuan Cao et al.: [Resource allocation in software-defined optical networks secured by quantum key distribution](#); Opto-Electronics and Communications Conference (OECC) and Photonics Global Conference (PGC), Jul/Aug 2017
- 2.2.c Rodolfo Alvizu, et al.: [Comprehensive Survey on T-SDN: Software-Defined Networking for Transport Networks](#); IEEE Communications Surveys & Tutorials, Vol. 19, No. 4, 2017
- 2.2.d Víctor López, Rodrigo Jiménez, Óscar González de Dios, Juan Pedro Fernández-Palacios: [Control plane architectures for elastic optical networks](#); IEEE/OSA Journal of Optical Communications and Networking, Vol. 10, Issue 2, Feb 2018
- 2.2.e Wei Li, Zhe Yang, Weihua Zhao, Zhengwei Qi, Fei Liu: [A Review of Research on Software-Defined Optical Network](#); 2019 International Conference on Intelligent Transportation, Big Data & Smart City, Jan 2019
- 2.2.f Anatol Badach: [SD-WAN Software Defined Wide Area Network](#); In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Feb 2021
- 2.2.g Wang Tong, Azhar Hussain, Wang Xi Bo, Sabita Maharjan: [Artificial Intelligence for Vehicle-to-Everything: A Survey](#); IEEE Access, Vol. 7, Jan 2019; DOI: 10.1109/ACCESS.2019.2891073

### 18.2.3 Software-Defined Data Centers (SDDCs)

Die Virtualisierung von Hard- und Software-Ressourcen im Datacenter führt zur Entstehung virtueller Datacenter. Ein virtuelles Datacenter (*Virtual Data Center*, VDC) kann aus einer vollständig virtualisierten, isolierten und verteilten Computing-Infrastruktur bestehen. Dies bedeutet, dass die wesentlichen funktionellen Komponenten dieser Infrastruktur virtualisiert und als *Data Center Services* (DC Services) eingerichtet werden können. Die hauptsächlichen Bausteine von DC Services sind: Netzwerk-Virtualisierung, Storage-Virtualisierung und Server-Virtualisierung. In einem physischen Datacenter können somit mehrere voneinander isolierte, dem individuellen Bedarf von Kunden angepasste virtuelle Datacenter eingerichtet werden. Das dem Konzept von SDN grundlegende Prinzip eignet sich ideal zur flexiblen Gestaltung solcher Services. Beim Einsatz der Idee von SDN zwecks der Bereitstellung virtueller Datacenter spricht man von *Software-Defined Data Centers* (SDDCs). Ein VDC kann somit als SDDC bezeichnet werden. Für Näheres über SDDCs sei auf die folgende Literatur verwiesen:

[SD Data Centers](#)

- 2.3.a Distributed Management Task Force, Inc. (DMTF): [Software Defined Data Center \(SDDC\) Definition](#); Document Identifier: DSP-IS0501; 2015-11-23; Version: 1.0.0
- 2.3.b Dell Inc.: [The Future of the Data Center is Software Defined](#); Mar 2016
- 2.3.c Jeremy van Doorn: [Software Defined Data Centers Network Virtualization & Security](#)
- 2.3.d M. Gharbaoui, B. Martini, D. Adami, S. Giordano, P. Castoldi: [Cloud and network orchestration in SDN data centers: Design principles and performance evaluation](#); Computer Networks, Vol. 108, Oct 2016; DOI: 10.1016/j.comnet.2016.08.029
- 2.3.e Guan Xu, Bin Dai, Benxiong Huang, Jun Yang, Sheng Wen: [Bandwidth-aware energy efficient flow scheduling with SDN in data center networks](#); Future Generation Computer Systems, Vol. 68, Mar 2017; DOI: 10.1016/j.future.2016.08.024
- 2.3.f Hong Zhong, Yaming Fang, Jie Cui: [LBBSRT: An efficient SDN load balancing scheme based on server response time](#); Future Generation Computer Systems, Vol. 68, Mar 2017; DOI: 10.1016/j.future.2016.10.001
- 2.3.g Bin Dai, Guan Xu, Bengxiong Huang, Peng Qin, Yang Xu: [Enabling network innovation in data center networks with software defined networking: A survey](#), Journal of Network and Computer Applications, Vol. 94, Sep 2017; DOI: 10.1016/j.jnca.2017.07.004
- 2.3.h VMware: [Architecture and Design: VMware Validated Design for Software-Defined Data Center 4.2](#); Feb 2018

### 18.2.4 Software-Defined IoT (SD-IoT)

Das Konzept von SDN (siehe zum Vergleich die Abbildungen 9766 bis 9769 in Quelle [2.4h]) hat eine ausgesprochen große Bedeutung im IoT, denn insbesondere in IoT-

[IoT Services](#)



Clouds können spezielle, sog. SDN-Controller eingesetzt werden, um SDN-enabled Access Gateways an der Internet Edge entsprechend der aktuell geltenden Anforderungen (z.B. in Bezug auf Sicherheit) mittels einer Cloud über das Internet schnell zu konfigurieren [Abb. 17.1-9]. Darüber hinaus soll das IoT einer enorm großen Menge auf der Erdoberfläche verteilter Geräte (Sensoren, Aktuatoren) das Sammeln und somit die Verarbeitung von Echtzeitinformationen ermöglichen, was dazu führt, dass diese zur Bereitstellung neuer intelligenter IoT Services genutzt werden können. Beim Einsatz von SDN zur Bereitstellung intelligenter IoT Services spricht man von *Software-Defined IoT* (SD-IoT). Für weitere Informationen über SD-IoT siehe:

- 2.4.a T. Ninikrishna, Sutapa Sarkar, Richa Tengshe, Mahesh K. Jha, Laxmi Sharma, V. K. Daliya, Sudhir K. Routray: [Software defined IoT: Issues and challenges](#); International Conference on Computing Methodologies and Communication, Jul 2017; DOI: 10.1109/ICCMC.2017.8282560
- 2.4.b Tryfon Theodorou, Lefteris Mamatras: [Software defined topology control strategies for the Internet of Things](#); IEEE Conference on Network Function Virtualization and Software Defined Networks (NFV-SDN), Nov 2017; DOI: 10.1109/NFV-SDN.2017.8169884
- 2.4.c Samaresh Bera, Sudip Misra, Athanasios V. Vasilakos: [Software-Defined Networking for Internet of Things: A Survey](#); IEEE Internet of Things Journal, Vol. 4(6), Dec 2017; DOI: 10.1109/JIOT.2017.2746186
- 2.4.d Pritish Mishra, Deepak Puthal, Mayank Tiwary, Saraju P. Mohanty: [Software Defined IoT Systems: Properties, State of the Art, and Future Research](#); IEEE Wireless Communications, Vol. 26, Issue 6, Dec 2019; DOI: 10.1109/MWC.001.1900083
- 2.4.e Abdullah Al Hayajneh, Md Zakirul Alam Bhuiyan, Ian McAndrew: [Improving Internet of Things \(IoT\) Security with Software-Defined Networking \(SDN\)](#); Computers, Vol 9, Feb 2020
- 2.4.f Iqbal Alam, et al.: [A Survey of Network Virtualization Techniques for Internet of Things Using SDN and NFV](#); ACM Computing Surveys, Vol 53, Apr 2020
- 2.4.g Wajid Rafique, Lianyong Qi, Ibrar Yaqoob, et al.: [Complementing IoT Services through Software Defined Networking and Edge Computing: A Comprehensive Survey](#); IEEE Communications Surveys & Tutorials (Early Access), May 2020
- 2.4.h Anatol Badach: [SD-IoT Software Defined Internet of Things](#), In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Oct 2020

### 18.2.5 Wireless Software-Defined Networking

#### Wireless SD Networking

Die grundlegende, auf der Trennung zwischen der *Network Plane* und der *Control Plane* in Netzwerken beruhende Idee von SDN [Abb. 12.1-3] eignet sich ideal für eine neue Gestaltung der Mobilität im IoT. In diesem Zusammenhang spricht man von *Wireless SD Networking*. Insbesondere die SDN-Idee bei der Integration verschiedener Ad-hoc Networks wie z.B. MANET (*Mobile Ad-hoc-NETwork*), VANET

(*Vehicle Ad-hoc-NETwork*) und FANET (*Flying Ad-hoc Network*) in das IoT kann die Bereitstellung von intelligenten IoT Services ermöglichen. Für weitere Informationen über Wireless SD Networking siehe:

- 2.5.a Ian Ku, et al.: [Towards Software-Defined VANET: Architecture and Services](#); 13th Annual Mediterranean Ad Hoc Networking Workshop (MED-HOC-NET), Jun 2014; DOI: 10.1109/MedHocNet.2014.6849111
- 2.5.b Nachikethas A. Jagadeesan, Bhaskar Krishnamachari: [Software-defined networking paradigms in wireless networks: A survey](#); ACM Computing Surveys, Vol. 47(2), Jan 2015
- 2.5.c Bin Cao, Fang He, Yun Li, Chonggang Wang, Wenqiang Lang: [Software defined virtual wireless network: framework and challenges](#); IEEE Network, Vol. 29(4), Jul-Aug 2015; DOI: 10.1109/MNET.2015.7166185
- 2.5.d S. V. Manisekaran, R. Venkatesan: [An analysis of software-defined routing approach for wireless sensor networks](#); Computers & Electrical Engineering, Vol. 56, Nov 2016
- 2.5.e Yanwen Wang, Hainan Chen, Xiaoling Wu, Lei Shu: [An energy-efficient SDN based sleep scheduling algorithm for WSNs](#); Journal of Network and Computer Applications, Vol. 59, Jan 2016; DOI: 10.1016/j.jnca.2015.05.002
- 2.5.f Israat Tanzeena Haque, Nael Abu-Ghazaleh: [Wireless Software Defined Networking: A Survey and Taxonomy](#); IEEE Communications Surveys & Tutorials, Vol. 18(4), May 2016; DOI: 10.1109/COMST.2016.2571118
- 2.5.g Hans C. Yu, Giorgio Quer, Ramesh R. Rao: [Wireless SDN mobile ad hoc network: From theory to practice](#); 2017 IEEE International Conference on Communications (ICC), May 2017; DOI: 10.1109/ICC.2017.7996340
- 2.5.h Junfeng Wang, et al.: [A software defined network routing in wireless multihop network](#); Journal of Network and Computer Applications, Vol. 85, May 2017; DOI: 10.1016/j.jnca.2016.12.007
- 2.5.i Manisha Chahal, et al.: [A Survey on software-defined networking in vehicular ad hoc networks: Challenges, applications and use cases](#); Sustainable Cities and Society, Vol. 35, Nov 2017
- 2.5.j Afsane Zahmatkesh; Thomas Kunz: [Software Defined Multihop Wireless Networks: Promises and Challenges](#); Journal of Communications and Networks, Vol. 19(6), Dec 2017; DOI: 10.1109/JCN.2017.000094
- 2.5.k Márcio L. F. Miguel, et al.: [A CoAP Based Control Plane for Software Defined Wireless Sensor Networks](#); Journal of Communications and Networks, Vol. 19(6), Dec 2017; DOI: 10.1109/JCN.2017.000095
- 2.5.l Konstantinos Poularakis, George Iosifidis, Leandros Tassiulas: [SDN-enabled Tactical Ad Hoc Networks: Extending Programmable Control to the Edge](#); arXiv:1801.02909v1, Jan. 2018
- 2.5.m Paolo Bellavista, Alessandro Dolci, Carlo Giannelli: [MANET-oriented SDN: Motivations, Challenges, and a Solution Prototype](#); 2018 IEEE 19th International Symposium on 'A World of Wireless, Mobile and Multimedia Networks' (WoWMoM), Jun 2018; DOI: 10.1109/WoWMoM.2018.8449805

## 18.2.6 Software-Defined Internet of Vehicles (SD-IoV)

Rekursiv-  
hierarchische  
Architektur

Die Unterstützung der Mobilität verschiedener Einrichtungen ist im IoT von großer Bedeutung. Dies gilt insbesondere für die Steuerung und Kontrolle mobiler Fahrzeuge unterschiedlicher Art im *Internet of Vehicles* (IoV). Um Mobilität mithilfe von SDN zu unterstützen, muss das Konzept eine besondere, rekursiv organisierte hierarchische Art der Steuerung mobiler Einrichtungen im IoT ermöglichen. Hierfür muss es nach einer rekursiv-hierarchischen SDN-Architektur organisiert werden. Bild 9548 in [2.4.h] illustriert die Idee dieser SDN-Architektur. Für Näheres über SD-IoV siehe:

- 2.6.a Saif Al-Sultan, Moath M. Al-Doori, Ali H. Al-Bayatti, Hussien Zedan: [A comprehensive survey on vehicular Ad Hoc network](#); Journal of Network and Computer Applications, Vol. 37, Jan 2014
- 2.6.b Fangchun Yang, Shangguang Wang, Jinglin Li, Zhihan Liu, Qibo Sun: [An overview of Internet of Vehicles](#); China Communications, Vol. 11, Issue 10, Oct 2014
- 2.6.c Chen Jiacheng, Zhou Haibo et al.: [Software defined Internet of vehicles: architecture, challenges and solutions](#); Journal of Communications and Information Networks; Vol. 1, Issue 1, Jun 2016
- 2.6.d Omprakash Kaiwartya, Abdul Hanan Abdullah et al.: [Internet of Vehicles: Motivation, Layered Architecture, Network Model, Challenges, and Future Aspects](#); IEEE Access, Special Section on Future Networks, Architectures, Protocols and Applications, Vol. 4, Sep 2016
- 2.6.e Sergio Correia, Azzedine Boukerche, Rodolfo I. Meneguette: [An Architecture for Hierarchical Software-Defined Vehicular Networks](#); IEEE Communications Magazine, Vol. 55, Jul 2017
- 2.6.f Eugen Borcoci, Serban Obreja, Marius Vochin: [Internet of Vehicles Functional Architectures - Comparative Critical Study](#); AFIN 2017 : The Ninth International Conference on Advances in Future Internet, Sep 2017
- 2.6.g Yaomin Zhang, Haijun Zhang, et al.: [Software-Defined and Fog-Computing-Based Next Generation Vehicular Networks](#); IEEE Communications Magazine, Vol. 56, Sep 2018
- 2.6.h Muhammad Tahir Abbas, Afaq Muhammad, Wang-Cheol Song: [SD-IoV: SDN enabled routing for internet of vehicles in road-aware approach](#); Journal of Ambient Intelligence and Humanized Computing, May 2019
- 2.6.i Lionel Nkenyereye, Lewis Nkenyereye, et al.: [Software-Defined Network-Based Vehicular Networks: A Position Paper on Their Modeling and Implementation](#); Sensors, Vol. 19, Issue 17, Aug 2019
- 2.6.j Shiva Raj Pokhre: [Software Defined Internet of Vehicles for Automation and Orchestration](#); IEEE Transactions on Intelligent Transportation Systems, Vol. 22, Issue 6, Jun 2021; DOI: 10.1109/TITS.2021.3077363
- 2.6.k Anteneh S. Al-Heety, Zahriladha Zakaria, et al.: [A Comprehensive Survey: Benefits, Services, Recent Works, Challenges, Security, and Use Cases for SDN-VANET](#); IEEE Access, Vol. 8, May 2020

## 18.3 Network Function Virtualization (NFV)

VM-based VNFs

Die Virtualisierung von Rechnern und deren Bereitstellung auf speziellen leistungsfähigen Wirt-Servern in Form von sog. *Virtual Machines* (VMs) sowie *Virtual Networking* als Vernetzung von sogar auf unterschiedlichen Wirt-Servern untergebrachten VMs sind in der Netzwerkwelt bereits geläufig. Und wenn man schon Rechner und ihre Vernetzung virtualisiert, so bietet es sich an, im folgenden Schritt verschiedene, auf der Basis von VMs realisierte Netzwerkkomponenten (Router, Switches, Firewalls usw.) und ihre Vernetzung, d.h. verschiedene Netzwerkfunktionen (*Network Functions*), als Softwarekomponenten in virtualisierter Form bereitzustellen. Diese Idee hat zu *Network Functions Virtualisation* (NFV) geführt, bei der man von *virtualisierten Netzwerkfunktionen* spricht. Sie werden kurz VNFs (*Virtualised Network Functions*) genannt. Im Zusammenhang mit NFV sind die Networking Trends *Software-Defined VNFs Networking* (*SD VNFs Networking*), *Service Function Chaining* (SFC), *VNFs Management and Orchestration* und *Network Slicing* hervorzuheben. Für Näheres über NFV siehe:

- 3.a ETSI GS NFV 001: [Network Functions Virtualisation \(NFV\); Use Cases](#); Oct 2013
- 3.b ETSI GS NFV-SEC 001 - V1.1.1: [Network Functions Virtualisation \(NFV\); NFV Security; Problem Statement](#); Oct 2014
- 3.c ETSI GS NFV 002 V1.2.1: [Network Functions Virtualisation \(NFV\) - Architectural Framework](#); Dec 2014
- 3.d ETSI GS NFV-MAN 001 V1.1.1: [Network Functions Virtualisation \(NFV\) - Management and Orchestration](#); Dec 2014
- 3.e ETSI GS NFV-INF 001 - V1.1.1: [Network Functions Virtualisation \(NFV\); Infrastructure Overview](#); Jan 2015
- 3.f Anatol Badach: [NFV – Network Functions Virtualisation](#); In book: *Protokolle und Dienste der Informationstechnologie*, WEKA-Verlag, Editor: Heinz Schulte; Jan 2015, DOI 10.13140/RG.2.1.4701.2562
- 3.g Rashid Mijumbi, et al.: [Network Function Virtualization: State-of-the-Art and Research Challenges](#); IEEE Communications Surveys & Tutorials, Vol. 18(1), Sep 2016; DOI: 10.1109/COMST.2015.2477041
- 3.h Eugen Borcoci: [Network Function Virtualization and Software Defined Networking Cooperation](#); InfoSys 2015 Conference, May 2015
- 3.i Rashid Mijumbi, et al.: [Network Function Virtualization: State-of-the-Art and Research Challenges](#); IEEE Communications Surveys & Tutorials, Vol. 18(1), Sep 2016; DOI: 10.1109/COMST.2015.2477041
- 3.j ETSI GR NFV 001 - V1.2.1: [Network Functions Virtualisation \(NFV\); Use Cases](#); May 2017
- 3.k Shariq Haseeb, et al.: [Network Function Virtualization \(NFV\) based architecture to address connectivity, interoperability and manageability challenges in Internet of Things \(IoT\)](#); IOP Conf. Series: Materials Science and Engineering 260 (2017); DOI: 10.1088/1757-899X/260/1/012033

- 3.l Michel S. Bonfim, Kelvin L. Dias, Stenio F. L. Fernandes: [Integrated NFV/SDN Architectures: A Systematic Literature Review](#); Jan 2018; arXiv:1801.01516v1
- 3.m U. Rehman, Rui L. Aguiar, João Paulo Barraca: [Network Functions Virtualization: The Long Road to Commercial Deployment](#); IEEE Access, Vol. 7, May 2019; DOI: 10.1109/ACCESS.2019.2915195
- 3.n Tianzhu Zhang, Han Qiu, Leonardo Linguaglossa, Walter Cerroni, Paolo Giaccone: [NFV Platforms: Taxonomy, Design Choices and Future Challenges](#); IEEE Transactions on Network and Service Management, Vol. 18, Issue 1, Mar 2021, DOI: 10.1109/TNSM.2020.3045381

### 18.3.1 Software-Defined VNFs Networking

#### SD VNFs Networking

Von großer Bedeutung ist die Tatsache, dass die Konzepte SDN und NFV sich sowohl ähneln als auch ideal ergänzen. Vor allem der Orchestrator bei SDN entspricht der Funktion nach vollkommen dem Orchestrator bei NFV. Folglich können einige Ideen und somit auch Funktionskomponenten von SDN für NFV übernommen werden, was zu SD VNFs Networking führt. Für Näheres darüber siehe:

- 3.1.a Anatol Badach: [NVGRE – Network Virtualization using Generic Routing Encapsulation](#); In book: Protokolle und Dienste der Informationstechnologie, WEKA-Verlag, Editor: Heinz Schulte; Oct 2014, DOI 10.13140/RG.2.1.2872.8802
- 3.1.b ETSI GS NFV-SWA 001 - V1.1.1: [Network Functions Virtualisation \(NFV\); Virtual Network Functions Architecture](#); Dec 2014
- 3.1.c ETSI GS NFV 002 - V1.2.1: [Network Functions Virtualisation \(NFV\); Architectural Framework](#); Dec 2014
- 3.1.d ETSI GS NFV-EVE 005 - V1.1.1: [Network Functions Virtualisation \(NFV\); Ecosystem; Report on SDN Usage in NFV Architectural Framework](#); Dec 2015
- 3.1.e Lorena Isabel Barona López, et al.: [Trends on virtualisation with software defined networking and network function virtualisation](#); IET Networks, Vol. 4(5), Sep 2015; DOI: 10.1049/iet-net.2014.0117
- 3.1.f Jie Li, Eitan Altman, Corinne Touati: [A General SDN-based IoT Framework with NVF Implementation](#); ZTE Communications, ZTE Corporation, 2015, Vol. 13 (3)
- 3.1.g Yong Li, Min Chen: [Software-Defined Network Function Virtualization: A Survey](#); IEEE Access, Vol. 3, Dec 2015c DOI: 10.1109/ACCESS.2015.2499271
- 3.1.h Verizon: [Verizon Network Infrastructure Planning: SDN-NFV Reference Architecture](#); Version 1.0, Feb 2016
- 3.1.i Qiang Duan, Nirwan Ansari, Mehmet Toy: [Software-Defined Network Virtualization: An Architectural Framework for Integrating SDN and NFV for Service Provisioning in Future Networks](#); IEEE Network, Vol. 30(5), Sep 2016; DOI: 10.1109/MNET.2016.7579021

- 3.1.j Shariq Haseeb, et al.: [Network Function Virtualization \(NFV\) based architecture to address connectivity, interoperability and manageability challenges in Internet of Things \(IoT\)](#); IOP Conference Series: Materials Science and Engineering, Vol. 260, 2017
- 3.1.k Open Networking Foundation: [REFERENCE DESIGN: ONF TS-101: Trellis: NFV Fabric, Version 1.0](#); Mar 2019
- 3.1.l Michel S. Bonfim, Kelvin L. Dias, Stenio F. L. Fernandes: [Integrated NFV/SDN Architectures: A Systematic Literature Review](#); ACM Computing Surveys, Vol. 51, Issue 6, Nov 2019
- 3.1.m Partha Pratim Ray, Neeraj Kumar: [SDN/NFV architectures for edge-cloud oriented IoT: A systematic review](#); Computer Communications, Vol. 169, Mar 2021; DOI: 10.1016/j.comcom.2021.01.018
- 3.1.n Ziye Jia, Min Sheng, Jiandong Li, Di Zhou, Zhu Han: [VNF-Based Service Provision in Software Defined LEO Satellite Networks](#); IEEE Transactions on Wireless Communications, Vol. 20, Issue 9, Sep 2021; DOI: 10.1109/TWC.2021.3072155

### 18.3.2 Service Function Chaining (SFC)

Mit der Verfügbarkeit von Rechnern in Form von VMs eröffnen sich vollkommen neue Möglichkeiten, unterschiedlich an Geschäftsprozesse angepasste Netzwerkdienste spontan bereitzustellen. Denn auf der Basis von VMs können zur Einrichtung verschiedener komplexer Netzwerkdienste diverse Funktionskomponenten als virtuelle, standardisierte Netzwerkfunktionsmodule im Voraus für einen Einsatz vorbereitet und dann bei Bedarf als Softwarekomponenten ad hoc verfügbar gemacht werden. Sie werden kurz als VNFs (*Virtualised Network Functions*) bzw. auch als SFs (*Service Functions*) bezeichnet. Da die Realisierung jedes Netzwerkdienstes auf der Basis von durch virtualisierte Rechner erbrachte SFs oft zu einer Verkettung von SFs führt, spricht man in diesem Zusammenhang von *Service Function Chaining* (SFC). Unter SFC werden somit zahlreiche Konzepte und Lösungen zur Kooperation von hauptsächlich softwaremäßig realisierten SFs zwecks der Erbringung diverser Netzwerkdienste verstanden. Für weitere Information über SFC siehe:

Rekursive  
Vernetzung von  
VNFs

- 3.2.a ETSI GS NFV 002, V1.2.1: [Network Functions Virtualisation \(NFV\); Architectural Framework](#); Dec 2014
- 3.2.b Anatol Badach: [SFC Service Function Chaining](#); In book: Protokolle und Dienste der Informationstechnologie, WEKA-Verlag, Editor: Heinz Schulte; Jan 2015, DOI 10.13140/RG.2.1.4701.2562
- 3.2.c Barbara Martini, Federica Paganelli: [A Service-Oriented Approach for Dynamic Chaining of Virtual Network Functions over Multi-Provider Software-Defined Networks](#); Future Internet, Vol. 8(2), Jun 2016; DOI:10.3390/fi802002
- 3.2.d Deval Bhamare, Raj Jain, Mohammed Samaka, Aiman Erbad: [A survey on service function chaining](#); Journal of Network and Computer Applications, Vol. 75, Nov 2016; DOI: 10.1016/j.jnca.2016.09.001

- 3.2.e Janos Elek, David Jocha, Robert Szabo: [Network Function Chaining in DCs: the Unified Recurring Control Approach](#); Fourth European Workshop on Software Defined Networks, Oct 2015; DOI: 10.1109/EWSDN.2015.54
- 3.2.f Deval Bhamare, et al.: [Optimal virtual network function placement in multi-cloud service function chaining architecture](#); Computer Communications, Vol. 102, Apr 2017; DOI: 10.1016/j.comcom.2017.02.011
- 3.2.g Ahmed AbdelSalam, et al.: [Implementation of Virtual Network Function Chaining through Segment Routing in a Linux-based NFV Infrastructure](#), Apr 2017, arXiv:1702.05157v4
- 3.2.g Taixin Li, Huachun Zhou, Hongbin Luo: [A new method for providing network services: Service function chain](#); Nov 17; DOI: 10.1016/j.osn.2015.09.005
- 3.2.h Haruna Umar Adoga, Dimitrios P. Pezaros: [Network Function Virtualization and Service Function Chaining Frameworks: A Comprehensive Review of Requirements, Objectives, Implementations, and Open Research Challenges](#); Future Internet, Vol. 14, Issue 2, Feb 2022; DOI: 10.3390/fi14020059
- 3.2.i Hajar Hantouti, Nabil Benamar, Tarik Taleb: [Service Function Chaining in 5G & Beyond Networks: Challenges and Open Research Issues](#); IEEE Network, Vol. 34, Issue 4, Jul/Aug 2020, DOI: 10.1109/MNET.001.1900554
- 3.2.j MIRJALILY Ghasem, LUO Zhiqian: [Optimal Network Function Virtualization and Service Function Chaining: A Survey](#); Chinese Journal of Electronics, Vol. 27, No 4, Jul 2018; DOI:10.1049/cje.2018.05.008

### 18.3.3 VNFs Management and Orchestration

#### SDN Controller als Dirigent von VNFs

Zur Schaffung eines Network Services auf der Grundlage von VNFs werden in der Regel mehrere VNFs benötigt. Diese VNFs werden durch verschiedene VMs erbracht und können räumlich weit auseinanderliegen. Ein solcher Network Service stellt de facto eine aus mehreren räumlich verteilten VNFs bestehende 'Service-Komposition' dar. Solch eine Komposition ist mit einer von mehreren Musikern gespielten Musikkomposition vergleichbar. Eine VNF entspricht in diesem Fall einem Musiker. Wird die Komposition von mehreren Musikern gespielt, müssen sie dirigiert werden, es ist also ein Dirigent nötig. So ist es auch im Falle der VNFs, wenn mehrere zusammen agieren müssen, um einen Network Service zu erbringen. Als ihr 'Dirigent' fungiert dann ein SDN Controller. So entspricht die Bereitstellung von Network Services, die durch mehrere VNFs erbracht werden, weitgehend der Vorbereitung eines von mehreren Musikern gespielten Konzerts. Es wird daher eine Orchestrierung von VNFs (*VNFs Orchestration*) und von Network Services sowie ihres Management benötigt. Für weitere Details zum VNFs Management und Orchestration siehe:

- 3.3.a ETSI GS NFV-MAN 001, V1.1.1: [Network Functions Virtualisation \(NFV\); Management and Orchestration](#); Dec 2014
- 3.3.b Daniel King, et al.: [Network service orchestration standardization: A technology survey](#); Computer Standards & Interfaces, Vol. 54(4), Nov. 2017; DOI: 10.1016/j.csi.2016.12.006

- 3.3.c Charalampos Rotsos, et al.: [Network service orchestration standardization: A technology survey](#); Computer Standards & Interfaces, Vol. 54(4), Nov 2017; DOI: 10.1016/j.csi.2016.12.006
- 3.3.d 3GPP TS 28.531: [Management and orchestration of networks and network slicing; Provisioning](#)
- 3.3.e 3GPP TS 28.533: [Management and orchestration; Architecture framework](#)
- 3.3.f ETSI GS NFV-IFA 014 V2.4.1: [Network Functions Virtualisation \(NFV\) Release 2; Management and Orchestration; Network Service Templates Specification](#), Feb 2018
- 3.3.g Karamjeet Kaur, Veenu Mangat, Krishan Kumar: [A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture](#); Computer Networks, Vol 217, Nov 2022; DOI: 10.1016/j.comnet.2022.109281
- 3.3.h Karamjeet Kaur, Veenu Mangat, Krishan Kumar: [A review on Virtualized Infrastructure Managers with management and orchestration features in NFV architecture](#); Computer Networks, Vol 217, Nov 2022; DOI: 10.1016/j.comnet.2022.109281

### 18.3.4 Network Slicing

Man könnte sich einzelne virtuelle private Netzwerkinfrastrukturen im Datacenter als 'virtuelle Netzwerkscheiben' vorstellen, welche voneinander isoliert werden. Da die virtuellen Netzwerkscheiben als *Network Slices* bezeichnet werden, spricht man im Zusammenhang mit der Bildung von *Network Slicing*. *Network Slices* können dank der Orchestrierung von VNFs gebildet werden. Ihr Management erfolgt nach dem Prinzip von SDN. Auf der Basis von Network Slicing werden beispielsweise private mobile 5G-Netzwerke gebildet. Es ist zu erwarten, dass Network Slicing in der Netzwerkwelt zukünftig von fundamentaler Bedeutung sein wird. Für weitere Details über Network Slicing siehe:

Bildung virtueller  
'Netzscheiben'

- 3.4.a NGMN Alliance: [Description of Network Slicing Concept](#), Version 1.0, Jan 2016
- 3.4.b ETSI GR NFV-EVE 012, V3.1.1: [Network Functions Virtualisation \(NFV\) Release 3; Evolution and Ecosystem; Report on Network Slicing Support with ETSI NFV Architecture Framework](#); Dec 2017
- 3.4.c 3GPP TR 28.801, V15.1.0: [Study on management and orchestration of network slicing for next generation network \(Release 15\)](#); Jan 2018
- 3.4.d Alex Galis: [Perspectives on Network Slicing – Towards the New 'Bread and Butter' of Networking and Servicing](#); IEEE Softwarization, Jan 2018
- 3.4.e Luis M. Contreras, Diego R. López: [A Network Service Provider Perspective on Network Slicing](#); IEEE Softwarization, Jan 2018
- 3.4.f Daniele Ceccarelli, Young Lee, Huawei: [Transport Aspects of Network Slicing: Existing Solutions and Gaps](#); IEEE Softwarization, Jan 2018



- 3.4.g Huanzhuo Wu, et al.: [Network Slicing for Conditional Monitoring in the Industrial Internet of Things](#); IEEE Softwarization, Jan 2018
- 3.4.h Ibrahim Afolabi, Tarik Taleb, Konstantinos Samdanis, Adlen Ksentini, Hannu Flinck: [Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions](#); IEEE Communications Surveys & Tutorials, Vol. 20, Issue 3, Mar 2018; DOI: 10.1109/COMST.2018.2815638
- 3.4.i Ibrahim Afolabi, Tarik Taleb, Konstantinos Samdanis, Adlen Ksentini, Hannu Flinck: [Network Slicing and Softwarization: A Survey on Principles, Enabling Technologies, and Solutions](#); IEEE Communications Surveys & Tutorials, Vol. 20, Issue 3, Mar 2018; DOI: 10.1109/COMST.2018.2815638
- 3.4.j Sławomir Kukliński, et al.: [A reference architecture for network slicing](#); NET-SOFT 2018, 4th IEEE Conference on Network Softwarisation, Jun 2018
- 3.4.k Hao Jiang, Nakjung Choi, Marina Thottan, Jacobus Van der Merwe: [Fest-Net: A Flexible and Efficient Sliced Transport Network](#); IEEE 7th International Conference on Network Softwarization, Jul 2021, DOI: 10.1109/Net-Soft51509.2021.9492625

## 18.4 (Docker) Container Networking

Container  
Technologie als  
Virtualisierung  
auf Betriebs-  
systemebene

Die Bereitstellung von *Virtual Machines* (VMs) und auf der Grundlage von VNFs (*Virtualized Network Functions*) kann als eine Art Virtualisierung auf Hardwareebene angesehen werden. Eine VNF kann aber auch auf der Basis eines oder mehrerer Rechner/s eingerichtet werden, in dem/denen – sozusagen als 'Virtualisierung auf Betriebssystemebene' – die sog. *Container-Technologie* (CT) realisiert wird. Die Idee dieser Virtualisierungsart basiert darauf, dass in einem physischen Rechner mit seinem Betriebssystem, z.B. Linux, eine besondere Applikation installiert wird, die als virtualisiertes Betriebssystem mit Applikationen angesehen werden kann. Dabei können die Applikationen ihren Funktionen entsprechend gruppiert und in sog. (virtuellen) Containern 'untergebracht' werden. Man spricht in diesem Zusammenhang von *Container-basierter Virtualisierung*.

Mobilität von  
Containern mit  
Applikationen

Man könnte sich so ein virtualisiertes Betriebssystem mit seinen Applikationen als ein als *Docker* bezeichnetes Schiff mit seinen Containern vorstellen. Ein wichtiger Vorteil nicht-virtueller Container besteht darin, dass sie relativ einfach von einem Ort zum anderen, z.B. Schiff zu Schiff, bewegt werden können. Auch die Mobilität virtueller Container mit Applikationen kann einfach erreicht werden, indem man diesem – auf einem Docker mit einer offiziellen IP-Adresse – eine private IP-Adressen zuweist. Auf jedem Docker kann das NAT-Verfahren (*Network Address Translation*) realisiert werden [Abschnitt 6.3]. Durch dieses kann jeder virtuelle Container mit seiner privaten IP-Adresse auf jedem Docker neu installiert werden und dabei – auch häufig – seine private IP-Adresse erhalten bleiben. In Folge kann jeder Container mit seiner privaten IP-Adresse von einem physischen Rechner auf einen anderen bewegt werden. Dies bedeutet, dass eine uneingeschränkte Mobilität von Containern möglich ist, in denen

verschiedene VNFs durch die in ihnen enthaltenen Applikationen realisiert werden können.

Die Mobilität von Containern trägt dazu bei, dass VNFs bei der Realisierung der Container-Technologie in einer Cloud mithilfe der Datenübermittlung von einer Cloud in andere transportiert werden können. Container Networking liegt insbesondere den Networking Trends *Container-based Network Services*, *Cloud Computing Containerization*, *Mobile VNFs Networking* und *Containerized IoT Services* zugrunde. Für weitere Informationen zum Thema Container Networking siehe:

- 4.a Martin Fowler: [Microservices Resource Guide](#)
- 4.b David Bernstein: [Containers and Cloud: From LXC to Docker to Kubernetes](#); IEEE Cloud Computing, Vol. 1(3), Sep 2014; DOI: 10.1109/MCC.2014.51
- 4.c Di Liu, Libin Zhao: [The research and implementation of cloud computing platform based on docker](#); 11th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP), Dec 2014; DOI: 10.1109/ICCWAMTIP.2014.7073453
- 4.d Richard Cziva, Simon Jouet, Kyle J. S. White, Dimitrios P. Pazaros: [Container-based Network Function Virtualization for Software-Defined Networks](#); 2015 IEEE Symposium on Computers and Communication (ISCC), Jul 2015 DOI: 10.1109/ISCC.2015.7405550
- 4.e Jason Anderson, et al.: [Performance considerations of network functions virtualization using containers](#); International Conference on Computing, Networking and Communications (ICNC), Feb 2016; DOI: 10.1109/ICNC.2016.7440668
- 4.f Roberto Morabito: [Virtualization on Internet of Things Edge Devices With Container Technologies: A Performance Evaluation](#); IEEE Access, Vol. 5, May 2017; DOI: 10.1109/ACCESS.2017.2704444
- 4.g Richard Cziva, Dimitrios P. Pazaros: [Container Network Functions: Bringing NFV to the Network Edge](#); IEEE Communications Magazine Vol. 55(6), Jun 2017; DOI: 10.1109/MCOM.2017.1601039
- 4.h Phil Lowden: [Cisco Container Networking Overview and Roadmap](#); Nov 2017
- 4.i VMware: [CONTAINERS AND CONTAINER NETWORKING: For Network Engineers](#); Jan 2018
- 4.j Jae-Geun Cha, Sun Wook Kim: [Design and Evaluation of Container-based Networking for Low-latency Edge Services](#); 2021 International Conference on Information and Communication Technology Convergence (ICTC), Oct 2021; DOI: 10.1109/ICTC52510.2021.9620212
- 4.k Sridhar K. N. Rao. Federica Paganelli, Al Morton: [Benchmarking Kubernetes Container-Networking for Telco Usecases](#); IEEE Global Communications Conference, Dec 2021; DOI: 10.1109/GLOBECOM46510.2021.9685803

### 18.4.1 Container-based Network Services

Grundlagen für verteilte Anwendungsarchitekturen

In einem Container können mehrere Applikationen enthalten sein, von denen jede eine eigenständige Ausführungsumgebung hat und dadurch isoliert von anderen Applikationen ausgeführt werden kann. Die voneinander isolierten Applikationen können dazu dienen, verschiedene Netzwerkfunktionen, sog. VNFs, zu kreieren. Daraufhin können mithilfe von VNFs bestimmte Netzwerkdienste erbracht werden. Sie werden als *Container-based Network Services* oder *Microservices* bezeichnet. Für weitere Informationen darüber siehe:

- 4.1.a Martin Šušal: [Container service chaining](#)
- 4.1.b Roberto Morabito, Nicklas Beijar: [Enabling Data Processing at the Network Edge through Lightweight Virtualization Technologies](#); IEEE International Conference on Sensing, Communication and Networking (SECON Workshops); Jun 2016; DOI: 10.1109/SECONW.2016.7746807
- 4.1.c Sergio Livi, et al.: [Container-Based Service Chaining: A Performance Perspective](#); 5th IEEE International Conference on Cloud Networking (Cloudnet), Oct 2016; DOI: 10.1109/CloudNet.2016.51
- 4.1.d Kuljeet Kaur, Tanya Dhand, Neeraj Kumar, Sherali Zeadally: [Container-as-a-Service at the Edge: Tradeoff between Energy Efficiency and Service Availability at Fog Nano Data Centers](#); IEEE Wireless Communications, Vol. 24(3), Jun 2017; DOI: 10.1109/MWC.2017.1600427
- 4.1.e Kyungwoon Lee, Youngpil Kim, Chuck Yoo: [The Impact of Container Virtualization on Network Performance of IoT Devices](#); Mobile Information Systems, Vol. 2018, Article ID 9570506, May 2018; DOI: 10.1155/2018/9570506
- 4.1.f Cisco: [Cloud-Native Network Functions \(CNFs\), White Paper](#); Jun 2018; Document ID:1529344804993194
- 4.1.g Qi Zhang, Ling Liu, Calton Pu, Qiwei Dou, Liren Wu, Wei Zhou: [Comparative Study of Containers and Virtual Machines in Big Data Environment](#); arXiv:1807.01842v1, Jul 2018

### 18.4.2 Cloud Computing Containerization

Container as a Service (CaaS)

Sowohl in einem physischen als auch in einem virtualisierten Rechner, d.h. auf einer Virtual Machine (VM), können mehrere Container mit diversen Microservices eingerichtet werden. Auf der Basis der beiden Rechnerarten, in denen verschiedene *Container-based Network Services* in Form von VNFs verfügbar sind, können sog. *Clouds* gebildet werden. Infolgedessen kann die Container Technologie auch in Clouds realisiert werden. Man spricht in diesem Zusammenhang von *Cloud Computing Containerization*. Für Näheres darüber siehe:

- 4.2.a Claus Pahl, Brian Lee: [Containers and Clusters for Edge Cloud Architectures - A Technology Review](#); The 3rd International Conference on Future Internet of Things and Cloud (FiCloud 2015); Aug 2015; DOI: 10.1109/FiCloud.2015.35

- 4.2.b Hui Kang, Michael Le, Shu Tao: [Container and Microservice Driven Design for Cloud Infrastructure DevOps](#), IEEE International Conference on Cloud Engineering (IC2E), Apr 2016; DOI: 10.1109/IC2E.2016.26
- 4.2.c Nane Kratzke: [A Brief History of Cloud Application Architectures](#); Applied Sciences, Vol. 8(8), Aug 2018, DOI: 10.3390/app8081368
- 4.2.d ETSI GS NFV-EVE 011 V3.1.1 (2018-10): [Network Functions Virtualisation \(NFV\) Release 3; Virtualised Network Function; Specification of the Classification of Cloud Native VNF Implementations Disclaimer](#)
- 4.2.e Anshita Malviya, Rajendra Kumar Dwivedi: [A Comparative Analysis of Container Orchestration Tools in Cloud Computing](#); 9th International Conference on Computing for Sustainable Global Development (INDIACom), Mar 2022; DOI: 10.23919/INDIACom54597.2022.9763171
- 4.2.f Sanjay Hardikar, Pradeep Ahirwar, Sameer Rajan: [Containerization: Cloud Computing based Inspiration Technology for Adoption through Docker and Kubernetes](#); Second International Conference on Electronics and Sustainable Communication Systems (ICESC), Aug 2021; DOI: 10.1109/ICESC51422.2021.9532917

### 18.4.3 Mobile VNFs Networking

Von einem Container in einem physischen bzw. in einem virtuellen Rechner können mehrere VNFs erbracht werden. Jedem Container kann eine private IP-Adresse zugewiesen werden. Dadurch entsteht die Möglichkeit, dass jeder Container mit einer privaten IP-Adresse von einem Docker, quasi einem 'virtuellen Schiff', zu einem anderen transportiert werden kann. Diese Mobilität von Containern mit VNFs schließt die *Mobilität von VNFs* mit ein. Verschiedene mobile VNFs können dank der Realisierung des Mobile VNFs Networking untereinander auf eine Weise vernetzt werden, dass die Einrichtung eines Mobile Network Service möglich ist. Für weitere Informationen darüber siehe:

[Mobile Virtual Network Services](#)

- 4.3.a Rajendra Chayapathi, Syed Farrukh Hassan, Paresh Shah: [Network Functions Virtualization \(NFV\) with a Touch of SDN](#); Addison-Wesley, Nov 2016; ISBN-13: 978-0-13-446305-6
- 4.3.b Ajay Simha: [Red Hat Reference Architecture Series: NFV reference architecture for deployment of mobile networks](#); Version 1.3, Jan 2017
- 4.3.c Project: H2020-ICT-2014-2 5G NORMA [Definition and specification of connectivity and QoE/QoS management mechanisms](#); Final Report, Jun 2017
- 4.3.3 Ana Hermosilla, Alejandro Molina Zarca, Jorge Bernal Bernabe, Jordi Ortiz, Antonio Skarmeta: [Security Orchestration and Enforcement in NFV/SDN-Aware UAV Deployments](#); IEEE Access, Vol. 8, Jul 2020; DOI: 10.1109/ACCESS.2020.3010209

## 18.4.4 Containerized IoT Services

Fog Node →  
Container für  
VNFs

Im IoT hat sowohl Cloud Computing als auch Fog Computing eine fundamentale Bedeutung. Wie bereits erwähnt, führt ein Networking Trend zur *Cloud Computing Containerization*. Da Fog Computing [Abb. 17.1-4] als eine besondere Art von Cloud Computing betrachtet werden kann, bei der eine Mini Cloud einen Fog Node darstellt, führt der Einsatz der Container Technologie zur Containerization beider Arten von Computing. Dank dieser Containerization kommt die Container Technologie auch im IoT zum Einsatz, sodass man von *Containerized IoT Services* sprechen kann. Für weitere Informationen darüber sei verwiesen auf:

- 4.4.a Azhar Sayeed, Dejan Leskaroski: [Cloud Native Applications in a Telco World - How Micro Do You Go?](#)
- 4.4.b Bukhary Ikhwan Ismail, et al.: [Evaluation of Docker as Edge computing platform](#); Proc. IEEE Conference on Open Systems (ICOS), Aug 2015; DOI: 10.1109/ICOS.2015.7377291
- 4.4.c Riccardo Petrolo, Roberto Morabito, Valeria Loscrì, Nathalie Mitton: [The design of the gateway for the cloud of things](#); Annals of Telecommunications, Vol. 72, Issue 1–2, Feb 2017; DOI 10.1007/s12243-016-0521-z
- 4.4.d Roberto Morabito, Ivan Farris, Antonio Iera, Tarik Taleb: [Evaluating Performance of Containerized IoT Services for Clustered Devices at the Network Edge](#); IEEE Internet of Things Journal, Vol. 4(4), Aug. 2017; DOI: 10.1109/JIOT.2017.2714638
- 4.4.e Koustabh Dolui, Csaba Kiraly: [Towards Multi-container Deployment on IoT Gateways](#); Oct 2018; arXiv:1810.07753v1
- 4.4.e Hyunsik Yang, Younghan Kim: [Design and Implementation of Fast Fault Detection in Cloud Infrastructure for Containerized IoT Services](#); Sensors, Vol. 20, Issue 16, Aug 2020; DOI: 10.3390/s20164592

## 18.5 Cloud Computing Services

Bedeutung von  
Cloud Computing

Mit der Entwicklung von IoT gewinnt das als Cloud Computing bezeichnete Service-Modell enorm an Bedeutung [Abb. 17.1-4]. Die große Bedeutung von Cloud Computing besteht hauptsächlich darin, dass man dem Cloud Computing zugrunde liegenden Modell nach bei Bedarf spontan über Netzwerke auf einen Pool konfigurierbarer Computing-Ressourcen (z.B. Netzwerke, Server, Speicher, Applikationen und Dienste) zugreifen kann. Infolge der immensen Menge verschiedener weltweit im IoT verteilter Devices und Objekte werden riesige global verstreute Datenmengen erzeugt. Diese müssen zuerst entsprechend gespeichert und dann schnell verarbeitet werden. Dabei kommt das Konzept von Cloud Computing zum Einsatz, wobei die IoT-spezifischen Clouds als eine Art 'IoT Service Platforms' fungieren. Mit Cloud Computing sind insbesondere die Networking Trends *Infrastructure as a Service* (IaaS), *Software-Defined CC Networking*, *Cloud Native Microservices* und *Mobile*

CC in 5G verbunden. Für weitere Informationen über Cloud Computing sei verwiesen auf die folgende Literatur:

- 5.a [i-SCOOP: Cloud computing – from private, public and hybrid cloud to cloud services and cloud evolutions](#)
- 5.b B. Wanga, Z. Qi, R. Ma, H. Guan, A. V. Vasilakos: [A survey on data center networking for cloud computing](#); Computer Networks, Vol. 91, 2015; DOI: 10.1016/j.comnet.2015.08.040
- 5.c Jatinder Singh, Thomas Pasquier, Jean Bacon, Hajoon Ko, David Eysers: [Twenty Security Considerations for Cloud-Supported Internet of Things](#); IEEE Internet of Things Journal, Vol. 3(3), Jun 2016; DOI: 10.1109/JIOT.2015.2460333
- 5.d Blesson Varghese, Rajkumar Buyya: [Next Generation Cloud Computing: New Trends and Research Directions](#), Sep 2017, arXiv:1707.07452v3
- 5.e Syed Noorulhassan Shirazi, Antonios Gouglidis, Arsham Farshad, David Hutchison: [The Extended Cloud: Review and Analysis of Mobile Edge Computing and Fog from a Security and Resilience Perspective](#); IEEE Journal on Selected Areas in Communications, Vol. 35(11), Nov 2017, DOI: 10.1109/JSAC.2017.2760478
- 5.f Yahya Al-Dhuraibi, Fawaz Paraiso, Nabil Djarallah, Philippe Merle: [Elasticity in Cloud Computing: State of the Art and Research Challenges](#); IEEE Transactions on Services Computing, Vol. 11(2), Mar - Apr 2018; DOI: 10.1109/TSC.2017.2711009
- 5.g Amirhossein Farahzadi, et al.: [Middleware technologies for cloud of things: a survey](#); Digital Communications and Networks, Vol. 4(3), Aug 2018; DOI: 10.1016/j.dcan.2017.04.005
- 5.h Shubham Gupta, Anand Gupta, Gori Shankar: [Cloud Computing: Services, Deployment Models and Security Challenges](#); 2nd International Conference on Smart Electronics and Communication (ICOSEC); Oct 2021; DOI: 10.1109/ICOSEC51865.2021.9591794
- 5.i Xuan-Quy Pham, Tien-Dung Nguyen, Thien Huynh-The, Eui-Nam Huh, Dong-Seong Kim: [Distributed Cloud Computing: Architecture, Enabling Technologies, and Open Challenges](#); IEEE Consumer Electronics Magazine Early Access); Jul 2022; DOI: 10.1109/MCE.2022.3192132

### 18.5.1 Infrastructure-as-a-Service (IaaS)

Enthält eine Cloud einen derartigen Pool konfigurierbarer Computing-Ressourcen, um die bedarfsabhängige Bereitstellung durch einen Cloud-Provider einer virtuellen, aus verschiedenen VNFs bestehenden netzwerkspezifischen Infrastruktur zu ermöglichen, wird von einem *Infrastructure-as-a-Service* (IaaS) gesprochen. Als IaaS können verschiedene private und voneinander isolierte, virtuelle Infrastrukturen angeboten werden. Dies wird auch *Network Slicing* genannt. Bei der Realisierung von IaaS spielt *Service Function Chaining* (SFC) eine wichtige Rolle. Für Näheres über IaaS siehe:

IaaS als Basis für  
Network Slicing

- 5.1.a Antonio Celesti, Davide Mulfari, Maria Fazio, Massimo Villari, Antonio Puliafito: [Exploring Container Virtualization in IoT Clouds](#); IEEE Interna-

tional Conference on Smart Computing (SMARTCOMP), May 2016; DOI: 10.1109/SMARTCOMP.2016.7501691

- 5.1.b Heli Amarasinghe, Abdallah Jarray, Ahmed Karmouch: [Fault-tolerant IaaS management for networked cloud infrastructure with SDN](#); IEEE International Conference on Communications (ICC'17), May 2017; DOI: 10.1109/ICC.2017.7996342
- 5.1.c Steven Van Rossem, et al.: [A Vision for the Next Generation Platform-as-a-Service](#); Proceedings of 2018 IEEE 1st 5G World Forum
- 5.1.d Jasmeen Kaur Ahluwalia, Carla Mouradian, Mohammad Nazmul Alam, Roch Glitho: [A Cloud Infrastructure as a Service for an Efficient Usage of Sensing and Actuation Capabilities in Internet of Things](#); IEEE/IFIP Network Operations and Management Symposium, Apr 2022; DOI: 10.1109/NOMS54207.2022.9789805
- 5.1.e Betty Elezebeth Samuel, Saahira Banu Ahamed, Padmanayaki Selvarajan: [A Review of Efficient Mobility Techniques for Privacy and Secured Cloud Computing Architectures for Infrastructure as a Service](#); 7th International Conference on Communication and Electronics Systems (ICCES); Jun 2022; DOI: 10.1109/ICCES54183.2022.9835763

## 18.5.2 Software-Defined Cloud Computing Networking

### Software-Defined CC Networking

Ein IaaS kann dem Bedarf entsprechend auf eine festgelegte Zeitdauer und sogar auf der Basis mehrerer vernetzter Clouds eingerichtet werden. Somit gilt im Allgemeinen die Vernetzung von Clouds, also *Cloud Computing Networking* (CC Networking), als Voraussetzung für die Bereitstellung von IaaS. Hierbei ist auch eine flexible Lösung nötig, um die notwendigen VNFs zu bestimmen, diese dem aktuellen Bedarf entsprechend untereinander virtuell zu vernetzen, zu konfigurieren und im Laufe der Zeit zu managen. Um diese Aufgaben bei IaaS zu bewältigen, werden einige Konzepte von SDN übernommen, und demzufolge spricht man von *Software-Defined CC Networking*. Für weitere Information darüber siehe:

- 5.2.a Rajkumar Buyya, Rodrigo N. Calheiros, Jungmin Son, Amir Vahid Dastjerdi, Young Yoony: [Software-Defined Cloud Computing: Architectural Elements and Open Challenges](#), Feb 2015; arXiv:1408.6891v2
- 5.2.b Foresta Francesco: [Integration of SDN Frameworks And Cloud Computing Platforms: An Open Source Approach](#); Master Thesis, Universita di Bologna; Academic Year 2016/2017
- 5.2.c Jungmin Son, Rajkumar Buyya: [A Taxonomy of Software-Defined Networking \(SDN\)-Enabled Cloud Computing](#); ACM Computing Surveys, Vol.51(3), May 2018; DOI: 10.1145/3190617
- 5.2.d Aaqif Afzaal Abbasi, Almas Abbasi, Shahaboddin Shamshirband, Anthony Theodore Chronopoulos, Valerio Persico, Antonio Pescapè: [Software-Defined Cloud Computing: A Systematic Review on Latest Trends and Developments](#); IEEE Access, Vol. 7, Jul 2019; DOI: 10.1109/ACCESS.2019.2927822

- 5.2.e Ahmad AA AlKhatib, Thaeer Sawalha, Shadi AlZu'bi: [Load Balancing Techniques in Software-Defined Cloud Computing: an overview](#); Seventh International Conference on Software Defined Systems (SDS), Apr 2020; DOI: 10.1109/SDS49854.2020.9143874
- 5.2.f David Espinel Sarmiento, Adrien Lebre, Lucas Nussbaum, Abdelhadi Chari: [Decentralized SDN Control Plane for a Distributed Cloud-Edge Infrastructure: A Survey](#); IEEE Communications Surveys & Tutorials, Vol. 23, Issue 1, Jan 2021; DOI: 10.1109/COMST.2021.3050297

### 18.5.3 Cloud-Native Microservices

Ein weiterer wichtiger Trend ist die Integration von Cloud Computing in öffentliche Netzwerkinfrastrukturen mit dem Ziel der Bereitstellung und flexiblen Nutzung virtueller Netzwerkfunktionen, d.h. VNFs, in diesen. Da VNFs als netzwerkspezifische Funktionsbausteine, also eine Art 'Network-App' dienen, werden sie auch als *Microservices* bezeichnet. Solche virtuellen Microservices (z.B. vRouter, vFirewalls) ermöglichen die schnelle Einrichtung diverser komplexer Network Services. Wurden VNFs bzw. Microservices speziell für Cloud-Computing-Architekturen entwickelt und optimiert, so werden sie entsprechend *Cloud-native VNFs* und *Cloud-native Microservices* genannt. Für Weiteres darüber siehe:

Cloud-native  
VNFs bzw.  
Microservices

- 5.3.a Azhar Sayeed, Dejan Leskaroski: [Cloud Native Applications in a Telco World - How Micro Do You Go?](#)
- 5.3.b Antonio Celesti, et al.: [Exploring Container Virtualization in IoT Clouds](#); IEEE International Conference on Smart Computing (SMARTCOMP), May 2016; DOI: 10.1109/SMARTCOMP.2016.7501691
- 5.3.c Hamzeh Khazaei, Hadi Bannazadeh, Alberto Leon-Garcia: [SAVI-IoT: A Self-Managing Containerized IoT Platform](#), IEEE 5th International Conference on Future Internet of Things and Cloud (FiCloud), Aug 2017; DOI: 10.1109/FiCloud.2017.27
- 5.3.d Cisco: [Cloud-Native Network Functions \(CNFs\)](#); White Paper, Jun 2018; Document ID:1529344804993194
- 5.3.e 5G-PPP Software Network Working Group: [From Webscale to Telco, the Cloud Native Journey](#); July 2018
- 5.3.f Tetiana Yarygina: [Exploring Microservice Security](#); PhD Thesis, Department of Informatics, University of Bergen, Jul 2018
- 5.3.g ETSI GS NFV-EVE 011 V3.1.1 (2018-10): [Network Functions Virtualisation \(NFV\) Release 3; Virtualised Network Function; Specification of the Classification of Cloud Native VNF Implementations Disclaimer](#)
- 5.3.h Shihabur Rahman Chowdhury, Mohammad A. Salahuddin, Noura Limam, Raouf Boutaba: [Re-Architecting NFV Ecosystem with Microservices: State of the Art and Research Challenges](#); IEEE Network, Vol. 33, Issue 3, May/Jun 2019; DOI: 10.1109/MNET.2019.1800082



- 5.3.i Rasel Chowdhury, Chamseddine Talhi, Hakima Ould-Slimane, Azzam Mourad: [A Framework for Automated Monitoring and Orchestration of Cloud-Native applications](#); International Symposium on Networks, Computers and Communications, Oct 2020; DOI: 10.1109/ISNCC49221.2020.9297238
- 5.3.j Syed Danial Ali Shah, Mark A. Gregory, Shuo Li: [Cloud-Native Network Slicing Using Software Defined Networking Based Multi-Access Edge Computing: A Survey](#); IEEE Access, Vol. 9, Jan 2021; DOI: 10.1109/ACCESS.2021.3050155

### 18.5.4 Mobile Cloud Computing in 5G

Mobility von  
VNFs in  
5G-Netzen

Heutzutage haben mobile Kommunikation und mobiles Computing in allen Bereichen unseres Lebens eine große Bedeutung. Die Möglichkeiten der Nutzung des Mobile Computing kann noch durch die Symbiose mit Cloud Computing verbessert werden. Um dies zu erreichen, wird ein neuer Trend namens *Mobile Cloud Computing* (MCC) verfolgt. Diesem wird aktuell, insbesondere im Hinblick auf die neu entwickelten zellularen 5G-Mobilfunknetze, im Forschungsbereich viel Aufmerksamkeit gewidmet. Für weitere Information über MCC siehe:

- 5.4.a Min Chen, Yin Zhang, Yong Li, Shiwen Mao, Victor C. M. Leung: [EMC: Emotion-Aware Mobile Cloud Computing in 5G](#); IEEE Network, Vol. 29(2), Mar - Apr 2015; DOI: 10.1109/MNET.2015.7064900
- 5.4.b Nasir Abbas, Yan Zhang, Amir Taherkordi, Tor Skeie: [Mobile Edge Computing: A Survey](#); IEEE Internet of Things Journal, 2018; DOI: 10.1109/JIOT.2017.2750180
- 5.4.c Talal H. Noor, Sherali Zeadally, Abdullah Alfazi, Quan Z. Sheng: [Mobile cloud computing: Challenges and future research directions](#); Journal of Network and Computer Applications, Vol. 115, Aug 2018; DOI: 10.1016/j.jnca.2018.04.018
- 5.4.d Lofty Sahi, Monica Sood. Sapna Saini: [Analysis and Evaluation of Mobile Cloud Computing: Service Models, Applications, and Issues](#); 4th International Conference for Convergence in Technology (I2CT), Oct 2018; DOI: 10.1109/I2CT42659.2018.9058061
- 5.4.e Zimutian Yang: [A Survey of Security Issues in Mobile Cloud Computing](#); [A Survey of Security Issues in Mobile Cloud Computing](#); International Conference on Signal Processing and Machine Learning (CONF-SPML), Nov 2021; DOI: 10.1109/CONF-SPML54095.2021.00032
- 5.4.f Nahla F. Omran, Sara A. Lotfy, Elnomery A. Zanaty: [A Systematic review of Mobile cloud computing Applications and its impact on Learning and Big data](#); Turkish Journal of Computer and Mathematics Education, Vol.13, No 02, 2022
- 5.4.g Ghadeer Alwafi, Mona Alrougi, Rahaf Alsulami, Shaimaa Salama: [A Survey of Mobile Cloud Computing Challenges and Solutions](#); International Journal of New Technology and Research (IJNTR); Vol. 7, Issue 3, Mar 2021; <https://doi.org/10.31871/IJNTR.7.3.6>

## 18.6 Fog Computing und Artificial Intelligence

*Fog Computing* (FC) kann als Ergänzung von Cloud Computing im IoT angesehen werden [Abschnitt 17.1]. Die Funktionen von FC werden im IoT durch eine horizontal verteilte große Menge von Fog Nodes, einer Art Mini-Clouds, entlang des Internet-Kontinuums zwischen Clouds und Things in die Nähe seiner Benutzer und somit der IoT-Devices gebracht. FC führt also zu einer Verteilung von Computing-Ressourcen. Dadurch können diese überall möglichst nah an Benutzern und IoT-Devices platziert werden. Die am Internet Edge entlang platzierten Computing-Ressourcen tragen dazu bei, dass die 'Intelligenz' verteilter Systeme aus IoT-Clouds zu den diese benötigten 'IoT-Objekten' hin bewegt werden kann.

Bedeutung von Fog Computing im IoT

Fog Computing stellt eine Computing-Architektur dar, die für am Internet Edge installierten IoT-Objekten die von ihnen benötigte, zusätzliche Intelligenz 'liefert'. Dadurch können diese Objekte lokal und alternativ zu Cloud Computing einige intelligente Funktionen durchführen. Aus diesem Grund gewinnen die von Fog Nodes am Internet Edge erbrachte künstliche Intelligenz (*Artificial Intelligence*, AI) und ihr maschinelles Lernen (*Machine Learning*, ML) ständig an Bedeutung. Mittels Fog Nodes können auch diverse Microservices, u.a. welche mit VNFs, am Internet Edge verfügbar gemacht werden.

Fog Computing: 'Lieferant' der Intelligenz für IoT-Objekte

Die Idee, Intelligenz und Verarbeitungsfähigkeiten möglichst in direkter Nähe des Internet Edge zu positionieren, wird auch bei Edge Computing verfolgt. Fog Computing und Edge Computing unterscheiden sich hauptsächlich darin, wo genau die Intelligenz und Rechenleistung erbracht werden. Mit Fog Computing kann diese Funktionalität überall im Internet-Kontinuum zwischen IoT Clouds und Internet Edge erbracht werden. Mit Edge Computing wird sie direkt am Internet Edge erbracht – und zwar oft in IoT Access Gateways. Um mobilen Endeinrichtungen in 5G-Mobilfunknetzen Intelligenz und Unterstützung bei der Informationsverarbeitung bereitzustellen, werden spezielle Clouds am Internet Edge in Basisstationen dieser Netze installiert. Man spricht in diesem Zusammenhang von *Mobile Edge Computing* (MEC).

Edge Computing, Mobile Edge Computing

Auf Fog Computing bzw. (Mobile) Edge Computing und der Nutzung von AI basieren die Networking Trends: *Time-Sensitive IoT / 5G Applications*, *Intelligent IoT*, *Cognitive IoT*, *Ambient Intelligence in IoT* und *IoT Service Orchestration*. Für weitere Information über Fog Computing und die Bedeutung von Artificial Intelligence (AI) bei Fog Computing siehe:

- 6.a i-SCOOP: [Edge computing and IoT 2018 – when intelligence moves to the edge](#)
- 6.b i-SCOOP: [Fog computing: fog and cloud along the Cloud-to-Thing continuum](#)
- 6.c i-SCOOP: [Artificial intelligence \(AI\) and cognitive computing: what, why and where](#)
- 6.d i-SCOOP: [The interaction and convergence of IoT and AI at work](#)
- 6.e Flavio Bonomi, Rodolfo Milito, Jiang Zhu, Sateesh Addepalli: [Fog Computing and Its Role in the Internet of Things](#); Workshop on Mobile Cloud Computing (MCC '12), Aug 2012; DOI: 10.1145/2342509.2342513

- 6.f Ivan Stojmenovic, Sheng Wen: [The fog computing paradigm: Scenarios and security issues](#); Federated Conference on Computer Science and Information Systems, Sep 2014; DOI: 10.15439/2014F503
- 6.g Shanhe Yi, Cheng Li, Qun Li: [Survey of Fog Computing: Concepts, Applications and Issues](#); Mobidata'15, Proceedings of the 2015 Workshop on Mobile Big Data, Jun 2015, DOI: 10.1145/2757384.2757397
- 6.h Yifan Wang, Tetsutaro Uehara, Ryoichi Sasaki: [Fog computing: Issues and challenges in security and forensics](#); IEEE 39th Annual Computer Software and Applications Conference, Vol. 3, Jul 2015; DOI: 10.1109/COMPSAC.2015.173
- 6.i Tom H. Luan, et al.: [Fog Computing: Focusing on Mobile Users at the Edge](#); Mar 2016; arXiv:1502.01815v3
- 6.j Lav Gupta, Raj Jain, H. Anthony Chan: [Mobile Edge Computing – An Important Ingredient of 5G Networks](#); Mar 2016
- 6.k Firas Al-Doghman, et al.: [A review on Fog Computing technology](#); IEEE International Conference on Systems, Man, and Cybernetics (SMC), Oct 2016; DOI: 10.1109/SMC.2016.7844455
- 6.l Eva Marín Tordera, et al.: [What is a Fog Node? A Tutorial on Current Concepts towards a Common Definition](#); Nov 2016; arXiv:1611.09193v1
- 6.m Farhoud Hosseinpour, et al.: [A Review on Fog Computing Systems](#); International Journal of Advancements in Computing Technology(IJACT), Vol. 8(5), Dec 2016
- 6.n Mung Chiang, Tao Zhang: Fog and IoT: [An Overview of Research Opportunities](#); IEEE Internet of Things Journal, Vol. 3(6), Dec 2016; DOI: 10.1109/JIOT.2016.2584538
- 6.o Arwa Alrawais, Abdulrahman Althothaily, Chunqiang Hu, Xiuzhen Cheng: [Fog Computing for the Internet of Things: Security and Privacy Issues](#); IEEE Internet Computing, Vol. 21(2), Mar-Apr 2017; DOI: 10.1109/MIC.2017.37
- 6.p Mithun Mukherjee, et al.: [Security and Privacy in Fog Computing: Challenges](#); IEEE Access, Vol. 5, Sep 2017; DOI: 10.1109/ACCESS.2017.2749422
- 6.q Redowan Mahmud, Ramamohanarao Kotagiri, Rajkumar Buyya: [Fog Computing: A Taxonomy, Survey and Future Directions](#); arXiv:1611.05539v4, Oct 2017; DOI: 10.1007/978-981-10-5861-5\_5
- 6.r Saad Khan, Simon Parkinson, Yongrui Qin: [Fog computing security: a review of current applications and security solutions](#); Journal of Cloud Computing: Advances, Systems and Applications, Vol. 6(1), 2017c DOI 10.1186/s13677-017-0090-3
- 6.s Carla Mouradian, et al.: [A Comprehensive Survey on Fog Computing: State-of-the-art and Research Challenges](#); IEEE Communications Surveys & Tutorials, Oct 2017; DOI: 10.1109/COMST.2017.2771153
- 6.t Pengfei Hu, Sahraoui Dhelim, Huansheng Ning, Tie Qiu: [Survey on fog computing: architecture, key technologies, applications and open issues](#); Journal of Network and Computer Applications, Vol. 98, Nov 2017; DOI: 10.1016/j.jnca.2017.09.002

- 6.u David Bermbach, et al.: [A Research Perspective on Fog Computing; Workshop on IoT Systems Provisioning and Management for Context-Aware Smart Cities](#); Nov 2017
- 6.v Shubha Brata Nath, Harshit Gupta, Sandip Chakraborty, Soumya K Ghosh: [A Survey of Fog Computing and Communication: Current Researches and Future Directions](#); Apr 2018; arXiv:1804.04365v1
- 6.w Ranesh Kumar Naha, et al.: [Fog Computing: Survey of Trends, Architectures, Requirements, and Research Directions](#), Jul 2018; arXiv:1807.00976v1
- 6.x Marcus Gomes, Miguel L. Pardal: [Cloud vs Fog: assessment of alternative deployments for a latency-sensitive IoT application](#); Procedia Computer Science, Vol. 130, 2018; DOI: 10.1016/j.procs.2018.04.059
- 6.y Jaspreet Kaur, Prabhpreet Kaur: [A Review: Artificial Neural Network](#); International Journal of Current Engineering and Technology, Vol. 8(4), July/Aug 2018; DOI: 10.14741/ijcet/v.8.4.2
- 6.z Anatol Badach: [Fog Computing](#); In book: Protokolle und Dienste der Informationstechnologie: WEKA, Ed. Heinz Schulte, Aug 2018
- 6.A Zhuo Zou, Yi Jin, Paavo Nevalainen, Yuxiang Huan, Jukka Heikkonen, Tomi Westerlund: [Edge and Fog Computing Enabled AI for IoT-An Overview](#); IEEE International Conference on Artificial Intelligence Circuits and Systems (AICAS); Mar 2019; DOI: 10.1109/AICAS.2019.8771621
- 6.B Mattia Antonini, Massimo Vecchio, Fabio Antonelli: [Fog Computing Architectures: A Reference for Practitioners](#); IEEE Internet of Things Magazine, Vol. 2, Issue 3, Sep 2019; DOI: 10.1109/IOTM.0001.1900029
- 6.C M. Arif Khan: [Fog Computing in 5G Enabled Smart Cities: Conceptual Framework, Overview and Challenges](#); IEEE International Smart Cities Conference (ISC2); Oct 2019, DOI: 10.1109/ISC246665.2019.9071695
- 6.D Koen Tange, Michele De Donno, Xenofon Fafoutis, Nicola Dragoni: [A Systematic Survey of Industrial Internet of Things Security: Requirements and Fog Computing Opportunities](#); IEEE Communications Surveys & Tutorials, Vol. 22, Issue 4, Jul 2020; DOI: 10.1109/COMST.2020.3011208

### 18.6.1 Time-Sensitive IoT/5G Applications

Es gibt einige intelligente IoT Applications, die in gewisser Weise zeitempfindlich (zeitsensitiv, *time sensitive*) sind. Sie werden häufig *Time-Sensitive Applications* genannt. Zu dieser Gruppe gehören auch einige intelligente Applikationen, die in 5G-Mobilfunknetzen realisiert werden. Dies zu ermöglichen, ist die wesentliche Aufgabe von Edge und Fog Computing. Für weitere Information über zeitempfindliche IoT/5G-Applikationen siehe:

Bedeutung von  
Edge und Cloud  
Computing

- 6.1.a ETSI GS MEC 002 v1.1.1: [Mobile Edge Computing \(MEC\): Technical Requirements](#); Mar 2016
- 6.1.b ETSI GS MEC 003 v1.1.1: [Mobile Edge Computing \(MEC\): Framework and Reference Architecture](#); Mar 2016

- 6.1.c Rodrigo Roman, Javier Lopez, Masahiro Mambo: [Mobile Edge Computing, Fog et al.: A Survey and Analysis of Security Threats and Challenges](#); arXiv:1602.00484v2, Nov 2016
- 6.1.d Ashkan Yousefpour, Genya Ishigaki, Jason P. Jue: [Fog Computing: Towards Minimizing Delay in the Internet of Things](#); IEEE International Conference on Edge Computing (EDGE), Jun 2017; DOI: 10.1109/IEEE.EDGE.2017.12
- 6.1.e Gaolei Li, Jianhua Li, and Jun Wu: [Fog-enabled Edge Learning for Cognitive Content-Centric Networking in 5G](#); arXiv:1808.09141v1, Aug 2018
- 6.1.f Ali Alnoman: [Supporting Delay-Sensitive IoT Applications: A Machine Learning Approach](#); IEEE Canadian Conference on Electrical and Computer Engineering (CCECE); Sep 2020; DOI: 10.1109/CCECE47787.2020.9255800
- 6.1.g Harindu Korala, Dimitrios Georgakopoulos, Prem Prakash Jayaraman, Ali Yavari: [Managing Time-Sensitive IoT Applications via Dynamic Application Task Distribution and Adaptation](#); Remote Sensing, Vol. 13 Issue 20, Oct 2021; DOI: 10.3390/rs13204148
- 6.1.h Ume Kalsoom Saba, Saif ulIslam, Humaira Ijaz, Joel J. P. C. Rodrigues, Abdullah Gani, Kashif Munir: [Planning Fog networks for time-critical IoT requests](#); Computer Communications, Vol. 172, Apr 2021; DOI:10.1016/j.comcom.2021.03.002

## 18.6.2 Intelligent IoT, Cognitive IoT

### Intelligent IoT

Ein wichtiger Trend bei der Weiterentwicklung von IoT trägt dazu bei, künstliche Intelligenz (*Artificial Intelligence*, AI) und die in IoT-Clouds gesammelten, immensen Datenmengen, sog. *Big Data*, im IoT zu analysieren (*Big Data Analytics*). Die Ergebnisse dieser Analysen sollen nicht nur dazu dienen, verschiedene IoT-Komponenten und -Objekte zum Erfassen von Informationen zu befähigen, damit sie diese Menschen signalisieren/anzeigen und die Informationen von Menschen genutzt werden. Die IoT-Komponenten und -Objekte sollen mittels der erfassten Informationen auch selbst lernen und sich dadurch in die Lage versetzen, intelligent (so wie Menschen, aber ohne menschliche Hilfe) auf verschiedene Situationen und plötzlich auftretende Ereignisse zu reagieren. Besäße das IoT die eben geschilderten Fähigkeiten, würde man von *Intelligent IoT* (IIoT) sprechen.

### Cognitive IoT

Die sog. *kognitiven Fähigkeiten* des Menschen ermöglichen es ihm, Signale aus der Umwelt wahrzunehmen und weiterzuverarbeiten. Da die Fähigkeiten von Intelligent IoT im Wesentlichen den kognitiven Fähigkeiten des Menschen entsprechen, wird es auch als *Cognitive IoT* (CIoT) bezeichnet. Es sei hervorgehoben, dass AI, (Big) Data Analytics, Cloud Computing und Fog Computing als die vier wichtigsten treibenden Kräfte, quasi als 'Zugpferde' einer IoT-Quadriga [Abb. 18.11-1], bei der IoT-Weiterentwicklung zum Intelligent IoT angesehen werden können.

Für detailliertere Information über Cognitive IoT und Intelligent IoT siehe:

- 6.2.a Charith Perera, Arkady Zaslavsky, Peter Christen, Dimitrios Georgakopoulos: [Context Aware Computing for The Internet of Things: A Survey](#); IEEE

- Communications Surveys & Tutorials, Vol. 16(1), First Quarter 2014, DOI: 10.1109/SURV.2013.042313.00197
- 6.2.b Qihui Wu, et al.: [Cognitive Internet of Things: A New Paradigm beyond Connection](#); Mar 2014; arXiv:1403.2498v1
- 6.2.c Djallel Eddine Boubiche, et al.: [Advanced Industrial Wireless Sensor Networks and Intelligent IoT](#); IEEE Communications Magazine, Vol. 56(2), Feb 2018; DOI: 10.1109/MCOM.2018.8291108
- 6.2.d Omer Berat Sezer, Erdogan Dogdu, Ahmet Murat Ozbayoglu: [Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey](#); IEEE Internet of Things Journal, Vol. 5(1), Feb 2018; DOI: 10.1109/JIOT.2017.2773600
- 6.2.e Nadeem Javaid, Arshad Sher, Hina Nasir, Nadra Guizani: [Intelligence in IoT-Based 5G Networks: Opportunities and Challenges](#); IEEE Communications Magazine, Vol. 56(10), Oct 2018; DOI: 10.1109/MCOM.2018.1800036
- 6.2.f Yin Zhang, Xiao Ma, Jing Zhang, M. Shamim Hossain, Ghulam Muhammad, Syed Umar Amin: [Edge Intelligence in the Cognitive Internet of Things: Improving Sensitivity and Interactivity](#); IEEE Network, Vol. 33, Issue 3, May/June 2019; DOI: 10.1109/MNET.2019.1800344
- 6.2.g Khondokar Fida Hasan, Tarandeep Kaur, Md. Mhedi Hasan, Yanming Feng: [Cognitive Internet of Vehicles: Motivation, Layered Architecture and Security Issues](#); International Conference on Sustainable Technologies for Industry 4.0 (STI); Dec 2019; DOI: 10.1109/STI47673.2019.9068070
- 6.2.h Hao Song, Jianan Bai, Yang Yi, Jinsong Wu, Lingjia Liu: [Artificial Intelligence Enabled Internet of Things: Network Architecture and Spectrum Access](#); IEEE Computational Intelligence Magazine, Vol. 15, Issue 1, Feb 2020; DOI: 10.1109/MCI.2019.2954643
- 6.2.i Rahul Keru Patil, Suhas Shivalal Patil: [Cognitive Intelligence of Internet of Things in Smart Agriculture Applications](#); IEEE Pune Section International Conference (PuneCon); Dec 2020; DOI: 10.1109/Pune-Con50868.2020.9362449
- 6.2.j William Grant Hatcher, Cheng Qian, Weichao Gao, Fan Liang, Kun Hua, Wei Yu: [Towards Efficient and Intelligent Internet of Things Search Engine](#); IEEE Access, Vol. 9, Jan 2021; DOI: 10.1109/ACCESS.2021.3052759
- 6.2.k Chao Zhang: [Intelligent Internet of things service based on artificial intelligence technology](#) IEEE 2nd International Conference on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE), Mar 2021; DOI: 10.1109/ICBAIE52039.2021.9390061
- 6.2.l Dinh C. Nguyen, Ming Ding, Pubudu N. Pathirana, Aruna Seneviratne, Jun Li, H. Vincent Poor: [Federated Learning for Internet of Things: A Comprehensive Survey](#); IEEE Communications Surveys & Tutorials, Vol. 23, Issue 3, Apr 2021; DOI: 10.1109/COMST.2021.3075439
- 6.2.m Fayaz Ahmad Fayaz, Arun Malik, Arshad Ahmad Yatoo: [Cognitive Internet of things \(CIoT\) a success for data collection](#); Sixth International

Conference on Image Information Processing (ICIIP), Nov 2021; DOI: 10.1109/ICIIP53038.2021.9702706

- 6.2.n Yuan Li, Wai Chen, Yu Ding, Yakun Qie, Chuntian Zhang: [A Vision of Intelligent IoT — Trends, Characteristics and Functional Architecture](#); International Wireless Communications and Mobile Computing (IWCMC), Jun 2022; DOI: 10.1109/IWCMC55113.2022.9824304

### 18.6.3 Ambient Intelligence in IoT

Basis für  
'intelligente'  
Umgebungen

Ein wichtiges Ziel der IoT-Entwicklung ist die Verbesserung der Lebensqualität von Menschen. Dies bedeutet, dass Intelligent IoT eine Intelligenz, die sich auf das direkte Lebensumfeld von Menschen bezieht, besitzen muss. Diese wird als *Umweltintelligenz* bzw. *Ambient Intelligence* (AmI) bezeichnet. Ein Beispiel für die Verbesserung der Lebensqualität von Menschen dank AmI im IoT ist *Ambient Assisted Living* (AAL). Als AAL wird ein IoT-Service verstanden, mit dem der Alltag älterer oder gesundheitlich benachteiligter Personen situationsabhängig und unaufdringlich unterstützt werden kann.

Für detaillierte Informationen über Bedeutung von Ambient Intelligence in IoT sei verwiesen auf:

- 6.3.a Emile Aarts, Boris de Ruyte: [New research perspectives on Ambient Intelligence](#); Journal of Ambient Intelligence and Smart Environments, Vol. 1(1), 2009; DOI: 10.3233/AIS-2009-0001
- 6.3.b A. Dohr, R. Modre-Osprian, M. Drobits, D. Hayn, G. Schreier: [The Internet of Things for Ambient Assisted Living](#); Seventh International Conference on Information Technology: New Generations, Apr 2010; DOI: 10.1109/IT-NG.2010.104
- 6.3.c Kun Wang, Yun Shao, Lei Shu, Guangjie Han, Chunsheng Zhu: [LDPA: A Local Data Processing Architecture in Ambient Assisted Living Communications](#); IEEE Communications Magazine, Vol. 53(1), Jan 2015; DOI: 10.1109/MCOM.2015.7010516
- 6.3.d Rodrigo Schmitt Meurer, Antônio Augusto Fröhlich, Jomi Fred Hübner: [Ambient Intelligence for the Internet of Things Through Context-Awareness](#); International Symposium on Rapid System Prototyping (RSP); Oct 2018; DOI: 10.1109/RSP.2018.8631989
- 6.3.e Carles Gomez, Stefano Chessa, Anthony Fleury, George Roussos, Davy Preuvenciers: [Internet of Things for enabling smart environments: A technology-centric perspective](#); Journal of Ambient Intelligence and Smart Environments; Vol. 11, No 1, Jan 2019; DOI 10.3233/AIS-180509
- 6.3.f Hakilo Sabit, Peter Han Joo Chong, Jeff Kilby: [Ambient Intelligence for Smart Home using The Internet of Things](#); 29th International Telecommunication Networks and Applications Conference (ITNAC), Nov 2019; DOI: 10.1109/IT-NAC46935.2019.9078001

## 18.6.4 IoT Service Orchestration

Müssen im IoT mehrere Fog Nodes beispielsweise von einer Cloud koordiniert werden, so ist die Nutzung von SDN fast unabdingbar. Bei einem Einsatz von SDN zur Unterstützung von Fog Computing spricht man von *SDN-enabled Fog Computing*. Diese besondere Art von Fog Computing besteht in der Konfigurierung und Steuerung der Fog Nodes durch SDN Controller. Wird ein IoT Service von mehreren Fog Nodes erbracht, so müssen diese entsprechend koordiniert werden, zum Beispiel von einem SDN Controller, der in einer Cloud untergebracht werden kann. Dies kann als eine Art 'IoT-Service-Orchestrierung' angesehen werden. Für Näheres darüber siehe:

Voraussetzung  
für flexible  
IoT-Services

- 6.4.a Harshit Gupta, et al.: [SDFog: A Software Defined Computing Architecture for QoS Aware Service Orchestration over Edge Devices](#); Sep 2016; arXiv:1609.01190v1
- 6.4.b Karima Velasquez, et al.: [Fog orchestration for the Internet of Everything: state-of-the-art and research challenges](#); Journal of Internet Services and Applications, Jul 2018; DOI: 10.1186/s13174-018-0086-3
- 6.4.c Ola Salman, Imad Elhadj, Ali Chehab, Ayman Kayssi: [IoT Survey: An SDN and Fog Computing Perspective](#); Computer Networks, Vol. 143, Jul 2018; DOI: 10.1016/j.comnet.2018.07.020
- 6.4.d José Santos, Tim Wauters, Bruno Volckaert, Filip De Turck: [Fog Computing: Enabling the Management and Orchestration of Smart City Applications in 5G Networks](#); Entropy, Vol. 20(1), Jan 2018; DOI:10.3390/e20010004
- 6.4.e Nam Yong Kim, et al.: [CF-CloudOrch: container fog node-based cloud orchestration for IoT networks](#); The Journal of Supercomputing, Jul 2018c DOI: 10.1007/s11227-018-2493-4
- 6.4.f Salman Taherizadeh, Vlado Stankovski, Marko Grobelni: [A Capillary Computing Architecture for Dynamic Internet of Things: Orchestration of Microservices from Edge Devices to Fog and Cloud Providers](#); Sensors, Vol. 18(9), Sep 2018.
- 6.4.g Wajid Rafique, Xuan Zhao, Shui Yu, Ibrar Yaqoob, Muhammad Imran, Wanchun Dou: [An Application Development Framework for Internet-of-Things Service Orchestration](#); IEEE Internet of Things Journal, Vol. 7, Issue 5, May 2020; DOI: 10.1109/JIOT.2020.2971013
- 6.4.h Daniil Ermolenko, Claudia Kilicheva, Ammar Muthanna, Abdukodir Khakimov: [Internet of Things Services Orchestration Framework Based on Kubernetes and Edge Computing](#); IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus), Jan 2021; DOI: 10.1109/ElConRus51938.2021.9396553
- 6.4.i Nor Syazwani Mohd Pakhrudin, Murizah Kassim, Azlina Idris: [A review on orchestration distributed systems for IoT smart services in fog computing](#); International Journal of Electrical and Computer Engineering, Vol. 11, No. 2, Apr 2021; DOI: 10.11591/ijece.v11i2.pp1812-1822
- 6.4.j Jen-Sheng Tsai, I-Hsun Chuang, Jie-Jyun Liu, Yau-Hwang Kuo, Wanjiun Liao: [QoS-Aware Fog Service Orchestration for Industrial Internet of Things](#); IEEE



Transactions on Services Computing, Vol. 15, Issue 3, May-Jun 2022; DOI: 10.1109/TSC.2020.2978472

## 18.7 Next 5G und 6G (Generation) Mobile Networks

Was bedeutet 5G?

Mit 5G wird die auf die UMTS-Technologie folgende Generation von Mobilfunknetzen bezeichnet. Seit nunmehr 2020 stehen Mobilfunknetze der 5. Generation zur Verfügung.

5G als Ergänzung zu 4G

Die 5G-Mobilfunknetze, als aktuelle Generation zellulärer Mobilfunknetze, haben die 4G-Mobilfunknetze nicht ersetzt, sondern ergänzen diese mit erheblich höheren Übertragungskapazitäten und geringeren Latenzzeiten. 5G-Mobilfunknetze können auf Basis kleiner Zellen eingerichtet werden und ermöglichen eine Übertragung von Daten über kurze Entfernungen mit großen, in Bereich von Gbit/s liegenden Bitraten. Mit einer breiten Verfügbarkeit von 5G-Mobilfunknetzen wird eine Netzwerkarchitektur geschaffen, die den vielfältigen Anforderungen des IoT sehr gerecht wird.

Auf dem Gebiet 5G Mobile Networks sind insbesondere die Networking-Trends *5G-enabled Mobile IoT Applications*, *Vehicle-to-Everything (V2X) Services*, *SDN and NFV for 5G Mobile Networks*, *5G Network Slicing* und *5G Security* hervorzuheben. Ergänzend sei bemerkt, dass die Ideen für die Realisierung der nach 5G folgenden, zukünftigen Generation (6G) der Mobilfunknetze bereits entwickelt werden.

- 7.a IEEE SPECTRUM: [What Does Every Engineer Need to Know about 5G?](#)
- 7.b SDxCentral: [Defining 5G Architecture](#)
- 7.c Chih-Lin I, Corbett Rowell, Shuangfeng Han, Zhikun Xu, Gang Li, Zhengang Pan: [Toward green and soft: a 5G perspective](#); IEEE Communications Magazine, Vol. 52(2), Feb 2014; DOI: 10.1109/MCOM.2014.6736745
- 7.d Patrick Kwadwo Agyapong, et al.: [Design considerations for a 5G network architecture](#); IEEE Communications Magazine, Vol. 52(11), Nov 2014; DOI: 10.1109/MCOM.2014.6957145
- 7.e NGMN Alliance: [5G White Paper - Executive Version](#); Dec 2014
- 7.f Akhil Gupta, Rakesh Kumar Jha: [A Survey of 5G Network: Architecture and Emerging Technologies](#); IEEE Access, Vol. 3, Jul 2015; DOI: 10.1109/ACCESS.2015.2461602
- 7.g Huawei Technologies: [5G Network Architecture: A High-Level Perspective](#); Technical Report, 2016
- 7.h Mamta Agiwal, Abhishek Roy, Navrati Saxena: [Next Generation 5G Wireless Networks: A Comprehensive Survey](#); IEEE Communications Surveys & Tutorials, Vol. 18, Issue 3, Feb 2016; DOI: 10.1109/COMST.2016.2532458
- 7.i 5G PPP Architecture Working Group: [View on 5G Architecture, Version 1.0](#); Technical Report, Version 1.0, Jul 2016

- 7.j Bundesministerium für Verkehr und digitale Infrastruktur (Hrsg.): [5G-Strategie für Deutschland: Eine Offensive für die Entwicklung Deutschlands zum Leitmarkt für 5G-Netze und -Anwendungen](#); Juli 2017
- 7.k 5G PPP Architecture Working Group: [View on 5G Architecture](#); Version 2.0; Technical Report, Jul 2017
- 7.l Ian F. Akyildiz, Shuai Nie, Shih-Chun Lin, Manoj Chandrasekaran: [5G roadmap: 10 key enabling technologies](#); Computer Networks, Vol. 106, 4 Sep 2016; DOI: 10.1016/j.comnet.2016.06.010
- 7.m 5G PPP Architecture Working Group: [View on 5G Architecture](#); Technical Report, Version 2.0, Jun 2017
- 7.n ETSI TR 138 913 V14.3.0: [5G; Study on scenarios and requirements for next generation access technologies \(3GPP TR 38.913 version 14.3.0 Release 14\)](#); Oct 2017
- 7.o Rojeena Bajracharya, et al.: [LWA in 5G: State-of-the-Art Architecture, Opportunities, and Research Challenges](#); IEEE Communications Magazine, Vol. 56(10), Oct 2018; DOI: 10.1109/MCOM.2018.1701177

### 18.7.1 5G-enabled Mobile IoT Applications

In zellularen 5G-Mobilfunknetzen werden Funktechnologien genutzt, in denen Signale im elektromagnetischen Spektrum im Millimeterbereich verwendet werden. 5G-Mobilfunknetze basieren also auf der Ausbreitung von sog. Millimeterwellen. Hierdurch sind in diesen mobilen Netzen kleine Zellen und große Übertragungsgeschwindigkeiten möglich. Und aus diesem Grund werden 5G-Mobilfunknetze bis zu 100 Mal schneller als bestehende 4G-Mobilfunknetze sein. Dies wird von großer Bedeutung bei der Integration von 5G-Mobilnetztechnologien in das IoT sein – insbesondere für Industrial IoT (IIoT) – und bestimmte andere Branchen, z.B. die Landwirtschaft. Die soeben erwähnten, IoT-relevanten Besonderheiten der 5G-Mobilnetztechnologien werden mit den drei Begriffen eMBB, URLLC und mMTC umschrieben. Dabei steht:

- **eMBB** (*enhanced Mobile Broadband*) für ein erweitertes mobiles Breitband (Nutzung von Millimeterwellen),
- **URLLC** (*Ultra Reliable Low Latency Communications*) für sehr zuverlässige Kommunikation mit geringer Latenz und
- **mMTC** (*massive Machine Type Communications*) für ein breites Spektrum von IoT-Einsatzmöglichkeiten.

Eine besonders wichtige 5G-Netztechnologie ist eine optische Übertragungstechnik, die als LiFi (*Light Fidelity*) bezeichnet wird. Sie wird zukünftig der lokalen Kommunikation, z.B. Realisierung von IoT-Services in großen Räumen, dienen können. LiFi stellt eine neue drahtlose Datenübertragungstechnik dar, die das Infrarot- und sichtbare Lichtspektrum nutzt und eine schnelle, bidirektionale drahtlose lokale Kommunikation ermöglicht. Mit LiFi ist eine Übertragungsgeschwindigkeit von 8 Gbit/s erreichbar. Für nähere Informationen über LiFi siehe [7.1.i].

eMBB, URLLC und mMTC als Merkmale von 5G-Mobilfunknetzen

Bedeutung von LiFi

### Internet of Everything

Die Integration neuer 5G-Mobilfunknetze in das IoT kann zu einer Erweiterung von IoT führen, bei der von *Internet of Everything* (IoE) gesprochen werden wird. Für weitere Information über verschiedene Arten von 5G-enabled Mobile IoT Applications siehe:

- 7.1.a i-SCOOP: [5G and IoT in 2018 and beyond: the mobile broadband future of IoT](#)
- 7.1.b Doruk Sahinel, et al.: [Beyond 5G Vision for IOLITE Community](#); IEEE Communications Magazine, Vol. 55(1), Jan 2017, DOI: 10.1109/MCOM.2017.1600372CM
- 7.1.c Sotirios K. Goudos, et al.: [A survey of IoT Key Enabling and Future Technologies: 5G, Mobile IoT, Semantic Web and Applications](#); Wireless Personal Communications, Jul 2017; DOI: 10.1007/s11277-017-4647-8
- 7.1.d Godfrey Akpakwu, et al.: [A Survey on 5G Networks for the Internet of Things: Communication Technologies and Challenges](#); IEEE Access, Vol. 5(12), Dec 2017; DOI: 10.1109/ACCESS.2017.2779844
- 7.1.e Yuh-Shyan Chen, Yi-Ting Tsai: [A Mobility Management Using Follow-Me Cloud-Cloudlet in Fog-Computing-Based RANs for Smart Cities](#); Sensors, Vol. 18(2), Feb 2018; DOI: 10.3390/s18020489
- 7.1.f Shancang Li, Li Da Xu, Shanshan Zhao: [5G Internet of Things: A Survey](#); Journal of Industrial Information Integration, Vol. 10, Jun 2018, DOI: 10.1016/j.jii.2018.01.005
- 7.1.g By Biswa P. S. Sahoo, et al.: [Enabling Millimeter-Wave 5G Networks for Massive IoT Applications](#); Aug 2018, arXiv:1808.04457v1
- 7.1.h Nadeem Javaid, Arshad Sher, Hina Nasir, Nadra Guizani: [Intelligence in IoT-Based 5G Networks: Opportunities and Challenges](#); IEEE Communications Magazine, Vol. 56(10), Oct 2018; DOI: 10.1109/MCOM.2018.1800036
- 7.1.i Harald Haas: [LiFi is a paradigm-shifting 5G technology](#); Reviews in Physics, Vol. 3, Nov. 2018, DOI: 10.1016/j.revip.2017.10.001
- 7.1.j Quoc-Viet Pham, Fang Fang, Vu Nguyen Ha, Md. Jalil Piran, et al: [A Survey of Multi-Access Edge Computing in 5G and Beyond: Fundamentals, Technology Integration, and State-of-the-Art](#); IEEE Access, Vol. 8, Jun 2020; DOI: 10.1109/ACCESS.2020.3001277

## 18.7.2 Vehicle-to-Everything (V2X) Services

### Bedeutung von V2X

In naher Zukunft wird es verschiedene autonom, d.h. ohne einen menschlichen Fahrer, fahrende Fahrzeuge geben. Um unfallfreies autonomes Fahren zu gewährleisten, sind aber noch diverse technische Probleme zu lösen. Flächendeckend muss eine besondere, als IoV (*Internet of Vehicles*) bezeichnete Variante von IoT eingerichtet werden. Dabei werden die 5G-Mobilfunknetze eine enorm große Rolle spielen. Jedes autonom fahrende Fahrzeug muss in der Lage sein, alles was auf Straßen passieren kann, wahrzunehmen und darauf zu reagieren. Das lässt sich nur dadurch erreichen, dass jedes autonom fahrende Vehikel nicht nur mit anderen Fahrzeugen, sondern mit allen

Dingen unterwegs auf eine spezielle Art und Weise kommunizieren kann. Diese Art der Kommunikation soll durch sog. *Vehicle-to-Everything* (V2X) Services ermöglicht werden.

Zum sicheren autonomen Fahren müssen Fahrzeuge mit anderen Fahrzeugen (V2V), mit der angrenzenden Infrastruktur (V2I), mit Internet-basierten Netzwerken (V2N) und auch mit Fußgängern (V2P) kommunizieren können. Daher sind die soeben genannten Arten der Kommunikation – V2V (*Vehicle-to-Vehicle*), V2I (*Vehicle-to-Infrastructure*), V2N (*Vehicle-to-Network*) und V2P (*Vehicle-to-Pedestrian*) – die funktionellen Bestandteile von V2X. Somit ist V2X als Oberbegriff für V2V, V2I, V2N und V2P anzusehen.

V2X als  
Oberbegriff für  
V2V, V2I, V2N  
und V2P

Für Näheres über V2X siehe:

- 7.2.a Dino Flore: [5G V2X: The automotive use-case for 5G](#); 2017
- 7.2.b Mate Boban, et al.: [Use Cases, Requirements, and Design Considerations for 5G V2X](#); Dec 2017, arXiv:1712.01754v1
- 7.2.c Claudia Campolo, et al.: [5G Network Slicing for Vehicle-to-Everything Services](#); IEEE Wireless Communications, Vol. 24(6), Dec 2017; DOI: 10.1109/MWC.2017.1600408
- 7.2.d 5G Americas White Paper: [Cellular V2X Communications Towards 5G](#); March 2018
- 7.2.e Claudia Campolo, Antonella Molinaro, Antonio Iera, Ramon R. Fontes, Christian E. Rothenberg: [Towards 5G Network Slicing for the V2X Ecosystem](#); IEEE Conference on Network Softwarization and Workshops, Jun 2018; DOI: 10.1109/NETSOFT.2018.8459911
- 7.2.f Irena Šeremet, Samir Čaušević: [Benefits of using 5G Network Slicing to implement Vehicle-to-Everything \(V2X\) technology](#); International Symposium INFOTEH-JAHORINA, Mar 2019; DOI: 10.1109/INFOTEH.2019.8717780
- 7.2.g Jie Mei, Xianbin Wang, Kan Zheng: [Intelligent Network Slicing for V2X Services Toward 5G](#); IEEE Network, Vol. 33, Issue 6, Nov -Dec 2019; DOI: 10.1109/MNET.001.1800528
- 7.2.h Md. Noor-A-Rahim, Zilong Liu, Haeyoung Lee, Mohammad Omar Khyam, et al: [6G for Vehicle-to-Everything \(V2X\) Communications: Enabling Technologies, Challenges, and Opportunities](#); Proceedings of the IEEE, Vol. 110, Issue 6, Jun 2022; DOI: 10.1109/JPROC.2022.3173031

### 18.7.3 SDN and NFV for 5G Mobile Networks

Die beiden Konzepte SDN (*Software-Defined Networking*) und NFV (*Network Functions Virtualization*) gelten als neue, sich gegenseitig ergänzende Entwicklungstrends auf dem Gebiet Networking und haben einen großen Einfluss auf die Entwicklungen von 5G Mobile Communications. Mit SDN ist es auf der Grundlage von 5G-Netzwerktechnologien möglich, private 5G-Netzwerke (*private 5G Networks*) zur Unterstützung von Multimedia- und Gruppenkommunikation, z.B. in einem Unternehmen, einzurichten. Um private 5G-Netzwerke einrichten zu können, werden sehr

SDN-enabled 5G  
private Netze

häufig verschiedene virtualisierte netzwerkspezifische Funktionen, sog. VNFs (*Virtualized Network Functions*), eingesetzt. Das SDN-Konzept eignet sich ideal zur Einrichtung eines 5G-Netzwerkes auf Basis von VNFs, zu dessen Management und Adaption an aktuellen Anforderungen. In diesem Zusammenhang kann von 'SD-enabled 5G Private Networks' gesprochen werden.

Für weitere Informationen darüber siehe:

- 7.3.a Junyu Lai, et al.: [Software-defined cellular networking: A practical path towards 5G](#), International Journal of Communication Networks and Distributed Systems; Vol. 14(1), Jan 2015, DOI 10.1504/IJCND.2015.066019
- 7.3.b Ian F. Akyildiz, Pu Wang, Shih-Chun Lin: [SoftAir: A software defined networking architecture for 5G wireless systems](#); Computer Networks, Vol. 85, Jul 2015; DOI: 10.1016/j.comnet.2015.05.007
- 7.3.c Sherif Abdelwahab, Bechir Hamdaoui, Mohsen Guizani, Taieb Znati: [Network function virtualization in 5G](#); IEEE Communications Magazine, Vol. 54, Issue 4, Apr 2016; DOI: 10.1109/MCOM.2016.7452271
- 7.3.d Ricard Vilalta, et al.: [SDN/NFV orchestration of multi-technology and multi-domain networks in cloud/fog architectures for 5G services](#); 21st OptoElectronics and Communications Conference (OECC) held jointly with 2016 International Conference on Photonics in Switching (PS), Jul 2016
- 7.3.e 5G PPP Software Networks WG: [Vision on Software Networks and 5G](#); White Paper, Jan 2017
- 7.3.f Pedro Neves, et al.: [Future mode of operations for 5G – The SELFNET approach enabled by SDN/NFV](#); Computer Standards & Interfaces, Vol. 54(4), Nov 2017; DOI: 10.1016/j.csi.2016.12.008
- 7.3.g Luis Tello-Oquendo, Ian Akyildiz, Shih-Chun Lin, Vicent Pla: [SDN-Based Architecture for Providing Reliable Internet of Things Connectivity in 5G Systems](#); Jul 2018, HAL Id: hal-01832537
- 7.3.h Lu Ma, et al.: [An SDN/NFV Based Framework for Management and Deployment of Service Based 5G Core Network](#); China Communications, Vol. 15(10), Oct. 2018; DOI: 10.1109/CC.2018.8485472
- 7.3.i Faqir Zarrar Yousaf, Michael Bredel, Sibylle Schaller, Fabian Schneider: [NFV and SDN – Key Technology Enablers for 5G Networks](#); IEEE Journal on Selected Areas in Communications, Vol. 35, Issue 11, Nov 2017; DOI: 10.1109/JSAC.2017.2760418
- 7.3.j Srinivasan Sridharan: [A Literature Review of Network Function Virtualization \(NFV\) in 5G Networks](#); International Journal of Computer Trends and Technology, Vol. 68, Issue 10, Oct 2020; DOI: 10.14445/22312803/IJCTT-V68I10P109

#### 18.7.4 5G Network Slicing

In einem speziell für den Support von 5G Mobile Services eingerichteten Datacenter, bzw. in einer speziell hierfür installierten 5G Cloud können aus einzelnen VNFs

(eine Art *Microservices*) isolierte Gruppen untereinander vernetzter VNFs gebildet werden. Eine isolierte Gruppe vernetzter VNFs kann ein privates 5G-Netzwerk bilden. Solch eine Vorgehensweise basiert auf der Realisierung von 5G Network Slicing, und es kommen dabei die Konzepte von SDN und *Network Functions Virtualization* (NFV) zum Einsatz. 5G Network Slicing wird allgemein als Schlüsseltechnologie zur Bildung spontaner, oft privater, an aktuelle Anforderungen anpassungsfähiger (*adaptiver*) 5G-Netzwerke angesehen.

Für weitere Informationen zu diesem Thema siehe:

- 7.4.a SDxCentral: [What is Network Slicing?](#)
- 7.4.b SDxCentral: [What is Dynamic Network Slicing?](#)
- 7.4.c Jose Ordonez-Lucena, et al.: [Network Slicing for 5G with SDN/NFV: Concepts, Architectures, and Challenges](#); IEEE Communications Magazine, Vol. 55(5), May 2017; DOI: 10.1109/MCOM.2017.1600935
- 7.4.d Xenofon Foukas, et al.: [Network Slicing in 5G: Survey and Challenges](#); IEEE Communications Magazine, Vol. 55(5), May 2017, DOI: 10.1109/MCOM.2017.1600951
- 7.4.e Xin Li, et al.: [Network Slicing for 5G: Challenges and Opportunities](#); IEEE Internet Computing, Vol. 21(5) Sep 2017; DOI: 10.1109/MIC.2017.3481355
- 7.4.f Tony Saboorian, Amanda Xiang: [Network Slicing and 3GPP Service and Systems Aspects \(SA\) Standard](#); IEEE Softwarization, Dec 2017
- 7.4.g Claudia Campolo, et al.: [5G Network Slicing for Vehicle-to-Everything Services](#); IEEE Wireless Communications, Vol. 24(6), Dec 2017; DOI: 10.1109/MWC.2017.1600408
- 7.4.h Bessem Sayadi, Laurent Roulet: [5G: Platform and Not Protocol](#), IEEE Softwarization, Jan 2018
- 7.4.i Emmanuel Dotaro: [5G Network Slicing and Security](#); IEEE Softwarization, Jan 2018
- 7.4.j Zbigniew Kotulski, Tomasz Wojciech Nowak, Mariusz Sepczuk, Marcin Tunia, et al: [Towards constructive approach to end-to-end slice isolation in 5G networks](#); EURASIP Journal on Information Security, Vol. 2018, Mar 2018; DOI: 10.1186/s13635-018-0072-0
- 7.4.k Alexandros Kaloylos: [A Survey and an Analysis of Network Slicing in 5G Networks](#); IEEE Communications Standards Magazine, Vol. 2, Issue 1, Mar 2018; DOI: 10.1109/MCOMSTD.2018.1700072
- 7.4.l Ruihan Wen, Gang Feng, Jianhua Tang, Tony Q. S. Quek, Gang Wang, Wei Tan, Shuang Qin: [On Robustness of Network Slicing for Next-Generation Mobile Networks](#); IEEE Transactions on Communications, Vol. 67, Issue 1, Jan 2019; DOI: 10.1109/TCOMM.2018.2868652
- 7.4.m Alcardo Alex Barakabitze, Arslan Ahmad, Rashid Mijumbi, Andrew Hines: [5G network slicing using SDN and NFV: A survey of taxonomy, architectures and future challenges](#); Computer Networks, Vol. 167, Feb 2020; DOI: 10.1016/j.comnet.2019.106984

- 7.4.n Bin Han, Ji Lianghai, Hans D. Schotten: [Slice as an evolutionary service: genetic optimization for inter-Slice resource management in 5G networks](#); IEEE Access, Vol. 6, Jun 2018; DOI: 10.1109/ACCESS.2018.2846543
- 7.4.o Shunliang Zhang: [An Overview of Network Slicing for 5G](#); IEEE Wireless Communications, Vol. 26, Issue 3, Jun 2019; DOI: 10.1109/MWC.2019.1800234

## 18.7.5 5G Network Security

### 5G Network Slicing Security

In den zukünftigen 5G-Mobilfunknetzen kommen die Netzwerktechnologien SDN und NFV zum Einsatz, und darüber hinaus werden diese Mobilfunknetze in das IoT integriert. Aus diesem Grund müssen alle Schwachstellen und Bedrohungen, die in IoT, SDN und NFV vorkommen können, auch bei der Analyse der Sicherheit in 5G-Mobilfunknetzen berücksichtigt werden. Die Bildung von virtuellen privaten 5G-Netzwerken mit SDN und NFV, was man als *5G Network Slicing* bezeichnet, schafft dabei auch zusätzlich neue Sicherheitslücken und Bedrohungen. Folglich ist die Sicherheit in zukünftigen 5G-Mobilfunknetzen, kurz als *5G Security* bezeichnet, ein sehr wichtiges, breites und komplexes Forschungs- und Entwicklungsgebiet.

Daher muss die Analyse der Sicherheit in 5G-Mobilfunknetzen global und systematisch durchgeführt werden, um dabei möglichst sämtliche Sicherheitslücken und Bedrohungen zu erfassen und damit die entsprechenden Sicherheitsmaßnahmen einplanen zu können.

Eine Sammlung von Sicherheitsrichtlinien zur Analyse der Sicherheit in 5G-Mobilfunknetzen ist in [5G PPP Security WG] und [3GPP TS 33.501x] enthalten. Für weitere Information zu '5G Security' ist zu empfehlen:

- 7.5.a [3GPP 5G Security](#)
- 7.5.b Huawei White Paper: [5G Security: Forward Thinking](#)
- 7.5.c SDxCentral: [What Are the Top 5G Security Challenges?](#)
- 7.5.d ITU-T: [Security in Telecommunications and Information Technology](#); An overview of issues and the deployment of existing ITU-T Recommendations for secure telecommunications, September 2015
- 7.5.e 5G PPP Security WG: [5G PPP Phase 1 Security Landscape](#); Jun 2017
- 7.5.f Ijaz Ahmad, et al.: [5G Security: Analysis of Threats and Solutions](#); 2017 IEEE Conference on Standards for Communications and Networking (CSCN), Sep 2017; DOI: 10.1109/CSCN.2017.8088621
- 7.5.g Dongfeng Fang, Yi Qian, Rose Qingyang Hu: [Security for 5G Mobile Wireless Networks](#); IEEE Access, Vol. 6, Dec 2017; DOI: 10.1109/ACCESS.2017.2779146
- 7.5.h Emmanuel Dotaro: [5G Network Slicing and Security](#); IEEE Softwarization, Jan 2018

- 7.5.i Ijaz Ahmad, et al.: [Overview of 5G Security Challenges and Solutions](#); IEEE Communications Standards Magazine, Vol. 2(1), Mar 2018; DOI: 10.1109/MCOMSTD.2018.1700063
- 7.5.j 3GPP TS 33.501: [Technical Specification Group Services and System Aspects; Security architecture and procedures for 5G system](#); Sep 2018
- 7.5.j Jiaying Yao, Zhigeng Han, Muhammad Sohail, Liangmin Wang: [A Robust Security Architecture for SDN-Based 5G Networks](#); Future Internet, Vol. 11 Issue 4, Mar 2019; DOI: 10.3390/fi11040085

### 18.7.6 6G als zukünftige Vision der Mobilfunknetze

Obwohl die 5G-Mobilfunknetze noch nicht weitgehend im Einsatz sind, arbeiten führende Technologieunternehmen bereits an der Entwicklung des nächsten Meilensteins für die drahtlose universelle Kommunikation – dieser wird als sechste Generation (6G) der Mobilfunknetze bezeichnet. Ein wichtiges Ziel der Entwicklung der 6G-Mobilfunknetze ist es, verschiedene technische Möglichkeiten der künstlichen Intelligenz (KI) in sich zu integrieren. Die 6G-Mobilfunknetze sollen adaptive Netzwerkarchitekturen mit allgegenwärtigen KI-Fähigkeiten bilden. Die Vision für 6G und seine technischen Grundlagen ist jedoch noch im Entstehen. Für fundierte Informationen über 6G-Mobilfunknetze sei verwiesen auf:

KI-fähige und  
adaptive  
Mobilfunknetze

- 7.6.a Marco Giordani, Michele Polese, Marco Mezzavilla, Sundeep Rangan, Michele Zorzi: [Towards 6G Networks: Use Cases and Technologies](#); arXiv:1903.12216v2, Feb 2020; DOI: 10.48550/arXiv.1903.12216
- 7.6.b Yifei Yuan, Yajun Zhao, Baiqing Zong, Sergio Parolari: [Potential Key Technologies for 6G Mobile Communications](#); arXiv:1910.00730; Mar 2020; DOI: 10.48550/arXiv.1910.00730
- 7.6.c Mohammed H. Alsharif, Anabi Hilary Kelechi, Mahmoud A. Albreem, Shehzad Ashraf Chaudhry, M. Sultan Zia, Sunghwan Kim: [Sixth Generation \(6G\) Wireless Networks: Vision, Research Activities, Challenges and Potential Solutions](#); Symmetry, Vol. 12, Issue 4, Apr 2020; DOI: 10.3390/sym12040676
- 7.6.d Pawani Porambage, Gürkan Gür, Diana Pamela Moya Osorio, Madhusanka Liyanage, Andrei Gurtov, Mika Ylianttil: [The Roadmap to 6G Security and Privacy](#); IEEE Open Journal of the Communications Society, Vol. 2, May 2021; DOI: 10.1109/OJCOMS.2021.3078081
- 7.6.e Nei Kato, Bomin Mao, Fengxiao Tang, Yuichi Kawamoto, Jiajia Liu: [Ten Challenges in Advancing Machine Learning Technologies toward 6G](#); IEEE Wireless Communications, Vol. 27, Issue 3, Jun 2020; DOI: 10.1109/MWC.001.1900476
- 7.6.f Ian F. Akyildiz, Ahan Kak, Shuai Nie: [6G and Beyond: The Future of Wireless Communications Systems](#); IEEE Access, Vol. 8, Jul 2020; DOI: 10.1109/ACCESS.2020.3010896



- 7.6.g Guangyi Liu, Yuhong Huang, Na Li, Jing Dong, Jing Jin, Qixing Wang, Nan Li: [Vision, requirements and network architecture of 6G mobile network beyond 2030](#); China Communications, Vol. 17, Issue 9, Sep 2020; DOI: 10.23919/JCC.2020.09.008
- 7.6.h Alcardo Alex Barakabitze, Ray Walshe: [SDN and NFV for QoE-driven multi-media services delivery: The road towards 6G and beyond networks](#); Computer Networks, Vol. 214, Sep 2022; DOI: 10.1016/j.comnet.2022.109133
- 7.6.i Mohammed Banafaa, Ibraheem Shaye, Jafri Din, Marwan Hadri Azmi, Abdulaziz Alashbi, Yousef Ibrahim Daradkeh, Abdurraqeb Alhammadi: [6G Mobile Communication Technology: Requirements, Targets, Applications, Challenges, Advantages, and Opportunities](#); Alexandria Engineering Journal, Sep 2022; DOI: 10.1016/j.aej.2022.08.017

## 18.8 Information-Centric Networking and Services

### Host-Centric Networking im Internet

Das Internet dient heutzutage nicht nur der Kommunikation zwischen Rechnern, sondern ist ein universales Informationsnetz, d.h. quasi eine weltweit verteilte Informationsbasis. Da im Internet die Kommunikation zwischen Rechnern, sog. Hosts, heute aber noch im Vordergrund steht, ist es aktuell ein rechnerzentriertes Netz – also ein Host-Centric Network. Die Charakteristik eines rechnerzentrierten Netzes besteht darin, dass jede Internetadresse in der Form von URL (*Uniform Resource Locator*) bzw. von URI (*Uniform Resource Identifier*), in der Regel mithilfe von DNS, auf eine Host-Adresse aufgelöst (quasi abgebildet) werden muss. Das heutige DNS stellt de facto ein weltweit verteiltes Resolving-System von URLs bzw. URIs auf Host-Adressen dar. Man könnte aber ein anderes globales Resolving-System bzw. mehrere lokale, weltweite verteilte, kleinere Resolving-Systeme nutzen. Die Folge wäre u.a. beispielsweise Information-Centric Networking.

### Information-Centric Networking (ICN)

Damit das Internet zukünftig den stark wachsenden, mit einem universalen Informationsnetz verbundenen Herausforderungen gerecht werden kann, muss das ihm zugrunde liegende rechnerzentrierte Kommunikationsprinzip um ein neues, zukunftsweisendes Prinzip erweitert werden. Das Kommunikationsprinzip im Internet sollte in Zukunft nicht nur *Rechner-zentriert (Host-Centric)*, sondern auch *Informations-zentriert (Information-Centric)* sein. Der Zugriff auf eine gewünschte Information sollte also nur durch die Angabe von deren Namen – und nicht die ihrer Lokation – erfolgen. In diesem Zusammenhang spricht man heute von *Information-Centric Networking (ICN)*. Da Daten bzw. verschiedene Content-Arten (z.B. Audio, Video, Streaming Medien) allgemein betrachtet als Arten von Information anzusehen sind, werden als Synonyme für ICN häufig die Begriffe NDN (*Named Data Networking*) und CCN (*Content-Centric Networking*) verwendet.

### Internet-Dual-Mode: 'Host-Centric' und 'Information-Centric'

Es sei angemerkt, dass das Internet (theoretisch betrachtet) nach zwei Prinzipien, also 'Host-Centric' und 'Information-Centric', genutzt werden kann. Somit könnte es in einer Art Dual-Mode betrieben werden. Zu diesem Zweck müssen weitere Resolving-

Systeme – zusätzlich zum DNS – installiert werden. Mit deren Hilfe werden Informationsnamen, z.B. in Form von URNs (*Uniform Resource Names*), auf speziellen Containern, quasi Speicherplätzen, in denen auf die Rechnern mit gewünschten Informationen verwiesen wird, aufgelöst/abgebildet. Nach einem ähnlichen Prinzip funktioniert das als ENUM bezeichnete Resolving von Telefonnummern auf IP-Adressen zwecks Internettelefonie [Abschnitt 5.7].

ICN ist ein neuer Ansatz, der über das Internet den direkten Zugriff auf mit eindeutigen Namen/Identifikationen versehene Informationen, unabhängig von deren Herkunft und aktueller Lokation im Internet ermöglicht, ohne hierfür vorher Verbindungen zu Rechnern mit diesen Informationen aufbauen zu müssen. Es wird in diesem Zusammenhang von *IC Services* (IC: Information-Centric) gesprochen. Die Erbringung verschiedener Arten von IC Services lässt sich gut mit dem Konzept *Location-to-Service Translation* (LoST) unterstützen. LoST kann dazu verwendet werden, mittels mobiler Endgeräte (Smartphones, Bordcomputern in Autos) unterwegs Informationen darüber zu erhalten, welche IoT-Services es in direkter Nähe gibt, damit diese daraufhin mit den mobilen Endgeräten abgerufen werden können.

LoST als Support  
zu IC Services

Auf dem Konzept von ICN basieren u.a. die folgenden Networking-Trends: *Software-Defined ICN* (SD ICN), *IC Internet of Things* (IC IoT). Insbesondere sind *IC Services in Smart Cities* hervorzuheben. Diese eben genannten Trends werden mit dem Trend *Information-Centric Networking Security* (ICN Security) zusammengefasst. Für allgemeine Information darüber siehe:

- 8.a Aytac Azgin, Ravishankar Ravindran, Guoqiang Wang: [A Scalable Mobility-Centric Architecture for Named Data Networking](#); Jun 2014; arXiv:1406.7049v1
- 8.b Marica Amadeo, Claudia Campolo, Antonella Molinaro, Giuseppe Ruggeri: [Content-centric wireless networking: A survey](#); Computer Networks, Vol. 72, Oct 2014; DOI: 10.1016/j.comnet.2014.07.003
- 8.c RFC 7476: [Information-Centric Networking: Baseline Scenarios](#), Mar 2015
- 8.d Anatol Badach: [LoST - Location-to-Service Translation](#); In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Aug 2015; DOI: 10.13140/RG.2.1.4314.2887
- 8.e RFC 7927: [Information-Centric Networking \(ICN\) Research Challenges](#); Jul 2016
- 8.f José Quevedo, et al.: [On the application of contextual IoT service discovery in Information Centric Networks](#); Computer Communications, Vol. 89–90, Sep 2016; DOI: 10.1016/j.comcom.2016.03.011
- 8.g Marica Amadeo, et al.: [Information-centric networking for M2M communications: Design and deployment](#); Computer Communications, Vol. 89–90, Sep 2016; DOI: 10.1016/j.comcom.2016.03.009
- 8.h Bin Da, Richard Li, Xiaofei Xu: [ID Oriented Networking \(ION\) for IoT Interoperation](#); 2017 Global Internet of Things Summit (GIoTS), Jun 2017; DOI: 10.1109/GIOTS.2017.8016237
- 8.i Dennis Grewe, et al.: [Information-Centric Mobile Edge Computing for Connected Vehicle Environments: Challenges and Research Directions](#); MECOMM '17

- Proceedings of the Workshop on Mobile Edge Communications, Aug 2017; DOI: 10.1145/3098208.3098210
- 8.j Cenk Gündogan, et al.: [Information-Centric Networking for the Industrial IoT](#); ICN '17 Proceedings of the 4th ACM Conference on Information-Centric Networking, Sep 2017; DOI 10.1145/3125719.3132099
- 8.k Bin Da, et al.: [Identity/Identifier-Enabled Networks \(IDEAS\) for Internet of Things \(IoT\)](#); 2018 IEEE 4th World Forum on Internet of Things (WF-IoT), Feb 2018; DOI: 10.1109/WF-IoT.2018.8355102
- 8.l Chao Fang, Haipeng Yao, Zhuwei Wang, Wenjun Wu, Xiaoning Jin, F. Richard Yu: [A Survey of Mobile Information-Centric Networking: Research Issues and Challenges](#); IEEE Communications Surveys & Tutorials, Vol. 20, Issue 3, Feb 2018; DOI:10.1109/COMST.2018.2809670
- 8.m Rehmat Ullah, Syed Hassan Ahmed, Byung-Seo Kim: [Information-Centric Networking With Edge Computing for IoT: Research Challenges and Future Directions](#); IEEE Access, Vol. 6, Dec 2018; DOI: 10.1109/ACCESS.2018.2884536
- 8.n Keping Yu, Suyong Eum, Toshihiko Kurita, Qiaozhi Hua, Takuro Sato, Hidenori Nakazato, Tohru Asami, Ved P. Kafle: [Information-Centric Networking: Research and Standardization Status](#); IEEE Access, Vol. 7, Aug 2019; DOI: 10.1109/ACCESS.2019.2938586
- 8.o RFC 8763; [Deployment Considerations for Information-Centric Networking \(ICN\)](#), Apr 2020
- 8.p Armielle Noulapeu Ngaffo, Walid El Ayeb, Zièd Choukair: [Information-Centric Networking Challenges and Opportunities in Service Discovery: A Survey](#); IEEE Eighth International Conference on Communications and Networking (ComNet), Oct 2020; DOI: 10.1109/ComNet47917.2020.9306088
- 8.q Boubakr Nour, Spyridon Mastorakis, Rehmat Ullah, Nicholas Stergiou: [Information-Centric Networking in Wireless Environments: Security Risks and Challenges](#); IEEE Wireless Communications, Vol. 28, Issue 2, Apr 2021; DOI: 10.1109/MWC.001.2000245
- 8.r RFC 9139: [Information-Centric Networking \(ICN\) Adaptation to Low-Power Wireless Personal Area Networks \(LoWPANs\)](#); Nov 2021

### 18.8.1 Software-Defined ICN (SD ICN)

Software definierte, informationszentrische Netzwerke

Moderne Geräte wie Smartphones, Laptops und Tablets, die über drahtlose Netzwerke den Zugang zum Internet haben, werden immer beliebter. Sie ermöglichen den Benutzern Mobilität und Flexibilität beim Zugriff auf das Internet an jedem Ort (z.B. zu Hause, im Büro, in Geschäften, Autos) und zu jeder Zeit. Die Internet-Nutzung mithilfe dieser Geräte sollte in der Zukunft nicht nur wie heute rechnerzentrisch (Host-Centric) sein, sondern auch informationszentrisch (Information-Centric). Es sollte möglich sein, die gewünschte Information durch die Angabe ihrer strukturierten Namen – einer Art URNs (*Uniform Resource Names*) – aus dem Internet zu erhalten, ohne dabei eine Suchmaschine (wie z.B. Google) nutzen zu müssen. Um eine solche Wunschvorstellung zu verwirklichen, also ein ICN einzurichten, können einige Kon-

zepte aus dem Gebiet SDN (*Software-Defined Networking*) übernommen werden. Ist dies der Fall, spricht man von *Software-Defined ICN* (SD ICN). Dabei liefert SDN einige Ideen zur Bereitstellung von ICN-Architekturen und kann die Funktionalität und Verwaltung von ICNs erheblich vereinfachen. Für weitere Information über SD ICN ist zu empfehlen:

- 8.1.a Jinfan Wang, Wei Gao, Yuqing Liang, Rui Qin, Jianping Wang, Shucheng Liu: [SD-ICN: An interoperable deployment framework for software-defined information-centric networks](#); IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), May 2014; DOI: 10.1109/INFOCOMW.2014.6849199
- 8.1.b Shuai Gao, Yujing Zeng, Hongbin Luo, Hongke Zhang: [Scalable Area-based Hierarchical Control Plane for Software Defined Information Centric Networking](#); 23rd International Conference on Computer Communication and Networks (ICCCN), Aug 2014; DOI: 10.1109/ICCCN.2014.6911839
- 8.1.c Niels L. M. van Adrichem, Fernando A. Kuipers: [NDNFlow: Software-defined Named Data Networking](#), 1st IEEE Conference on Network Softwarization (NetSoft), Apr 2015; DOI: 10.1109/NETSOFT.2015.7116131
- 8.1.d Suyong Eum, Masahiro Jibiki, Masayuki Murata, Hitoshi Asaeda, Nozomu Nishinaga: [A design of an ICN architecture within the framework of SDN](#); Seventh International Conference on Ubiquitous and Future Networks, Jul 2015; DOI: 10.1109/ICUFN.2015.7182521
- 8.1.e Alex F R Trajano, Marcial P Fernandez: [ContentSDN: A Content-Based Transparent Proxy Architecture in Software-Defined Networking](#); IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Mar 2016; DOI: 10.1109/AINA.2016.103
- 8.1.f Sergio Charpinel, Celso Alberto Saibel Santos, Alex Borges Vieira, Magnos Martinello, Rodolfo Villaca: [SDCCN: A Novel Software Defined Content-Centric Networking Approach](#); IEEE 30th International Conference on Advanced Information Networking and Applications (AINA), Mar 2016; DOI: 10.1109/AINA.2016.86
- 8.1.g Changyou Xing, Ke Ding, Chao Hu, Ming Chen, Bo Xu: [SD-ICN: Toward Wide Area Deployable Software Defined Information Centric Networking](#); KSII Transactions on Internet and Information Systems, Vol. 10(5), May 2016; DOI: 10.3837/tiis.2016.05.017
- 8.1.h Anwar Kalghoum, Mettali Gammar: [Towards New Information Centric Networking Strategy Based on Software Defined Networking](#); IEEE Wireless Communications and Networking Conference (WCNC), Mar 2017; DOI: 10.1109/WCNC.2017.7925536
- 8.1.i Rihab Jmal, Lamia Chaari Fourati: [Content-Centric Networking Management Based on Software Defined Networks: Survey](#); IEEE Transactions on Network and Service Management, Vol. 14(4), Dec 2017; DOI: 10.1109/TNSM.2017.2758681

- 8.1.j Qing-Yi Zhang, Xing-Wei Wang, Min Huang, Ke-Qin Li, Sajal K. Das: [Software Defined Networking Meets Information Centric Networking: A Survey](#); IEEE Access, Vol. 6, Jul 2018; DOI: 10.1109/ACCESS.2018.2855135
- 8.1.k Yousef Fazea, Fathey Mohammed: [Software Defined Networking based Information Centric Networking: An Overview of Approaches and Challenges](#) International Congress of Advanced Technology and Engineering (ICOTEN), Jul 2021; DOI: 10.1109/ICOTEN52080.2021.9493541
- 8.1.l P. Benedetti, G. Piro, L. A. Grieco: [An Energy Efficient and Software-Defined Information-Centric Networking Approach to Consumer Mobility](#); 22nd International Conference on Transparent Optical Networks (ICTON), Jul 2020; DOI: 10.1109/ICTON51198.2020.9203400

## 18.8.2 Information-Centric IoT (IC IoT)

### IC Internet of Things (IC IoT)

Die Ideen von ICN werden auch in das Internet of Things (IoT) integriert. In diesem Zusammenhang wird von *ICN-based IoT* oder von *ICN-enabled IoT* gesprochen, und man bezeichnet diese Art von IoT kurz als *ICN IoT*. Um Information-Centric (IC) Services im IoT zu ermöglichen, können sowohl spezielle Clouds als auch Fog Nodes eingesetzt werden [Abb. 17.1-4], um IoT-relevante Informationen zentral in Clouds oder entlang des Internet Edge lokal in Fog Nodes zu speichern. In diesem Fall können Clouds als 'Central Information Caches' und Fog Nodes als 'Local Information Caches' dienen. Denn in diesen Caches gespeicherte Informationen können so strukturierte Namen wie z.B. URNs zugewiesen werden, damit sie durch die Angabe von URNs von mobilen Endgeräten abgerufen werden können. Für Näheres darüber siehe:

- 8.2.a Marica Amadeo, Claudia Campolo, Antonio Iera, Antonella Molinaro: [Named data networking for IoT: An architectural perspective](#); European Conference on Networks and Communications (EuCNC), Jun 2014; DOI: 10.1109/EuCNC.2014.6882665
- 8.2.b Emmanuel Baccelli, et al.: [Information Centric Networking in the IoT: Experiments with NDN in the Wild](#); Proceeding ACM-ICN '14, Proceedings of the 1st ACM Conference on Information-Centric Networking, Sep 2014; DOI: 10.1145/2660129.2660144
- 8.2.c José Quevedo, Daniel Corujo, Rui Aguiar: [A case for ICN usage in IoT environments](#); IEEE Global Communications Conference, Dec 2014; DOI: 10.1109/GLOCOM.2014.7037227
- 8.2.d Marica Amadeo, Claudia Campolo, Antonella Molinaro: [Forwarding strategies in named data wireless ad hoc networks: Design and evaluation](#); Journal of Network and Computer Applications, Vol. 50, Apr 2015; DOI: 10.1016/j.jnca.2014.06.007
- 8.2.e Riccardo Petrolo, Valeria Loscri, Nathalie Mitton: [Towards a smart city based on cloud of things, a survey on the smart city vision and paradigms](#); Transactions on Emerging Telecommunications Technologies, Mar 2015; DOI: 10.1002/ett.2931

- 8.2.f Marica Amadeo, Claudia Campolo, Antonio Iera, Antonella Molinaro: [Information Centric Networking in IoT scenarios: the Case of a Smart Home](#); IEEE International Conference on Communications (ICC), Jun 2015; DOI: 10.1109/ICC.2015.7248395
- 8.2.g Zhou Su, Qichao Xu: [Content Distribution over Content-Centric Mobile Social Networks in 5G](#); IEEE Communications Magazine, Vol. 53(6) , Jun 2015; DOI: 10.1109/MCOM.2015.7120047
- 8.2.h Marica Amadeo, et al.: [Information-centric networking for the internet of things: challenges and opportunities](#); IEEE Network, Vol. 30(2), Mar-Apr 2016; DOI: 10.1109/MNET.2016.7437030
- 8.2.i Yongrui Qin, et al.: [When things matter: A survey on data-centric Internet of Things](#); Journal of Network and Computer Applications, Vol. 64, Apr 2016; DOI: 10.1016/j.jnca.2015.12.016
- 8.2.j Soumya Kanti Datta, et al.: [DataTweet: An Architecture Enabling Data-Centric IoT Services](#); IEEE Region 10 Symposium (TENSYMP), May 2016; DOI: 10.1109/TENCONSpring.2016.7519430
- 8.2.k Marica Amadeo, et al.: [Information-centric networking for M2M communications: Design and deployment](#); Computer Communications, Vol. 89–90, Sep 2016; DOI: 10.1016/j.comcom.2016.03.009
- 8.2.l Xuan Liu, Zhuo Li, Peng Yang, Yongqiang Dong: [Information-centric mobile ad hoc networks and content routing: A survey](#); Ad Hoc Networks, Vol. 58, 2017; DOI: 10.1016/j.adhoc.2016.04.005
- 8.2.m Toshihiko Kurita, Izuru Sato, Kenichi Fukuda, Toshitaka Tsuda: [An Extension of Information-Centric Networking for IoT Applications](#); International Conference on Computing, Networking and Communications (ICNC), Jan 2017; DOI: 10.1109/ICCNC.2017.7
- 8.2.n draft-zhang-icnrg-icniot-architecture-01: [ICN based Architecture for IoT](#); Jul 2017
- 8.2.o Sripriya Srikant Adhatarao, Mayutan Arumaiturai, Xiaoming Fu: [FOGG: A Fog Computing Based Gateway to Integrate Sensor Networks to Internet](#); 29th International Teletraffic Congress (ITC 29), Sep 2017; DOI: 10.23919/ITC.2017.8065709
- 8.2.p Marica Amadeo, Claudia Campolo, Antonella Molinaro: [A novel hybrid forwarding strategy for content delivery in wireless information-centric networks](#); Computer Communications, Vol. 109, Sep 2017; DOI: 10.1016/j.comcom.2017.05.012
- 8.2.q Maroua Meddeb: [Information-Centric Networking, A natural design for IoT applications ?](#); INSA de Toulouse, 2017; HAL Id: tel-01661302
- 8.2.r Soumya Kanti Datta, Christian Bonnet: [Next-Generation, Data Centric and End-to-End IoT Architecture Based on Microservices](#), 3rd International Conference on Consumer Electronics (ICCE), Jun 2018
- 8.2.s Sobia Arshad, et al.: [Recent Advances in Information-Centric Networking based Internet of Things \(ICN-IoT\)](#); arXiv:1710.03473v3; Oct 2018

- 8.2.t Marica Amadeo, Giuseppe Ruggeri, Claudia Campolo, Antonella Molinaro, Valeria Loscrí, Carlos T. Calafate: [Fog Computing in IoT Smart Environments via Named Data Networking: A Study on Service Orchestration Mechanisms](#); Future Internet, Vol. 11, Issue 11, Oct 2019; DOI:10.3390/fi11110222
- 8.2.u Wajid Rafique, Abdelhakim Senhaji Hafid, Soumaya Cherkaoui: [Complementing IoT Services Using Software Defined Information Centric Networks: A Comprehensive Survey](#); IEEE Internet of Things Journal, Sep 2022;

### 18.8.3 Information-Centric Services für Smart Cities

#### Location-based IC Services

Wir nutzen mobile Endgeräte wie Smartphones und Tablets mit Internetzugang. Diese Endgeräte verfügen in der Regel über eine wichtige Komponente – nämlich ein Navigationssystem. Dadurch können sie dem Internet die Angaben über ihre Lokation/Position auf der Erdkugel liefern. Das bereits eben erwähnte Konzept LoST kann dazu verwendet werden, die Lokation mobiler Endgeräte im Internet so zu nutzen, dass verschiedene, von den mobilen Internetnutzern nicht weit entfernte, verfügbare Dienste/Angebote ermittelt werden. Daraufhin können sie den Internetnutzern bekannt gemacht und somit von diesen unterwegs in Anspruch genommen werden. Dies kann zu neuen Formen von Internetdiensten führen. Diese Services kann man als Location-based IC Services bezeichnen [Abschnitt 17.4]

#### IC Services für Smart Cities

IC Services und insbesondere Location-based IC Services haben eine wichtige Bedeutung bei der Entwicklung der Konzepte für Smart Cities. Damit man diese Services realisieren kann, ist ein verteiltes (dezentrales) Resolving-System in Form von strukturierten Informationsnamen erforderlich, also von den lokalen/ortsgebundenen Informationen zugewiesenen URNs auf die Adressen von Rechnern mit diesen Informationen. Um Location-based IC Services mit einem mobilen Endgerät in Anspruch zu nehmen, muss die Angabe über die Geo-Lokation dieses Endgeräts auf die IP-Adresse des benötigten lokalen Resolving-Systems von strukturierten Informationsnamen (URNs nämlich) auf die Adressen von Rechnern mit diesen gewünschten Informationen erfolgen. Für weitere Information über IC Services für Smart Cities sei verwiesen auf:

- 8.3.a I. Cianci, G. Piro, L. A. Grieco, G. Boggia, P. Camarda: [Content Centric Services in Smart Cities](#); Sixth International Conference on Next Generation Mobile Applications, Services and Technologies; Sep 2012; DOI 10.1109/NG-MAST.2012.20
- 8.3.b G. Piro, et al.: [Information Centric Services in Smart Cities](#); Journal of Systems and Software, Vol. 88(C), Feb 2014; DOI: 10.1016/j.jss.2013.10.029
- 8.3.c Marica Amadeo, et al.: [Information-Centric Networking for Connected Vehicles: A survey and Future Perspectives](#); IEEE Communications Magazine, Vol. 54(2), Feb 2016; DOI: 10.1109/MCOM.2016.7402268
- 8.3.d Ali Shariat, Ali Tizghadam, Alberto Leon-Garcia: [An ICN-Based Publish-Subscribe Platform to Deliver UAV Service in Smart Cities](#); IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), Apr 2016, DOI: 10.1109/INFCOMW.2016.7562167

- 8.3.e Rida Khatoun, Sherali Zeadally: [Smart cities: concepts, architectures, research opportunities](#); Communications of the ACM, Vol. 59(8), Aug 2016; DOI: 10.1145/2858789
- 8.3.f [LASER: Lightweight Authentication and Secured Routing for NDN IoT in Smart Cities](#); Mar 2017; arXiv:1703.08453v1
- 8.3.g Meng Wang, et al.: [Toward mobility support for information-centric IoV in smart city using fog computing](#); IEEE International Conference on Smart Energy Grid Engineering (SEGE), Aug 2017; DOI: 10.1109/SEGE.2017.8052825
- 8.3.h M. Govoni, et al.: [An Information-Centric Platform for Social- and Location-Aware IoT Applications in Smart Cities](#); EAI Endorsed Transactions on Internet of Things, Vol. 17(9), Aug 2017; DOI: 10.4108/eai.31-8-2017.153049
- 8.3.i Carmen Rotuna, et al.: [Smart City Applications Built on Big Data Technologies and Secure IoT](#);
- 8.3.j Yang Zhang, Zehui Xiong, Dusit Niyato, Ping Wang, Zhu Han: [Market-Oriented Information Trading in Internet of Things \(IoT\) for Smart Cities](#); Jun 2018, arXiv:1806.05583v1
- 8.3.k Sobia Arshad, et al.: [Towards Information-Centric Networking \(ICN\) Naming for Internet of Things \(IoT\): The Case of Smart Campus](#); Jun 2018; arXiv:1711.10304v1
- 8.3.l Hong Xu, Xuexian Geng: [People-Centric Service Intelligence for Smart Cities](#); Smart Cities, Vol. 2 Issue 2, Apr 2019; DOI: 10.3390/smartcities2020010
- 8.3.m Atiyeh Javaheri, Seyyed Naser Seyyed Hashemi, Ali Bohlooli: [Hybrid Naming Scheme Based PURSUIT Architecture for Smart City](#); 4th International Conference on Smart City, Internet of Things and Applications (SCIOT); Sep 2020; DOI: 10.1109/SCIOT50840.2020.9250207

#### 18.8.4 ICN Security

Das ICN ist ein neues Kommunikationsparadigma, das sich auf das Abrufen von Informationen aus dem Internet bzw. aus einem privaten Netzwerk konzentriert, wobei die abzurufenden Informationen mit ihren Namen angegeben werden und nicht – wie im heutigen Internet – mit den Adressen von Rechnern, auf denen sie zu finden sind. Ein derartiges neues Kommunikationsparadigma bringt auch neue Sicherheitsprobleme mit sich. Beim ICN ist die Sicherung der Information, also der Inhalte selbst, auf den ersten Blick viel wichtiger als die Probleme der klassischen Netzwerksicherheit. Um die Sicherheitsziele in diesem neuen ICN-Paradigma zu erreichen, ist ein umfassendes Verständnis der ICN-spezifischen Angriffe, ihrer Klassifizierung und der Lösungsvorschläge von entscheidender Bedeutung. Es gibt verschiedene Angriffsarten – und zwar solche, die direkt nur ICN betreffen, und solche, die sich indirekt auf ICN auswirken.

Neue Sicherheitsanforderungen beim ICN

Für weitere Information über ICN Security ist zu empfehlen:



- 8.4.a Abdelberi Chaabane, et al.: [Privacy in Content-Oriented Networking: Threats and Countermeasures](#); ACM SIGCOMM Computer Communication Review, Vol. 43(3), Jul 2013; DOI 10.1145/2500098.2500102
- 8.4.b Nikos Fotiou, et al.: [A Framework for Privacy Analysis of ICN Architectures](#); Proc. Second Annual Privacy Forum (APF), Springer, 2014; DOI 10.1007/978-3-319-06749-0\_8
- 8.4.c Eslam G. AbdAllah, Hossam S. Hassanein, Mohammad Zulkernine: [A Survey of Security Attacks in Information-Centric Networking](#); IEEE Communications Surveys & Tutorials, Vol. 17(3), Jan 2015; DOI: 10.1109/COMST.2015.2392629
- 8.4.d Muhammad Aamir, Syed Mustafa Ali Zaidi: [Denial-of-service in content centric \(named data\) networking: a tutorial and state-of-the-art survey](#); Security and Communication Networks, 2015; DOI: 10.1002/sec.1149
- 8.4.e Mahdi Aiash, Jonathan Loo: [An integrated authentication and authorization approach for the network of information architecture](#); Journal of Network and Computer Applications, Vol. 50, Apr 2015; DOI: 10.1016/j.jnca.2014.06.004
- 8.4.f Roman Lutz: [Security and Privacy in Future Internet Architectures: Benefits and Challenges of Content Centric Networks](#); Jan 2016; arXiv:1601.01278v2
- 8.4.g RFC 7945: [Information-Centric Networking: Evaluation and Security Considerations](#); Sep 2016
- 8.4.h Sabrina Sicari, et al.: [A Secure ICN-IoT Architecture](#); IEEE International Conference on Communications; May 2017; DOI: 10.1109/ICCW.2017.7962667
- 8.4.i Reza Tourani, Travis Mick, Satyajayant Misra, Gaurav Panwar: [Security, Privacy, and Access Control in Information-Centric Networking: A Survey](#); Jun 2017, arXiv:1603.03409v
- 8.4.j Kaiping Xue, Xiang Zhang, Qiudong Xia, David S.L. Wei, Hao Yue, Feng Wu: [SEAF: A Secure, Efficient and Accountable Access Control Framework for Information Centric Networking](#); INFOCOM 2018 - IEEE Conference on Computer Communications, Apr 2018; DOI: 10.1109/INFOCOM.2018.8486407
- 8.4.k Xiaoming Fu, Dirk Kutscher, Satyajayant Misra, Ruidong Li: [Information-Centric Networking Security](#); IEEE Communications Magazine, Vol. 56, Issue 11, Nov 2018; DOI: 10.1109/MCOM.2018.8539022

## 18.9 Time-Sensitive and Deterministic Networking

### IT/OT-Konvergenz

Die Migration zum IoT (insbesondere zum IoT im industriellen Bereich, also zum Industrial IoT (IIoT)) führt dazu, dass zwei Bereiche in industriellen Unternehmen konvergieren: nämlich der Bereich IT (*Information Technology*, Informationstechnologie) und der Bereich OT (*Operational Technology*, Betriebstechnologie/Betriebstechnik). In diesem Zusammenhang und in Verbindung zur Industrie 4.0 spricht man von der

*IT/OT-Konvergenz*. Diese neue Konvergenz stellt besondere Anforderungen an Netzwerke und Kommunikationsprotokolle in industriellen Bereichen.

In der Vergangenheit war die Trennung der Bereiche IT und OT vor allem sachlich begründet, denn die Bereiche IT und OT hatten vorher getrennte Aufgabenprofile, und aus diesem Grund waren in diesen beiden Bereichen verschiedene Netzwerkkonzepte und Kommunikationsprotokolle im Einsatz. In OT-Bereichen wurden lange Zeit in sich geschlossene, proprietäre Systeme eingesetzt, und diese verfügten oft über keine Verbindungen zur Außenwelt. Die IT/OT-Konvergenz, insbesondere die Verwirklichung von IIoT, verlangt aber, dass neue Anforderungen an industrielle Netzwerke gestellt werden müssen. Dabei unterscheidet man zwischen zwei Arten von Anforderungen, und um diese zu erfüllen, wurden diese beiden Arten von Networking konzipiert, und sie werden noch weiter intensiv entwickelt. Es handelt sich um: *Time-Sensitive Networking* (TSN) und *Deterministic Networking* (DetNet).

Anforderungen  
der IT/OT-  
Konvergenz

Für weitere und allgemeine Information über diese beiden Arten von Networking im industriellen Bereich sei verwiesen auf:

- 9.a Martin Wollschlaeger, Thilo Sauter, Juergen Jasperneite: [The Future of Industrial Communication: Automation Networks in the Era of the Internet of Things and Industry 4.0](#); IEEE Industrial Electronics Magazine, Vol. 11(1), Mar 2017; DOI: 10.1109/MIE.2017.2649104
- 9.b Norman Finn: [Time-sensitive and Deterministic Networking; Whitepaper](#); Huawei Technologies Co. Ltd; Jul 2017
- 9.c Ahmed Nasrallah, et al.: [Ultra-Low Latency \(ULL\) Networks: The IEEE TSN and IETF DetNet Standards and Related 5G ULL Research](#); Sep 2018; arXiv:1803.07673v3
- 9.d Xiaotian Yang, Dominik Scholz, Max Helm; [Deterministic Networking \(DetNet\) vs Time Sensitive Networking \(TSN\)](#); In "Proceedings of the Seminar Innovative Internet Technologies and Mobile Communications (IITM), Network Architectures and Services; Eds.: Georg Carle, Stephan Gunther, Benedikt Jaeger", Oct 2019; DOI: 10.2313/NET-2019-10-1\_13
- 9.e Yudong Huan, Shuo Wang, Tao Huang, Yunjie Liu: [Cycle-Based Time-Sensitive and Deterministic Networks: Architecture, Challenges, and Open Issues](#); IEEE Communications Magazine, Vol. 60, Issue 6, Jun 2022; DOI: 10.1109/MCOM.001.2100865

### 18.9.1 Time-Sensitive Networking

Eine Art von Anforderungen an industrielle Netzwerke verlangt von Netzwerken die Unterstützung von zeitsensitiven/zeitsensiblen Prozessen. Um solche Anforderungen zu erfüllen, muss die zeitsensitive Kommunikation, quasi Echtzeitkommunikation, in industriellen Netzwerken möglich sein. In diesem Zusammenhang spricht man von *Time-Sensitive Networking* (TSN) bzw. von zeitsensitiven Netzwerken. Von einem *zeitsensitiven Netzwerk* werden u.a. die folgenden Eigenschaften verlangt: minimale Übertragungszeiten auf Links, abschätzbare und garantierte Ende-zu-Ende-

Time-Sensitive  
Networking  
(TSN)

Latenzzeiten, minimale Paketverlustraten und hohe Verfügbarkeiten der Verbindungen.

Real-Time  
Ethernet und  
IEEE 802.1

Um Ethernet als Netzwerktechnologie für TSN einsetzen zu können, muss die Ethernet-Technologie hierfür entsprechend funktionell so erweitert werden, dass sie einige Echtzeitfähigkeiten besitzt. Daher wird die speziell zur Unterstützung von TSN erweiterte Ethernet-Technologie als *Real-Time Ethernet (Echtzeit-Ethernet)* bezeichnet. Ethernet ist somit aus dem industriellen Bereich nicht mehr wegzudenken. Um für industrielle Anwendungen zukünftig eine standardisierte Lösung für Echtzeit-Ethernet bereitzustellen, wurde die Arbeitsgruppe Time-Sensitive Networking (TSN) bei der IEEE 802.1 mit dem Ziel gegründet, Standards für Echtzeit-Ethernet so zu entwickeln, dass industrielle Netzwerke auf der Grundlage von Echtzeit-Ethernet den Anforderungen industrieller Anwendungen gerecht werden.

Für Näheres über Time-sensitive Networking, Real-Time Ethernet und die Standards von der IEEE 802.1 siehe:

- 9.1.a IEEE 802: [Time-Sensitive Networking \(TSN\) Task Group](#)
- 9.1.b Andre Hennecke, Stephan Weyer: [Time-Sensitive Networking in modularen Industrie 4.0 Anlagen](#); Conference: Automation 2017
- 9.1.c Levi Pearson: [TSN IN LINUX](#); Nov 2017
- 9.1.d Norman Finn: [Introduction to Time-Sensitive Networking](#); IEEE Communications Standards Magazine, Vol. 2(2), Jun 2018; DOI: 10.1109/MCOMSTD.2018.1700076
- 9.1.e Wilfried Steiner, Silviu S. Craciunas, Ramon Serna Oliver: [Traffic Planning for Time-Sensitive Communication](#); IEEE Communications Standards Magazine, Vol. 2(2), Jun 2018; DOI: 10.1109/MCOMSTD.2018.1700055
- 9.1.f Bharat Bansal: [Divide-and-Conquer Scheduling for Time-sensitive Networks](#); Master Thesis; University of Stuttgart, Institute of Parallel and Distributed Systems, Mar 2018
- 9.1.g John L. Messenger: [Time-Sensitive Networking: An Introduction](#); IEEE Communications Standards Magazine, Vol. 2(2), Jun 2018; DOI: 10.1109/MCOMSTD.2018.1700047
- 9.1.h Paul Pop, Michael Lander Raagaard, Marina Gutiérrez, Wilfried Steiner: [Enabling Fog Computing for Industrial Automation Through Time-Sensitive Networking \(TSN\)](#); IEEE Communications Standards Magazine, Vol. 2(2), Jun 2018; DOI: 10.1109/MCOMSTD.2018.1700057
- 9.1.i Soheil Samii, Helge Zinner: [Level 5 by Layer 2: Time-Sensitive Networking for Autonomous Vehicles](#), IEEE Communications Standards Magazine, Vol. 2(2), Jun 2018; DOI: 10.1109/MCOMSTD.2018.1700079
- 9.1.j Csaba Simon, Markosz Maliosz, Miklós Máté: [Design Aspects of Low-Latency Services with Time-Sensitive Networking](#); IEEE Communications Standards Magazine, Vol. 2(2), Jul 2018; DOI: 10.1109/MCOMSTD.2018.1700081

- 9.1.k Carlos San Vicente Gutiérrez, Lander Usategui San Juan, Irati Zamalloa Ugarte, Víctor Mayoral Vilches: [Time-Sensitive Networking for robotics](#); Sep 2018, arXiv:1804.07643v2
- 9.1.l Maryam Pahlevan: [Time Sensitive Networking for Virtualized Integrated Real-Time Systems](#); Faculty of Elektrotechnik und Informatik, University of Siegen; 2019
- 9.1.m Lucia Lo Bello, Wilfried Steiner: [A Perspective on IEEE Time-Sensitive Networking for Industrial Communication and Automation Systems](#); Proceedings of the IEEE, Vol. 107, Issue 6, Jun 2019; DOI: 10.1109/JPROC.2019.2905334
- 9.1.n RFC 9023: [Deterministic Networking \(DetNet\) Data Plane: IP over IEEE 802.1 Time Sensitive Networking \(TSN\)](#); Jun 2021
- 9.1.o RFC 9024: [Deterministic Networking \(DetNet\) Data Plane: IEEE 802.1 Time-Sensitive Networking over MPLS](#); Jun 2021
- 9.1.p Siemens Industry Online Support; [Questions and Answers about TSN](#); Entry ID: 109757263, V 2.0, 07/2021
- 9.1.q Youhwan Seol, Doyeon Hyeon, Junhong Min, Moonbeom Kim, Jeongyeup Paek; [Timely Survey of Time-Sensitive Networking: Past and Future Directions](#); IEEE Access, Oct 2021, DOI: 10.1109/ACCESS.2021.3120769
- 9.1.r Martin Böhm, Diederich Wermser: [Multi-Domain Time-Sensitive Networks — Control Plane Mechanisms for Dynamic Inter-Domain Stream Configuration](#); Electronics, Vol. 10, Oct 2021, Issue 20; DOI: 10.3390/electronics10202477
- 9.1.s Tommaso Fedullo, Alberto Morato, Federico Tramarin, Luigi Rovati, Stefano Vitturi: [A Comprehensive Review on Time Sensitive Networks with a Special Focus on Its Applicability to Industrial Smart and Distributed Measurement Systems](#); Sensors (Basel), Feb 2022, PMC8879530; DOI: 10.3390/s22041638

## 18.9.2 Deterministic Networking

Infolge der Konvergenz IT und OT hat sich eine besondere Klasse von Anforderungen an heutige industrielle Netzwerke herauskristallisiert. Die Anforderungen dieser Klasse verlangen von industriellen Netzwerken ähnliche Eigenschaften, die man beispielsweise im S/U-Bahnnetz oder im Busnetz einer Stadt erkennen kann. Weil Züge oder Busse nach einem festgelegten Plan fahren, in der Tat nach einem deterministischen Plan also, ist eine derartige Eigenschaft der industriellen Netzwerke zur Unterstützung einiger Produktionsprozesse von fundamentaler Bedeutung. Es handelt sich hier z.B. um Prozesse, die oft auf der Basis einer Vernetzung von Robotern realisiert werden und ständig nach einem von vornherein festgelegten deterministischen Plan verlaufen müssen. Die Netzwerke, mit denen eine deterministische, nach einem Plan verlaufende Kommunikation realisiert werden kann, werden daher als *deterministische Netzwerke* bezeichnet. Im Hinblick darauf wird von *Deterministic Networking* (DetNet) gesprochen. Die Entwicklung der Konzepte für DetNet wird von der gleichnamigen Working Group bei der IETF (*Internet Engineering Task Force*) koordiniert

Deterministic  
Networking  
(DetNet)

und standardisiert [<https://datatracker.ietf.org/wg/detnet/about/>]. Für Näheres ist zu empfehlen:

- 9.2.a Henrik Austad: [Deterministic Networking for Real-Time Systems, \(Using TSN and DetNet\)](#); Cisco Systems, Oct 2017
- 9.2.b RFC 8557: [Deterministic Networking Problem Statement](#); May 2019
- 9.2.c RFC 8655: [Deterministic Networking Architecture](#); Oct 2019
- 9.2.d RFC 8578: [Deterministic Networking Use Cases](#); Oct 2018
- 9.2.e RFC 9023: [Deterministic Networking \(DetNet\) Data Plane: IP over IEEE 802.1 Time-Sensitive Networking \(TSN\)](#); Jun 2021
- 9.2.f RFC 9024: [Deterministic Networking \(DetNet\) Data Plane: IEEE 802.1 Time-Sensitive Networking over MPLS](#); Jun 2021
- 9.2.g RFC 9037: [Deterministic Networking \(DetNet\) Data Plane: MPLS over IEEE 802.1 Time-Sensitive Networking \(TSN\)](#); Jun 2021
- 9.2.h RFC 9055: [Deterministic Networking \(DetNet\) Security Considerations](#); Jun 2021

### 18.9.3 6TiSCH Wireless Industrial Networks

#### Verfahren TSCH

Um hohe QoS-Anforderungen erfüllen zu können, müssen zum Aufbau von IIoT spezielle Netzwerke zur Unterstützung der industriellen Kommunikation eingesetzt werden. Um Netzwerke mit solchen Eigenschaften aufbauen zu können, wurde das Verfahren TSCH (*Time-Slotted Channel Hopping*) konzipiert, sodass man auch von TSCH-Netzwerken spricht. Dieses Verfahren stellt eine spezielle, zeitsynchrone Realisierung des MAC-Protokolls (*Media Access Control*) zum Aufbau drahtloser, industrieller Netzwerke dar. Im Allgemeinen kann man das Verfahren TSCH als eine Kombination von zwei, seit Langem bei der digitalen Datenübertragung gut bekannten Multiplexverfahren ansehen. Es handelt sich hierbei um eine Kombination des *Frequenzmultiplex* und des synchronen *Zeitmultiplex*, also um eine Variante von Frequenz- und Zeitmultiplexverfahren FTDM (*Frequency-Time Division Multiplexing*) – siehe hierfür z.B. [9.3.h], [9.3.i] .

#### 6TiSCH Wireless Industrial Networks

Die Konzepte und Protokolle für den Einsatz von IPv6 in TiSCH-Netzwerken werden von der Working Group 6tisch (IPv6 over the TSCH mode of IEEE 802.15.4e) bei der IETF koordiniert. Dementsprechend spricht man im Zusammenhang mit IPv6 over TSCH von (6)TiSCH. Die Idee von TiSCH ermöglicht das Deterministic Networking. Das heißt, sie ermöglicht die Einrichtung einer neuen Generation drahtloser Netzwerke, in denen die Verzögerungs- bzw. Reaktionszeit, allgemein als Latenz(zeit) bezeichnet, mit einer bestimmten Genauigkeit berechenbar ist. Die Kommunikation zwischen Knoten in jedem TSCH-Netzwerk, das ein deterministisches Netzwerk darstellt, verläuft nach dem in Form einer TSCH-Schedule-Matrix festgelegten Kommunikationsplan. Die Festlegung eines solchen Plans bezeichnet man als Scheduling in TSCH-Netzwerken. Jede TSCH-Schedule-Matrix kann dynamisch aufgebaut und modifiziert werden. Für Näheres über 6TiSCH Wireless Industrial Networks ist zu verweisen auf:

- 9.3.a i-SCOOP: [IT and OT convergence – two worlds converging in Industrial IoT](#)
- 9.3.b RFC 7554: [Using IEEE 802.15.4e Time-Slotted Channel Hopping \(TSCH\) in the Internet of Things \(IoT\): Problem Statement](#); May 2015
- 9.3.c Pascal Thubert, Maria Rita Palattella, Thomas Engel: [6TiSCH Centralized Scheduling: when SDN Meet IoT](#); IEEE Conference on Standards for Communications and Networking (CSCN), Oct 2015; DOI: 10.1109/CSCN.2015.7390418
- 9.3.d Domenico De Guglielmo, Simone Brienza, Giuseppe Anastasi: [IEEE 802.15.4e: A survey](#); Computer Communications, Vol. 88, Aug 2016; DOI: 10.1016/j.comcom.2016.05.004
- 9.3.e Gopi Garge: [Industrial Internet and the need for guarantees \(6TiSCH\)](#); 2017
- 9.3.f ETSI GR IP6 009 V1.1.1: [IPv6-based Industrial Internet leveraging 6TiSCH technology](#); Mar 2017
- 9.3.g RFC 8180: [Minimal IPv6 over the TSCH Mode of IEEE 802.15.4e \(6TiSCH\) Configuration](#); May 2017
- 9.3.h Rodrigo Teles Hermeto, Antoine Gallais, Fabrice Theoleyre: [Scheduling for IEEE802.15.4-TSCH and slow channel hopping MAC in low power industrial wireless networks: A survey](#); Computer Communications, Vol. 114, Dec 2017; DOI: 10.1016/j.comcom.2017.10.004
- 9.3.i Anatol Badach: [TSCH – Time-Slotted Channel Hopping](#); In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Jan 2018
- 9.3.j Anatol Badach: [6P - 6top Protocol](#); In book: Protokolle und Dienste der Informationstechnologie; WEKA, Ed.: Heinz Schulte; Aug 2018
- 9.3.k RFC 8480: [6TiSCH Operation Sublayer \(6top\) Protocol \(6P\)](#); Nov. 2018
- 9.3.l Xavier Vilajosana, Thomas Watteyne, Tengfei Chang, Mališa Vučinić, Simon Duquennoy, Pascal Thubert: [IETF 6TiSCH: A Tutorial](#); IEEE Communications Surveys & Tutorials, Vol. 22, Issue 1, Sep 2019; DOI: 10.1109/COMST.2019.2939407
- 9.3.m Mina Rady, Quentin Lampin, Dominique Barthel, Thomas Watteyne: [g6TiSCH: Generalized 6TiSCH for Agile Multi-PHY Wireless Networking](#); IEEE Access, Jun 2021; DOI: 10.1109/ACCESS.2021.3085967
- 9.3.n Andreas Ramstad Urke, Øivind Kure, Knut Øvsthus: [A Survey of 802.15.4 TSCH Schedulers for a Standardized Industrial Internet of Things](#); Sensors (Basel), Vol. 22(1), Jan 2022; DOI: 10.3390/s22010015

## 18.9.4 Time-Sensitive SDN

In Time-Sensitive Networks (TS-Networks) muss überwiegend die verbindungsorientierte IP-Kommunikation, ähnlich dem Prinzip MPLS (*Multi-Protocol Label Switching*) [Abschnitt 12.2] realisiert werden. Dabei werden virtuelle Ende-zu-Ende-Verbindungen mit bestimmten QoS-Parametern in TS-Networks dynamisch auf- und abgebaut. Für diesen Zweck eignet sich das SDN-Konzept ideal. Beim Einsatz von

MPLS-Idee als  
Grundlage für TS  
SDN

SDN in TS-Networks spricht man von *Time-Sensitive SDN* (TS SDN). Um virtuelle Ende-zu-Ende-Verbindungen in TS-Networks – nach einem dem Prinzip MPLS ähnelnden Konzept – dynamisch auf- und abzubauen, ist eine spezielle Control Plane nötig. Beim Einsatz von TS SDN würde man SDN Controller innerhalb dieser Control Plane installieren. Für weitere Information über Time-Sensitive SDN ist zu empfehlen:

- 9.4.a Jiafu Wan, et al.: [Software-Defined Industrial Internet of Things in the Context of Industry 4.0](#); IEEE Sensors Journal, Vol. 16(20), Oct 2016; DOI: 10.1109/JSEN.2016.2565621
- 9.4.b Daniel Thiele, Rolf Ernst: [Formal analysis based evaluation of software defined networking for time-sensitive Ethernet](#); Design, Automation & Test in Europe Conference & Exhibition (DATE), Mar 2016
- 9.4.c Dominik Henneke, Lukasz Wisniewski, Jürgen Jasperneite: [Analysis of Realizing a Future Industrial Network by Means of Software-Defined Networking \(SDN\)](#); IEEE World Conference on Factory Communication Systems (WFCS), May 2016; DOI: 10.1109/WFCS.2016.7496525
- 9.4.d Naresh Ganesh Nayak, Frank Dürr, Kurt Rothermel: [Time-sensitive Software-defined Network \(TSSDN\) for Real-time Applications](#); Proceeding RTNS '16 Proceedings of the 24th International Conference on Real-Time Networks and Systems, Oct 2016; DOI: 10.1145/2997465.2997487
- 9.4.e Rakesh Kumar, et al.: [End-to-End Network Delay Guarantees for Real-Time Systems using SDN](#); May 2017, arXiv:1703.01641v2
- 9.4.f Ben Schneider, Alois Zoitl, Monika Wenger, Jan Olaf Blech: [Evaluating Software-defined Networking for Deterministic Communication in Distributed Industrial Automation Systems](#); 22nd IEEE International Conference on Emerging Technologies and Factory Automation (ETFA), Sep 2017; DOI: 10.1109/ETFA.2017.8247594
- 9.4.g Khandakar Ahmed, et al.: [Software Defined Industry Automation Networks](#); 27th International Telecommunication Networks and Applications Conference (ITNAC), Nov. 2017; DOI: 10.1109/ATNAC.2017.8215391
- 9.4.h Sebastian Schriegel, Thomas Kobzan, Jürgen Jasperneite: [Investigation on a distributed SDN control plane architecture for heterogeneous time sensitive networks](#); 14th IEEE International Workshop on Factory Communication Systems (WFCS); Jun 2018; DOI: 10.1109/WFCS.2018.8402356
- 9.4.i Khandakar Ahmed, Jan O. Blech, Mark A. Gregory, Heinz W. Schmidt: [Software Defined Networks in Industrial Automation](#); Journal of Actuator Networks, Vol. 7(3), Aug 2018; DOI: 10.3390/jсан7030033
- 9.4.j Dave Cronberger: [The software defined industrial network](#); Industrial Ethernet Book, Issue 84/5; Nov 2018
- 9.4.k Siwar Ben Hadj Said, Quang Huy Truong, Michael Boc: [SDN-based configuration solution for IEEE 802.1 time sensitive networking \(TSN\)](#); ACM SIGBED Review, Vol. 16, Issue 1, Feb 2019; DOI: 10.1145/3314206.3314210
- 9.4.l Martin Böhm, Jannis Ohms, Manish Kumar, Olaf Gebauer, Diederich Wermser: [Time-Sensitive Software-Defined Networking: A Unified Control-Plane](#)

for [TSN and SDN](#); Mobile Communication - Technologies and Applications; 24. ITG Fachtagung Mobilkommunikation, May 2019

- 9.4.m Timo Häckel, Philipp Meyer, Franz Korf, Thomas C. Schmidt: [Secure Time-Sensitive Software-Defined Networking in Vehicles](#); arXiv:2201.00589; Aug 2022; DOI:10.1109/TVT.2022.3202368

## 18.10 AI-based Networking

Da die heutigen Rechnernetze, also IP-Netze, immer flexibler, heterogener und komplexer werden, bietet es sich an, die Künstliche Intelligenz (KI, AI: *Artificial Intelligence*) in Verbindung mit *Maschinellem Lernen* (ML, *Machine Learning*) in technischen Konzepten zur Optimierung und Management von Rechnernetzen einzusetzen. Folglich führt ein aktueller und breiter Trend auf dem Gebiet Networking zur Entwicklung von Ideen und technischen Konzepten, um zukünftig intelligente Vernetzungen von verschiedenen Rechnern bauen zu können. Im Hinblick darauf ist AI in Verbindung mit ML von zukunftsweisender Bedeutung. Beim Einsatz von AI und ML auf dem Gebiet Networking spricht man von *AI-enabled Networking*. Demzufolge werden zukünftige IP-Netze mit Sicherheit die mithilfe von ML gewonnene AI so nutzen, um sich immer an jede neue Situation optimal adaptieren/anpassen und dadurch auch intelligente Services erbringen zu können. Das volle/optimale Nutzungspotenzial zukünftiger IP-Netze lässt sich nur mit der Unterstützung von AI erreichen.

Bedeutung von  
AI-enabled  
Networking

Um AI-enabled Networking zu realisieren und dabei insbesondere AI aus den gesammelten Daten gewinnen zu können, ist der Einsatz verschiedener ML-Techniken möglich. Dabei handelt es sich insbesondere um *Deep Learning* (DL) [10.c] und *Reinforcement Learning* (RL) [10.f]. Beide ML-Methoden haben in sog. Neuronalen Netzen (*Neural Networks*) fundamentale Bedeutung [10.n].

ML-Techniken  
zur  
AI-Gewinnung

Als wichtige Trends auf dem Gebiet AI-enabled Networking gelten die folgenden Trends: *AI-enabled SDN*, *Data-driven Networking*, *Cognitive Networks*, *Intent-based Networking*, *Autonomic Networking* und *AI, IoT and 5G Convergence*. Für weitere, aber immer noch allgemeine Informationen über AI-enabled Networking und die Nutzung von AI und ML sei verwiesen auf:

- 10.a i-SCOOP: [Artificial intelligence \(AI\) and cognitive computing: what, why and where](#)
- 10.b i-SCOOP: [Big data in action: definition, value, evolutions, benefits and context](#)
- 10.c Jeffrey O. Kephart, David M. Chess: [The vision of autonomic computing](#); Computer, Vol. 36(1), Jan 2003; DOI:10.1109/MC.2003.1160055
- 10.d Xiaofei Wang, Xiuhua Li, Victor C. M. Leung: [Artificial Intelligence-Based Techniques for Emerging Heterogeneous Network: State of the Arts, Opportunities, and Challenges](#); IEEE Access, Vol. 3, 2015; DOI: 10.1109/ACCESS.2015.2467174
- 10.e Zubair Md. Fadlullah, et al.: [State-of-the-Art Deep Learning: Evolving Machine Intelligence Toward Tomorrow's Intelligent Network Traffic Control](#)



- [Systems](#); IEEE Commun. Surveys & Tutorials, Vol. 19(4), 2017; DOI: 10.1109/COMST.2017.2707140
- 10.f Hongzi Mao, Mohammad Alizadeh, Ishai Menachey, Srikanth Kandulay: [Resource Management with Deep Reinforcement Learning](#); Proceedings of the 15th ACM Workshop on Hot Topics in Networks (HotNets '16), Nov 2016; DOI: 10.1145/3005745.3005750
- 10.g Nei Kato, Zubair Md. Fadlullah, et al.: [The Deep Learning Vision for Heterogeneous Network Traffic Control: Proposal, Challenges, and Future Perspective](#), IEEE Wireless Communications, Jun 2017; DOI: 10.1109/MWC.2016.1600317WC
- 10.h Roberto Gonzalez, et al.: [Net2Vec: Deep Learning for the Network](#); Big-DAMA '17 Proceedings of the Workshop on Big Data Analytics and Machine Learning for Data Communication Networks, Aug 2017; DOI: 10.1145/3098593.3098596
- 10.i Albert Mestres: [Knowledge-Defined Networking: A Machine Learning based approach for network and traffic modeling](#); Doctoral Thesis, Universitat Politècnica de Catalunya, Sep 2017
- 10.j Omer Berat Sezer, Erdogan Dogdu, Ahmet Murat Ozbayoglu: [Context-Aware Computing, Learning, and Big Data in Internet of Things: A Survey](#); IEEE Internet of Things Journal, Vol. 5(1), Feb 2018; DOI: 10.1109/JIOT.2017.2773600
- 10.k Mowei Wang, et al.: [Machine Learning for Networking: Workflow, Advances and Opportunities](#); IEEE Network, Vol. 32(2), Mar – Apr 2018; DOI: 10.1109/MNET.2017.1700200
- 10.l ITU: [Artificial Intelligence \(AI\) for Development Series - Report on AI and IoT in Security Aspects](#); Jul 2018
- 10.m ATIS: [Evolution to an Artificial Intelligence-Enabled Network](#); Sep 2018
- 10.n Wang Tong, Azhar Hussain, Wang Xi Bo, Sabita Maharjan: [Artificial Intelligence for Vehicle-to-Everything: A Survey](#); IEEE Access, Vol. 7, Jan 2019; DOI: 10.1109/ACCESS.2019.2891073
- 10.o Mohammad Azmi Ridwan, Nurul Asyikin Binti Mohamed Radzi, Fairuz Abdullah, Yanti Erana Jalil: [Applications of Machine Learning in Networking: A Survey of Current Issues and Future Challenges](#); IEEE Access, Mar 2021; DOI: 10.1109/ACCESS.2021.3069210
- 10.p Arnau Rovira-Sugranes, Abolfazl Razi, Fatemeh Afghah, Jacob Chakareski: [A Review of AI-enabled Routing Protocols for UAV Networks: Trends, Challenges, and Future Outlook](#); arXiv:2104.01283v2; Nov 2021; DOI: 10.48550/arXiv.2104.01283
- 10.q Tianzhu Zhang, Han Qiu, Marco Mellia, Yuanjie Li, Hewu Li, Ke Xu: [Interpreting AI for Networking: Where We Are and Where We Are Going](#); IEEE Communications Magazine, Vol. 60, Issue 2, Feb 2022; DOI: 10.1109/MCOM.001.2100736
- 10.r Arnau Rovira-Sugranes, Abolfazl Razi, Fatemeh Afghah, Jacob Chakareski: [A review of AI-enabled routing protocols for UAV networks: Trends, chal-](#)

[lenges, and future outlook](#); Ad Hoc Networks, Vol. 130, 1 May 2022; DOI: 10.1016/j.adhoc.2022.102790

### 18.10.1 AI-enabled SDN

Die eben genannten ML-Methoden können bei SDN eingesetzt werden. Die mittels dieser ML-Methoden gewonnene AI kann bei SDN dazu genutzt werden, um die zur Konfiguration und zum Management von Netzwerkkomponenten dienenden SDN Controller zu befähigen, die zu steuernden Netzwerkkomponenten in die Lage versetzen, sich an neue Situationen im Netzwerk optimal anzupassen. Werden SDN Controller befähigt, die AI so zu nutzen, um verschiedene Netzwerkkomponenten der aktuellen Situation im Netzwerk entsprechend optimal zu steuern und zu managen, kann von AI-enabled SDN gesprochen werden. Für Näheres darüber siehe:

AI-fähige SDN  
Controller

- 10.1.a Majd Latah, Levent Toker: [Artificial Intelligence Enabled Software Defined Networking: A Comprehensive Overview](#); arXiv:1803.06818
- 10.1.b Majd Latah, Levent Toker: [Application of Artificial Intelligence to Software Defined Networking: A Survey](#); Indian Journal of Science and Technology, Vol. 9(44), Nov 2016; DOI: 10.17485/ijst/2016/v9i44/89812
- 10.1.c Albert Mestres, Alberto Rodriguez-Natal, Josep Carner, et al: [Knowledge-Defined Networking](#); ACM SIGCOMM Computer Communication Review, Vol. 47(3), Jul 2017
- 10.1.d Elisa Rojas: [From Software-Defined to Human-Defined Networking: Challenges and Opportunities](#); IEEE Network, Vol. 32 (1), Jan - Feb 2018
- 10.1.e Weidong Fang, Chunsheng Zhu, F. Richard Yu, Kun Wang, Wuxiong Zhang: [Towards Energy-Efficient and Secure Data Transmission in AI-Enabled Software Defined Industrial Networks](#); IEEE Transactions on Industrial Informatics, Vol. 18, Issue 6, Jun 2022; DOI: 10.1109/TII.2021.3122370
- 10.1.f Jinfang Jiang, Chuan Lin, Guangjie Han, Adnan M. Abu-Mahfouz, Syed Bilal Hussain Shah, Miguel Martínez-García: [How AI-enabled SDN technologies improve the security and functionality of industrial IoT network: Architectures, enabling technologies, and opportunities](#); Digital Communications and Networks, Jul 2022; DOI: 10.1016/j.dcan.2022.07.001

### 18.10.2 Data-Driven Networking

Menschen erwerben ihr Wissen durch die Beobachtung von Umwelt und Natur, durch Gedanken, Erfahrungen und Lernen. Diese Art und Weise der Erwerbung des menschlichen Wissens muss auch in bestimmtem Grade in komplexen technischen Systemen – insbesondere in großen Netzwerken – nachgebildet werden. Dadurch soll ihnen eine bestimmte künstliche Intelligenz beigebracht werden, um sie auf diese Art zu befähigen, wichtige Prozesse im Laufe des Netzwerkbetriebs selbst- und eigenständig optimieren zu können. Damit man eine derartige Wunschvorstellung verwirklichen

Notwendigkeit  
der Erfassung  
von Messdaten

kann, müssen alle relevanten Messwerte im Laufe der Zeit zuerst erfasst, dann auf eine spezielle Art dokumentiert und archiviert werden.

#### Big Data Analytics

Demzufolge müssen die Daten über den Betrieb des Netzwerkes kontinuierlich erfasst werden. Hierdurch wird die Menge von Messdaten im Laufe der Zeit immer größer. Im Hinblick darauf spricht man von *Big Data*, also einer überproportional großen Datenmenge. Diese Daten müssen zuerst analysiert werden, um sie im nächsten Schritt zum maschinellen Lernen in Netzwerken benutzen zu können. Eine derartige Analyse von Big Data als eine Art Vorbereitung von großen Daten zu deren Einsatz bei der Unterstützung von Lernprozessen wird als *Big Data Analytics* bezeichnet. Für Näheres darüber siehe [10.2.b], [10.2.c].

#### (Big-)Data-Driven Networking

Im Zusammenhang mit Big Data Analytics in Netzwerken spricht man von *Data-Driven Networking* (DDN) bzw. von *Big-Data-Driven Networking* (kurz BDDN oder bDDN). (B)DDN ist als ein sehr allgemeines Konzept, als eine Art 'zukünftiges Network-Framework' zu verstehen, in dem die Antworten auf die folgenden vier Fragestellungen spezifiziert werden:

1. **Erfassung von Big Data:** Welche Messdaten sollen über den Netzbetrieb gesammelt, dokumentiert und archiviert werden?
2. **Big Data Analytics:** Wozu und wie sollen diese Messdaten verarbeitet werden?
3. **Maschinelles Lernen:** Wie sollen die Ergebnisse der Datenanalyse (Big Data Analytics) zur Befähigung des Netzwerks verwendet werden?
4. **Optimierung/Verbesserung des Systemverhaltens:** Wie soll die durch maschinelle Lernen erworbene Intelligenz zur Optimierung bzw. Verbesserung des Systemverhaltens im laufenden Netzbetrieb eingesetzt werden?

#### (B)DDN an andere Arten von Networking

Im Trend zu (B)DDN wird hauptsächlich das Ziel verfolgt, intelligentes, autonomes und optimiertes Netzwerkmanagement sowie selbst adaptierte Sicherheit zu ermöglichen. (B)DDN kann dazu führen, dass man zwischen Netzwerken mit unterschiedlichen Intelligenzarten unterscheiden kann – und zwar zwischen Cognitive Networks, Intent-based Networking und Autonomic Networking. Für weitere allgemeine Information über (B)DDN und über verschiedene intelligente Arten von Networking ist zu empfehlen:

- 10.2.a Haipeng Yao, Chao Qiu, Chao Fang, Xu Chen, F. Richard Yu: [A Novel Framework of Data-Driven Networking](#); IEEE Access, Vol. 4, Nov 2016; DOI: 10.1109/ACCESS.2016.2624781
- 10.2.b Junchen Jiang, Vyas Sekar, Ion Stoica, Hui Zhang: [Unleashing the potential of data-driven networking](#); Proceedings of 9th International Conference on COMMunication Systems & NETWORKS (COMSNET), 2017.
- 10.2.c Junchen Jiang, Vyas Sekar, Ion Stoica, Hui Zhang: [Data-Driven Networking: Harnessing the "Unreasonable Effectiveness of Data" in Network Design](#); Carnegie Mellon University, Pittsburgh, Feb 2016
- 10.2.d ITU-T: [Y.3650 - Framework of big-data-driven networking](#), Jan 2018
- 10.2.e Wolfgang Kellerer, Patrick Kalmbach, Andreas Blenk, Arsany Basta, Martin Reisslein, Stefan Schmid: [Adaptable and Data-Driven Softwarized Networks](#):

[Review, Opportunities, and Challenges](#); Proceedings of the IEEE, Vol. 107, Issue 4, April 2019; DOI: 10.1109/JPROC.2019.2895553

- 10.2.f Alessio Sacco, Flavio Esposito, Guido Marchetto: [On Control and Data Plane Programmability for Data-Driven Networking](#); IEEE 22nd International Conference on High Performance Switching and Routing (HPSR), Jun 2021; DOI: 10.1109/HPSR52026.2021.9481859
- 10.2.g ITU-T: Recommendation Y.3654: [Big data driven networking – Machine learning mechanism](#); 2022-02-13; <https://handle.itu.int/11.1002/1000/14862>

### 18.10.3 Cognitive Networks

Falls die Messdaten in einem Netzwerk zuerst über gewisse Zeit erfasst, gespeichert, analysiert (Big Data Analytics) und danach beim Maschinellen Lernen so verwendet werden, um sog. *kognitive Fähigkeiten* des Menschen, d.h. Signale aus der Umwelt wahrzunehmen und weiterzuverarbeiten, dann besitzt das Netzwerk auch bestimmte kognitive Fähigkeiten und kann folglich als *kognitives Netzwerk (Cognitive Network)* bezeichnet werden.

Somit ist ein kognitives Netzwerk ein Netzwerk mit bestimmten kognitiven Fähigkeiten, das durch maschinelles Lernen befähigt wurde, die aktuelle Netzwerksituation wahrzunehmen, diese zu erfassen und zu analysieren, um sich immer an jede neue Netzwerksituation optimal anzupassen, will heißen, einige der wichtigen Konfigurationsparameter des Netzwerks optimal einzustellen. Ein kognitives Verhalten kann in Netzwerken vor allem dazu dienen, die QoS (Quality of Service) und Netzwerksicherheit zu verbessern. Insbesondere die Fähigkeit von Cognitive Networks, verschiedene Anomalien zu erkennen und darauf optimal zu reagieren, kann zur Erhöhung der Netzwerksicherheit beitragen. Für Näheres über Cognitive Networks siehe:

Kognitive  
Fähigkeiten

- 10.3.a Valter Popeskic, Božidar Kovačić: [COGNITIVE NETWORKS THE NETWORKS OF THE FUTURE](#); Conference Paper, June 2012
- 10.3.b Michele Zorzi, et al.: [COBANETS: A new paradigm for cognitive communications systems](#); International Conference on Computing, Networking and Communications, Feb 2016; DOI: 10.1109/ICCNC.2016.7440625
- 10.3.c Michele Zorzi, Andrea Zanella, Alberto Testolin, Michele De Filippo De Grazia, Marco Zorzi: [Cognition-Based Networks: A New Perspective on Network Optimization Using Learning and Distributed Intelligence](#); IEEE Access, Vol. 3, Aug 2015; DOI: 10.1109/ACCESS.2015.2471178
- 10.3.d Mario Bkassiny, Yang Li, Sudharman K. Jayaweera: [A Survey on Machine-Learning Techniques in Cognitive Radios](#); IEEE Communications Surveys & Tutorials, Vol. 15(3), 2013; DOI: 10.1109/SURV.2012.100412.00017
- 10.3.e Marco Levorato: [Cognitive Networking with Dynamic Traffic Classification and QoS Constraints](#); IEEE Wireless Communications and Networking Conference (WCNC); Mar 2017; DOI: 10.1109/WCNC.2017.7925717

- 10.3.f Ijaz Ahmad: [Improving Software Defined Cognitive and Secure Networking](#); University of Oulu, 2018; ISBN: 978-952-62-1951-6
- 10.3.g Cynthia S. Q. Siew; U. Wulff; Nicole M. Beckage; Yoed N. Kenett: [Cognitive Network Science: A Review of Research on Cognition through the Lens of Network Representations, Processes, and Dynamics](#); Complexity, Vol. 2019, Article ID 2108423, 2019; DOI: 10.1155/2019/2108423
- 10.3.h Ijaz Ahmad: [Improving Software Defined Cognitive and Secure Networking](#); arXiv:2007.05296; Jul 2020; DOI: 10.48550/arXiv.2007.05296
- 10.3.i Martins O. Osifeko, Gerhard P. Hancke, Adnan M. Abu-Mahfouz: [Artificial Intelligence Techniques for Cognitive Sensing in Future IoT: State-of-the-Art, Potentials, and Challenges](#); Journal of Sensor and Actuator Networks, Vol. 9 Issue 2, Apr 2020; DOI: 10.3390/jsan9020021

### 18.10.4 Intent-based Networking

Ziel von  
Intent-based  
Networking

Eine besondere Art von Data-Driven Networking wird als *Intent-based (absichtsbasiertes) Networking* bezeichnet. Man betrachtet absichtsbasiertes Networking als Grundstein für eine neue Ära von Networking. Dem Intent-based Networking liegt das folgende Ziel zugrunde: Ein Netzwerk soll in der Lage sein, sich – der Absicht seines Administrators entsprechend – selbst so zu konfigurieren, um die in Form von sog. Konfigurationsrichtlinien allgemein formulierten Absichten des Administrators in die entsprechenden Konfigurationsparameter umzusetzen.

Idee von  
Intent-based  
Networking

Die grundlegende Idee von Intent-based Networking ist, dass das Netzwerk eigenständig die geschäftlichen Absichten/Ziele berücksichtigen muss und diese selbst/automatisch in Konfigurationsparametern seiner Funktionskomponenten (Router, Switches, Firewalls) abbilden kann. Als Folge dessen sollen manuelle Konfigurationseingriffe in Intent-based Networks auf ein Minimum reduziert werden. Darüber hinaus soll jedes Intent-based Network von vornherein ausgewählte Parameter, insbesondere dabei die sog. QoS-Metriken, kontinuierlich überwachen und im Bedarfsfall entsprechende Anpassungen der Konfigurationsparameter vornehmen, um sicherzustellen, dass alle ausgewählten Parameter im 'grünen Bereich' sind. Für weitere Informationen über Intent-based Networking ist zu empfehlen:

- 10.4.a David Lenrow: [Intent-Based Networking Seeks Network Effect](#); Sep 2015
- 10.4.b Susan Hares: [2015 ONF/SDN Market Opportunities, Tutorial Intent Networking](#), Open Networking Foundation
- 10.4.c ONF TR-523: [Intent NBI – Definition and Principles](#); Oct 2016
- 10.4.d Franco Callegati, Walter Cerroni, Chiara Contoli, Francesco Foresta: [Performance of Intent-based Virtualized Network Infrastructure Management](#); IEEE International Conference on Communications (ICC), May 2017; DOI: 10.1109/ICC.2017.7997431
- 10.4.e Alexander Thiele: [Future Ready Networking Solutions for the Datacenter](#); Dell EMC Forum, Frankfurt 24.10.2017

- 10.4.f Carlos Infante: [Cisco SD-WAN: Intent-based networking for the branch and WAN](#); Mar 2018
- 10.4.g Walter Cerroni: [Intent-based Network Programmability](#); IRTF NMRG 56 – Interim Meeting, Oct 2019
- 10.4.h Engin Zeydan, Yekta Turk: [Recent Advances in Intent-Based Networking: A Survey](#); IEEE 91st Vehicular Technology Conference (VTC2020-Spring), May 2020; DOI: 10.1109/VTC2020-Spring48590.2020.9128422
- 10.4.i Yiming Wei, Mugen Peng, Yaqiong Liu: [Intent-based networks for 6G: Insights and challenges](#); Digital Communications and Networks, Vol. 6, Issue 3, Aug 2020; DOI: 10.1016/j.dcan.2020.07.001
- 10.4.j Adeel Rafiq, Asif Mehmood, Talha Ahmed Khan, Khizar Abbas, Muhammad Afaq, Wang-Cheol Song: [Intent-Based End-to-End Network Service Orchestration System for Multi-Platforms](#); Sustainability, Vol. 12, Issue 7, Apr 2020; DOI:10.3390/su12072782

### 18.10.5 Autonomic Networking

Seit Beginn der 2000er-Jahre wird der Begriff 'Autonomic Systems' (*Autonome Systeme*) geprägt [Abschnitt 10.5]. Diese Idee von *Autonomic Systems* wird in den letzten zehn Jahren auch auf dem Networking-Gebiet übernommen, sodass man von *Autonomic Networking* bzw. *Autonomic Networks* spricht. In RFC 7575 wird 'Autonomic Networking' definiert und dessen Ziele werden hier näher dargestellt. Das wesentliche Ziel eines autonomen Netzwerks ist dessen *Selbstmanagement*, einschließlich *Selbstkonfiguration*, *Selbstoptimierung*, *Selbstheilung* und *Selbstschutz*. Autonomic Networking kann auch als eine besondere Variante von *Data-Driven Networking* (DDN) betrachtet werden. Daher spielen (Big) Data Analytics und Maschinelles Lernen auch bei Autonomic Networking eine fundamentale Rolle. Um Autonomic Networking zu verwirklichen, werden hierfür verschiedene Architekturmodelle und Protokolle entwickelt. Diese Aktivitäten werden von der Working Group *anima* (*Autonomic Networking Integrated Model and Approach*) bei der IETF koordiniert. Für weitere Informationen über *Autonomic Networking* siehe:

- 10.5.a Jeffrey O. Kephart, David M. Chess: [The Vision of Autonomic Computing](#); IEEE Computer, Vol. 36(1), Jan 2003; DOI: 10.1109/MC.2003.1160055
- 10.5.b EU FP6 IST Project 27489: [ANA Project; Autonomic Network Architecture](#); Feb 2007
- 10.5.c Zeinab Movahedi, Mouna Ayari, Rami Langar, Guy Pujolle: [A Survey of Autonomic Network Architectures and Evaluation Criteria](#), IEEE Communications Surveys & Tutorials, Vol. 14(2), May 2012; DOI 10.1109/SURV.2011.042711.00078
- 10.5.d ETSI GS AFI 002 V1.1.1: [Autonomic network engineering for the self-managing Future Internet \(AFI\); Generic Autonomic Network Architecture \(An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management\) Disclaimer](#); Apr 2013

5-S-  
Besonderheiten  
beim Autonomic  
Networking

- 10.5.e CISCO: [Autonomic Networking Configuration and Deployment Guide](#); Dec 2016
- 10.5.f Zhongliang Zhao, Eryk Schiller, Eirini Kalogeiton, Torsten Braun, Burkhard Stiller, Mevlut Turker Garip, Joshua Joy, Mario Gerla, Nabeel Akhtar, Ibrahim Matta: [Autonomic Communications in Software-Driven Networks](#); IEEE Journal on Selected Areas in Communications, Vol. 35(11), Nov 2017; DOI: 10.1109/JSAC.2017.2760354
- 10.5.g RFC 7575: [Autonomic Networking: Definitions and Design Goals](#); Jun 2015
- 10.5.h RFC 8368: [Using an Autonomic Control Plane for Stable Connectivity of Network Operations, Administration, and Maintenance \(OAM\)](#); May 2018
- 10.5.i ETSI TS 103 195-2 V1.1.1: [Autonomic network engineering for the self-managing Future Internet \(AFI\); Generic Autonomic Network Architecture; Part 2: An Architectural Reference Model for Autonomic Networking, Cognitive Networking and Self-Management](#); Mai 2018
- 10.5.j draft-ietf-anima-autonomic-control-plane-18: [An Autonomic Control Plane \(ACP\)](#); Jul 2018
- 10.5.k ETSI TR 103 626 V1.1.1: [Autonomic network engineering for the self-managing Future Internet \(AFI\); An Instantiation and Implementation of the Generic Autonomic Network Architecture \(GANA\) Model onto Heterogeneous Wireless Access Technologies using Cognitive Algorithms](#); Feb 2020
- 10.5.l RFC 8993: [A Reference Model for Autonomic Networking](#); May 2021
- 10.5.m RFC 8990: [A Generic Autonomic Signaling Protocol](#); May 2021
- 10.5.n RFC 8994: [Autonomic Control Plane](#); May 2021

## 18.10.6 AI, IoT and 5G Convergence

### Zukünftige Netzwerkvisionen

Die 5. Generation (5G) der Mobilfunknetze wird eine fundamentale Bedeutung bei der Weiterentwicklung des IoT haben. In Bezug darauf kann man bereits heute von einer Konvergenz der 5G-Mobilfunknetze mit dem IoT sprechen. Die Ideen für die Unterstützung dieser Konvergenz werden intensiv entwickelt. Bei diesen Entwicklungen spielen die Konzepte für (Big) Data Analytics und Maschinelles Lernen eine sehr wichtige Rolle. Für weitere Informationen darüber siehe:

- 10.6.a Ying Wang, et al.: [A Data-Driven Architecture for Personalized QoE Management in 5G Wireless Networks](#); IEEE Wireless Communications, Vol. 24(1), Feb 2017; DOI: 10.1109/MWC.2016.1500184WC
- 10.6.b Chunxiao Jiang, et al.: [Machine Learning Paradigms for Next-Generation Wireless Networks](#); IEEE Wireless Communications, Vol. 24(2), Apr 2017; DOI: 10.1109/MWC.2016.1500356WC
- 10.6.c Zhiyuan Xu, Yanzhi Wang, Jian Tang, Jing Wang, Mustafa Cenk Gursoy: [A deep reinforcement learning based framework for power-efficient resource allocation in cloud RANs](#); IEEE International Conference on Communications (ICC), May 2017; DOI: 10.1109/ICC.2017.7997286

- 10.6.d Paulo Valente Klaine, et al.: [A Survey of Machine Learning Techniques Applied to Self-Organizing Cellular Networks](#); IEEE Communications Surveys and Tutorials, Vol. 19(4), Jul 2017; DOI: 10.1109/COMST.2017.2727878
- 10.6.e Rongpeng Li, et al.: [Intelligent 5G: When Cellular Networks Meet Artificial Intelligence](#); IEEE Wireless Communications, Vol. 24(5), Oct 2017; DOI: 10.1109/MWC.2017.1600304WC
- 10.6.f Magnus Malmström: [5G Positioning using Machine Learning](#); Master of Science Thesis in Applied Mathematics, Department of Electrical Engineering, Linköping University, 2018
- 10.6.g Yang Yang, et al.: [DECCO: Deep-Learning Enabled Coverage and Capacity Optimization for Massive MIMO Systems](#); IEEE Access, Apr 2018; DOI: 10.1109/ACCESS.2018.2828859
- 10.6.h Mowei Wang, et al.: [Machine learning for networking: Workflow, advances and opportunities](#); IEEE Network; Vol: 32(2), Mar - Apr 2018; DOI: 10.1109/MNET.2017.1700200
- 10.6.i Zhifeng Zhao, et al.: [Deep Reinforcement Learning for Network Slicing](#); arXiv:1805.06591v2, May 2018
- 10.6.j Chaoyun Zhang, Paul Patras, Hamed Haddadi: [Deep Learning in Mobile and Wireless Networking: A Survey](#); arXiv:1803.04311v2, Sep 2018
- 10.6.k Na Chen, Minoru Okada: [Toward 6G Internet of Things and the Convergence With RoF System](#); IEEE Internet of Things Journal, Vol. 8, Issue 11, Jun 2021; DOI: 10.1109/JIOT.2020.3047613
- 10.6.l Yushan Siriwardhana, Pawani Porambage, Madhusanka Liyanage, Mika Ylianttila: [AI and 6G Security: Opportunities and Challenges](#); Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit), Jun 2021; DOI: 10.1109/EuCNC/6GSummit51104.2021.9482503
- 10.6.m Ebenezer Esenogho, Karim Djouani, Anish M. Kurien: [Integrating Artificial Intelligence Internet of Things and 5G for Next-Generation Smartgrid: A Survey of Trends Challenges and Prospect](#); IEEE Access, Vol. 10, Jan 2022; DOI: 10.1109/ACCESS.2022.3140595
- 10.6.n Leila Ismail, Rajkumar Buyya: [Artificial Intelligence Applications and Self-Learning 6G Networks for Smart Cities Digital Ecosystems: Taxonomy, Challenges, and Future Directions](#); Sensors, Vol. 22, Issue 15, Aug 2022; DOI:10.3390/s22155750

## 18.11 Abschließende Bemerkungen

Wissen wird von Menschen durch die Beobachtung von Umwelt und Natur, Gedanken, Erinnerungen, Erfahrungen und Lernen erworben. Die zu diesen Fähigkeiten führenden informationsverarbeitenden Prozesse im menschlichen Gehirn werden als *menschliche Kognition* (Human Cognition) bezeichnet. Um technische Systeme zu befähigen, ebenso intelligent wie Menschen zu sein und sich folglich an neue Situationen möglich optimal anzupassen, muss in diesen die menschliche Kognition im



bestimmten Grade nachgebildet werden. Demzufolge gilt als wichtiger Trend bei technischer Entwicklung die Erarbeitung von Ideen zur Einrichtung von auf den Prinzipien menschlicher Kognition basierenden intelligenten Systemen. Es wird also versucht, die menschliche Kognition, d.h. kontextbewusstes Denken, in technischen Systemen nachzubilden. Man spricht in diesem Zusammenhang von intelligenten bzw. kognitiven Systemen, die als *kontextbewusste Systeme* (Context-Aware Systems) angesehen werden können.

### 18.11.1 Vom IoT zum Intelligent IoT

Intelligent IoT

Von enorm großer Bedeutung ist die Nachbildung der menschlichen Kognition im heutigen Internet of Things (IoT). Bestrebungen in diese Richtung führen zur Entstehung von Intelligent IoT (IIoT). Dies bedeutet, dass Komponenten/Systeme im zukünftigen IIoT eine *künstliche Intelligenz* (KI, *Artificial Intelligence*, AI) besitzen werden. Infolge werden sie in der Lage sein, situationsbewusst zu handeln und somit, wichtige Prozesse im Laufe der Zeit eigenständig zu optimieren und sich an eine neue Situation möglichst optimal anzupassen. Bevor diese Idee im heutigen IoT verwirklicht werden kann, müssen relevante Messwerte und Ereignisse kontinuierlich erfasst und dann auf eine spezielle Art für weitere Analysen bzw. zu Lernzwecken dokumentiert und archiviert werden.

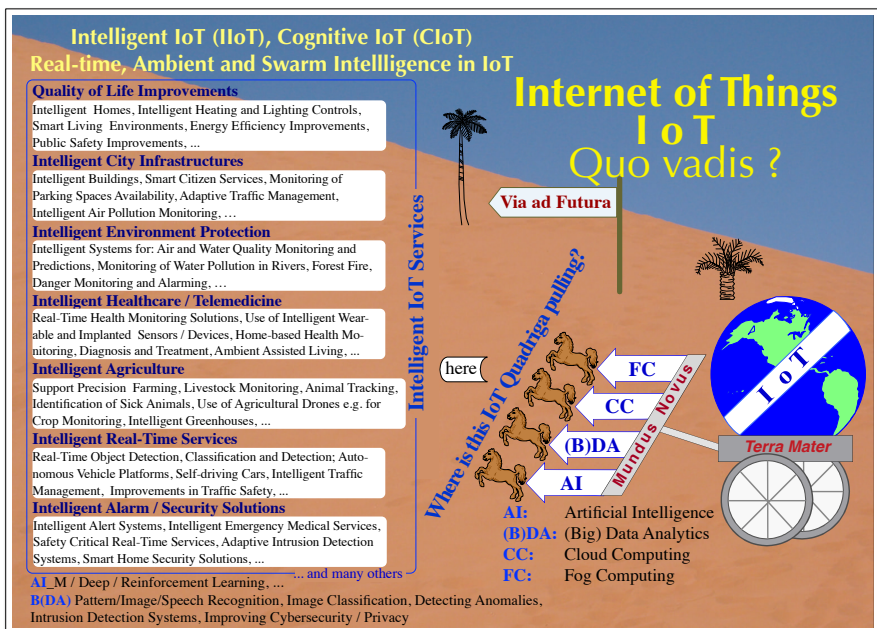


Abb. 18.11-1: Internet: Quo vadis?

Big IoT Data

Durch das kontinuierliche Erfassen verschiedener Arten von Daten im IoT wird ihre Menge jedoch immer größer. Man spricht von *Big Data* bzw. *Big IoT Data*. Bevor sie beim maschinellen Lernen zum Einsatz kommen, müssen diese Daten entspre-

chend analysiert werden. Die Analyse von Big Data als eine Art 'Vorbereitung auf ihren Einsatz', u.a. zur Unterstützung von Lernprozessen im IoT, wird als *Big Data Analytics* bezeichnet. Das wesentliche Ziel der Analysen von Big Data ist die Entdeckung von versteckten Mustern, unbekanntem Korrelationen und anderen nützlichen Informationen in den gesammelten 'riesigen Datenmengen'. Die Ergebnisse dieser Analysen im IoT werden einerseits Menschen angezeigt, damit sie die gewonnenen Informationen nutzen können. Andererseits sollen verschiedene IoT-Komponenten auf der Basis dieser Informationen selbständig lernen und sich dadurch in die Lage versetzen, auf verschiedene Situationen und plötzlich auftretende Ereignisse im IoT fast so intelligent wie Menschen zu reagieren. Sobald das IoT die eben geschilderten Fähigkeiten besitzt, immer kontextbewusst (situationsbewusst) agieren zu können, wird man von IIoT sprechen.

Die Evolution des IoT zum IIoT schreitet unaufhörlich voran und führt zu solchen Erweiterungen des IoT, um den Verlauf der menschlichen Kognition im IoT nachbilden zu können. Die kognitiven Fähigkeiten des Menschen ermöglichen ihm, verschiedene Arten von Informationen aus der Umwelt wahrzunehmen und weiterzuverarbeiten. Da die Fähigkeiten von IIoT im gewissen Grade den kognitiven Fähigkeiten des Menschen entsprechen werden, wird es als Cognitive IoT (CIoT) bezeichnet. Es sei hervorgehoben, dass AI, (Big) Data Analytics, Cloud Computing und Fog Computing als die vier wichtigsten treibenden Kräfte, quasi als 'Zugpferde' einer IoT Quadriga, bei der Weiterentwicklung des IoT zum IIoT angesehen werden können. Abb. ?? bringt dies illustrativ zum Ausdruck.

Cognitive IoT

Die Garantie der Sicherheit im IoT ist heutzutage ein enorm breites und wichtiges Thema. Man kann sich heute noch kaum vorstellen, mit welchen bösartigen Angriffen und anderen Unsicherheiten im zukünftigen IIoT gerechnet werden muss. Es bleibt nur zu hoffen, dass es statt 'Intelligent Internet of Things (IIoT)' nicht gesagt werden muss: 'Intelligent Internet of Threats (IIoT)'.

Intelligent  
Internet of  
Threats

### 18.11.2 Rückblick auf 50 Jahre Rechnerkommunikation

Nachdem die Networking Trends, die facto Internet Trends, und dabei auch die Migration von IoT zum IIoT, also zukünftige Internet-Aspekte, kurz erläutert wurden, stellt es sich die Frage: Welche relevante, technische sowie organisatorische Entscheidungen und Entwicklungen gab es auf dem Weg zum heutigen Internet? Eine Antwort darauf soll nun ein kurzer Rückblick auf 50 Jahre der Rechnerkommunikation geben.

Zur Entstehung des Internet in der 'heutigen Form' haben zahlreiche, aus letzten fünf Jahrzehnten stammenden Entwicklungen auf dem Gebiet der Rechnerkommunikation geführt. Heutzutage stellt das Internet – organisatorisch und technisch gesehen – ein immens komplexes, über die ganze Welt verteiltes technisches Gebilde dar. Wegen seiner Komplexität folgt es dem Hummel-Phänomen und funktioniert. Daher soll die in Abb. 18.11-2 gezeigte Internet-Hummel die fünf Jahrzehnte der Rechnerkommunikation auf dem Weg zum heutigen Internet anschaulich zum Ausdruck bringen.

Rückblick auf 50  
Jahre der  
Rechnerkommunikation

Um die bedeutenden, zur Entstehung des Internet führenden Ereignisse zu nennen, müssen wir nicht nur die letzten fünf Jahrzehnte nach dem historischen Datum 29. Oktober 1969 betrachten, sondern auch die 60er Jahre. In diesem Zeitraum – besonders

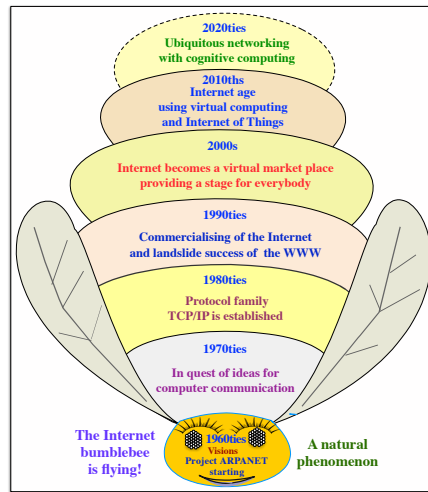


Abb. 18.11-2: Die Internet-Hummel fliegt – ein Naturphänomen

in den 1960er, 1970er, 1980er und 1990er Jahren – gab es eine Vielzahl technischer Ereignisse und Entwicklungen, die als Meilensteine auf dem Weg zum heutigen Internet angesehen werden sollen [Abb. 18.11-3]. Im Hinblick hierauf lassen sich die einzelnen Jahrzehnte kurz wie folgt charakterisieren:

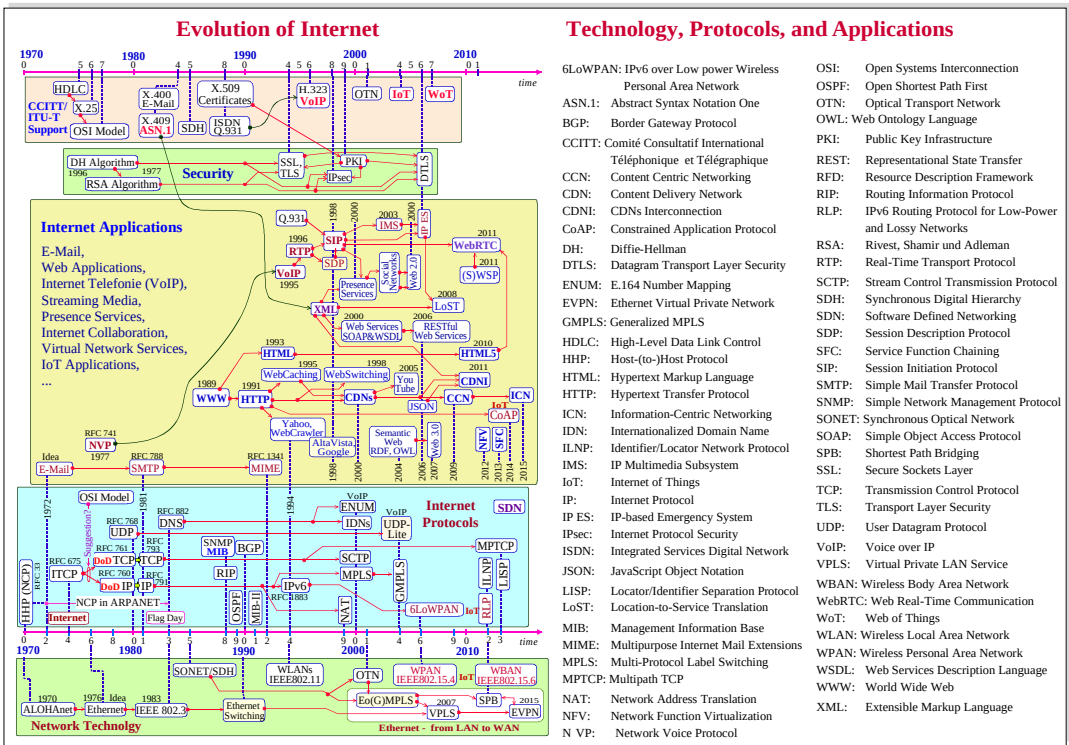
- Die 1960er Jahre Das erste experimentelle Rechnernetz namens ARPA(NET) entsteht und die Ära der Rechnerkommunikation beginnt.
- 1964
  - Das Konzept für *Packet Switching Networks* wird von Paul Baran veröffentlicht.
- 1965
  - Ted Nelson prägt die Begriffe *Hypertext* und *Hypermedia* – also jene, die man heute mit dem Begriff WWW verbindet.
- 1966
  - Die Entwicklung des Rechnernetzes namens ARPANET beginnt.
- 1969
  - Im März 1969 ist die Idee entstanden, die ARPANET-betreffenden Entwicklungen als sog. *Request for Comments* (RFC) zu dokumentieren.
- Ur-Internet
  - Am 29. Oktober 1969 wird das ARPANET mit vier IMPs (*Interface Message Processor*) als Knoten in Betrieb genommen. Somit war das erste Rechnernetz mit Paketvermittlung geboren.  
Die Daten zwischen Hosts werden nach den in RFC 11 (August 1969) spezifizierten *Host-Host Software Procedures* ausgetauscht. Die IMPs, als Vorfahren von heutigen Routern im Internet, wurden damals untereinander über Telefonleitungen verbunden und dienten als Netzknoten mit Paketvermittlung.
- Die 1970er Jahre Die Suche nach Ideen/Konzepten für die Rechnerkommunikation.
- 1970
  - ALOHAnet – das erste Funkrechnernetz – wird in Betrieb genommen.
  - Das *Host-to-Host-Protocol* für das ARPANET wird als RFC 33 spezifiziert und im ARPANET vom Januar 1972 bis zur Umstellung auf TCP/IP (1. Januar 1983) verwendet.

- Entwicklung des ersten E-Mail-Programms und Erfindung des @-Zeichens durch R. Tomlinson. 1972
- Die Gründung von NIC (*Network Information Center*) u.a. zur Dokumentation und Registrierung von Netzparametern, der Vorläufer von IANA (*Internet Assigned Numbers Authority*).
- ITCP und NCP werden im RFC 675 spezifiziert [Abb. 18.11-3]. 1974
- In diesem RFC wird das Wort *Internet* zum ersten Mal offiziell verwendet. Internet
- CCITT-Standard X.25 für *Packet Switching*: Verbindungsorientierte Übermittlung der Datenpakete – die Grundlage für das spätere MPLS. 1976
- Veröffentlichung des Konzepts von *Ethernet*, Robert M. Metcalfe und David R. Boggs.
- Whitfield Diffie und Martin Hellman publizieren die Idee zur Realisierung eines *Schlüsseltauschs mittels kryptographischer Funktionen* und somit der Verständigung auf einen gemeinsamem geheimen Schlüssel. DHE
- Das *OSI-Referenzmodell* entsteht und wird später in der CCITT X.200 Empfehlung spezifiziert. 1977
- Das *RSA-Verfahren* (Rivest, Shamir und Adelman) als Grundlage für den Aufbau asymmetrischer Kryptosysteme mit öffentlichen Schlüsseln (*public keys*), wird zum Patent angemeldet.
- Das *Network Control Protocol* (NCP) und das *Internet Transmission Control Program* (ITCP) werden durch IP und TCP (*Transmission Control Protocol*) funktionell ersetzt [Abb. 18.11-3]. Dies ist die Geburtsstunde der Protokolle IP und TCP; eine verbindungslose 'Alternative' zum TCP ist ebenso vorgesehen. 1978
- Das Gremium *Internet Configuration Control Board* (ICCB) wird gegründet, um die Entwicklung des Internets zu koordinieren. 1979

Die Etablierung des Internets mit der TCP/IP-Protokollfamilie.

Die 1980er Jahre

- Der Aufbau von CSNET (*Computer Science Network*) wird initiiert und dieses dient u.a. als Vorläufer von NSFNET (*National Science Foundation Network*). 1981
- Der Plan für die ARPANET-Umstellung von ITCP/NCP auf TCP/IP wird entwickelt.
- Am 1. Januar 1983 (sog. *Flag Day*) wird das ARPANET auf TCP/IP umgestellt und damit hat die Ära von TCP/IP begonnen. 1983
- Aus dem ARPANET entsteht das MILNET (*Military Network*) und der restliche Teil bildet das wissenschaftliche, zivile ARPANET.
- Der Aufbau von DFN (*Deutsches Forschungsnetz*) beginnt und damit auch die Einführung des Internets in Deutschland.
- Die Kopplung des DFN mit dem CSNET führt dazu, dass die erste, über das Internet transportierte E-Mail in Deutschland an der Universität Karlsruhe am 3. August 1984 empfangen werden kann [Zor14]. 1984
- Das NSFNET in einer modernen hierarchischen Struktur (*Backbone-Konzept*) wird etabliert (eine Art Internet-Backbone und die große Akzeptanz von NSFNET führt zur Stilllegung des ARPANET). 1986



**Abb. 18.11-3:** Evolution der Internet-Technologien; das 1977 in RFC 741 beschriebene 'Network Voice Protocol' von Danny Cohen kann als früher erster Versuch gewertet werden, über das damalige ARPANet voll-duplex Sprachkommunikation in Echtzeit zu führen.

TLD .de

- Am 5. November 1986 wird die Top-Level-Domain .de für Deutschland im DNS eingetragen.

Die 1990er Jahre

Die Kommerzialisierung des Internet und der Siegeszug des WWW.

1990

- Am 28. Februar 1990 wird das alte, ausgediente ARPANET offiziell stillgelegt. Seine Rolle übernimmt das moderne, in den 80er Jahren eingerichtete, Backbone-basierte NSFNET.

1991

- Das NSFNET wird für kommerzielle Nutzung als eine Art Internet-Backbone freigegeben. Die Folge ist die Kommerzialisierung des Internet und der Internet-basierten Technologien.

1995

- Der Backbone-Teil im NSFNET wird auf neue Struktur mit NAPs (Network Access Point) umgestellt. Diese waren Vorläufer moderner IXPs (Internet eXchange Point) und führen zur Entstehung von ISPs (Internet Service Provider).

Die 2000er Jahre

Das Internet als Information Delivery Network, als virtueller Marktplatz und der Beginn von Internet of Things.

Das Internet im Zeitalter von Virtual Computing und von Internet of Things.

Die 2010er Jahre

Für eine Vertiefung der chronologischen Entwicklung des Internet sei verwiesen auf:

- [Meilensteine in der Entwicklung des Internets](#)
- [Evolution of the Internet – Significant Technical Events](#)

Das Internet im Zeichen der *Künstlichen Intelligenz* ist im Entstehen. Die Künstliche Intelligenz stellt die Grundlage dafür dar, dass eine *Federation* verschiedener digitaler Zwillinge als eine Art globaler Digitaler Zwilling der Erde (*Digital Twin of the Earth*) mit dem Ziel einrichtet werden kann, das Leben auf der Erdkugel auf Dauer bewahren zu können. Eine entsprechende Initiative hierfür wurde unter dem Titel *Destination Earth*<sup>1</sup> (DestinE) von der Europäischen Union bereits gestartet.

Die 2020er Jahre

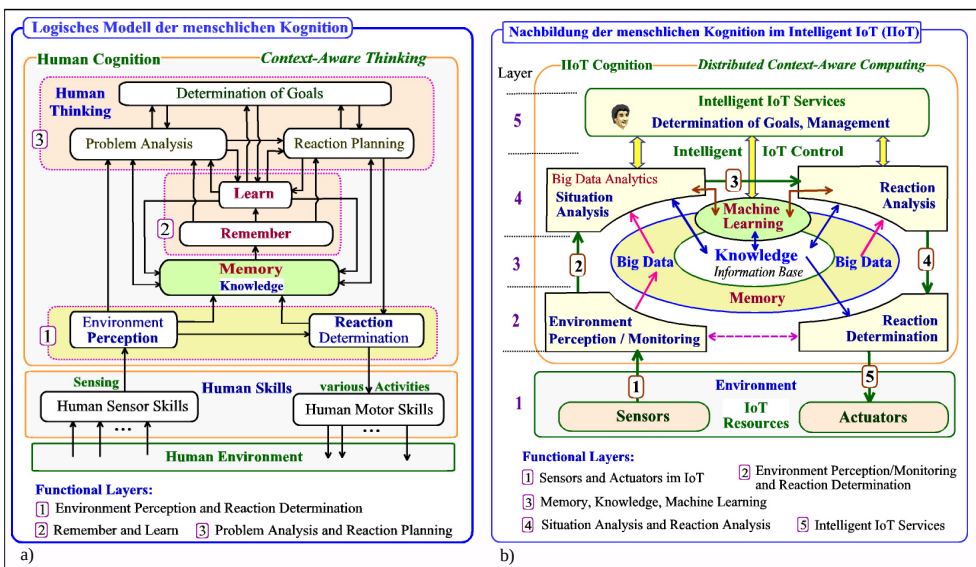


Abb. 18.11-4: Kognition der realen Welt a) Modell der menschlichen Kognition, b) Abbildung durch Intelligent IoT (IIoT) in der virtuellen Welt

Abb. 18.11-4a) vergleicht das Modell für kontextbewusstes Denken (*Context-Aware Thinking*) des Menschen mit dem in Abb. 18.11-4b) gezeigten Verlauf der kontextbewussten Informationsverarbeitung (*Context-Aware Computing*) im IIoT, d.h. mit dem Verlauf von *Distributed CAC*. Hierbei können die einzelnen Layer im Modell der IIoT-Kognition wie folgt beschrieben werden:

Distributed CAC

- **Layer 1:** *Sensors and Actuators im IoT*. Die Funktionalität dieses Layers entspricht weitgehend der menschlichen Sensorik (*Human Sensor Skills*) und Motorik (*Human Motor Skills*).
- **Layer 2:** *Environment Perception/Monitoring and Reaction Determination*. Dieses Layer im IIoT ist der Funktion nach mit dem in Abb.18.11-4a) gezeigten Layer 'Environment Perception and Reaction Determination' im Modell für das kontextbewusste Denken von Menschen vergleichbar.

<sup>1</sup>siehe: <https://digital-strategy.ec.europa.eu/en/policies/destination>

- **Layer 3: *Memory, Knowledge, Machine Learning*.** Dieser Layer entspricht dem in Abb. 18.11-4a) dargestellten Layer 'Remember and Learn' des menschlichen Gedächtnis (*Memory*), dem dort gespeicherten Wissen (*Knowledge*) und den menschlichen Fähigkeiten Erinnern (*Remember*) und Lernen (*Learn*).
- **Layer 4: *Situation Analysis and Reaction Analysis*.** Dieses Layer entspricht weitgehend dem in Abb. 18.11-4a) dargestellten menschlichen Denken (*Human Thinking*) bei der Analyse wahrgenommener Informationen (*Problem Analysis*) und der Vorbereitung einer Reaktion auf diese (*Reaction Analysis*).
- **Layer 5: *Intelligent IoT-Services*.** Die intelligenten IoT-Services und ihre Ziele (*Goals*) basieren auf dem beim maschinellen Lernen erworbenem Wissen. Folglich entsprechen diese weitgehend den hier erwähnten *Goals* der menschlichen Strategie (*Human Strategy*) in Abb. 18.11-4a).

**Dank an Alle!**

Das Internet ist eine der größten technischen Schöpfungen des 20ten Jahrhunderts mit der Beteiligung einer enormen Vielzahl der Menschen auf der ganzen Welt. Dafür geht unseren Dank an Alle, die sich mit ihrem organisatorischen und technischen Engagement, Wissen und Können zur Entstehung des Internet beigetragen haben.

Die zur Entstehung des intelligenten "Internet von morgen" führenden technischen Ideen und Systemlösungen möchten wir im nächsten Jahr in einem zusätzlichen, dieses Buch ergänzendes Werk ausführlich präsentieren.

# Stichwortverzeichnis

## Symbole

- (G)MPLS-Netze ..... 710
  - (G)MPLS-Switches ..... 32
  - 0-RTT Packet ..... 254
  - 4B/5B ..... 109
  - 5G Network Slicing 1076, 1082
  - 5G Security ..... 1076, 1082
  - 6LoWPAN ..... 977
  - 6to4 ..... 518
  - Adresse ..... 518, 578
  - Host ..... 578
  - Site ..... 578
  - Translation ..... 566
  - 6top Protocol ..... 978
- ## A
- AAA
    - Protokoll ..... 914
    - Server ..... 391, 914
  - Abandoning Initial Packet . 254
  - Abstract Syntax Notation ... 25
  - Abstract-Node ..... 749
  - Access
    - Area ..... 889
    - Control ..... 762
    - Control List 398, 399, 813, 815, 883
    - Gateway ..... 960
    - Point . 327, 392, 775, 776, 779, 810, 912, 947
    - Router ..... 947
    - Switch ..... 810
    - VPLS ..... 889
  - Accounting ..... 391
  - Daten ..... 392
  - ACK . 191, 193–195, 198, 203, 222
  - PDU ..... 190
  - Acknowledgement ... 187, 459, 657, 761, 771, 774, 978, 1024
  - Number ..... 188, 195
  - Selective ..... 190, 205, 247
  - Active Directory ..... 100
  - Active Router ..... 685
  - Active-Close ..... 195
  - Actuator ..... 962
  - Adaptivitätsattribute ..... 740
  - Additional Authenticated Data 84
  - Additional Section ..... 291
  - Address
    - Harvesting ..... 401
    - Spoofing ..... 254
  - Address Family
    - Identifier ..... 671, 672
    - Transition Router ..... 572
  - Address Mask
    - Request ..... 165, 168
    - Response ..... 165, 168
  - Address Resolution
    - Protocol 39, 115, 141, 155, 489, 534, 564, 613, 855
  - Ad-Hoc-Mode ..... 778
  - Adjacency ..... 643
  - Adresspräfix ..... 505
  - Advertisement Interval .... 683
  - Affinität ..... 741
  - Agent
    - Discovery ..... 922
    - Solicitation ..... 925
  - Aggregatable Global Unicast Ad-dresses ..... 512
  - Aggregation Layer ... 809, 810, 822
  - Aggregation Switches . 810, 895
  - Aging Time .... 814, 816, 883
  - AGU-Adressen ..... 512
  - AI, IoT and 5G Convergence 1099
  - AI-enabled Networking .. 1099
  - AI-enabled SDN ..... 1099
  - Aktives Queue Management 215
  - Aktoren ..... 962
  - Aktuatoren ..... 962, 1045
  - Alert Protocol ..... 415
  - Aliasname ..... 55, 280
  - All Station Address ..... 767
  - All-Active Redundancy Mode 899, 901
  - All\_DHCP\_Servers ..... 555
  - All-Host
    - Group ..... 170
  - All-Nodes ..... 518
  - Multicast Address ..... 545
  - All-Ones subnet ..... 146
  - All-Router
    - Group ..... 170
    - Multicast ..... 545
  - All-Zeros subnet ..... 146
  - ALT-Infrastruktur ..... 862
  - Ambient Intelligence .... 1074
  - in IoT ..... 1069
  - American National Standards In-stitute ..... 760
  - Amplification Attacks . 296, 307
  - Anchor ..... 307
  - Angriff
    - Chosen-ciphertext ..... 77
    - Chosen-plaintext ..... 77
    - Ciphertext-only ..... 76
    - Known-plaintext ..... 76, 82
  - Announcement ..... 835
  - Anonymous DH ..... 424
  - Answer ..... 460
  - Section ..... 290, 343
  - Anti-Replay-Schutz ..... 368
  - Anwendungsschicht ... 38, 108
  - Anycast
    - Adresse ..... 503, 580
    - Routing ..... 270
  - Anycasting ..... 270
  - Anything-in-Anything 570, 608
  - Apex ..... 285, 300, 303
  - AppleTalk ..... 331
  - Application
    - Data ..... 421
    - Layer ..... 25
    - Layer Gateway ..... 365, 604
    - Layer Notification Information 421
    - Program Interface ..... 210
    - Support Protokolle 28, 40, 407
  - Applications Area ..... 45
  - Applikationstyp ..... 202
  - A-Query ..... 273
  - Architektur
    - Software ..... 62
  - Area Border Router .. 648, 649, 652
  - Area Director ..... 45
  - a.root-servers.net ..... 269
  - ARP
    - Cache ..... 156, 162
    - Reply ..... 156, 157, 161, 162
    - Request ..... 156–158, 816
    - Server ..... 141
    - Tabelle ..... 160
  - arpa ..... 268, 281
  - Artificial Intelligence .... 1069, 1072, 1099, 1108
  - AS
    - Border Router ..... 663, 664
    - Boundary Router .... 648, 651
  - ASCII Compatible Encoding 283
  - ASN.1 ..... 101
  - Associate
    - Message ..... 473
  - Association ..... 774, 778, 780
  - ID ..... 777
  - Number ..... 830, 831, 833



- Request ..... 777
  - Response ..... 777
  - Asynchronous Transfer Mode  
724
  - ATM-Label ..... 726
  - Atomuhren ..... 463
  - Attribut ..... 101, 399
  - Ausgangsport ..... 642, 730
  - Authenticate ..... 305
  - Authenticate ..... 772
  - Authenticated Encryption with  
Associated Data ..... 82
  - Authentication .. 409, 655, 734,  
770, 778
  - Data ..... 376, 377, 683, 686
  - Enabled ..... 1018
  - Header 176, 369, 378, 488, 493,  
494
  - Indicator ..... 593
  - Protocol
    - Extensible ..... 383
    - Server ..... 384
    - Tag ..... 84
    - Type ..... 637, 683  - Authenticator 99, 100, 384, 772
  - Authentisiert ..... 777
  - Authentisierung .. 55, 360, 391,  
393, 494, 774, 783
  - äußere ..... 99, 384, 388
  - innere ..... 99, 384, 388
  - Mechanismus ..... 386
  - Authentisierung, Autorisierung,  
Accounting ..... 390
  - Authentizität . 62, 101, 108, 112,  
388, 827
  - Authority
    - Information Access ..... 107
    - Section ..... 290, 291, 344  - Autoconf ..... 342
  - Autoconfiguration 332, 488, 527
    - stateless ..... 331  - Auto-Discovery ..... 887, 888
  - Autokey ..... 467, 472
  - Autokey-Mechanismus ..... 473
  - Autokonfiguration ..... 339
  - Automatic
    - Private IP Addressing ..... 342  - Autonomes System ..... 648
  - Autonomic
    - Networking ..... 1099, 1105
    - System ..... 1105  - Autonomic Networks ..... 1105
  - Autorisierung 57, 112, 391, 548
  - Autotuning ..... 208
  - Availability ..... 113
- B**
- B4-Interface ..... 573
  - Backbone ..... 648
  - Anbindung ..... 650
  - Bereich ..... 648
  - Bridges Provider ..... 839
  - Core Bridge ..... 842
  - Edge Bridge ..... 842
  - Netz ..... 6
  - Router ..... 143, 648, 650
  - Service Instance Identifier 844
  - Service Instance Tag ..... 844
  - VLAN ..... 794
  - VLAN Identifier ..... 841
  - Backend-Datenbank ..... 391
  - Backlog-Puffer ..... 212
  - Backup
    - Designated Router ..... 656
    - DR ..... 646, 655, 656  - Bandbreiten/Delay-Produkt 215
  - Bandwidth Broker ..... 715
  - Base Object ..... 1013
  - Basic Service Set ..... 775
    - Identifier ..... 779  - Baumwurzel ..... 691
  - Beacon Frames .. 776–778, 978,  
980
  - Benutzer
    - Authentisierung . 401, 402, 481
    - dienstprotokolle ..... 42, 44
    - ID ..... 389
    - Profile ..... 391
    - Bereichs-ID ..... 647  - Berkeley Internet Name Dae-  
mon ..... 296
  - Berkeley Software Distribution  
5
  - BGP
    - based VPLS ..... 888
    - Header ..... 665
    - Identifier ..... 666
    - MPLS IPv4-VPN ..... 673
    - MPLS IPv6-VPN ..... 674
    - Multiprotocol ..... 670
    - Nachrichten ..... 664
    - Speaker ..... 662  - B-Header ..... 843
  - Big Data 964, 1072, 1102, 1108
  - Analytics ..... 1072, 1102
  - Driven Networking ..... 1102
  - Bind ..... 398, 401
  - Binding ..... 360, 422
  - Acknowledge ..... 938
  - Acknowledgement ..... 943
  - Cache ..... 937, 939
  - Information Base .... 605, 606
  - Request ..... 360
  - Response ..... 360
  - Update ..... 938, 949, 951
  - Bindung
    - Update ..... 943  - Bit
    - Destuffing ..... 768
    - Error Rate ..... 108
    - Stuffing ..... 767  - Bitfehler ..... 108, 109
  - Bitlabel ..... 281
  - Bitübertragung ..... 774
  - Blockchain ..... 66, 428
  - Blockchiffre ..... 79
    - AES ..... 59
    - DES ..... 59  - Blockverschlüsselung ..... 76
  - Bonjour Protokoll ..... 330, 342
  - BOOT Protocol ..... 344
  - Border Bit ..... 701
  - Border Gateway
    - Multicast Protocol ..... 688
    - Protocol 40, 43, 565, 624, 639,  
662, 872  - Border Router ..... 960
  - Boundary clock ..... 477
  - Bridge Port Extension ..... 822
  - Bridging-Mode ..... 765
  - Broadcast ..... 999
    - limited ..... 924  - Broadcast, Unknown and Multi-  
cast ..... 879, 886,  
900
  - Broadcast-Frame ..... 884
  - Bucket-Größe ..... 744
  - Byte-stream ..... 187
  - Byzantinischen Generäle .. 472
- C**
- Call
    - Forwarding ..... 452
    - Hold ..... 452
    - Session Control Function . 481
    - Transfer ..... 452  - Canonical
    - Name ..... 446
    - Order ..... 300  - Canonicalization ..... 311
  - Capability Information 776, 777
  - Care-of-Address . 917, 922, 936
  - Carriage Return ..... 324
  - Carrier Sense
    - Multiple Access Collision Avoi-  
dance ..... 761
    - Multiple Access Collision De-  
tection ..... 761  - Carrier-Grade NAT .. 403, 566,  
574, 584, 608
  - Cascading Style Sheets ..... 8
  - CE-Paket ..... 219
  - Certificate ..... 416

- Authorities ..... 324
- Authority . 101, 103, 105, 280, 413, 547
- Chain ..... 107
- Client
  - Authority ..... 418
  - Verify ..... 418
- Exchange ..... 418
- Path Advertisement . 532, 548, 549
- Path Solicitation ..... 532, 548
- Request ..... 105
- Revocation List ..... 103
- Usage ..... 320
- Verify ..... 418
- Certification Authority Authorization ..... 324
- ChaCha-Poly1305 ..... 255
- Chain of Trust . . . 101, 299, 307
- Challenge ..... 388, 773
  - Authenticator ..... 99
  - Handshake Authentication Protocol ..... 765, 768, 772
  - Peer ..... 99
- Challenge/Response-Verfahren 578
- Change-Cipher-Spec ..... 388
- Protocol ..... 415
- Chaosnet ..... 279
- Checking Disabled ..... 304
- Checksum . . . 70, 110, 164, 172, 243, 605
  - UDP ..... 183
- Chiffren ..... 75
- Chunk ..... 242
  - Bundling ..... 243
  - DATA ..... 243–245, 247, 248
  - ID ..... 244
  - Type ..... 244
- Cipher
  - Block Chaining . . 81, 108, 111
  - Block Feedback ..... 81
  - Output Feedback ..... 81
  - Suite . 414, 417, 420, 426, 827
- Circuit Emulation over MPLS 792
- Class ..... 124, 127, 278
- Class of Service . 727, 737, 741
- Classless Inter-Domain Routing 662
- classless IP ..... 143
- Client
  - Access Layer ..... 809, 810
  - Authentisierung ..... 400
  - Autorisierung ..... 481
  - Client
    - Kommunikation ..... 808
  - Error ..... 1026, 1035
  - Server
    - Anwendung ..... 808
  - Clock ..... 438
  - Cloud ..... 964, 1062
  - Computing 807, 859, 958, 964, 965
  - Containerization . 1061, 1062, 1064
  - Networking ..... 1066
  - Native
    - Microservice ..... 1064
    - Microservices ..... 1067
    - VFN ..... 1067
  - C-LSR ..... 716
  - CN-Binding ..... 938
  - Coalescing Packets ..... 252
  - CoAP
    - Messages ..... 1020, 1029
    - Method ..... 1021
    - Options ..... 1029
    - Requests ..... 1020
    - Responses ..... 1020
    - Secure ..... 1029
    - to-HTTP Mapping ..... 1021
    - to-HTTP Proxy ..... 1021
    - to-HTTP Proxying ..... 1021
  - Code ..... 164
  - CodeBook ..... 75
  - Coding2 ..... 78
  - Cognitive IoT ..... 1069
  - Cognitive Network . 1099, 1103
  - Collaboration Services ..... 452
  - Collision Count ..... 547
  - colocated CoA . . . 922, 928, 931
  - Common
    - Gateway Interface ..... 8
    - Header ..... 243, 746
    - Internet File System ..... 208
    - Name ..... 398, 399
    - Open Policy Service ..... 715
  - Common Address Redundancy Protocol ..... 707
  - Communities ..... 678
  - Compound Packet ..... 447
  - Compound Session Key . . . 389
  - compressed NH Value . . . . . 983
  - Compressed RTP ..... 439
  - compressed UDP ..... 983
  - Concise Binary Object Representation ..... 1038
  - Cone NAT ..... 356, 591
  - Confidentiality ..... 255
  - Configuration Options 768, 769, 771
  - Configure-Request ..... 771
  - Confirmable ..... 1024
  - Non ..... 1024
  - Congestion ..... 207, 214
    - Avoidance ..... 205
    - Control ..... 17, 120, 261
    - Experienced ..... 215–217
    - Window ..... 205
    - Window Reduced . . . 188, 219
  - Connection Association . . . 834
  - Connection Association Name 834
  - Connection ID ..... 252
  - Connection Identifier ..... 254
  - Connectivity Association . . 827, 828, 831, 834
    - Key ..... 829, 834
    - Name ..... 829
  - Connectivity Security Association ..... 832
  - Conseil Européen pour la Recherche Nucléaire ..... 6
  - Constrained Application Protocol ..... 957, 969, 975, 976, 1019
  - Constrained Networks 957, 963, 975, 1019
  - Constrained RESTful Environment ..... 976
  - Constrained Shortest Path First 715, 738, 741
  - Constraint-Routing . . . 712, 715, 738
    - Label Distribution Protocol 908
    - LDP ..... 715, 744, 751
  - Contact Port ..... 193
  - Container ..... 784, 958
  - Container-based Network Service ..... 1062
  - Container-based Network Services ..... 1061, 1062
  - Containerized IoT Services 1064
  - Container-Technologie . . . 1060
  - Content Centric Networking 1084
  - Content Delivery Network . 213, 250
  - Content Encoding ..... 1032
  - Content Format ..... 1032
  - Content Nameserver ..... 327
  - Content Type ..... 1032
  - Contrained RESTful Environment ..... 1019
  - Contributing Source Identifier 439
  - Control ..... 764
    - Channel Management . . . 734
    - Feld ..... 762, 767
    - Flags ..... 188, 219
    - Frames ..... 777

- Plane . 713, 733, 815, 871, 899, 906, 1050, 1052
  - Points . . . . . 335, 336
  - Protocol . . . . . 768
  - Protocol IPCP . . . . . 772
  - Register . . . . . 778
  - Word . . . . . 786, 876
  - Cookie . . . . . 245, 430, 431, 1023
    - Ack . . . . . 245
    - Echo . . . . . 245
  - Coppersmith . . . . . 97
  - Core Area . . . . . 889
  - Core Based Trees . . . . . 688
  - Core-LSR . . . . . 716
  - Core-VPLS . . . . . 889
  - Correctness . . . . . 255
  - Correspondent
    - Node . . . . . 936, 947
    - Node Binding . . . . . 938, 944
    - Node Deregistration . . . . . 940
  - COSINE-Schema . . . . . 399
  - Counter Mode Cipher Block Chaining Message Authentication Code Protocol . . . . . 780
  - Counter-Mode . . . . . 82
  - Country Code . . . . . 398
  - Count-to-Infinity-Problem . 629
  - CRC . . . . . 214
  - Credentials . 339, 385, 389, 400
  - Cross-Connect-Systeme . . 733
  - Cryptobox . . . . . 308
  - Cryptographically Generated Addresses . . . . . 547
  - CSMA/CA . . . . . 774
  - C-TSN Ack . . . . . 247
  - Current Hop Limit . . . . . 540
  - Currently Unused . . . . . 120
  - Curve25519 . . . . . 307, 308
  - CurveDNS . . . . . 294, 337
    - Qname . . . . . 310
  - Customer
    - Area . . . . . 889
    - Edge . . . . . 673, 874, 889, 897
    - Premises Equipment . 566, 572, 584
    - Premises Network . . . . . 809
  - Cyberspace . . . . . 6
  - Cyclic Redundancy Checksum . . . . . 110
  - Code . . . . . 108
- D**
- dACKs . . . . . 205, 206
  - Dark Fiber . . . . . 60
  - Data . . . . . 126
    - leakage . . . . . 52
  - Data Center Services . . . . 1051
  - Data Dissemination . . . . . 1019
  - Data Frames . . . . . 978
  - Data in flight . . . . . 197
  - Data Plane 815, 871, 899, 1050
  - Data Safety . . . . . 54
  - Datacenter . . . . . 809
  - Data-Driven Networking . 1099, 1102, 1105
  - Datagram
    - Congestion Control Protocol 261, 434, 450
    - Prinzip . . . . . 710
    - TLS . . . . . 429
  - Data-Link
    - Connection Identifier 719, 726
    - Frame . . . . . 29, 30, 108
    - Layer . . . . . 25, 774
    - Verbindung . . . . . 768
  - Datamining . . . . . 53
  - Daten . . . . . 24
    - Frames . . . . . 777, 778
    - Leakage . . . . . 336
    - Semantik . . . . . 51
  - Daten Attribut . . . . . 52
    - Gültigkeit . . . . . 52
    - Herkunft . . . . . 52
    - Vertraulichkeit . . . . . 52
  - Datenbank-Backend . . . . . 400
  - Datendirektverbindungen . 759
  - Datenflusskontrolle . . . . . 195
  - Datenlink . . . . . 827
  - Datenquelle . . . . . 55
  - Datensegmente . . . . . 30, 187
  - Datensenke . . . . . 55
  - Datensicherungsschicht . . 108
  - Datenstromverschlüsselung . 76
  - Datenworts . . . . . 51
  - Decapsulation . . . 573, 784, 785
  - Decomposing URIs into Options . . . . . 1029
  - Deep Learning . . . . . 1099
  - Default
    - Free Zone . . . . . 859
    - Gateway . . 139, 168, 169, 345, 540, 546, 679, 817, 821, 903, 935
    - Lifetime . . . . . 1018
    - Route . . . . . 620, 622, 859
    - Router . . . . . 533, 540, 679
  - Defense Communication Agency . . . . . 5
  - Delay . . . . . 22
  - Delegated Präfix . . . . . 583
  - Delegating Router . . . . . 557
  - Delegation . . . . . 267, 276, 285
    - Signer . . . . . 280, 301, 302
  - DeMilitarized Zone . . . 326, 381
  - Denial of Service . . . . . 245
    - Angriffe . . . . . 211
  - Deployment . . . . . 548
  - Deregistrierung . . . . . 928, 932
  - Derive-Secret . . . . . 427
  - Designated Forwarder 900, 901
  - Designerter Router . . . . . 646
  - Destination . . . . . 26
    - Address . . . 119, 491, 599, 779
    - Advertisement Object . . 1018
    - Cache . . . . . 536
    - EID . . . . . 861
    - IP Address . . . . 183, 372, 601
    - IPv6-Address . . . . . 542
    - Options Header . 493–498, 938, 940, 942, 943
    - Port . . . . . 183, 187
    - Port Number . . . . . 243
    - RLOC . . . . . 861
    - SAP . . . . . 763
    - Unreachable . . 165, 166, 169, 171, 496, 530, 602
  - Destination-Oriented Directed Acyclic Graph . . . . 998, 1000
  - Deterministic Networking 1041, 1095
  - Detour LSP . . . . . 749
  - DHCP
    - ACK . . . . . 348
    - Client . . . . . 345
    - DECLINE . . . . . 349
    - DISCOVER . . . . . 347
    - INFORM . . . . . 349
    - NAK . . . . . 349
    - OFFER . . . . . 348
    - Offer . . . . . 347
    - Relay-Agent . . . . . 345
    - RELEASE . . . . . 349
    - REQUEST . . . . . 348, 349
    - Server . . . . . 345
  - DHCPv6 . . . . . 523
    - Client . . . . . 550
    - Nachricht . . . . . 552
    - Port . . . . . 550
    - Relay . . . . . 551
    - Server . . . . . 550
    - Unique Identifier . . . . . 551
  - Dial-In-Zugang . . . . . 390
  - Diameter . . . . . 44
  - Differentiated Services 118, 120, 175
    - Code Point . . . . . 120, 218
  - Diffie-Hellman . . . . 84, 85, 424
    - Verfahren . . . . . 64, 87
  - DiffServ . . . . . 120
  - Diffusion . . . . . 79
  - Digital Subscriber Line . . . 201
  - Digitalisierung . . . . . 84
  - Dijkstra . . . . . 612
  - Algorithmus . . . . . 642

- Ding ..... 960
- DIO-Dissemination ..... 1019
- Directory
  - Access Protocol ..... 397
  - Information Base ..... 400
  - Information Tree ..... 398
  - User Agent ..... 401
- Discover-Process ..... 383
- Discovery ..... 335, 554
- Dispatch Header ..... 983, 988
- Distance Vector
  - Multicast Routing Protocol 688
  - Routing ..... 621
- Distanzvektor ..... 624
- Routing-Protokoll ..... 624
- Distinguished Name . . . 101, 102, 398, 401
- Distributed
  - Ethernet-Switch ..... 869
  - FT ..... 872
  - Multilayer Switch ..... 903
  - Switch ..... 872
  - Systems ..... 462
- Distribution
  - Layer ..... 809, 810
  - Switch ..... 810
  - System ..... 776, 778
  - System Services ..... 781
- DNS
  - based Service Directory . . 333
  - based Service Discovery . . 330, 331
  - Cache Poisoning ..... 295
  - Cache-Server ..... 269, 271
  - Datenbaum ..... 266
  - Dumping ..... 337
  - Extended ..... 289
  - Forwarder ..... 271, 341
  - Query ..... 308
  - Registrar ..... 269, 276, 328
  - Response ..... 308
  - DNS64 ..... 567, 571, 603
  - DNSCrypt ..... 337
  - DNSKEY ..... 299
  - DNSSEC ..... 337
  - aware ..... 303
  - DNSSECbis ..... 294
  - Docker ..... 1060
  - DODAG Information Object 1002
  - Domain ..... 266, 268
  - Component ..... 399
  - Grabbing ..... 329
  - Label ..... 267
  - Name ..... 267, 280
  - Suffix ..... 267, 345
- Domain Name
  - Service ..... 44
  - System 182, 263, 264, 269, 336, 489, 565, 853, 860
  - DomainKeys Identified Mail 313
  - Domain-Parameter ..... 92, 96
  - Don't Fragment . 118, 122, 169, 600, 601
  - Doppelpunkt-Hexadezimalnotation 503, 523
  - DoS-Attacke ..... 211
  - Dot-net ..... 414
  - Downstream ..... 753
  - Knoten ..... 750
  - Router ..... 747
  - System ..... 753
  - Downward Routes ..... 1017
  - DTLS-Record ..... 431
  - Dual-Queue/Dual Bus ..... 761
  - Dual-Stack ..... 526, 564
  - Betrieb ..... 566
  - Gateway ..... 567
  - Host ..... 571
  - Lite ..... 566, 571
  - Router ..... 571
  - Transition Mechanism . . . 570
  - Duplicate Address Detection 521, 524, 525, 535, 544, 545, 945
  - Dynamic Host Configuration Protocol . . . 43, 167, 182, 344, 489, 565
  - for IPv6 ..... 529
  - DynDNS ..... 367
- E**
- e164.arpa ..... 268
- EAP
  - Body ..... 386
  - Method Key Derivation . . 829
  - Nachricht ..... 396
  - over LAN ..... 386
  - over WiFi ..... 386
  - Packet ..... 386
  - PEAP ..... 388
  - Request-ID ..... 388
  - Request-PEAP ..... 388
  - Response-PEAP ..... 388
  - Response-Success ..... 389
  - TLS ..... 387
  - Tunnel TLS ..... 387
- EAP Supplicant ..... 832
- Early Data ..... 421, 422
- Eavesdropper ..... 49
- ECC
  - double-based ..... 94
  - fixed-base ..... 92
  - Signatur-Prüfziffer ..... 95
- Echo
  - Funktion ..... 167, 531
  - Reply ..... 163, 165, 167, 531
  - Request ..... 163–165, 167, 531
- ECN
- Echo ..... 189, 219
- Feld ..... 218
- Setup ..... 220
- Setup-ACK-Paket ..... 220
- Setup-SYN-ACK-Paket . . . 220
- Setup-SYN-Paket ..... 221
- Edge Virtual Bridging ..... 823
- Edge-LSR ..... 716
- EDNS ..... 289
- Egress ..... 727
- RBridge ..... 837
- Router ..... 861
- Tunnel Router ..... 861
- Eifel-Algorithmus ..... 206
- Eingangsport ..... 730
- Eintrag ..... 399
- Einwegfunktionen ..... 65
- Electronic Code Book ..... 80
- Element
  - primitives ..... 92
- ElGamal ..... 85
- Elliptic Curve Cryptography 305
- Embedded-System ..... 823
- Emulation ..... 785
- Encapsulation . . . 566, 573, 784, 785
- Security Header ..... 176
- Security Payload 369, 488, 494, 943
- Encrypted Handshake Message 388, 420
- Encryption ..... 425
- Algorithmus . . . . . 371
- End Node ..... 999, 1002
- Ending Delimiter ..... 762
- Endlicher Körper ..... 92
- Endpoint Identifier . . . 858, 859
- End-to-end transparent clock 477
- End-to-End-VPN ..... 787
- Enigma ..... 75
- Entity Tag ..... 1033
- Entropie ..... 56, 75, 97
- Entry ..... 399
- Epoche ..... 429, 430, 464
- Equal Cost ..... 895
- Multi-Path . . . . . 892, 895, 908
- Erweiterungs-Header . 491, 492
- ES Identification ..... 898
- ESS Identifier ..... 776
- Establish ..... 771–773
- Ethernet ..... 775
- Auto-Discovery (A-D) Route 907

- Cloud ..... 836
- Emulation ..... 873
- LAN ..... 869
- over PW ..... 792, 875
- Passive Optical Network .. 831
- Segment ..... 898
- Segment Route ..... 907
- V2 ..... 763
- Virtual Private Network .. 869, 892
- EtherType ..... 37, 763, 983
- EUI-64-Adressen ..... 508
- European Academic Research Network ..... 6
- EVPN Instance ..... 872
- Exchange Protocol ... 646, 656
- Expected Transmission Count 998, 1010
- Expected Transmission Time 1010
- Experimental-ID ..... 189
- Explicit Congestion Notification 120, 206, 214, 261
- Explicit Path ..... 740
- Extended
  - DNS ..... 292
  - Key Usage ..... 104
  - Master Session Key ..... 389
  - RPL Node Trustworthiness 1010
  - Sequence Number ..... 371
  - Service Set ..... 775
  - Unique Identifier ... 508, 1000
- eXtended Reports ..... 449
- Extended Unique Identifier 851
- Extensible Authentication Protocol .. 339, 404, 770, 774, 781, 783, 826, 829, 835
- eXtensible Markup Language 25
- Extension
  - Field ..... 547
  - Header 176, 369, 488, 491, 492
- Extensions ..... 420
- externe Route ..... 651
- F**
- Fast
  - DETOUR ..... 749
  - Handover ..... 953
  - Handover for Mobile IPv6 954
  - Open
    - Cookie Request Option .. 209
  - Recovery ..... 205
  - Re-Routing ..... 713
  - Retransmit ..... 205
- ROUTE ..... 749
- Fault
  - Control ..... 17
  - Management ..... 735
- Fehlerfreiheit ..... 112
- Fehlerkontrolle ..... 17
- Fenstermechanismus ... 21, 191
- Fensterprinzip ..... 195
- Fiber Bundle ..... 730
- Fiber Data Distributed Interface 760
- Fibre Channel over IP ..... 117
- FIFO
  - Prinzip ..... 215
  - Queue ..... 215
- File Transfer Protocol ..... 42
- FIN ..... 191, 195
- Fingerprint ..... 301
- Finite Fields ..... 64
- Firewall ..... 125, 211, 326
- First-In/First-Out ..... 215
- Fixed-Length Portion ..... 929
- Flag Day ..... 1111
- Flight ..... 431
- Flooding ..... 623
  - Protocol ..... 646
- Flow Control ..... 17, 195
- Flow Label ..... 254, 986
- Flusskontrolle ..... 17, 21
- Flying Ad-hoc Network .. 1053
- Füllzeichen ..... 119
- Fog Computing .. 958, 964, 1069
- Fog Nodes ..... 964
- Foreign Agent ..... 916, 922
- Forward
  - Error Correction .... 108–110
- Forwarder ..... 215, 272, 331
- Forwarding
  - Entry ..... 815
  - Equivalence Class ... 718, 722, 737
  - Table . 840, 875, 879, 881, 907, 998
- Forwarding Table ..... 871
- FQDN ..... 266
- Fragment
  - Identification ..... 501
  - Offset ..... 119, 123, 502
  - Pakete ..... 501
  - Fragmentation needed ..... 169
  - Fragmentierung ..... 501
- Frame ..... 25–27, 51, 252
  - Check Sequence ..... 110, 762
  - Control ..... 762, 778
  - Klasse ..... 777
  - klassen ..... 777
  - Status ..... 762
  - Type ..... 253, 255
- Framed
  - Compression ..... 396
- IP-Adresse ..... 396
- IP-Netmask ..... 396
- MTU ..... 396
- Protocol ..... 396
- Frameklasse ..... 777
- Framework ..... 848
- Fremd
  - Agent ..... 916
  - Hotspot ..... 913
  - subnetz ..... 915
- Frequency-Time Division Multiplexing ..... 1041, 1096
- FR-Label ..... 726
- Full Cone NAT ..... 356
- Full Qualified Domain Name 264, 266
- Full Resolver ... 269, 277, 303
- Full-Duplex-Verbindung ... 186
- Full-Function Devices ..... 980
- Function Instability ..... 1001
- Funktionale Gruppe ..... 522
- G**
- Galois
  - Counter Mode ..... 82, 425
  - Field ..... 83, 92
  - Message Authentication Code 71, 831
- Gason ..... 755
- Gateway ..... 612, 619
  - Access ..... 962
- Generalized MPLS 32, 709, 711, 728
- Generator ..... 92
  - Polynom ..... 110
  - punkt ..... 92
- Generic
  - Framing Procedure ..... 729
- Label ..... 726
  - Patch Selection and Maintenance ..... 740
  - Routing Encapsulation ... 566, 567, 569, 691, 875
- Geographische Domains ... 268
- Gigabit Networking ..... 710
- Global Routing
  - Prefix ..... 512, 849
  - Tabelle ..... 859
- Global Unicast Addresses . 510–512
- Global-ID ..... 516
- Glue ..... 275, 285, 286, 303
- Glueless Delegation ..... 275
- GMPLS TE ..... 736
- Gültigkeitsdauer ..... 102
- Grafting ..... 692
- Grandmaster ..... 478

- Graphenform ..... 612  
 Gratuitous ARP ..... 343, 932  
 Greenwich Mean Time ..... 464  
 Group Address ..... 172, 173  
 Group Transient Key ..... 389  
 Group-and-Source-Specific-  
   Query ..... 174
- H**
- HAA Discovery ..... 940  
 halb-duplex ..... 774  
 Handshake ..... 430  
   Extensions ..... 417–420  
   Packet ..... 254  
   Protokoll ..... 415, 416, 422  
 Happy Eyeball ..... 527  
 Hardware  
   Address Length ..... 157  
   Typ ..... 157  
 Hash ..... 516  
   funktion ..... 108  
   salted ..... 70  
 Hash based  
   Message Authentication Code  
     368  
   Message Authentication Code  
     71  
   Hashsumme ..... 70  
   Hashwert ..... 70, 108  
   keyed ..... 108  
 Header ..... 26, 116, 1013  
   Extension ..... 439  
   Length ..... 496  
   Form ..... 253  
   Lines ..... 1031  
   Next ..... 494  
 Heartbeat  
   Extension ..... 430  
   Funktion ..... 577  
   Nachrichten ..... 430  
   Payload ..... 431  
   Protokoll ..... 415, 430  
   Request ..... 431  
   Response ..... 431  
 Heimataadresse ..... 922  
 Heimat-Hotspot ..... 913  
 Hello  
   Intervall ..... 656  
   Nachricht ..... 686  
   Nachrichten ..... 430  
   Paket ..... 623, 643, 645, 655, 656  
   Protokoll ..... 645  
   Protool ..... 646  
   VerifyRequest ..... 429, 430  
 Hesiod ..... 279  
 Hierarchical Mobile IPv6 ..... 911,  
   912, 946  
 Hierarchical VPLS ..... 873, 889
- High-Level Data-Link Control  
   767  
 HINFO ..... 280  
 Hint ..... 272  
   Datei ..... 269, 274, 303  
   Group ..... 394  
 HIP Security Association ..... 867  
 HMAC ..... 95  
   based Key Derivation Function  
     56, 60, 74, 413, 426  
   Holding-Priorität ..... 712, 738  
 Home Address ..... 916, 922  
   Option ..... 940, 943  
 Home Agent ..... 916  
   Address ..... 937, 940  
   Address Discovery Request ..... 945  
   Binding ..... 937, 943  
   Discovery Reply ..... 532  
   Discovery Request ..... 532  
 Home Subscriber Server ..... 481  
 Hop ..... 119, 619, 622, 739, 840  
   Anzahl ..... 629  
   Count ..... 1010  
   Limit ..... 491, 531, 534, 540, 553,  
     599, 625, 987  
 Hop-by-Hop Options Header  
   493, 495–499, 502  
 Host  
   Candidate ..... 364  
   Centric ..... 1084  
   ID ..... 127, 128, 130–138,  
     143–145, 147, 152, 343, 519,  
     535, 616  
   Identity Protocol ..... 866  
   IPv6-Adresse ..... 507  
   Mobility ..... 849  
   Multihoming ..... 849, 850  
   Route ..... 270, 619, 620  
   Hostname ..... 267  
 Hot Standby Routing Protocol  
   679, 685  
 Hotspot ..... 557, 776, 912  
   Roaming ..... 912  
 HTTP  
   over TLS ..... 42  
   Request ..... 212, 213  
   to-CoAP  
     Proxying ..... 1021  
 HTTP-to-CoAP  
   Mapping ..... 1020, 1021  
   Proxy ..... 1021  
 Hunt-Group ..... 392  
 Hybrid Unicast ..... 333  
 Hypertext Markup Language . 7,  
   8
- Hypertext Transfer Protocol ..... 976,  
   1019  
 Hypertext Transport Protocol . 7,  
   8, 42
- I**
- IA for Non-temporary Address  
   551  
 IA for Temporary Address . 551  
 IC Internet of Things ..... 1085  
 IC Service ..... 1085  
 IC Services in Smart Cities ..... 1085  
 iCache-Server ..... 303  
 ICMP  
   Data ..... 164, 165  
   Source Quench ..... 164  
 ICMPv6  
   Header ..... 530  
   Nachricht ..... 530  
 ICN-based IoT ..... 1088  
 ICN-enabled IoT ..... 1088  
 Identification ..... 134, 290, 310,  
   648, 772, 1032  
 Identifier-Locator Network Pro-  
   tocol ..... 807, 848,  
   953  
 Identität ..... 55, 106  
   öffentlich ..... 55  
 Identity ..... 867  
   Provider ..... 98  
   Service Provider ..... 56  
 IDN Domain-Labels ..... 283  
 IEEE802-Adresse ..... 508  
 in-addr.arpa ..... 265, 268, 275, 276,  
   279  
 Inbound Streams ..... 242  
 Inclusive Multicast Ethernet Tag  
   Route ..... 907  
 Indikatoren ..... 593  
 Industrial IoT . 978, 1040, 1041  
 Information ..... 762, 764  
   Element ..... 978  
   Reply ..... 165  
   Request ..... 165  
 Information-Centric ..... 1084  
   Networking ..... 1084  
   Networking Security ..... 1085  
 Infrastructure-as-a-Service  
   1064, 1065  
 Ingress ..... 727  
   BRridge ..... 837  
   Router ..... 861  
   Tunnel Router ..... 861  
 INIT ACK ..... 245  
 Init Bit ..... 657  
 Initial Packet ..... 254  
 Initial Sequence Number . 188,  
   193

- Initialisierungsvektor 77, 78, 81, 82, 108, 111, 112, 782
- Initiator . . . . . 100, 384, 772, 856
- Inner Label . . . . . 786
- Innere Authentisierung 384, 386
- Instant Messaging . . . . . 452
- Institute of Electrical and Electronics Engineers . . . . . 760
- Integrated
  - Routing and Bridging 897, 903
  - Switching und Routing . . . 893
- Integrity . . . . . 62, 322
- Integrity Check
  - Algorithmus . . . . . 371
  - Key . . . . . 829
  - Value . . . . . 376, 377, 830
- Intelligent IoT . . . . . 1069, 1072
- Intent-based Networking . 1099, 1104
- Inter Access Point Protocol 776, 913
- Interactive Connectivity Establishment . . . . . 365
- Inter-Area-Routing . . . . . 648
- Inter-Asterisk eXchange . . . . 44
- Interconnection Network . . . 871
- Inter-Domain
  - MC-Routing . . . . . 689
  - Protocol . . . . . 624
  - Routing . . . . . 634
    - Classless . 130, 143, 144, 512
    - IPv6 . . . . . 672
- Interface . . . . . 619
  - ID488, 503, 512, 544, 849, 851
  - Identifier . . . . . 509
  - Index . . . . . 282, 509
- Interior Gateway Protocol . 624, 640
- Intermedia-Synchronisation 438
- Intermediate Node . . 999, 1002
- Intermediate System to Intermediate System . . 715, 742, 836, 839
- Internal Router . . . . . 648
- International Organization for Standardization . . . . . 24
- Internationalized Domain Name 283
- Internationalizing Domain Name
  - in Applications . . . . . 283
- Internet . . . . . 3
  - Activity Board . . . . . 5
  - Architect . . . . . 45
  - Architecture Board . . . . . 5, 45
  - Area . . . . . 45
  - Assigned Numbers Authority 32, 46, 507
  - Backbone . . . . . 10
  - Cache Protocol . . . . . 43
  - Class . . . . . 332
  - Configuration Control Board 5
  - Control Message Protocol . 34, 39, 115, 163, 489, 530, 564, 858
  - Control Plane . . . . . 860
  - Core . . . . . 10
  - Corporation for Assigned Names and Numbers . . . . . 5
  - Draft . . . . . 46
  - Engineering and Planning Group . . . . . 5
  - Engineering Steering Group . 5, 46
  - Engineering Task Force . 5, 44, 1095
  - Group Management Protocol 39, 115, 170, 171, 520, 564, 688, 696
  - Header Length . . . . . 117
  - Key Exchange . . 367, 369, 370, 373
  - Low Bitrate Codec . . . . . 440
  - Message Processor . . . . . 4
  - Network Information Center 267
  - Protocol . . . . . 3, 39
  - Research Task Force . . . . . 45
  - Service Provider . 10, 365, 572, 576
  - Standards . . . . . 45
  - Task Force . . . . . 5
- Internet Access Router . . . 1022
- Internet Control Message Protocol . . . . . 975
- Internet der Dinge . . . . . 1040
- Internet of Drones . . 1040, 1044
- Internet of Robotic Things 1040, 1042
- Internet of Things 460, 760, 957, 1040
- Internet of Vehicles . 966, 1040, 1043, 1078
- Internetprotokoll
  - Version 4 . . . . . 115
  - Version 6 . . . . . 115
- Internetwork Packet eXchange 624
- Initialization Vector . . . . . 428
- Intra-Area-Routing . . . . . 648
- Intra-Domain
  - MC-Routing . . . . . 689
  - Protokolle . . . . . 624
- Intranet . . . . . 783
- Intra-Site Automatic Tunnel Addressing Protocol . . . 517, 518, 584
- IoT
  - Application Support . . . . . 964
  - Security . . . . . 1040
  - Service Orchestration . . . 1069
  - Service Platform . . . . . 958
- IP
  - Adresse . . . . . 341, 615, 771
    - privat . . . . . 132
  - Adressklassen . . . . . 127
  - Checksum . . . . . 110
  - Compression Protocol . . . 771
  - Header
    - Checksum . . . . . 119
  - ID . . . . . 118
  - Kommunikation . . . . . 567
  - Multicasting . . . . . 169
  - Multiplexer . . . . . 37
  - Network . . . . . 659
  - Next Generation . . . . . 661
  - Optionen . . . . . 124
  - Paket . . . . . 29
  - Paketlänge . . . . . 118
  - Pseudo-Header . . . . . 183
  - Quelladresse . . . . . 119
  - Router . . . . . 611
  - Routing . . . . . 612
    - Security . . . . . 61, 176, 784
  - Subnetz . . . . . 811
  - Switching . . . . . 215
  - Telephony . . . . . 30
  - Übermittlungsdienst . . . . 180
  - Zieladresse . . . . . 119
- IP/ICMP Translation Algorithm 596
- IP4-in-IPv4-Tunneling . . . . . 861
- ip6.arpa . . . . . 268, 279, 281, 282
- ip6.int . . . . . 281
- IP-in-IP-Encapsulation 116, 690, 692, 862, 917, 924, 934
- IP-in-IP-Tunneling . . . . . 691
- IP-Name
  - reverser . . . . . 276, 286
- IPsec
  - Header . . . . . 369
  - Initiator . . . . . 370
  - Responder . . . . . 370
  - Security Association and Key Management Protocol . . . 373
- IPTV . . . . . 452
- IPv4
  - Adresse
    - mapped . . . . . 591
  - compatible IPv6-Address . 517, 572

- embedded IPv6-Address . . . 518, 604
  - Link-Local Address . . . . . 342
  - mapped IPv6-Address . . . . . 517
  - Netz . . . . . 563
  - over IPv6 . . . . . 493, 570
  - Quelladresse . . . . . 573
  - translated IPv6-Address . . . 517
  - IPv6 . . . . . 487
  - Header Compression . . . . . 988
  - in-IPv4-Tunnel . . . . . 572
  - in-IPv6-Encapsulation . . . . 938
  - in-IPv6-Tunneling . . . . . 938
  - Jumbogram . . . . . 498
  - Name
  - reverser . . . . . 281
  - Netz . . . . . 563
  - over Low power Wireless Personal Area Network . . . . . 978
  - over Low-power Wireless Personal Area Network . . . . . 963, 976
  - over Low-power Wireless Personal Area Networks 957, 958, 974
  - over Low-power WPAN . . . 969
  - Sites . . . . . 563, 567
  - unspecified Address . . . . . 511
  - IQUERY . . . . . 276
  - iResolver . . . . . 303
  - ISAKMP
  - Aggressive Mode . . . . . 374
  - ISATAP
  - Adresse . . . . . 518, 584
  - ISO/OSI-Referenzmodell . . . 24
  - Isochronität . . . . . 442
  - Issuer . . . . . 101, 102, 324
  - IT/OT-Konvergenz . . . . . 1093
  - iterative Query . . . . . 274
- J**
- Jacobsen/Karel-Implementierung . . . . . 203
  - Jahr
  - siderisch . . . . . 463
  - tropisch . . . . . 463
  - JavaScript Object Notation 1038
  - Jitter . . . . . 442, 443
  - Ausgleichspuffer . . . . . 710
  - Jumbo
  - Paket . . . . . 491
  - Payload Option . . . . . 498
- K**
- kanonischer Hostname . . . . 280
  - Kanonisierung . . . . . 96, 324
  - Karn/Partridge-Implementierung 203
  - Keep-Alives . . . . . 187
  - Keep-Alive-Verfahren . . . . 202
  - Kernbereich . . . . . 809
  - Kernel . . . . . 52
  - Key Agreement Entity . . . . . 832
  - Key Derivation Function . . . 676, 829
  - Key Encryption Key . . . . . 829
  - Key Encryption Method . . . . 64
  - Key Exchange . . . . . 389, 392, 414, 424
  - Key Exchange Method . . . . . 64
  - key file . . . . . 86, 97, 101, 103, 106, 418
  - Key Identifier . . . . . 829
  - Key Management Domain . . . 834
  - Key Number . . . . . 829
  - Key Performance Indicators 392
  - Key Phase Bit . . . . . 254
  - Key Roll-Overs . . . . . 301
  - Key Schedule . . . . . 426, 834
  - Key Server . . . . . 829
  - Key Share . . . . . 421, 422
  - Key Signing Key . . . . . 299, 300
  - Key Store . . . . . 103
  - keyed Hash . . . . . 577
  - keyed MAC . . . . . 392
  - Kiss-o'-Death . . . . . 471
  - Klasse . . . . . 278
  - Known-Plaintext-Attacken . . 431
  - Kodierungsverfahren . . . . . 108
  - Kofaktor . . . . . 96
  - Kommunikationsprotokolle . . 3, 24
  - Konfiguration
  - link-scoped . . . . . 272
  - Konfigurationsphase . . . . . 767
  - Konfigurationsserver . . . . . 529
  - Konfusion . . . . . 79
  - Kontrollchunks . . . . . 244
  - Kontrollkanal . . . . . 435
  - Konvergenzzeit . . . . . 627
  - Kreditmechanismus . . . . . 21
- L**
- L2 Forwarding Table . . . . . 812
  - L2-Switches . . . . . 891
  - L2TPv3 . . . . . 800
  - L3 Forwarding Table . . . . . 814
  - Label . . . . . 267, 427, 526
  - Distribution Protocol 715, 716, 744, 751, 888
  - Entry . . . . . 725
  - Mapping . . . . . 753
  - Raum . . . . . 718, 719
  - Request . . . . . 753
  - Stack . . . . . 725, 752
  - Switched Path . . . . . 714, 716, 720, 731, 732, 785, 790, 875
  - Switching Router . . . . . 751
  - Switching Tabelle . . . . . 718
  - Verteilung . . . . . 753
  - Zuweisung . . . . . 753
  - LAC-LAC . . . . . 802
  - LAC-LNS . . . . . 802
  - LAN-Emulation . . . . . 873
  - Längsparität . . . . . 255
  - Latenzzeit . . . . . 22
  - Lawinen-Effekts . . . . . 70
  - Layer . . . . . 809
  - Layer Management Interface 827
  - Layer-1
  - VPN . . . . . 788
  - Layer-2
  - Tunnel . . . . . 787
  - Tunneling Protocol . . . . . 784
  - VPN . . . . . 788
  - Layer-2/3-Switching . . . . . 869
  - Layer-3
  - VPN . . . . . 788
  - LDAP
  - Data Interchange Format . . . 400
  - LDP
  - based VPLS . . . . . 888
  - Peer . . . . . 751, 753
  - Session . . . . . 751
  - Learning Bridge
  - transparente . . . . . 782
  - Lease
  - Ablauf . . . . . 349
  - Dauer . . . . . 341, 344, 524
  - Erneuerung . . . . . 349
  - Least-Significant Bit . . . . . 51
  - Lebensdauer . . . . . 883
  - Legitimierung . . . . . 548
  - Legitimität . . . . . 101
  - Leitungsdurchsatz . . . . . 207
  - Leitungsschwindigkeit . . . . 207
  - Length . . . . . 124, 987
  - libresolv . . . . . 271, 283
  - Lifetime Unit . . . . . 1018
  - Light Fidelity . . . . . 1077
  - Lightweight Directory Access Protocol . . . . . 43
  - Lightweight Extensible Authentication Protocol . . 387
  - Line Feed . . . . . 324
  - Link 27, 509, 532, 533, 717, 761
  - Affinity . . . . . 741
  - Color . . . . . 741
  - Connectivity Verification . . 735
  - Control Protocol . . . . . 768, 769
  - ID . . . . . 131, 341, 480, 507, 509, 521, 534, 579, 851
  - Management Protocol 714, 733



- Metric ..... 1002
- Prefix ..... 533, 538
- Property Correlation ..... 735
- Protection ..... 713, 749
- Quality Report ..... 770
- Segment ..... 327, 332, 333
- Token 488, 507, 509, 520, 534, 558, 579
- Transmission Reliability . 1010
- Link State ..... 623
  - Advertisement . 623, 640, 641, 647, 654, 657, 659, 662
  - Database ..... 640
  - Pakete ..... 657
  - Routing ..... 622
  - Routing Protocol ..... 640
- Linkadresse ..... 341, 532, 533
- Link-based Metrics ..... 1001
- Link-Layer
  - Adresse ..... 508
- Link-Local ..... 934
  - Address ... 331, 341, 342, 551, 586
- Multicast
  - Name Resolution ... 331, 334
  - Unicast Address 488, 509, 510, 515
- Link-scoped
  - All-Node
    - Multicast ..... 548
- Linksegment ..... 134, 515
- Lippensynchronisation ... 444
- LISP
  - Alternative Logical Topology 860
  - Domain ..... 859
  - Site ..... 859
  - Listen ..... 191
  - Listener ..... 172, 520
  - Listening ..... 555
  - Listenmodus ..... 193
- LLC
  - Schicht ..... 25
- LNS-LNS ..... 802
- Load
  - Balancer ..... 212, 859
  - Dienstfunktion ..... 761
  - Diensttyp ..... 762
  - Frame ..... 762
  - Sharing ..... 681
  - Transport ..... 762
- Loadsharing ..... 62
- Local
  - Area Networks ..... 869, 891
  - Interface Gateway ... 390, 392
  - Internet Registry ..... 514
  - Learning ..... 899
  - Scope ..... 532, 690
- Locality ..... 399
- Location-Server ..... 454
- Location-to-Service Translation 1085
- Locator .... 848, 849, 851, 867
  - 32 ..... 854
  - Pointer ..... 854
- Locator/ID Separation Protocol 848
- Locator/Identifier Separation Protocol ..... 848
- Logarithmus
  - diskreter ..... 87, 90
- Logical Link Control ... 25, 761
- Long Fat Networks ..... 201
- Lookup-Tabelle ..... 80
- Loopback
  - Adresse ..... 132, 523
  - IPv6-Adresse ..... 511
  - Schnittstelle ..... 340
- Loops ..... 668
- Loose explicit Route ..... 748
- Low power and Lossy Networks 957, 963, 974, 997
- Low-Rate Wireless Body Area Networks ..... 974
- Low-Rate Wireless Personal Area Networks 957, 974, 977, 978
- LSA ..... 640, 647
  - Header ..... 657, 660
  - ID ..... 660
  - Paket ..... 623
  - Typ ..... 660
- M**
- MAC
  - Address Aging ..... 883
  - Adressen .. 156, 341, 761, 778
  - Broadcast ..... 156, 846
  - Command Frame ..... 978
  - Frame ..... 612, 717, 762
  - Frame Encapsulation ..... 761
  - Header ..... 762
  - Layer ..... 761
  - Protocol Data Unit ... 778, 779
  - Schicht ..... 25
  - Trailer ..... 762
  - Unicast ..... 156
- MAC Security ..... 830
- MAC/IP Advertisement Route 907
- Machine Learning . 1069, 1099
- Machine to Machine ..... 1041
- MACsec
  - Entity ..... 832
  - Key Agreement Protocol . 835
- magic key ..... 307
- Mail eXchange ..... 311
- Mail Transfer Agent .. 311, 321
- Makromobilität ..... 947
- Managed Address Configuration 540
- Management
  - Frame ..... 777, 778
  - Node ..... 477
  - Plane ..... 714
- Mandanten ..... 889
- Man-in-the-Middle 86, 106, 295
- MAP
  - Discovery ..... 948
  - Domain ..... 947
  - Option ..... 950
- Mapping ..... 341, 605
  - Attribute ..... 393
  - automatisch ..... 565
  - DN ..... 333
  - EID-to-RLOC ..... 860, 862
  - Ports ..... 382, 383
  - stateless ..... 565
  - Tabelle ..... 593, 595
  - Telephone Number URI ... 311
- Master ..... 775
  - Down ..... 684
  - key ..... 676, 828
  - key Tuple ..... 676
  - Router ..... 680
  - Down ..... 684
  - Secret ..... 425–427
  - Session Key 389, 829, 832, 834
  - Subsocket ..... 228
- Master/Slave Bit ..... 657
- Maximum
  - Life Time ..... 1013
  - of Inbound Streams ..... 243
  - Receive Unit ..... 767
  - Response Time ..... 172
  - Segment Lifetime ... 195, 200
  - Segment Size ... 191, 192, 207
  - Transfer Unit ... 122, 164, 168, 763
- MBone ..... 170
- MC-Routing-Protokoll ... 688
- mDNS-Dienst ..... 520
- Media ..... 432
- Media Access Control .. 25, 30, 507, 871, 974, 1041, 1096
  - Virtual Routing and Forwarding ..... 899, 905
- Media Control Channel ... 434
- Media Gateway Control Protocol ..... 43
- Media-Kanal ..... 433, 434
- Medien ..... 432
- Medienzugriffsverfahren ... 761

- Medium Access Control... 155, 976  
 Member Identification... 827  
 Membership  
   Leave Group... 172  
   Query... 172  
   Report... 172  
   V1-Report... 172  
   V2-Leave... 172  
   V2-Report... 172  
   V3-Report... 172  
 Mesh Header 980, 984, 989, 993  
 Mesh WPAN... 979  
 Message  
   Authentication Code... 71, 297, 308, 423  
   Authenticator... 396  
   Body... 460  
   Compression... 291  
   Data... 941  
   Digest... 67, 414, 423, 933  
   Digest 5... 71, 636  
   ID... 1024  
   keyed... 296  
   Sequence... 430  
   Transfer Unit... 538, 994  
   Type... 753  
 Messages... 1024  
 Metadaten... 52, 446  
 Meta-RR... 297  
 Meta-Type... 281  
 Metric  
   Container... 1011  
   Link-base... 1010  
   Node-based... 1010  
 Metrik... 625, 639, 642  
 Michael-MIC... 780  
 Microservice... 1067, 1081  
 Microservices... 1062  
 Middlebox... 366, 566, 584, 608  
   Control Protocol... 365  
 Mikromobilität... 947, 949  
 MILNET... 5  
 Mini Clouds... 958  
 Mini-CA... 414  
 Minimum Rank with Hysteresis  
   Objective Function 1002, 1004  
 MIP für IPv6... 912  
 MIPv4... 916  
 MIPv6... 911, 912, 936  
 Miredo... 590  
 Mixer... 445  
   Funktion... 444  
 Mobile  
   CC in 5G... 1065  
   Cloud Computing... 1068  
   Edge Computing... 1045, 1069  
   Home Authentication... 933  
   IoT Application... 1076  
   IP... 163, 489, 912, 915, 916  
   IPv4... 176, 916  
   IPv6... 176, 495, 532, 911, 936  
   Mode... 936  
   Node... 947  
   Prefix Advertisement 532, 940  
   Prefix Solicitation... 532, 940  
   VNFs Networking und Containerized IoT Services... 1061  
 Mobile Ad-hoc-NETwork 1052  
 Mobility... 999  
   Agents... 916  
   Anchor Point... 946  
   Binding Table... 924, 928  
   Header... 495  
   Options... 495  
   Mobility in IoT... 1040  
   Mode of Operation... 1009  
   Modulus... 87  
   Montgomery-Leiter... 90  
   More Bit... 657  
   More Fragments... 118, 600, 601  
   Bit... 123, 600  
   Most-Significant Bit... 51  
   Movement Detection... 949  
 MPLS  
   Header... 719  
   Multiplexer... 32  
   Switching Network... 716  
   TE... 736  
   Traffic Engineering... 711, 794  
 m.root-servers.net... 269  
 MSL... 195, 199  
 MSS... 213  
   Clamping... 214  
 MTU... 190, 213, 763  
   Path-Discovery... 213, 292, 431  
 Multi Tenancy Network Architecture... 891, 892  
 Multicast... 333  
   Address Resolution Server 537  
   Adresse... 503, 506  
   Backbone... 170  
   Datenverkehr... 783  
   Distribution Tree... 691  
   DNS... 330–332, 337  
   DNS based Service Discovery 333  
   Forwarding... 691, 693  
   Gruppen... 39  
   IP-Adressen... 169, 331  
   Listener Discovery... 172, 520, 564, 688  
   Listener Done... 531  
   Listener Query... 531  
   Listener Report... 531  
   Version 2... 531  
   MAC-Adresse... 171  
   OSPF... 688  
   Query... 332  
   Routing... 169, 170, 175  
   Routing-Protokoll... 175, 688  
   Source Discovery Protocol 688, 701  
   Multicasting... 999  
   Multigroup HSRP... 686  
   Multi-homed... 133, 340  
   Device... 898  
   Network... 898  
   Multihoming... 807, 850, 892  
   Multihoming-System... 503  
   Multi-hop Communication 980, 984, 992  
   Forwarding... 984  
   Multilayer-Switch... 812, 892  
   Multilinked... 340  
   Multimedia-Session... 435  
   Multipath TCP... 259  
   Multipathing 836, 838, 892, 999  
   Multiplane-Architektur... 713  
   Multiplexer  
   funktion... 761  
   IP... 31  
   LAN... 37  
   logischer... 180, 186  
   Multipoint-Sessions... 437, 459  
   Multi-Protocol... 715  
   Multiprotocol BGP... 872, 881, 888  
   Multi-Protocol Label Switching 32, 142, 709, 715, 873, 1097  
   Multisource File Transfer Protocol... 352  
   Multi-Tenant Unit... 889  
   Multi-Topology Routing... 1005  
**N**  
 Nachbar  
   Bekanntmachung... 537  
   Nachbarschaft... 643, 702  
   Nachrichten... 24, 27  
   authentizität... 108  
   integrität... 108  
   verschlüsselung... 305  
   verschränkung... 108  
   Nachsendeadresse... 916, 922  
   NaCl Library... 308  
   Nagle-Algorithmus... 201, 202  
   Name... 278  
   Name Server  
   caching... 327  
   Content... 327  
   forwarding-only... 326

- primary ..... 285
- secondary ..... 285
- Named Data Networking . 1084
- Namensauflösung
  - reverse ..... 275
- Namespace ..... 331
- Naming Authority PoinTeR 314
- NAPT
  - Symmetric ..... 356
- NAS-Client ..... 914
- NAT
  - Basic ..... 353
  - bidirektionales ..... 353
  - Port Restricted Cone ..... 357
  - PT ..... 567
  - Restricted Cone ..... 357
  - Router ..... 353
  - symmetric ..... 356
- NAT44 ..... 573, 606
- NAT64 ..... 518, 567, 571
  - Adressen ..... 518
  - State Machine ..... 603
- NAT444 ..... 366
- National Internet Registry . 515
- National Science Foundation . 6
- Near Real-Time Services .. 966
- Nebensprechen ..... 17
- Negative acknowledgment . 771
- Neighbor
  - Advertisement ..... 531, 537
  - Cache ..... 533, 535, 538
  - Discovery ..... 508, 521, 533
  - Discovery Protocol .. 489, 524, 527, 529, 533, 564, 937, 944
  - Solicitation ..... 531
  - Unreachability Detection . 535
  - Unreachable Detection ... 538
- Nested VLAN ..... 837
- NetBIOS Frame Control Proto-  
col..... 765
- net-ldap..... 398
- Network ..... 772
  - Access Control ..... 835
  - Access Server..... 378, 390
  - Address Port Translation . 353, 355
  - Address Translation . 132, 339, 595, 1060
  - Attached Station ..... 384, 392
  - Basic Input Output System . 41
  - Bootstrap Program ..... 352
  - Control Program ..... 5, 768
  - Directory Service ..... 397
  - File System..... 182
  - Functions Virtualization. 1055, 1079, 1081
  - Identity ..... 827, 834
  - Intrusion Prevention System 809
  - Layer ..... 25
  - Layer Reachability Information 666, 672, 888
  - LSA ..... 659
  - Mask ..... 656
  - Multihoming ..... 850
  - Plane ..... 1052
  - Prefix ..... 143
  - Programmability ..... 1047
  - Service Provider 378, 784–786
  - Slices ..... 1059
  - Slicing ..... 1055, 1059, 1065
  - Time Protocol ... 43, 465, 467
  - Time Security ..... 474
- Netz
  - ID ..... 127–131, 133–135, 137–139, 143, 144, 159, 160, 505–507, 513, 604
- Netzwerk
  - ID ..... 127
  - Neutralität ..... 117
  - Präfix ..... 143, 533, 546
  - Präfixnotation ..... 143
  - Schicht ..... 29, 38
- Neural Networks ..... 1099
- New Care-of-Address ..... 954
- Next Generation IP-Networks 449
- Next Header ..... 986
- Next Hop
  - Network Address ..... 672
  - Resolution Protocol ..... 141
- Nibble-Format ..... 281
- Node ..... 266
  - ID ..... 851, 853
  - Identifier ..... 848, 849, 851
  - Metrics ..... 1002
  - Node Interface ..... 734
  - Protection ..... 713, 749
- Nomadic Computing ..... 859
- Non-Broadcast Multiple Access 644
- Nonce 77, 78, 82, 308, 419, 431, 547, 549, 773
  - Header Option ..... 856, 857
  - Sum ..... 219, 222
  - Bit ..... 222
- Nonces ..... 308
- None-linear Feedback Shift Re-  
gister ..... 77
- None-Repudiation ..... 308
- Non-temporary Address ... 555
- Northbound API ..... 972
- Notification Type, ..... 335
- Null
  - Frames ..... 777, 778
  - Register ..... 698
  - Bit ..... 701
  - Nachricht ..... 701
  - Verschlüsselung ..... 425
- Number of GABs ..... 247
- Nutzlast ..... 26
  - Typ ..... 438
- NXDOMAIN ..... 275
- O**
  - Obfuskation ..... 70
  - Object-Identifier ..... 101, 399
  - Objective Code Point .... 1002, 1014
  - Objective Function .. 999, 1002, 1003, 1007, 1037
  - Zero ..... 1002, 1004
  - Objekte ..... 398
  - Obscured
    - External Address ..... 591
    - External Port ..... 591
  - Offene Resolver ..... 296
  - Öffentliche Cloud ..... 847
  - Offer ..... 460
  - Offer-Answer-Modell .... 460
  - OKay ..... 459
  - one-armed Router ..... 818
  - One-hop Communication .. 984
  - One-Time Pad ..... 77
    - Pseudo ..... 82
  - Online Certificate Status Proto-  
col ..... 107, 321
  - On-Link CoA ..... 947
  - On-Link Prefix ..... 546
  - on-the-fly ..... 307
  - Opcode ..... 290
  - Open Shortest Path First 40, 489, 564, 622, 624, 640, 715, 872, 887
    - Traffic Engineering ..... 742
  - Open System Interconnection 3, 23, 836
  - Operation ..... 163
  - Optical
    - Electrical-Optical ..... 731
    - Optical-Optical ..... 731
  - OPTion ..... 292
  - Option Number ..... 124
  - Options ..... 1033
  - Ordinary clock ..... 477
  - Organisation ..... 398
  - Organizational Unit ..... 399
  - Organizationally Unique Identifi-  
er ..... 171, 680, 764
  - Origin Indicator ..... 593

Ortszeit  
wahre ..... 463

OSI  
Referenzmodell ..... 3  
Schichtenmodell ..... 24

OSPF  
Database Description ..... 654  
Header ..... 655  
Hello Paket ..... 654  
Link State Informationen ..... 654  
Pakete ..... 640  
Traffic Engineering ..... 715

OSPFng ..... 661

OSPFv2 ..... 640

OSPFv3 ..... 640, 661

Other Stateful Configuration 540

Outband-Signalisierung ... 713

Outbound Streams ..... 242

Outer Label ..... 786

Out-of-Bailliwick ..... 273

Out-of-Fiber-Steuerkanal ... 734

Output Key Material ..... 75

Override Flag ..... 537

**P**

Packet  
Error Rate ..... 108  
Length ..... 599, 655  
Loss Rate ..... 1010  
Number ..... 831, 833  
Too Big ..... 252, 531

Padding . 79, 82, 110, 111, 423, 447, 470  
Options ..... 497

Pairwise Transient Key ... 389

Paket ..... 26, 51

Paketfehler ..... 108, 109

Paketierung ..... 26

Paketlänge ..... 109

Paketvermittlungsschicht ... 25

Parameter Problem ... 165, 166, 531

Parent ..... 1006

Parent Candidate ... 1006, 1007  
List ..... 1006, 1007

Paritätsbit ..... 109

Passphrase ..... 103

Pass-through ..... 386

Password ..... 56  
Authentication Protocol .. 765, 768, 772  
expired ..... 100

Path  
Control Size ..... 1018  
Error ..... 746  
Maximum Transmission Unit 184

Maximum Transmission Unit  
Discovery ..... 251

Metric ..... 1012

MTU ..... 494

MTU Discovery ..... 168, 531

Selection Algorithm ..... 998

Teardown ..... 746

path-abempty ..... 1030

Payload .26, 116, 374, 434, 491, 761, 766, 778, 784, 1032  
Data ..... 377  
Header ..... 443  
Length 375, 491, 498, 499, 599  
Marker ..... 1032

Protocol ..... 941  
Type ..... 438

Payload Length ..... 986

PEAP/EAP MS-ChapV2 .. 388

Peer-to-peer transparent clock 477

Peer-to-Peer-Topologie ... 979

Peer-Verbindung ..... 662

Perfect Forward Secrecy 78, 85, 88, 419, 421, 422

Pfad-Attribute ..... 666

Phishing ..... 296

photonische Switches ..... 731

Physical Layer ..... 25, 760  
Convergence Protocol ..... 774

physikalische Adressen ... 614

Piggy-backed Responses . 1027, 1028

PIM  
Dense-Mode ..... 688  
Domain ..... 701  
Sparse-Mode ..... 688

ping ..... 163

PKI Extension ..... 107

Planes ..... 815

Pluggable Authentication Modu-  
le ..... 402

PMTU Discovery ..... 169

Point of Presence ..... 10

Pointer ..... 125, 276

Point-to-Point Protocol 30, 159, 614, 765, 787

Poisoning ..... 295

Policies ..... 714

Policing ..... 740

Policy ..... 104, 714  
Table ..... 526

Poll Interval ..... 471

Poodle-Angriff ..... 82

Port ..... 730  
Access Entity ..... 827  
Address Translation . 353, 355  
basierte Access Control... 405  
Control Protocol ..... 333

Extender ..... 822  
mapped ..... 591  
Restricted Cone NAT ..... 358

Portscans ..... 211

POSIX-Attribute ..... 400

PPP ..... 30  
Frame ..... 30  
over Ethernet ..... 201  
Payload ..... 766  
Verbindung ..... 768

PPVPNs ..... 786

Präambel ..... 762

Präferenz ..... 311

Präsentations-Schicht ..... 28

Preboot Execution Environment 352

Precedence ..... 341, 526, 1017

Precision Time Protocol ... 465, 475

Preempter  
enabled ..... 740

Preemption ..... 738, 740, 743

Preference ..... 311, 853

Prefix ..... 579  
Bit ..... 519  
Cache ..... 535  
Delegation ..... 557  
Discovery ..... 545  
Length ..... 341, 639  
Extension ..... 925  
List ..... 535, 546  
Notation ..... 394

Prefixing ..... 393

PreMasterSecret . 103, 416, 425, 426

Presence Services ..... 452

Pre-shared Key ... 56, 389, 419, 427, 676, 827, 828

Pretty Good Privacy ..... 101

Primalität ..... 86

primary Name Server ..... 285

Primzahl ..... 90

Priority ..... 727  
Preemption ..... 740

Privacy ..... 774  
Enhanced Mail ..... 103  
Extensions ..... 509, 524

Private Key ... 85, 86, 101, 107, 296–299, 301, 418, 547, 548

private Key ..... 88

Probe  
Frames ..... 777  
Request ..... 776, 778  
Response ..... 776

Profile Specifications ..... 448

Profiling ..... 336, 337

Programmable Network Ser-  
vices ..... 1047

- Proposals ..... 374
- Protect Against Wrapped Sequences ..... 190
- Protected Data ..... 780
- Protected EAP ..... 387
- Protection Against Wrapped Sequence Number ..... 206
- Protocol ..... 331
  - Address Length ..... 158
  - Data Unit . . . 26, 116, 415, 752
  - Field Compression ..... 770
  - Identifier ..... 26, 763, 764
  - Independent Multicast 688, 695
  - Mapping ..... 1020
  - Translation 565, 570, 602, 603
  - Type ..... 157, 691
- Protocol 41 Encapsulation . 569
- Protocol 47 Encapsulation . 569
- Protokoll
  - familie ..... 127
  - instanz ..... 140
  - nummer ..... 117, 119
  - stack ..... 132
- Provider
  - Edge . 673, 784, 785, 874, 897
  - Provisioned VPN . . . 786, 788
- Provisionierung ..... 573
- Provisioning-Domain ..... 366
- Proxy ..... 934
  - ARP . 155, 157, 159–161, 613, 900, 902, 934
- Nameserver ..... 327
  - Views ..... 327
- Pruning ..... 692, 699
- Pseudo Random
  - Funktion ..... 426
- Pseudo Wire 755, 785, 790, 873, 875, 903
- Emulation Edge-to-Edge . 755, 789, 875
- Header ..... 786
- Pseudo-Draht ..... 785, 790
- Pseudonym ..... 55
- Pseudo-One-Time-Pad ..... 79
- Pseudo-Random
  - Function ..... 56, 420
  - Keys ..... 75
  - Number Generator ..... 829
- Pseudo-RR ..... 292
- PSH-Bit ..... 210
- Public Cloud ..... 847
- Public Key 85, 86, 88, 101, 102, 296–299, 305, 307–310, 418, 426, 547
- Infrastructure 60, 86, 101, 404, 413
- Public WLAN ..... 912
- Punkt-zu-Punkt-Verbindungen 759
- Punycode ..... 283
- PW
  - Label ..... 876
  - Table ..... 881
- LAN ..... 912
- Roaming ..... 912
- Q**
  - Q Tagging ..... 825
  - Q-in-Q ..... 795, 890
  - Q-in-Q-Encapsulation 795, 890
  - QNAME ..... 290
  - QoS ..... 490
  - QoS-Parameter ..... 432
  - Quad-A RR ..... 281
  - Qualifikationsprozedur 591, 593
  - Quality of Service . . . 40, 432, 490, 712, 736, 744, 774, 1041, 1049
  - Quantencomputer ..... 114
  - Quantenkryptographie . . . 114
  - Quell-DR ..... 696
  - Quellen-Routing ..... 622
  - Querparität ..... 110
  - Query ..... 277, 398
    - inverse ..... 276
    - iterativ ..... 274, 277
    - rekursiv ..... 274
    - Type ..... 281
  - Question
    - Section ..... 290, 332, 343
  - Queue Management ..... 215
  - Queues ..... 813
  - Quick UDP Internet Connections . . . 40, 181, 250
  - QUIC-Socket ..... 256
  - Quittung ..... 187
  - Quittungsnummer . . . 189, 194
- R**
  - RADIUS
    - Attribute ..... 393
    - Client ..... 392
    - Server ..... 392
  - Rainbow
    - Tabellen ..... 66, 70
  - Random ..... 417, 419
    - Early Detection/Discarding 216
    - Identifier ..... 524
    - Rank ..... 1002
  - Rapid STP ..... 836, 879, 901
  - RAPR
    - Reply ..... 162, 163
    - Request ..... 163
    - Server ..... 162
  - RBridge ..... 836
  - Rcode ..... 290
  - RDATA ..... 278–281
  - Read Secret ..... 428
  - Real\_Time
    - Streaming Protocol ..... 41
  - Realm ..... 353, 393, 394
    - Address ..... 353
    - Specific IP ..... 353
  - Real-Time
    - Blacklists ..... 312
    - Clock ..... 126
    - Ethernet ..... 1094
    - Onsite Operations Facilitation 958, 967
    - Services ..... 966
    - Transport Control Protocol . 41
    - Transport Protocol 41, 44, 169, 182, 261, 432, 434, 449
  - Real-time
    - Transport Protocol ..... 407
  - Re-Binding ..... 260
  - Receiver
    - Report ..... 446
  - Record ..... 27, 110, 415
  - Record Layer ..... 415
    - Frame ..... 415
    - Protocol ..... 415, 422
  - Recording Route ..... 125, 126
  - Recovery Algorithmus . . . 206
  - Recursion Desired . . . 277, 304
  - recursive Query ..... 274
  - Recursive Resolver ..... 327
  - Redirect ..... 165–167, 531
    - Function ..... 535
    - Funktion ..... 542
  - Reduced-Function Devices . 980
  - Reed-Solomon
    - Code ..... 109
    - Verfahren ..... 109
  - Reference Identifier ..... 471
  - Referrals ..... 273, 290
  - Regional
    - Care-of-Adress . . . 946, 947
    - Internet Registry ..... 514
  - Register
    - Phase ..... 696
    - Stop ..... 696, 698, 701
  - Registered Ports ..... 182
  - Registration Lifetime . 924, 929
  - Registree ..... 269
  - Regular Expressions . . . 314
  - Reinforcement Learning . 1099
  - Relative Distinguished Name 398
  - Relay Blacklists ..... 312
  - Relayed Candidate ..... 364
  - Reliability ..... 112

- Remote
  - Access Service . . . . . 390, 800
  - Access-VPN . . . . . 787
  - Authentication Dial-In User Service . . . . . 44, 390, 914
  - Interface Gateway . . . . . 390, 392
  - Learning . . . . . 899
  - Procedure Call . . . . . 182
- Rendezvous . . . . . 330
- Bit . . . . . 519
- Point . . . . . 519, 691, 696, 701, 846
- Point Tree . . . . . 696
- Rendezvous Point . . . . . 872
- Rendezvous Server . . . . . 867
- Replies . . . . . 769
- Replikat . . . . . 285
- Report Blocks . . . . . 449
- Request . . . . . 769, 1024
  - Authenticator . . . . . 396, 397
  - for Comments . . . . . 45
- Request/Reply . . . . . 929
- Request/Response-Prinzip . . . . . 451
- Requesting Router . . . . . 557
- Re-Routing 712, 738, 743, 1005
- Réseaux IP Européens 268, 514
- Reservation
  - Confirmation . . . . . 746
  - Error . . . . . 746
  - Request . . . . . 746
- Reset . . . . . 189
- Resilience . . . . . 740
- Resolver . . . . . 264, 606
- Resource Data . . . . . 278
- Resource Object . . . . . 1030
- Resource Record 267, 273, 277, 333, 853
  - Set . . . . . 287, 298, 330
  - Signatur . . . . . 299
- Resource Reservation Protocol 40, 715, 743
- Responder . . . . . 772, 856
- Response . . . . . 1024
  - Authenticator . . . . . 396
  - Nachricht . . . . . 396
  - Paket . . . . . 99
- Restricted Cone NAT . . . . . 357
- Resumable . . . . . 417
- Retransmission
  - Algorithmus . . . . . 202
  - Timer . . . . . 431, 540
- Retrieval in der DIB . . . . . 400
- Retry Packet . . . . . 254
- Retry Token . . . . . 254
- Return Routability Procedure 938, 953
- Reverse
  - Address Resolution . . . . . 155
  - Address Resolution Protocol 39, 162
    - Path Forwarding . . . . . 693
  - Ringig . . . . . 456
  - RIP-1 Entry . . . . . 632
  - RIPEMD . . . . . 71
  - RIPng . . . . . 638
  - RIPv6 . . . . . 638
  - Rivest/Shamir/Adleman . . . . . 84
  - RL-Header . . . . . 422
  - Roaming . . . . . 451, 775
    - Agreement . . . . . 914, 918
  - Robust Explicit Congestion Notification . . . . . 222
  - RObust Header Compression 439
  - Robust Security Network Association . . . . . 783
  - Robustness . . . . . 112
  - ROOF Computing . . . . . 958
  - Root . . . . . 266, 652
    - Delay . . . . . 471
    - Dispersion . . . . . 471
  - Round Trip Time 190, 192, 200, 203, 204, 207
  - Round-Robin-Verfahren . . . . . 344
  - Round-Trip-Time . . . . . 420
  - Route
    - Designator . . . . . 159, 639
    - Distinguisher . . . . . 673, 907
    - Lifetime . . . . . 1013
    - Optimazation . . . . . 938
    - Reflector . . . . . 872, 887
    - Selection . . . . . 999, 1005, 1007
    - Spezifikation . . . . . 500
    - Tag . . . . . 637
    - Type . . . . . 907
  - Routen . . . . . 611, 612
  - Routenabschnitte . . . . . 691
  - Router . . . . . 611
    - Advertisement . . . . . 165, 168, 531, 546, 554, 593, 927, 945, 948–950
    - Advertisement Daemon . . . . . 546
    - Advertisement Protocol . . . . . 524, 533, 679
    - Cache . . . . . 536
    - Designated 644, 646, 655, 656, 691, 695, 696
    - Discovery . . . . . 533
    - Flag . . . . . 537
    - ID . . . . . 650, 655
    - LSA . . . . . 652, 659
    - Priority . . . . . 656
    - Reflector . . . . . 893
    - Renumbering . . . . . 532
    - Solicitation 165, 168, 531, 540, 541
- Routing . . . . . 611, 612
  - adaptives . . . . . 622
  - Area . . . . . 45
  - Bereich . . . . . 849
  - Bridge . . . . . 836
  - Domain . . . . . 120, 624
  - Header 491, 492, 494, 500, 502
  - Information . . . . . 615, 618, 621
  - Information Base . . . . . 663
  - Information Protocol . . . . . 40, 44, 489, 565, 622, 624
  - Locator . . . . . 858, 859
  - Loops . . . . . 1000
  - Metrik . . . . . 621, 1002
  - Segmente . . . . . 500
  - Table . . . . . 617, 871
  - Table Entry . . . . . 638
  - Type 2 . . . . . 500
- Routing Protocol . . . . . 611, 618
  - for Low Power and Lossy Networks . . . . . 957, 980, 997
- RP-Baum . . . . . 696
- RPL-Modi . . . . . 1009
- RPL-Options . . . . . 1013
- RPT . . . . . 696
- RR
  - Set . . . . . 287, 299, 300
  - Type . . . . . 278
- RSA
  - Signatur . . . . . 547
  - Verfahren . . . . . 64, 85
- RST . . . . . 191
- RSVP
  - Checksum . . . . . 747
  - Nachricht . . . . . 746
  - Ojekt . . . . . 746
  - TE-Objekte . . . . . 747
  - Traffic Engineering Extensions 908
    - with Traffic Engineering . . . . . 715, 743
- RTC
  - Control Protocol . . . . . 407
- RTCP
  - extended Reports . . . . . 449
  - Kanal . . . . . 435
  - Pakete . . . . . 435
- RTP
  - Control Protocol . . . . . 44, 432
  - Header . . . . . 437
  - Kanal . . . . . 433
  - over TCP . . . . . 434
  - Pakete . . . . . 434
  - Quellport . . . . . 437
  - Session . . . . . 434
  - Zielport . . . . . 437

- S**
- SA Redundancy Mode . . . . . 898
  - SACK . . . . . 205, 247, 248
  - Salt . . . . . 420
  - S-Boxen . . . . . 77
  - S-Channels . . . . . 824
  - Scheduler . . . . . 744
  - Schema . . . . . 398
  - Schicht 2a . . . . . 25
  - Schicht 2b . . . . . 25
  - Schlüssel . . . . . 75, 777
    - abgleich . . . . . 85
    - beglaubigung . . . . . 86
    - ephemeral . . . . . 63
    - länge . . . . . 75
    - material . . . . . 112, 426
    - strom . . . . . 77
    - tausch anonym . . . . . 64, 86
    - wort . . . . . 108
    - zustandsbehaftet . . . . . 63
    - zustandslos . . . . . 63
  - S-Components . . . . . 824
  - Scope . . . . . 402, 488, 507, 519
    - Id . . . . . 509, 510
  - Scoping . . . . . 689
    - administrativ . . . . . 689, 690
    - Organisation Local . . . . . 690
    - TTL . . . . . 689
  - SCTP
    - Assoziation . . . . . 40, 181, 241
    - Streams . . . . . 240, 242
    - Verbindung . . . . . 181
  - SDN-enabled Devices . . . . . 971
  - SDP
    - Offer . . . . . 441
  - Seamless Handover . . . . . 953
  - Search . . . . . 277
  - Second-Level Domains . . . . . 268
  - Secret . . . . . 427
  - Secure
    - Hash Algorithm . . . . . 71
    - Neighbor Discovery . . . . . 532, 547
    - RTP . . . . . 41, 44
    - Socket Layer . . . . . 40, 60, 61, 481
  - Secure Channel . . . . . 831
    - Broadcast . . . . . 831, 833
    - Identifier . . . . . 830, 831
  - Secure Shell . . . . . 408
  - Secure Socket Layer . . . . . 412, 481
  - Secure Tag . . . . . 833
  - Security . . . . . 999
    - Architecture for the Internet-Protocol . . . . . 367, 371
    - Area . . . . . 45
    - Association . . . . . 61, 365, 372, 373, 381, 827, 831, 833, 834, 937
    - Gateway . . . . . 378
    - Parameters Index . . . . . 372, 376, 377
    - Policy Database . . . . . 372
  - SecurityTag . . . . . 830
  - Seed . . . . . 308
    - initial . . . . . 426
  - Segmente . . . . . 27
  - Seitenkanalangriffe . . . . . 78
  - Selbstsynchronisation . . . . . 82
  - Selector . . . . . 323
  - selektives Flooding . . . . . 623
  - Semantik . . . . . 51
  - Sendeblockade . . . . . 196
  - Sendefenster . . . . . 197
  - Sender
    - Information . . . . . 447
    - Policy Framework . . . . . 313
    - Report . . . . . 446
  - Senderecht . . . . . 774
  - Sensor . . . . . 962
  - Sensor/Aktor-Netzwerken . . . . . 760
  - Sensoren . . . . . 1045
  - Separate Responses . . . . . 1027
  - Sequence
    - Number . . . . . 188, 195, 206
    - Number initial . . . . . 188, 193
    - Sequence Number . . . . . 438
  - Sequenzierung . . . . . 70
  - Sequenznummer 187, 193, 429, 438
  - Serial Line IP . . . . . 765
  - Serial Number . . . . . 102, 103, 288
  - Server Access Layer . . . . . 809, 823
  - Server Error . . . . . 1027, 1035
  - Server LAN . . . . . 809
  - Server Layer . . . . . 823
  - SeRVer location . . . . . 454
  - Server Name Indication . . . . . 421
  - Server Reflexive Candidate . . . . . 364
  - SERVFAIL . . . . . 275
  - Service Access Point . . . . . 117, 761
  - Service Data Unit . . . . . 26, 116, 830
  - Service Function . . . . . 1057
  - Service Function Chaining . . . . . 1057, 1065
  - Service Level Agreements . . . . . 392
  - Service Namen . . . . . 333
  - Session . . . . . 27, 434
    - Accociation Key . . . . . 829
    - Description Protocol . . . . . 407, 432, 433, 436, 451, 459
    - Forwarding . . . . . 456, 457
    - ID . . . . . 389, 417, 800
    - Initiation Protocol . . . . . 44, 182, 407
    - Layer . . . . . 25
    - Resumption . . . . . 257, 389, 417, 422
    - State Table . . . . . 605
    - Table Entry . . . . . 605
  - Ticket . . . . . 422
  - Traversal Utilities . . . . . 360
  - SessionID . . . . . 419, 422
  - Setup-Priorität . . . . . 712, 738
  - SHA-1 Hash . . . . . 547
  - Shared Key . . . . . 421
  - Shared Medium . . . . . 532
    - LAN . . . . . 140, 156, 159, 759, 761
  - Shared Secret . . . . . 72, 296, 297, 371, 392, 396, 397, 577
  - Shared Tree . . . . . 691
  - Short Header . . . . . 254
  - Short Length . . . . . 831
  - Shortest Path
    - Bridging . . . . . 807, 835, 838, 839, 908
    - First . . . . . 640, 652
    - Tree . . . . . 691, 839
    - Tree Algorithmus . . . . . 840
    - VID . . . . . 841
  - Shutdown . . . . . 335
  - Sicherungsschicht . . . . . 109
  - Signaling . . . . . 888
  - Signalisierung . . . . . 714, 759
  - Signalisierungsangaben . . . . . 44
  - Signalisierungsprotokoll . . . . . 44, 436, 1050
  - Signalisierungssystem Nr. 7 . . . . . 240
  - Signatur . . . . . 102, 368
  - SIGnature . . . . . 296
  - Silent-RIP-Rechner . . . . . 634
  - Silly Window Syndrome . . . . . 202
  - Simple Authentication and Security Layer . . . . . 401
  - Simple Bind . . . . . 402
  - Simple Mail Transport Protocol . . . . . 42, 311
  - Simple Network Management Protocol . . . . . 43, 715
  - Simple Object Access Protocol . . . . . 250
  - Simple Service Discovery Protocol . . . . . 334
  - Simple Traversal of UDP through NAT . . . . . 365
  - Single Copy Broadcast . . . . . 833
  - Single Points of Failure . . . . . 679
  - Single-Active Redundancy Mode . . . . . 898
  - Single-Homed Device . . . . . 898
  - Single-Homed Network . . . . . 898
  - Singlemedia-Session . . . . . 435
  - Single-Sign-On . . . . . 100
  - SIP
    - Adresse . . . . . 452
    - INVITE . . . . . 441, 453, 455–459, 461, 462

- Nachricht ..... 433, 451
- over DCCP ..... 450
- over DTLS ..... 451
- over TLS ..... 450
- over UDP ..... 451
- Proxy ..... 451–453
- Registrar ..... 456
- Request ..... 451, 458
- Response ..... 451, 458
- Security ..... 450, 453
- Trapezoid ..... 454
- UPDATE ..... 462
- URI ..... 451
- SIPS
- over UDP ..... 451
- Site ... 516, 783, 784, 849, 850
- Border Router ..... 849
- Mobility ..... 849
- Multihoming ..... 849
- Site-Local
- Unicast Address ..... 510, 515
- Sites ..... 849
- Site-to-Site-VPN ..... 787
- Sitzung ..... 27, 751
- Sitzungsschlüssel ..... 783
- Slave
- SubSocket ..... 228
- Sliding Window ..... 195
- Sliding-Window-Prinzip ... 187, 195, 197
- Slow Start ..... 205
- Slow start and congestion avoidance algorithm ..... 218, 222
- Slow Start Threshold ..... 205
- Smart Home Monitoring System 1022
- Smart Objects ... 959, 962, 979
- Smooth Handover ..... 953
- SNA Control Protocol ..... 765
- Socket ..... 180, 256
- Cloning ..... 213
- Exhaustion ..... 366
- SOCKS ..... 41, 407, 408
- Software-Defined
- CC Networking ... 1064, 1066
- Data Centers ..... 1051
- ICN ..... 1085, 1087
- IoT ..... 1052
- Networking 957, 958, 966, 971, 1079, 1087
- VNFs Networking ..... 1055
- Solicited-Node
- Multicast-Adresse ... 520, 521
- Source ..... 26
- Source Description ..... 446
- Source EID ..... 861
- Source Filtering ..... 174
- Source Network Prefix ... 990
- Source Quench ... 124, 165, 166, 214
- Source RLOC ..... 861
- Source Routing ... 125, 159, 499, 622
- loose ..... 124, 126, 500
- strict ..... 124, 125
- Source Tree ..... 691
- Source-SAP ..... 763
- Source-specific
- Multicasting ..... 170
- Multicasting Address ... 519
- Spanning Tree Protocol ... 836, 879, 884, 901
- Sparse Mode ..... 695, 696
- SPB MAC ..... 841
- Spectre ..... 52
- SPF-Baum ..... 640
- Spin Bit ..... 254
- Split Horizon ... 326, 327, 623, 879, 884
- Methode ..... 627, 630
- mit Poison-Reverse ... 627, 631
- Spoofing ..... 337, 546, 549
- SPT ..... 691
- SSLeay ..... 6, 60, 414
- Stammzertifikat ..... 101, 103
- Standard
- Route ..... 620
- Subnetzmaske ..... 139
- Standards Track ..... 429
- Standardzertifikate ..... 103
- Standby
- Cold ..... 62
- Group ..... 681, 685
- Hot ..... 62
- Router ..... 685
- Standortadresspräfix ..... 513
- Starting Delimiter ..... 762
- Start-of-Authority ..... 285
- STARTTLS ..... 428
- State ..... 781
- State Engine ..... 525, 538
- State Table ..... 366
- Stateful
- Addressmapping ..... 602
- Autoconfiguration ... 529, 540, 550
- Inspection ..... 211
- Mapping ..... 565
- Translation ..... 603
- Stateless
- Address Autoconfiguration 524, 529, 531, 533, 543, 545
- Adressen ..... 524
- Autoconfiguration ... 529, 540, 549
- DHCPv6 ..... 550, 558
- IP/ICMP Translation ..... 517
- IP/ICMP Translation Algorithm ..... 571, 595
- Mapping ..... 565
- Translation ..... 603
- statisches Routing ..... 622
- Status Code ..... 777
- Stealth
- Mode ..... 290, 561
- Server ..... 327
- Sternenjahr ..... 463
- STLS ..... 428
- Storage Area Network ..... 809
- Stratum ..... 468, 471
- Stream
- Control Transmission Protocol 40, 179, 181, 431
- Format ..... 309
- Identifier ..... 243, 245
- Nachricht ..... 309, 310
- Sequence Nr. .... 245
- Sequence Number ..... 246
- Strict explicit Route ..... 748
- Strict Source Route ..... 500
- Strictly-Ordered service class 779
- Stromchiffren ..... 77, 429
- RC4 ..... 59
- Stub
- Area ..... 651
- Bereich ..... 651
- Resolver ..... 271
- Stun
- classic ..... 360
- Sub-AFI ..... 671
- Sub-DODAG ..... 1009
- Subdomains ..... 266
- Subject ..... 101, 102
- Subject Alternate Name ... 97
- Subject Alternative Name ... 106
- Subject-DN ..... 102
- Subnet
- ID ..... 516
- Prefix ..... 547
- Route ..... 618
- Router ..... 522
- Subnetting ..... 144
- Sub-Network Access Protocol 764



- Subnetwork Point of Attachment  
615, 672
- Subnetz ..... 133, 134  
ID ..... 134, 144, 513, 516, 579
- Subnetz-Maske ..... 341
- Subsequent AFI ..... 671, 672
- Substitutionsboxen ..... 79, 80
- Subtype ..... 778
- Success ..... 1026, 1035
- Suffix  
Notation ..... 394
- Summary-LSA ..... 659, 660
- Supervisory ..... 762
- Supplementary Services ..... 452
- Supplicant ..... 98, 99, 384, 385
- Supported Channels ..... 777
- Supported Rates ..... 776
- Switched Medium ..... 761
- Switching Fabric ..... 871
- SYN ..... 191–193  
Cookie ..... 212  
Flooding ..... 212
- Synchronisation ..... 25
- Synchronization Source ..... 445–447  
Identifier ..... 438
- Synchronous Digital Hierarchy  
710, 711, 731
- Syntax ..... 51
- System  
autonomes 611, 624, 626, 640,  
647, 651–653, 661, 663, 664,  
689, 696, 702–704, 749, 859
- Systeme  
verteilte ..... 462
- T**
- T/TCP ..... 190
- TAG Control Information . 830
- TB-Modell ..... 744
- TCP ..... 35  
Abort ..... 210  
Authentication Option ..... 676  
Backlog ..... 211  
Close ..... 210  
Control Block ..... 211  
Fast Open ..... 208  
Haltezeit ..... 202  
Handoff ..... 213  
Header ..... 187  
Instanz ..... 35  
KEEPALIVE ..... 211  
Keep-Alive ..... 202  
LINGER ..... 210  
Multiplexer ..... 35  
NODELAY ..... 210  
Nutzlast ..... 187  
Open ..... 210
- Pakete ..... 187
- PDU ..... 187
- Peer ..... 219
- Puffer ..... 202
- Receive ..... 210
- RST ..... 210
- Send ..... 210
- Slow Start ..... 205
- Spoofing ..... 211
- Stack ..... 201
- State ..... 210
- Timeouts ..... 190
- Verbindung ..... 36, 181, 186
- Window ..... 191
- Wrapper ..... 211
- Teardown ..... 747
- Telephony Routing over IP . 44
- Temporal Key Integrity Protocol  
780
- Temporary Address ..... 555
- Temps Atomic International 466
- Tenants ..... 889
- Teredo ..... 518, 567  
Adresse ..... 518, 590  
Client ..... 589, 590  
Flags ..... 591  
navalis ..... 589  
Präfix ..... 591  
Relay ..... 589, 590  
Server ..... 518, 589, 590  
Server-Adresse ..... 591
- Terminate ..... 772
- Three-Way Handshake 191, 207
- Throughput ..... 22
- Tickmark ..... 190, 204, 465
- Time Division Multiplexing 786  
over IP ..... 792
- Time Exceeded . 165, 166, 531
- Timeout . . . 158, 191, 200, 202,  
203, 209, 354, 393
- Timeout-Mechanismus 195, 429,  
1025
- Time-Sensitive Application  
1071
- Time-Sensitive IoT / 5G Appli-  
cations ..... 1069
- Time-Sensitive Networking  
1093
- Time-Sensitive SDN ..... 1098
- Time-Slots ..... 733
- Time-Slotted Channel Hopping  
978, 1041, 1096
- Timestamp . 124, 126, 164, 206,  
308, 438, 442, 547, 549, 776
- Echo Reply ..... 190
- Option ..... 190
- Originate ..... 471
- Receive ..... 471
- Reference ..... 471
- Reply ..... 165, 167
- Request ..... 165, 167
- Transmit ..... 471
- Value ..... 190
- Time-to-Live 34, 119, 166, 171,  
188, 214, 278, 491, 553, 727
- Time-Wait ..... 195
- TLS-Schlüssel ..... 426
- TLV-Angaben ..... 493
- Token ..... 56  
Bucket-Modell ..... 744  
Length ..... 1032  
Rate ..... 744  
Ring ..... 761
- Top Level  
Aggregator ..... 513
- Domains  
generic ..... 267, 268
- traceroute ..... 164
- Traffic  
Class ..... 490, 598, 986  
Engineering . . . 707, 710, 711,  
715, 728, 736  
Flow ..... 736, 737  
Key ..... 420, 676  
Parameter ..... 740  
Secret ..... 252, 254  
Selector ..... 370, 374  
Shaping ..... 207  
Trunk ..... 736
- Trailer ..... 26, 108
- Transaction  
Security ..... 296  
SIGNature ..... 296  
TCP ..... 39
- Transaktions-Identifizier . . . 99
- Transcript-Hash ..... 420, 427
- Transient-Bit ..... 518
- Transitnetz ..... 568, 571
- Translation ..... 567, 570  
Bridging ..... 781, 782
- Translator ..... 603  
Funktion ..... 444
- Transmission Control Protocol 3,  
8, 28, 39, 179, 181, 431, 975
- Transmission Sequence Number  
244
- Transparent Interconnection of  
Lots of Links . . . . 807, 835
- Transport  
Area ..... 45  
Mode ..... 369, 378  
Plane ..... 713  
Service ..... 385  
Verschlüsselung ..... 61
- Transport Layer ..... 25

- Security . . . 28, 40, 61, 77, 110, 407, 412, 450, 453
  - Support Protokolle . . . . . 40
  - Transportdienst . . . . . 26
  - Transportprotokollinstanz . . 180
  - Transportschicht . . . . . 3, 29, 38
  - Trap . . . . . 834
  - Trapdoor-Funktionen . . . . . 63
  - Traversal Using Relays around NAT . . . . . 365
  - Trickle Algorithm . . 1006, 1018, 1019
  - Trivial File Transfer Protocol 182, 352
  - Truncation . . . . . 289, 292
  - Trunk . . . . . 833
  - Trust
    - Anchor . . . . . 303, 305, 547–549
    - Center . . . . . 105, 413
    - Chain . . . . . 303, 305, 548, 549
    - Store . . . . . 103, 106, 107
  - Trustee . . . . . 269
  - TSecr . . . . . 204
  - TSopt . . . . . 204
  - TSVal . . . . . 204
  - TTL . . . . . 278
  - Tunnel
    - Broker . . . . . 567, 575
    - Header . . . . . 876
    - ID . . . . . 800
    - Information and Control Protocol . . . . . 577
    - Mode . . . . . 369, 378
    - Switching-Funktion . . . . . 382
    - Tunneling . . . . . 566, 724, 935
    - automatisches . . 572, 575, 580
    - Tunneling über IP-Netze . . 783
    - Tunneling-Protokoll . . . . . 784
    - Type . . . . . 164, 278, 504, 1032
    - Type of Service . 118, 119, 218, 652
  - Type-Length-Value . . . 395, 493
- U**
- Überlastkontrolle . . . . . 17, 22
  - Übertragungssicherung . . . 761
  - UDP
    - Encapsulation . . . . . 569
    - Keepalive . . . . . 383
    - Lite . . . . . 179
    - Pakete . . . . . 182
  - UI
    - Frame . . . . . 762
  - Umcodierung . . . . . 444
  - Umweltintelligenz . . . . . 1074
  - Unicast . . . . . 132, 335, 539
    - Adresse . . . . . 503
    - IP-Adresse . . . . . 127
    - Query . . . . . 332
  - Unified Messaging . . . . . 450
  - Uniform
    - Resource Identifier . . 313, 451, 452, 1029, 1084
    - Resource Locator . . . 7, 8, 454, 1084
    - Resource Name . . . 1085, 1086
  - Unique Local
    - Unicast Address 488, 510, 511, 515, 516, 533
  - Unique Service Name . . . . . 335
  - Universal Plug-and-Play . . 331, 334, 335
  - Universal Time Coordinated 464
  - Universalzeit . . . . . 464
  - Unmanned Aerial Vehicle 1044
  - Unnumbered Information . . 762, 764, 765
  - Unspecified Addresses . . . 548
  - UPnP
    - Device . . . . . 335
  - Upstream . . . . . 216
    - Knoten . . . . . 750
    - Label . . . . . 751
    - Router . . . . . 747
    - System . . . . . 753
  - URG-Bit . . . . . 210
  - Urgent
    - Daten . . . . . 189
    - Pointer . . . . . 189
  - Usage . . . . . 103
    - Attribute . . . . . 106
  - User
    - Agent . . . . . 455
    - Agent Server . . . . . 455
    - Experience . . . . . 250
    - ID . . . . . 399
    - Interface . . . . . 527
    - Network Interface . . . . . 734
    - PEs . . . . . 889
    - User Datagram Protocol 28, 39, 179, 180
- V**
- Validierung . . . . . 106
  - Variable Length Encoding . 258
  - Variable Length Subnet Mask 143, 147, 636
  - Vector Clock . . . . . 465
  - Vehicle Ad-hoc-NETwork 1053
  - Vehicle-to-Everything . . . 1076, 1079
  - Vehicle-to-Infrastructure . 1043, 1079
  - Vehicle-to-Network 1043, 1079
  - Vehicle-to-Pedestrian . . . . 1043, 1079
  - Vehicle-to-Vehicle . 1043, 1079
  - Vendor
    - Option . . . . . 345
    - specific Attribute . . . . . 396
  - Verbindung . . . . . 27
    - λ-Verbindung . . . . . 731
  - Verification . . . . . 101
  - Verification Tag . . . . . 243
  - Verkehrsstrom-ID . . . . . 718
  - Verschlüsselung . . . . . 62
    - Algorithmus . . . . . 75
    - asymmetrisch . . . . . 84
    - symmetrisch . . . . . 75
  - Version . . . . . 986, 1032
  - Version Negotiation . . . . . 252
  - Verteilbaum . . . . . 691
  - Vertrauenssystem . . . . . 86
  - Vertraulichkeit . . 112, 494, 827
  - Verzeichnisbaum . . . . . 400
  - Verzeichnisdienst . . . . . 397
  - Views . . . . . 327
  - Virtual
    - Bridge Layer . . . . . 823
    - Circuit Identifier . . . . . 719
    - Classroom . . . . . 437
    - extensible LAN . 807, 826, 908
    - extensible Local Area Network 844
      - IP-Address . . . . . 680
      - LAN . 810, 811, 873, 874, 890
      - Link . . . . . 817
      - MAC Address . . . . . 680, 681
      - Machine . 822, 844, 911, 1045, 1055, 1060
      - Mobility . . . . . 807, 844
      - Network Mobility . . . . . 807
      - Networking . . . 807, 812, 1055
      - Overlay Network . . . . . 846
      - Path Identifier . . . . . 719
      - Private LAN Service . 869, 892
      - Private Network 727, 755, 783
      - Private Wire Service . 789, 790
      - Router . . . . . 679
      - Router Identifier . . . . . 683
      - Router Redundancy Protocol 679, 682, 903
      - Routing and Forwarding . . 872
      - Switching
        - Instance . . . . . 874, 897
      - Interface . . . . . 874
    - Virtual Data Center . . 891, 1051
    - Virtual Distributed Ethernet Switch . . . . . 873, 878, 892
    - Virtual Distributed IP-Router 902

- Virtual Distributed L2-Switch  
892, 900, 904
- Virtual Distributed Switch . 845, 897
- Virtual Ethernet WAN . . . . . 869
- Virtualized Network Function  
1055, 1057, 1060, 1080
- virtuelle Router . . . . . 680
- virtuelle Standleitung . . . . . 800
- VLA  
Identification . . . . . 818
- VLAN  
aware bundling Service Interface . . . . . 904  
based Service Interface . . . . . 904  
bundle Service Interface . . . . . 904  
Identification . . . . . 904  
Identifier . . . . . 811, 812, 824  
in-VLAN . . . . . 844, 890  
over VLAN . . . . . 838  
Stacking . . . . . 795, 844, 890  
Tagging . . . . . 812, 817, 818, 825, 905  
Trunking . . . . . 812, 818  
Tunneling . . . . . 844
- VLSM-Networking . . . . . 143
- VNFs  
Management and Orchestration  
1055  
Orchestration . . . . . 1058
- VoIP-Gateways . . . . . 43
- VPI/VCI . . . . . 726
- VPLS  
Edges . . . . . 881  
Signaling . . . . . 887
- VR . . . . . 680
- VRID . . . . . 680
- VRP . . . . . 679
- VR-Protokoll . . . . . 679
- vUplinks . . . . . 847
- VXLAN  
Instanzen . . . . . 845  
Network Identifier . . . . . 845  
Tunnel End Points . . . . . 847
- W**
- Wavelength Division Multiplexing . . . . . 614, 710
- WDM . . . . . 733  
Link . . . . . 733
- Web of Trust . . . . . 101
- Web Switching . . . . . 1023
- Webtechnologien . . . . . 46
- Well-known  
discretionary . . . . . 668  
List . . . . . 332  
mandatory . . . . . 668
- Port . . . . . 35, 181, 184, 193, 346, 355, 434, 550, 590
- Prefix . . . . . 603
- WEP40 . . . . . 780
- WEPI28 . . . . . 780
- Whois-Lookup-Mechanismus  
329
- Wide Area Networks . . . . . 869
- WiFi . . . . . 774  
Alliance . . . . . 774  
Protected Access . . . . . 774
- Window . . . . . 191, 195–197
- Window Scale . . . . . 208
- Windowsize 191, 192, 202, 207, 208  
advertised . . . . . 192
- WinSock2 . . . . . 414
- Wire Equivalent Privacy . . . . . 774
- Wire Fidelity . . . . . 774
- Wireless  
Distribution System . 776, 779, 781  
Equivalent Privacy . . . . . 779  
ISPs . . . . . 913  
LANs . . . . . 912  
Local Area Networks . . . . . 959  
Protected Access . . . . . 780  
SD Networking . . . . . 1052  
Sensor Actuator Networks 957, 962, 974, 997
- Wirespeed . . . . . 207
- WISPs . . . . . 913
- WLAN  
Roaming . . . . . 782, 912  
Supplicant . . . . . 384
- Working Groups . . . . . 45
- WPA2 . . . . . 780
- WPAN Coordinator . . . . . 979, 980
- Write Secret . . . . . 428
- WSopt . . . . . 191
- X**
- X.509  
Issuer . . . . . 324, 325  
Subject . . . . . 325  
Zertifikat . . . . . 86, 101, 324
- Xerox Network Services . . . . . 624
- Y**
- Yellow Pages . . . . . 401
- Z**
- Zeitmarkenanfrage . . . . . 167
- Zeitmultiplex . . . . . 1096
- Zeitstempel . . . . . 438
- Zeitsynchronisation . . . . . 462
- Zelle . . . . . 775
- Zero Window Probe . . . . . 202
- Zeroconf . . . . . 331, 335, 342, 403
- Zertifikat  
Extended Key Usage . . . . . 104  
Liste . . . . . 388  
X.509 . . . . . 58
- Zertifikatsprüfung . . . . . 388
- Zone . . . . . 284  
file . . . . . 285  
Signing Key . . . . . 299, 301  
Transfer . . . . . 285, 333  
Authoritive . . . . . 285  
Incremental . . . . . 285  
Walking . . . . . 300, 307
- Zonendatei . . . . . 279, 285
- Zustandsinformationen . . . . . 27