

# HANSER



## Leseprobe

zu

### „Rechnernetze“

von Wolfgang Riggert und Ralf Lübben

Print-ISBN: 978-3-446-46309-7

E-Book-ISBN: 978-3-446-46369-1

Epub-ISBN: 978-3-446-46673-9

Weitere Informationen und Bestellungen unter  
<http://www.hanser-fachbuch.de/978-3-446-46309-7>  
sowie im Buchhandel

© Carl Hanser Verlag, München

# Vorwort zur 6. Auflage

Trends wie die zunehmende Globalisierung, der digitale Wandel oder die Nachhaltigkeit in allen Bereichen der Wirtschaftstätigkeit betreffen auch immer die Netzwerke als Basisinfrastruktur. So zeigt die Globalisierung, dass die Verbindungen zwischen Systemen, Menschen, Geschäftsprozessen und Orten nicht nur verteilter, sondern auch zunehmend komplexer werden und dadurch die Bedeutung der Netzwerke steigen, sowie ihre Architektur und Sicherheit herausfordern. Die Digitalisierung setzt Netzwerke voraus, die flexibel auf neue Herausforderungen reagieren und sich innovativen Dienstleistungen und Prozessen anpassen. Begleitet wird die steigende Automatisierung durch zeitsensitive und ausführungskritische Aspekte, die eine zuverlässige und zeitgerechte Zustellung der übertragenen Daten sicherstellen müssen. Aus diesen Erkenntnissen resultiert die Einschätzung, dass bis 2023 mehr als 60 % der Unternehmen Netzwerke als den Kern ihrer digitalen Strategie einschätzen [PiSK19]. Die technologischen Trends, die diese Entwicklung unterstützen, konzentrieren sich auf fünf Bereiche:

- **IoT (Internet of Things):** Anwendungen nutzen zunehmend die Daten von Sensoren, die als Microservices nahe an den erfassenden Devices entstehen. Damit ergeben sich nicht nur Anforderungen an die Sicherheit, sondern auch Fragen des Datentransports.
- **Künstliche Intelligenz:** Um das Potenzial zu erschließen, bedarf es Rechenleistung zur Entscheidungsunterstützung vor Ort. Dies bringt neue Gesichtspunkte der Verteilung automatisierter Systeme mit sich.
- **Mobilität:** Nutzer sind es heutzutage gewohnt, alle benötigten Dienste und Applikationen auf jedem Gerät unabhängig vom Ort zu nutzen. Hierzu sind Wireless-Verbindungen notwendig, die Skalierbarkeit, Sicherheit und ausreichende Kapazität zur Verfügung stellen.
- **Sicherheit:** Durch die zunehmende Digitalisierung der Wirtschaft erhöhen sich die Angriffsflächen für Hacker. Das Netzwerk muss daher Bedrohungen frühzeitig erkennen und darauf angemessen reagieren.

- **Datenverkehr:** Durch die weiter wachsende Nutzung von Videodaten und das Auftauchen von Virtual und Augmented Reality steigt der Austausch von Daten, die besondere Anforderungen an die Qualität der Übertragung stellen.

Vor diesem Hintergrund greift die neue Auflage Gesichtspunkte wie Sicherheit, QoS (Quality of Service) und aktuelle Wireless-Technologien auf. Damit sollen aktuelle Entwicklungen antizipiert und dem Lehrenden/Lernenden ein zukunftsorientiertes Lehrbuch angeboten werden. Wir – das Autorenteam – hoffen, dass uns dieser Anspruch gelingt.

Ergänzendes Material zum Buch steht unter dem Link [plus.hanser-fachbuch.de](http://plus.hanser-fachbuch.de) zur Verfügung. Online ist auf HanserPlus umfangreiches Zusatzmaterial erhältlich: Quizzes, Linksammlungen und die Lösungen zu den Aufgaben.

# Inhalt

<b>Vorwort zur 6. Auflage .....</b>	<b>v</b>
<b>1 Netzwerkgrundlagen und -architektur .....</b>	<b>1</b>
1.1 Basiselemente eines Netzwerkes .....	3
1.2 Netzwerkategorien .....	5
1.3 Netzwerkarchitekturen .....	8
1.4 Netzzugang und Pakettransport .....	13
1.5 ISO/OSI-Referenzmodell .....	19
1.6 Zusammenfassung .....	28
1.7 Wissensüberprüfung .....	29
<b>2 Übertragungsmethoden und -medien .....</b>	<b>31</b>
2.1 Übertragungsverfahren – Signalisierung .....	32
2.2 Strukturierte Verkabelung .....	37
2.3 Glasfaserverkabelung .....	41
2.3.1 Historie .....	42
2.3.2 Kabelaufbau .....	42
2.3.3 Arbeitsweise .....	43
2.3.4 Eingesetzte Technik .....	44
2.3.5 Qualitätsparameter .....	46
2.3.6 Glasfaserprofile .....	49
2.3.7 Glasfaserkabelarten .....	51
2.3.8 Steckverbindungen .....	52
2.3.9 Bewertung .....	53
2.4 Twisted-Pair-Verkabelung .....	55
2.4.1 Qualitätsparameter .....	56
2.4.2 EIA/TIA-568-Standard .....	58
2.4.3 ISO/IEC-Standard 11801 und EN 50173 .....	60
2.4.4 Bewertung .....	64

2.5	Zusammenfassung .....	65
2.6	Wissensüberprüfung .....	66
<b>3</b>	<b>Ethernet-Technologie .....</b>	<b>67</b>
3.1	Historie .....	68
3.2	Paketaufbau .....	71
3.3	Zugriffsverfahren: CSMA/CD .....	76
3.4	Signalverlauf .....	82
3.5	Standards .....	84
3.6	Fehlerquellen .....	90
3.7	Verfahrensbewertung .....	91
3.8	Zusammenfassung .....	93
3.9	Wissensüberprüfung .....	94
<b>4</b>	<b>Ethernet-Standards .....</b>	<b>95</b>
4.1	Die nahe Vergangenheit: Fast-Ethernet .....	95
4.1.1	Vorteile .....	96
4.1.2	Bestandteile .....	97
4.1.3	Varianten .....	98
4.1.4	Auto-Negotiation-Technologie .....	101
4.1.5	Topologie .....	102
4.1.6	Migration von Standard- zu Fast-Ethernet .....	103
4.2	Die Gegenwart: Gigabit-Ethernet .....	104
4.2.1	Physikalische Grundlagen .....	105
4.2.2	Varianten .....	106
4.2.3	Besonderheiten .....	109
4.3	Gegenwart und Zukunft: 10-GbE und höher .....	111
4.3.1	Eigenschaften .....	111
4.3.2	Vorteile .....	115
4.4	Technologische Trends .....	116
4.5	Zusammenfassung .....	120
4.6	Wissensüberprüfung .....	121
<b>5</b>	<b>IP-Protokollfamilie .....</b>	<b>123</b>
5.1	IP – Internet Protocol .....	124
5.1.1	Fragmentierung .....	130
5.1.2	Routing-Optionen .....	131
5.1.3	Routing .....	132

5.2	ARP – Address Resolution Protocol . . . . .	134
5.3	ICMP – Internet Control Message Protocol . . . . .	137
5.4	Dynamic Host Configuration Protocol & Domain Name System . . . . .	141
5.4.1	Dynamic Host Configuration Protocol . . . . .	141
5.4.2	Domain Name System . . . . .	145
5.5	Zusammenfassung . . . . .	149
5.6	Wissensüberprüfung . . . . .	150
<b>6</b>	<b>IP-Adressierung . . . . .</b>	<b>151</b>
6.1	IP-Adressstruktur . . . . .	152
6.1.1	Class A-Adressen . . . . .	154
6.1.2	Class B-Adressen . . . . .	154
6.1.3	Class C-Adressen . . . . .	155
6.1.4	IP-Adressinterpretation . . . . .	155
6.1.5	IP-Adressen mit besonderer Bedeutung . . . . .	156
6.2	Subnetzbildung . . . . .	158
6.3	VLSM – Variabel lange Subnetzmasken . . . . .	162
6.3.1	Grenzen der Subnetzbildung . . . . .	163
6.3.2	VLSM – Voraussetzungen . . . . .	164
6.4	Private Adressvergabe oder Network Address Translation . . . . .	166
6.5	CIDR – Classless-Inter-Domain-Routing . . . . .	168
6.6	Verwaltungsfunktionen auf IP-Basis . . . . .	170
6.7	Zusammenfassung . . . . .	171
6.8	Übungen . . . . .	173
6.9	Wissensüberprüfung . . . . .	174
<b>7</b>	<b>IPv6 . . . . .</b>	<b>175</b>
7.1	Historie . . . . .	176
7.2	Entwurfsziele . . . . .	177
7.3	Technische Betrachtung . . . . .	179
7.4	Die wichtigsten Merkmale . . . . .	179
7.4.1	Header . . . . .	179
7.4.2	Headererweiterungen . . . . .	182
7.4.3	Adressformat . . . . .	186
7.4.4	Adressmanagement . . . . .	189
7.4.5	Begleitprotokolle . . . . .	191
7.5	Migrationswege . . . . .	193

7.5.1	Tunneling .....	193
7.5.2	Dual-IP-Stack .....	194
7.6	Mobile IPv6 .....	195
7.6.1	Kommunikationsablauf .....	195
7.6.2	Technischer Hintergrund .....	196
7.7	Überlegungen zur Sicherheit .....	199
7.8	Zusammenfassung .....	204
7.9	Übungen .....	205
7.10	Wissensüberprüfung .....	206
<b>8</b>	<b>TCP/UDP-Protokoll .....</b>	<b>207</b>
8.1	TCP im Detail .....	208
8.1.1	Besonderheiten .....	209
8.1.2	Merkmale .....	209
8.1.3	Verbindungsmanagement .....	213
8.1.4	Fehlervermeidungsmechanismen .....	215
8.2	UDP – User Datagram Protocol .....	220
8.3	Überlegungen zur Sicherheit .....	221
8.4	QoS – Quality-of-Service .....	224
8.4.1	Klassifikation .....	227
8.4.2	Congestion Avoidance .....	228
8.4.3	Congestion Management .....	230
8.5	Netzneutralität .....	233
8.6	Zusammenfassung .....	235
8.7	Wissensüberprüfung .....	236
<b>9</b>	<b>Layer 2 – Geräte, Protokolle und Konzepte .....</b>	<b>237</b>
9.1	Switches .....	238
9.1.1	Eigenschaften .....	238
9.1.2	Arbeitsweise .....	240
9.1.3	Switching-Verfahren .....	242
9.1.4	Erweiterungsmöglichkeiten .....	245
9.1.5	Kapazitätssteigerung .....	246
9.1.6	Switch-Architekturen .....	247
9.2	Spanning-Tree .....	249
9.3	Virtuelle LANs .....	255
9.3.1	VLAN-Typen .....	256
9.3.2	Trunk .....	257

9.3.3	VLAN-Management . . . . .	258
9.3.4	Link-Aggregation, Spanning-Tree und VLAN . . . . .	259
9.4	Überlegungen zur Sicherheit . . . . .	260
9.4.1	Angriffsziel: STP-Bridge . . . . .	260
9.4.2	Angriffsziel: STP-Parameter . . . . .	261
9.4.3	Angriffsziel: MAC-Tabelle . . . . .	263
9.5	Zusammenfassung . . . . .	265
9.6	Übungen . . . . .	266
9.7	Wissensüberprüfung . . . . .	266
<b>10</b>	<b>Layer 3 – Geräte, Protokolle und Konzepte . . . . .</b>	<b>267</b>
10.1	Router . . . . .	267
10.1.1	Bedeutung . . . . .	268
10.1.2	Routing-Ablauf . . . . .	270
10.1.3	Routing-Methoden . . . . .	273
10.1.4	Unterschiede zwischen Routern und Switches . . . . .	275
10.2	Routing . . . . .	277
10.2.1	Bedeutung . . . . .	278
10.2.2	Routing-Protokolle – allgemeine Klassifizierung . . . . .	278
10.3	Routing-Protokolle . . . . .	283
10.3.1	RIP – Routing Information Protocol . . . . .	283
10.3.2	OSPF – Open Shortest Path First . . . . .	286
10.4	Routing-Probleme . . . . .	288
10.5	Einsatzaspekte von Switches und Routern . . . . .	290
10.6	Überlegungen zur Sicherheit . . . . .	292
10.7	Zusammenfassung . . . . .	293
10.8	Wissensüberprüfung . . . . .	294
<b>11</b>	<b>Verwaltung von Netzwerken . . . . .</b>	<b>295</b>
11.1	Netzwerkmanagement . . . . .	296
11.1.1	Netzwerkstatistiken . . . . .	298
11.1.2	FCAPS-Modell . . . . .	300
11.1.3	SNMP . . . . .	301
11.1.4	syslog . . . . .	307
11.2	Überlegungen zur Sicherheit . . . . .	308
11.2.1	Allgemeine Bedrohungen . . . . .	308
11.2.2	Fehleranalyse . . . . .	311
11.2.3	Übungen . . . . .	316

11.3 Zusammenfassung .....	317
11.4 Wissensüberprüfung .....	318
<b>12 Wireless Local Area Networks .....</b>	<b>319</b>
12.1 IEEE 802.11-Standards .....	321
12.2 Wireless-Architekturen .....	327
12.3 Modulationsverfahren und Kanäle .....	329
12.4 Zugriffsmethoden: CSMA/CA .....	332
12.5 Rahmentypen .....	336
12.6 Anmeldeverfahren .....	340
12.7 Sicherheit .....	341
12.8 Zusammenfassung .....	347
12.9 Wissensüberprüfung .....	347
<b>13 Literatur .....</b>	<b>349</b>
<b>Index .....</b>	<b>355</b>

- die Erfolgsabhängigkeit von der Komplexität des Soft- und Hardwareangebots – insbesondere Anwendungssysteme wie ERP-Software erfordern spezialisiertes Know-how durch die Komplexität der Optionen,
- die Einhaltung der vereinbarten Service-Level-Agreements mit den Kunden.

Die Idee der Verlagerung von Anwendungen und Infrastrukturkomponenten überzeugt nicht nur durch die technische Machbarkeit, sondern auch durch ihre handfesten Vorteile. Diese Vorteile beurteilen kleinere und mittlere Unternehmen mit wenig IT-Know-how naturgemäß anders als große Unternehmen. Letztlich ergibt sich aber eine weitere Option zur Gestaltung der IT-Landschaft.

## ■ 1.4 Netzzugang und Pakettransport

Eine Kernfrage ist die Regelung des Zugangs der einzelnen Stationen zum Übertragungsmedium. Für die Ankopplung eines Rechners sind zwei Verfahren denkbar:

- **Aktive Ankopplung:** Der Netzeilnehmer nimmt das gesamte Paket vom Medium, prüft es daraufhin, ob es an ihn gerichtet ist, und generiert es für die Nachfolgestationen vollständig neu. Der Netzknopen fungiert als Paketregenerator, ein Konzept, das bei Einsatz von Glasfaserkabeln geboten ist, da optische Signale nicht aufspaltbar sind.
- **Passive Ankopplung:** Jede Station auf dem Weg zum Ziel prüft das Paket. Damit wird das Ursprungssignal des Paketes im Zeitverlauf immer schwächer, sodass nach einer bestimmten Anzahl passierter Teilnehmer, die Qualität nicht mehr ausreicht, um die Wertigkeit des Signals eindeutig zu erkennen.

Auf die Art der Ankopplung hat die einzelne Station jedoch keinen Einfluss. Sie wird von der zugrunde liegenden Technologie bestimmt. Ebenso verhält es sich mit der Steuerung der Konkurrenzsituation der einzelnen Teilnehmer, die sich um das Senderecht und die Übertragungskapazität bewerben. Auch für die Koordination des Zugriffs kommen zwei Strategien in Frage:

- **Wahlfreier Zugriff:** Alle Stationen arbeiten unabhängig voneinander und versuchen autonom einen Zugriff, sobald das Medium nicht belegt ist. Für diesen Vorschlag sind keine Kontroll- und Steuerinformationen notwendig.
- **Verteilt gesteuerter Zugriff:** Alle Stationen erhalten einen Zugriff, sobald sie im Besitz einer Sendeberechtigung sind, die sie zuvor beantragen und erhalten müssen. Die Existenz dieser Sendeberechtigung macht ein Management für die Vergabe und ihren Fehler- und Verlustfall notwendig.

Die grundlegende Idee des Informationstransportes in Netzwerken besteht darin, Nachrichten in kleine Einheiten, sog. Pakete oder Frames, zu zerlegen, diese mit Adress- und Steuerdaten zu versehen und sie dann zuzustellen. Vor einer Übertragung der Daten erfolgt ihre logische Gruppierung in Pakete. Diese Fragmente der Ursprungsdaten sind leichter zu handhaben und für den Nutzer besser zu interpretieren. Darüber hinaus besitzen Pakete mehrere Vorteile:

- Die Paketeinteilung hindert Rechner daran, die Netzwerkbandbreite zu monopolisieren.
- Gehen Pakete auf dem Übertragungsweg verloren, muss nicht die gesamte Information neu gesendet werden, sondern nur Teile.
- Abhängig von der Auslastung können Pakete unterschiedliche Wege zum Ziel nehmen.

Das Konzept erinnert an die Versendung von Postpaketen. Auch dort wird eine Sendung zunächst in mehrere Einzelteile gestückelt, die den Größen- und Gewichtsanforderungen der Post entsprechen. Anschließend werden sie verpackt und mit den Empfängerdaten beschriftet. Als letzter Schritt erfolgt dann die Übergabe an das Verteilsystem der Post. Damit wird die Übertragung beliebig großer Informationsblöcke möglich, d. h. das Volumen unterliegt keinerlei Größenbeschränkungen. Allerdings können die einzelnen Pakete verschiedene Wege durch das Netz nehmen (Wegewahl) und müssen – abhängig von der Technologie – möglicherweise häufiger fragmentiert werden.

Je nach Distanz zwischen den kommunizierenden Rechnern unterscheiden sich die für die Paketzustellung verwendeten Verfahren:

- **Teilstrecken- oder Store-and-Forward-Netze** übertragen die einzelnen Pakete als eigenständige Einheiten vollständig getrennt voneinander. Für das Auffinden des optimalen Weges durch den Netzdschungel nutzen sie spezielle Algorithmen. Die Folge dieser Art des Paketversands ist, dass die einzelnen Pakete ihren Empfänger in beliebiger Reihenfolge erreichen und dort erst wieder zu einer einheitlichen Sendung zusammengesetzt werden müssen. Allerdings können die einzelnen Pakete auf ihrem Weg zum Ziel auch Staus umgehen und trotz längerer Strecke ihr Ziel schneller erreichen als Pakete, die auf den kürzesten aber verstopften Weg warten. Voraussetzung für eine erfolgreiche Paketvermittlung ist eine ausreichende Zwischenspeicherkapazität der Vermittlungsstellen, denn erst nach genauer Kenntnis des Ziels und der Informationen über die Strecke dorthin kann der Knoten eine verlässliche Entscheidung über den weiteren Weg in Richtung Ziel treffen.
- **Diffusions- oder Broadcast-Netze** sind auf kleine Entfernung ausgerichtet. Die Nachricht erreicht alle angeschlossenen, aktiven Knoten und der Empfänger wählt das an ihn gerichtete Paket aus. Dieses Verfahren verlangt keine aufwendige Wegewahl und keine Zwischenspeichermöglichkeit. Wohl aber

müssen alle potenziellen Empfänger das Paket daraufhin prüfen, ob es an sie adressiert ist. Hierfür sind einerseits CPU-Ressourcen der einzelnen Netzknoten notwendig, andererseits verlangt die Prüfung eine gewisse Zeitspanne.

Der Kommunikationsfluss zwischen den Netzteilnehmern verläuft abhängig von der Technologie in drei Formen:



### Kommunikationsrichtungen

**Simplex:** In dieser Variante läuft der Nachrichtenfluss nur in eine Richtung, nämlich vom Sender zum Empfänger – Kabelfernsehen oder Rundfunk.

**Halbduplex:** Hier kann zwar jeder Knoten senden und empfangen, aber nicht beides gleichzeitig – Ampelregelung zur Verkehrsführung auf einer normalen Straße mit halbseitiger Baustelle.

**Vollduplex:** Jeder Knoten kann sowohl Nachrichten senden als auch gleichzeitig empfangen. Für den Netzbetrieb ist dieses Verfahren charakteristisch, da kein Netzteilnehmer ausschließen kann, dass er während einer Sendung Kontrollinformationen empfangen muss, um seine Übertragung einzustellen. Gleichermaßen gilt für einen Server, der Anforderungen von vielen Clients erhält und diese simultan verarbeiten.



Das ursprüngliche Ethernet wird im Halbduplex-Modus betrieben, das heutzutage verbreitete, modernere Switched-Ethernet nutzt einen Vollduplex-Modus. Beim WLAN spielt allerdings der Halbduplex-Gedanke weiterhin eine entscheidende Rolle.

Die unterschiedlichen Formen können als Gradmesser der Übertragungskapazität gelten. Dabei lassen Vollduplex-Verbindungen, da sie in beide Richtungen simultan übertragen, als die ausgereifteste Variante die doppelte Datenübertragungsrate zu. Aber auch die Zahl der involvierten Netzteilnehmer kann Rückschlüsse auf die Netzleistung geben.



### Anzahl der Kommunikationsteilnehmer

**Unicast:** Hierbei handelt es sich um die klassische Form des Datenaustausches in Form einer Punkt-zu-Punkt-Verbindung, bei der einem Sender genau ein Empfänger zugeordnet ist.

**Anycast:** Stellt eine Unicast-Verbindung zu der nächstgelegenen Station einer Gruppe her.

**Multicast:** Eine ausgewählte Gruppe ist das Ziel der Nachricht. Daraus ergeben sich mehrere Einsatzfelder:

- **Content-Push-Distribution:** Informationsdienste wie Wetter, Nachrichten, Börsenkurse, Software-Updates.

- **Verteilung zentraler Datenbestände:** Informationskioske, Produktdatenblätter, Service- und Schulungsunterlagen, Videokonferenzen.
- **Broadcast:** Eine Sendung wird allen erreichbaren Stationen des Netzes zugestellt. Dieser Mechanismus findet z. B. bei der Ermittlung der logischen Adresse eines Rechners oder im Netzwerkmanagement Anwendung.



Das Anycast-Konzept wird insbesondere durch die neue Internet Protocol Version 6 (IPv6) unterstützt.

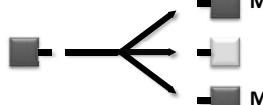
#### Unicast:

*One-to-one Kommunikation*



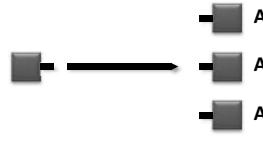
#### Multicast:

*One-to-many Kommunikation*



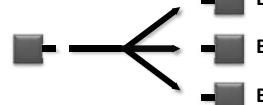
#### Anycast:

*One-to-nearest Kommunikation*



#### Broadcast:

*One-to-all Kommunikation*



**Bild 1.4** Anzahl der Kommunikationsteilnehmer

Die Übertragungsform selbst trennt zwischen **Leitungs- und Paketvermittlung**. In Analogie zum Telefondienst wird bei der Leitungsvermittlung für die Dauer der Sitzung bzw. des Telefongespräches eine exklusive Verbindung zwischen den Kommunikationspartnern aufgebaut. Eine Alternative bietet sich mit der Paketvermittlung an, deren Ablauf dem der Briefpost entspricht. Die zu übermittelnde Nachricht wird zu mehreren Paketen zusammengestellt, mit Absender- und Empfängeradresse versehen und einer bekannten Versandstelle übergeben. Jedes Paket nimmt nun – ähnlich wie ein Brief – einen Weg durch das Beförderungsnetz, ohne dass der Absender den genauen Weg kennen muss. Im Gegensatz zur Leitungsvermittlung besteht zwischen Absender und Adressat keine ständige Verbindung.

Die **Leitungsvermittlung** hat den Vorteil, dass Dienstgüten im Hinblick auf die Übertragungsgeschwindigkeit jederzeit eingehalten werden können und die Sig-

nallaufzeiten konstant sind, d.h. keine variablen Verzögerungen zwischen Sender und Empfänger auftreten. Allerdings ist der Verbindungsauflauf zeitintensiv. Kommunikationsbeziehungen mit mehreren Partnern bedürfen eines wiederholten Aufbaus und beide Teilnehmer müssen mit gleicher Kapazität senden und empfangen. Gleiches gilt, wenn nur kurze Nachrichten übertragen werden. Dann kann die Verbindungsverwaltung mehr Zeit als die eigentliche Übertragung beanspruchen.

Bei der **Paketvermittlung** durchqueren die Pakete das Netz als unabhängige und eigenständige Einheiten und können in den Vermittlungsknoten zwischengespeichert werden. Hierin liegt ein wesentlicher Vorteil, da nun die Übertragungsgeschwindigkeit zwischen einzelnen Teilstrecken keine Begrenzung mehr darstellt. Damit wird das Netzwerk aber zu einem Netzwerk von Warteschlangen. Jeder zu passierende Netzknoten empfängt das Paket und leitet es an seine Ausgangsschnittstelle, die aber Ziel vieler Sendungen sein kann, sodass die Möglichkeit von Überlastsituationen entsteht. Die Existenz der Warteschlangen erzeugt Verzögerungen in der Paketzustellung oder Paketverluste, wenn die Warteschlangen überlaufen. Die Paketverluste verursachen Paketwiederholungen (Retransmission) und haben damit eine weitere Belastung des Übertragungsweges zur Folge. Für den Anwender ist dieser Ablauf transparent. Er benötigt und erhält keinerlei Informationen über den Übertragungsweg, der sich zudem dynamisch ändern kann. Die Paketvermittlung weist insbesondere dann einen großen Vorteil auf, wenn Informationen nur sporadisch übertragen werden (Aufruf einer Webseite, Abrufen/Versenden von E-Mails), da Zeiten, in denen das Übertragungsmedium ungenutzt ist, es durch andere Teilnehmer verwendet werden kann. Hierdurch kann eine Steigerung der Auslastung erreicht werden.

Ein lokales Netz besitzt nur eine begrenzte Ausdehnung. Häufig ist es auf eine Abteilung oder ein Gebäude ausgelegt. Im Zeitalter des Intra-/Internets sind Kommunikationsinseln aber ein Fremdkörper, sodass es nur folgerichtig sein kann, eine unternehmensweite Vernetzung anzustreben. Folgende Sachverhalte sind dabei zu beachten:

- **Gemeinsame Datenbestände sorgen für aktuelle Information:** Die wohl wichtigste Aufgabe eines Netzwerkes ist die zentrale Speicherung von Datenbeständen. Änderungen und Aktualisierungen der Daten finden ihren sofortigen Niederschlag im System, ohne dass es der individuellen Abstimmung und des bidirektionalen Austausches der Anwender bedarf.
- **Transparenz:** Zu den Basiseigenschaften verteilter Systeme gehört es, ihre Komplexität vor dem Benutzer geheim zu halten. Dies geschieht hinsichtlich des Ortes, des Zugriffs, der Namen, der Replikation oder des Ausfalls. Der Zugriff auf Netzressourcen bildet damit keinen gesonderten und schwierigen Vorgang, sondern im Gegenteil, das Netzwerk erweitert die Möglichkeiten des Anwenders, ohne dass dieser seine bisherigen Arbeitsgewohnheiten ändern muss.

- **Teilung teurer Peripherie:** Aufgrund der Ablage von Programmen und Daten auf einer zentralen Station muss auch nur diese mit großen Speichermedien ausgestattet sein. Die einzelnen Rechnerknoten selbst benötigen nur noch eine geringe Speicherkapazität. Darüber hinaus können hochwertige Geräte in das Netzwerk integriert werden, die, einmal angeschafft, allen Anwendern gleichermaßen zur Verfügung stehen.
- **Zentrale Programmverteilung:** Da jeder Rechner über das Netzwerk erreicht werden kann, gibt es die Alternative, ein Anwendungsprogramm nur einmal auf einem zentralen Server zu installieren und von allen Anwendern gleichermaßen nutzen zu lassen oder eine gezielte Verteilung dieses Programms über das Netzwerk auf bestimmte Rechnerknoten vorzunehmen. Auf diese Weise ist es nicht mehr notwendig, jeden einzelnen Arbeitsplatz aufzusuchen, um dort Installation, Wartung oder Aktualisierung auszuführen.
- **Kontrollmöglichkeiten:** Da Netzwerkressourcen nicht im Überfluss existieren, besteht der Bedarf nach einer gerechten Zuteilung. Spätestens hier sind Einsichten in das Nutzungsmuster nötig, um die Erfassung, Abrechnung und Aufbereitung der Leistungen zu ermöglichen. Dass diese Auswertung zuvor erfasste Daten voraussetzt, zeigt, dass eine gewisse Nutzerkontrolle unumgänglich ist.
- **Verschlechterung der Antwortzeiten:** Da ein Wesensmerkmal eines Netzwerkes die gemeinsame Nutzung von Ressourcen ist, besteht auf dem Weg zu zentralen Elementen eine Konkurrenz zwischen allen Teilnehmern. Diese Situation schließt ein, dass jeder Nutzer nur über einen bestimmten Anteil der Übertragungskapazität verfügen kann. Je höher die Nutzerzahl, desto geringer die Kapazität des Einzelnen. Als Folge eines sinkenden Bandbreitenanteils steigt die Antwortzeit. Der Verteilungsaspekt der Software selbst erlangt damit eine bedeutende Rolle. Geleitet von dem Verlangen nach hoher Performance und kurzen Antwortzeiten, ist die Frage nach der optimalen Verteilung keineswegs trivial, sondern hängt im Gegenteil von einer Vielzahl von Rahmenbedingungen wie Lokalität oder Netzdesign ab.
- **Notwendigkeit eines Netzadministrators:** Durch die Verteilung der Daten und Programme auf heterogene, autonome, miteinander kooperierende Rechnersysteme erhöht sich die Komplexität des Gesamtsystems, dessen Pflege, Wartung und Ausbau viel Aufwand und technisches Know-how erfordert.
- **Sicherheit:** Da verteilte Systeme allen Benutzern den gemeinsamen Gebrauch der Ressourcen ermöglichen, treten Sicherheitsanforderungen auf:
  - Autorisierung – ist der Benutzer berechtigt, auf Netzressourcen zuzugreifen?
  - Vertraulichkeit – werden die Daten nur von den Berechtigten verarbeitet?
  - Integrität – erreicht die Nachricht den Empfänger unverändert?

- Authentisierung – ist der Kommunikationspartner derjenige, der er vorgibt zu sein?
- Nichtabstreitbarkeit – ist das Absenden bzw. Empfangen der Nachricht eindeutig beweisbar?

Auf dem Weg zu einem Netzwerk ist es aber nicht nur bedeutsam, die genauen Anforderungen festzulegen, sondern auch deren Umsetzung. Zu den wichtigen Eigenschaften, die heutige Netzwerke umfassen sollten, gehören:

- **Skalierbarkeit:** Einem Netz müssen problemlos weitere Knoten hinzuzufügen sein. Mit dieser Eigenschaft wird dem weiteren Ausbau und der flexiblen Reaktion auf geänderte Rahmenbedingungen sowie der stetigen Zunahme des Vernetzungsgrades Rechnung getragen.
- **Robustheit:** Die Netzinfrastruktur muss durch Stabilität und Fehlertoleranz geprägt sein. Da Netzwerke in Client/Server-Umgebungen zu einer kritischen Komponente für das gesamte Unternehmen geworden sind und der Unternehmenserfolg entscheidend auf einem funktionstüchtigen Netz beruht, bedeuten minimale Ausfallzeiten einen Wettbewerbsverlust.
- **Migration:** Das Netzdesign muss den leichten Übergang auf neue Techniken und Netztopologien zulassen. Der stete Wandel in der Informationsverarbeitung bringt die Notwendigkeit mit sich, einen Übergang auf technologische Änderungen zu ermöglichen, ohne die gesamte Netzinfrastruktur auszutauschen. In diesem Sinne wird Investitionssicherheit für ein Netzdesign großgeschrieben.
- **Autokonfiguration:** Neue Netzkomponenten müssen ohne großen Aufwand integrierbar sein. Nicht nur höhere Bandbreite für Multimedia-Anwendungen steht auf der Wunschliste der Netzbetreiber, sondern auch zunehmend die Möglichkeit, alle Daten von Sprache bis Video über eine Netzinfrastruktur abzuwickeln. Derartig komplexe Anforderungen können nur durch spezielle Kopplungsgeräte erbracht werden. Der einfache Austausch alter gegen neue Geräte, ohne Störung des Netzbetriebs, ist hier die Idealvorstellung.

## ■ 1.5 ISO/OSI-Referenzmodell

Die Beschreibung der Möglichkeiten, wie eine Station in das Netzwerk integriert wird, zeigt, dass es allgemeiner Verhaltensrichtlinien bedarf, auf deren Grundlage sich Stationen miteinander unterhalten und sich gegenseitig verstehen. Sende- und Empfangsstationen müssen sich an bestimmte Spielregeln halten, damit die Übertragungswünsche der Netzteilnehmer nicht im Chaos enden.

Zur Veranschaulichung der Struktur eines Kommunikationsablaufs zwischen zwei Teilnehmern dient ein logisches Modell. Die Grundidee besteht darin, den Kommunikationsvorgang in eine Hierarchie von Funktionsschichten zu gliedern. Jede Schicht bietet der ihr übergeordneten Schicht Funktionen an und kann Dienste der unter ihr liegenden Schicht in Anspruch nehmen, ohne ihre Funktionsweise zu kennen. Dem Anwender bleibt die Schichtung verborgen. Die Schichten der gleichen Ebene kommunizieren über Protokolle miteinander. Sie beinhalten definierte Regeln, nach denen die beiden Kommunikationspartner zusammenarbeiten und der nächst höheren Ebene ihre Dienstleistung anbieten.

Die Kommunikation zwischen Rechnern in offenen, heterogenen Systemen wird heutzutage durch das ISO/OSI-Referenzmodell beschrieben. Das Referenzmodell ist ein konzeptioneller Rahmen, der Funktionen und Schemata für den Kommunikationsvorgang enthält. Dieser Rahmen teilt den Kommunikationsvorgang in sieben aufeinander aufbauende Schichten ein, denen allgemeine Vereinbarungen und Inhalte zugrunde liegen. Allerdings enthält diese Spezifikation keine Implementierungsvorgaben, sodass eine generelle Umsetzung in Produkte nicht möglich ist. Sie dient lediglich als Leitlinie für den Entwurf und die Implementierung von Standards, Geräten und Kommunikationsverfahren. Der Vorteil dieser Vorgabe beruht in erster Linie auf der offenen allgemein verbindlichen Vorstellung eines Kommunikationsvorganges in Form eines Architekturmodells. Darüber hinaus dient die Beschreibung der Funktionen der einzelnen Schichten als Basis für eine präzise Spezifikation von Protokollen und schafft dadurch letztlich eine weitgehend herstellerneutrale Begriffswelt. Daher ist es theoretisch möglich, das Protokoll einer einzelnen Schicht durch eine Neuentwicklung zu ersetzen, ohne die Funktionen der anderen Schichten zu beeinträchtigen.

Die Protokolle regeln den Kommunikationsablauf, ähnlich wie die Unterhaltung zweier Personen bestimmten Vereinbarungen folgt. Jede Schicht des Senders nutzt ihr eigenes Protokoll, um virtuell mit der entsprechenden Schicht des Empfängers zu kommunizieren. Die ausgetauschten Informationen werden in sog. **PDUs** (Protocol Data Units) übertragen. Diese PDUs enthalten je nach Schicht Prüfdaten, Adressen oder Informationen über übergeordnete Protokolle.



Der Prozess des Durchwanderns der OSI-Schichten macht eine permanente Neuauflistung der Informationen notwendig, da alle Protokolle nur bestimmte Paketgrößen akzeptieren – **Fragmentierung**. Zur Übertragung selbst werden die PDU-spezifischen Informationen an die zu übertragenen Daten angeheftet – **Encapsulation**. Auf Empfängerseite verläuft der Prozess analog – **De-Encapsulation**:

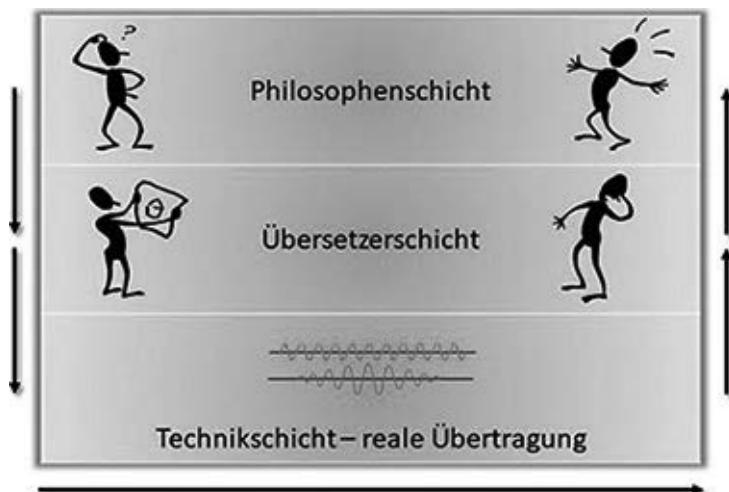
1. Lesen der schichtspezifischen Information.
2. Abtrennen der PDU-spezifischen Daten.
3. Weiterleiten der verbliebenen Daten an die übergeordnete Schicht.

Den Ablauf auf drei Ebenen verkürzt zeigt folgendes Beispiel:

**Verkürztes Philosophenmodell**

Der Philosoph Hill in England möchte seinem chinesischen Kollegen Xiu eine wichtige Fachfrage stellen. Ihr Kommunikationsmedium wäre die Fachsprache der Philosophen. Nun spricht Herr Hill nur englisch, Herr Xiu nur chinesisch. Um dennoch eine Verständigung zu ermöglichen, bedienen sich beide der Hilfe von Dolmetschern. Wie gewöhnlich verfasst Herr Hill seine Frage in Englisch und übergibt diese einem Dolmetscher, der sie in eine beliebige Zwischensprache z.B. italienisch übersetzt. Wie kommt nun die Nachricht vom Dolmetscher des Herrn Hill zum Dolmetscher des Herrn Xiu? Da beide Philosophen Computer-Freaks kennen, die ständig über das Internet miteinander Nachrichten austauschen, lassen sie ihre ins Italienische übersetzte Frage einfach von diesen übermitteln. Beide Computernutzer müssen dazu kein Wort italienisch kennen; sie haben lediglich die Aufgabe, die Worte korrekt zu übertragen. Sobald die Nachricht den chinesischen Computer-Freak erreicht, übergibt er diese dem Dolmetscher, der sie ins Chinesische transformiert und Herrn Xiu überreicht. Auf diese Art können zwei Philosophen miteinander sprechen, ohne die Muttersprache ihres Partners zu beherrschen.

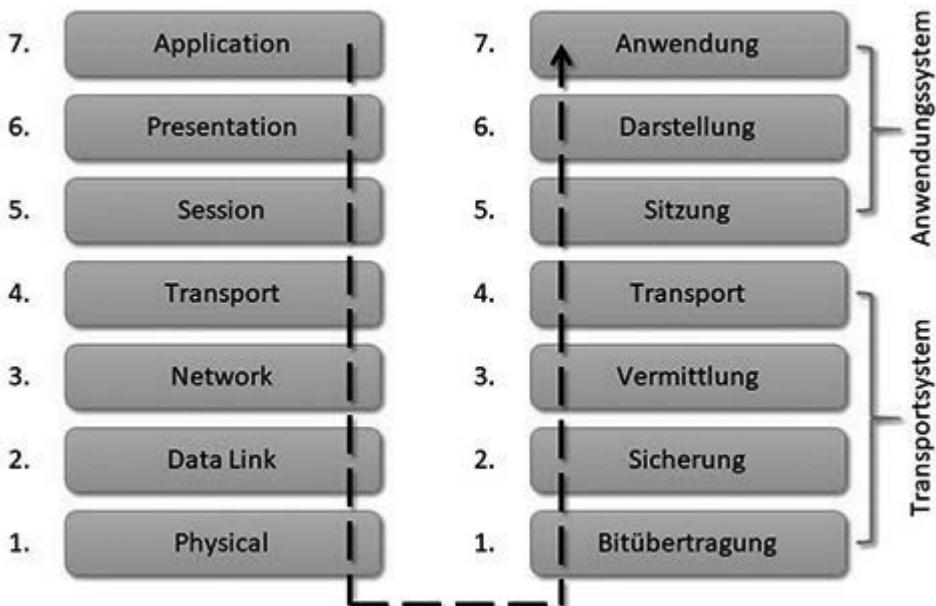
Wie Bild 1.5 verdeutlicht, findet die eigentliche Übertragung ausschließlich auf der untersten, der Techniksicht statt. Diese Ebene und die Übersetzungsschicht können ohne Funktionseinbuße ausgetauscht werden. Falls der italienische Dolmetscher ausfällt, könnte Französisch als Zwischensprache dienen bzw. falls die Internetnutzung nach China untersagt ist, kann auf Fax ausgewichen werden. Damit wird deutlich, dass die Protokolle bis auf die Schnittstellen voneinander unabhängig und beliebig ersetzbare sind.



**Bild 1.5** Philosophenmodell mit drei Schichten

Im Unterschied zu den Diensten oder Funktionen, die für die vertikale Kommunikation zwischen den Schichten verantwortlich sind, regeln Protokolle die Kommunikation zweier Partner auf gleicher Ebene, also in horizontaler Richtung. In diesem Sinne ist die Einigung auf Italienisch als Übersetzungs- und das Internet als Transportmedium die Verständigung auf Protokolle.

 Die detaillierte und standardisierte Kommunikation nach dem ISO/OSI-Referenzmodell im Netzwerkumfeld basiert auf sieben Schichten. Die Gesamtheit der sieben OSI-Schichten wird oft als Stack bezeichnet. Die untersten Schichten dieses Modells präsentieren netzorientierte Funktionen, die oberen werden als anwendungsbezogen eingestuft. Der Ablauf erfolgt beim Sender streng von oben (Schicht 7) nach unten (Schicht 1) und beim Empfänger in der umgekehrten Richtung.



**Bild 1.6** ISO/OSI-Referenzmodell

Neben dem OSI-Modell existiert die Vorstellung der Internetwelt in Form des DoD (Department-of-Defense)-Modells über eine funktionale Gliederung des Kommunikationsvorganges. Eine Gegenüberstellung beider Konzepte zeigt das nachfolgende Bild 1.7.

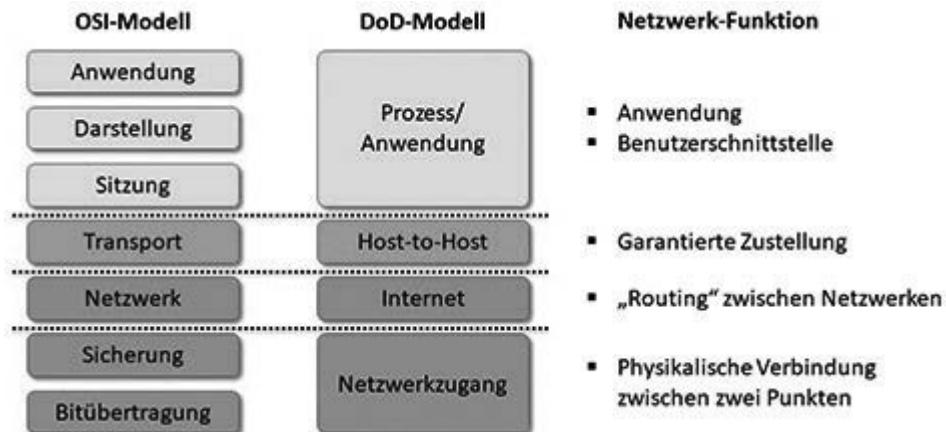


Bild 1.7 Vergleich: ISO/OSI-Referenzmodell – DoD-Modell

Was ist nun der Inhalt der einzelnen Schichten?

- **Bitübertragungsschicht:** Hier werden die elektrischen, mechanischen und funktionalen Parameter zur physikalischen Übertragung festgelegt. Die Grundfunktion besteht in der Bereitstellung der physikalischen Verbindung und deren kontinuierlicher Betriebsbereitschaft. Zur Gewährleistung dieser Anforderungen sind mehrere grundlegende Details zu klären:
  - Wie wird gewährleistet, dass ein Bit der Wertigkeit 1 sowohl vom Sender als auch vom Empfänger als solches erkannt wird?
  - Welcher elektrischen Größe entspricht eine logische Eins, welcher eine logische Null?
  - Wie viele Mikrosekunden soll die Dauer der Übertragung eines Bits dauern?
  - Wie wird eine Verbindung aufgebaut und wie wird sie eingestellt?
  - Kann eine Übertragung in beide Richtungen erfolgen?
 In Netzwerken werden drei Medien genutzt:
  - **Kupfer:** hier beruht die Signalisierung auf elektrischen Impulsen.
  - **Glasfaser:** hier bildet ein optisches Signal die Grundlage der Signalisierung.
  - **Luft:** hier werden Radio- oder Lichtwellen über die Luft übertragen.
 In allen drei Formen ist es notwendig, den Beginn und das Ende einer Übertragung mitzuteilen. Dies geschieht über besondere Bitfolgen. Um die Bitfolgen selbst mit semantischem Inhalt zu versehen, ist ein Codierungsschema erforderlich, das Gruppen von Bits zu logischen Einheiten zusammenfasst. Auf diese Weise gelingt es, Buchstaben, Zei-

# Index

## Symbolle

2-1-Regel 102  
5-4-3-Regel 87  
10Base 85f., 88f.  
10GBase 111  
10-Gigabit-Ethernet 111  
100Base 97, 99  
100GBase 117  
1000Base 105ff.

## A

Access Control List 292, 341  
Access-Point 320  
ACK 210  
Acknowledgement 143, 210  
- -Nummer 211  
ACL 292  
ACR 57  
Address Mask  
- Reply 140  
- Request 140  
Address Resolution Protocol 134  
- Cache 134  
- Reply 135  
- Request 135  
Adresse  
- Link-Local- 188  
- Loopback- 189  
- Multicast- 188  
- private 188  
- reservierte 188  
- Unicast- 187

- Unique-Local- 188  
- unspezifizierte 189  
Adresskonfiguration  
- automatisch 178  
Advanced Encryption Standard 344  
AES 344  
Aging-Timer 240  
Alohanet 68  
Antivirus-Software 310  
Anwendungsklasse 59  
Anwendungsschicht 26  
Anycast 15, 178  
AP 320  
Applikationsmanagement 297  
ARP 134  
ARP-Cache-Poisoning 263  
asynchron 36, 73  
Attempt Limit 79  
Attenuation to Crosstalk Ratio 57  
Autodiscovery 297  
Autokonfiguration 19  
Auto-Negotiation 81, 101  
Autosensing 64  
Autotopology 297

## B

Backbone  
- Collapsed- 40  
- Distributed- 39  
Backoff 334  
Bandbreite 5, 47  
Bandbreitenreservierung 178

- Base **71**  
 baseline **317**  
 Basic Service Set **327**  
 Basisband **84**  
 Basisdatentransfer **209**  
 Beacon Frame **336**  
 Beamforming **326**  
 Begleitprotokoll **191, 207**  
 Best-Effort-Prinzip **124**  
 Best-Effort-Service **226**  
 Betriebssystem **4**  
 Biegeradius **58**  
 Bitfolge **23**  
 Bitrate **58**  
 Bitübertragungsschicht **23**  
 Block Acknowledgement **335**  
 Border Gateway Protocol **281**  
 Botnetz **221**  
 BPDU **251**  
 Break-Out-Kabel **52**  
 Brechungsindex **44, 46**  
 Bridge **238**  
 Bridge Protocol Data Unit **251**  
 Broadcast **16**  
   - -adresse **157**  
   - -Domäne **76**  
   - -Netz **14**  
 Brute-Force **309**  
 BSS **327**  
 BSS Coloring **336**  
 Bündelader **52**  
 Busy Waiting **77**
- C**
- Cache-Poisoning **148**  
 Carrier Extension **109**  
 Carrier Sense **77**  
 Category **59**  
 CATNIP **176**  
 CBWFQ **233**  
 CIDR **168**  
 Cladding **43**  
 Classless-Inter-Domain-Routing **168**  
 Client **9**
- Client/Server-Architektur **9**  
 Cloud-Computing **11**  
 Coating **51**  
   - Primary **43**  
   - Secondary **43**  
 Codierung **32**  
   - 4Bit/5Bit- **34**  
   - 8B/6T- **99**  
   - Bit- **33**  
   - Manchester- **34**  
   - MLT-3- **34**  
   - Multilevel- **33**  
 Collision Detection **78**  
 Congestion  
   - -Avoidance **217, 225, 228**  
   - -Collapse **217**  
   - -Management **225, 230**  
 Converged Interface Adapters **118**  
 Core **43**  
 Crosstalk **62**  
   - Alien- **63, 113**  
 CSMA/CA **332**  
 CSMA/CD-Verfahren **76, 82**  
 Cut-Through **242**
- D**
- DAD **199**  
 Dämpfung **47, 56**  
 Darstellungsschicht **25**  
 Datenaustausch **32**  
 Datenflusskontrolle **81, 210, 215**  
 Datenkompression **26**  
 Datenverbund **4**  
 DCF **332**  
 Defaultroute **272, 274**  
 Deferring **77**  
 Delay Skew **63, 108**  
 Denial of Service **221, 264, 310**  
 Destination-Adresse **74**  
 Deutsches Network Information Center  
   **128**  
 DHCP **141**  
 Dienstgüte **125, 177**  
 DiffServ **127, 226**

- Diffusionsnetz 14  
Direct Sequence Spread Spectrum 329  
Distributed Coordination Function 332  
DNS 141  
Domain Name System 141, 145  
DoS 221  
Drei-Schichten-Modell 10  
DS-Byte 127  
DSSS 329  
Dual-IP 193  
- -Stack 194  
Duplicate Address-Detection 199  
Durchsatz 5  
Dynamic Host Configuration Protocol 141f.
- E**
- Echo 138  
- Reply 138  
EDIFACT 26  
Einkopplungswinkel 44  
Electronic Data Interchange for Administration, Commerce and Transport 26  
Elektromagnetische Verträglichkeit 42, 62  
Encapsulation 20, 193  
Energy Efficient-Ethernet 118  
Ethernet 68  
- Distanz 82  
- Namenskonvention 71  
- Paket 71  
- Paketfelder 72  
Eventhandling 297
- F**
- Fast-Ethernet 95  
FCAPS-Modell 300  
FEXT 63  
FHSS 329  
Fibre Channel 105  
FIFO 231  
File Transfer Protocol 26  
Firewall 310
- First-in-First-out 231  
Flag 127, 211  
Flooding 241f.  
Flow Control 179  
Flow Label 178, 181  
Flusskontrolle 110  
Forwarding 184  
Fragmentation Offset 127  
Fragment Free 244  
Fragmentierung 14, 130, 179, 184  
Fragment Offset 185  
Fragmentprüfung 80  
Frame 14, 25  
Frame Aggregation 335  
Frame Check Sequence 91  
Frequency Hopping Spread Spectrum 329  
Fresnel-Verlust 48  
FTP 26  
Funktionsverbund 4
- G**
- Gerätehärtung 310  
Ghost 91  
Gigabit-Ethernet 62, 104, 109  
Glasfaser 41  
- -Kabelarten 51  
- -Steckverbindungen 52  
- -Typen 49  
Goodput 5
- H**
- Halbduplex 15  
HardwareAdresse 73  
Header  
- ARP- 135  
- Authentification 185  
- Destination Options- 183  
- Encapsulation 185  
- -Erweiterung 182  
- Fragment- 184  
- Hop-by-Hop Options- 183  
- IP 125

- IPv6- 179  
 - Routing- 184  
 - TCP-Protokoll 210  
 Hello-Paket 280, 286  
 Hello-Timer 252  
 Helper Address 143  
 Hidden Node 334  
 Hohlader 52  
 Hold Down Timer 282  
 Hop Count 277  
 Hop-Count-Limit 282  
 Hop-Limit 179, 182  
 Hostadresse 152  
 HTTP 26  
 Hub 88  
 Hyper Text Transfer Protocol 26

## I

ICMP 137  
 Idle 77  
 IEEE 67  
 IEEE 802.3 68, 70  
 IEEE 802.11 321  
 Induktivität 57  
 Initialisierungsvektor 342  
 Integritätsprüfung 81  
 Interframe Gap 77, 84  
 Internet Control Message Protocol 137  
 Internetprotokoll 124  
 - IPv4 175  
 - IPv6 175  
 Int-Serv 226  
 IP 124  
 - -Adressierung 151  
 - Adressklasse 153  
 ISO/OSI-Referenzmodell 20, 124

## J

Jabber 91  
 JAM-Signal 78  
 Jitter 226  
 Jumbo-Frame 92  
 Jumbograms 179

## K

Kanal 36  
 Kapazität 5, 57  
 Kaskadierung 88  
 - von Switches 246  
 Kern 43  
 Keystream 342  
 Klasse 60  
 Kollision 78  
 - Early- 80, 90  
 - Late- 80, 90  
 Kollisions-Domäne 76  
 Kollisionserkennung 78

## L

LAN 5  
 Laser 46  
 Lastverbund 4  
 Latenz 226  
 Layer 2 237  
 Layer 3 267  
 Learn-and-Stay-Verfahren 241  
 Least Significant Byte 25  
 LED 46  
 Leistungsverbund 4  
 Leistungsverlust 47  
 Leitungsvermittlung 16  
 Lichtwellenleiter 37, 44  
 Lifetime 197  
 Link Aggregation 82, 246  
 LLC 24  
 Local Area Network 5  
 Logical Link Control 24  
 Long Wave 106  
 Loopback 156

## M

MAC 24  
 - -Adresse 73, 151  
 - -Flooding 263  
 - -Schicht 98  
 Malware 310

- MAN 5  
Managed Devices 301  
Management Information Base 301, 304  
Man-in-the-Middle 199, 263, 310  
Maximum Transfer Unit 180  
Maximum Transmission Unit 125  
MBZ 126  
Media Access Control 24  
Media Independent Interface 97  
Metrik 269, 284  
Metropolitan Area Network 5  
MIB 301  
MII 97  
MII-Schicht 98  
MIMO 326  
MLT-3-Verfahren 34  
Mobile IP 195  
Mode 46  
Modendispersion 47  
Modulation  
– Amplituden- 32  
– Frequenz- 32  
– Phasen- 32  
Modulationsverfahren 329  
Monomodefaser 49  
Most Significant Byte 25  
MTU 125  
Multicast 15  
Multicasting 178  
Multicast Listener Discovery Protocol 191  
Multimode-Gradientenfaser 50  
Multimode-Stufenfaser 49  
Multiple Access 76, 78  
Multiple Input Multiple Output 326  
Multiplexing 35, 210, 212  
– Frequenz- 36  
– Zeit- 36  
Multiprotokoll 194  
Multi-User-MIMO 326
- N  
Nameserver 145  
NAT 166
- Nebensprechen 57  
– Fernnebensprechdämpfung (FEXT) 63  
– Nahnebensprechdämpfung (NEXT) 57  
Neighbor Discovery Protocol 190f.  
netstat 298  
Network Address Translation 166  
Netzkennung 152, 156  
Netzneutralität 233  
Netzpräfix 152  
Netzwerk 3  
– -adresse 152  
– -architektur 8  
– -kabel 4  
– -karte 4  
– -management 170, 296  
– -schicht 24  
– virtuelles lokales 245, 255, 290  
Netzwerkpräfix 197  
NEXT 57  
Next Header 179, 181  
Non-Blocking 245  
NRZI-Verfahren 34  
Numerische Apertur 48
- O  
OFDM 329  
OFDMA 329  
Open Shortest Path First 126  
Open-Shortest-Path-First-Protokoll 279, 286  
Open-System-Authentifizierung 340  
Orthogonal Frequency Division Multiple Access 329  
Orthogonal Frequency Division Multiplexing 329  
OSI-Schichten 22  
OSPF 126, 279
- P  
Packet Bursting 109  
Padding 129  
Paket 14, 25  
Paketvermittlung 16

- Patchpanel 65  
Payload-Length 179  
PDU 20  
PHY-Spezifikation 98, 108, 114  
PHY-Typen 115  
Pigtail 46  
ping 140, 288, 298  
PLCP-Header 336  
Polling 297  
Port 110, 240  
Port Security 144  
Power-over-Ethernet (PoE) 118  
Präambel 72, 336  
Priorität 179  
Priority Queuing 231  
Propagation Delay 62  
Protocol Data Unit 20  
Protokoll 3  
Protokollfamilie 123  
Prüfsumme 24, 74, 128, 179, 212  
Punkt-zu-Punkt-Verbindung 15, 257
- Q**
- QoS 224  
Quality-of-Service 224
- R**
- Random Early Detection 229  
RARP 137  
Rayleigh-Streuung 47  
Reassemblierung 131  
RED 229  
Reflexion 48  
Registrierungsprozess 198  
Repeater 83, 85  
– Klasse 1 102  
– Klasse 2 102  
Resource Reservation Protocol 181  
Ressourcenreservierung 226  
Retransmission 17  
Reverse Address Resolution Protocol 137  
RIP 161, 279
- RJ-45-Stecker 60, 88  
Roaming 340  
Rogue Device 199  
Root-Bridge 251  
Route Poisoning 282  
Router 267  
Router Advertisement 190  
Route-Tag-Feld 286  
Routing 24, 277  
– indirekt 132  
– Loose-Source 131  
– Methoden 273  
– Recorded 132  
– Strict-Source 131  
Routing-Algorithmus 277  
Routing Information Protocol 161, 169, 279, 283  
Routing-Protokoll 278, 283  
– Classful 280  
– Classless 281  
– Distance-Vector 279  
– Exterior-Gateway 278  
– Interior-Gateway 279  
– Link-State 280  
Routing-Schleife 282  
Routing-Tabelle 269, 274, 277  
RSVP 181  
Rückflussdämpfung 56, 62, 108
- S**
- Scanning  
– aktiv 340  
– passiv 340  
Schichtenmodell 23  
Second-Level-Domain 145  
Segment 25, 208  
Sequenznummer 138, 211, 213  
Server 9  
Service Set Identifier 327, 341  
Short Frame 91  
Short Wave 106  
Sicherheitspolitik 309  
Sicherungsschicht 24  
Signalcodierung 72

- Signalisierung 3, 32
  - Simple Internet Protocol Plus 176
  - Simple Mail Transfer Protocol 26
  - Simple Network Management Protocol
    - 301
    - Befehle 303
  - Simplex 15
  - Sitzungsschicht 25
  - Skalierbarkeit 19
  - Sliding Window 210
  - Slot-Time 79
  - SMI 302
  - SMTP 26
  - SNMP 301
  - Snooping
    - DHCP- 144
  - Socket 210, 212
  - Solicitation Request 190
  - Source-Adresse 74
  - Spanning-Tree 249
  - Split Horizon 282
  - Spoofing 143
    - DNS- 148
  - SSID 327
  - Stabilität 19
  - Stack 22
  - Starvation 143
  - Stateful 190
  - Stateless 190
    - -Autoconfiguration 190
  - Staukontrolle 210, 217, 230
  - Store and Forward 243
  - Store-and-Forward-Netz 14
  - Structure of Management Information 302, 306
  - Subnetz 158
    - -Adresse 152
    - -Identifikator 160
    - Strukturierung 164
    - variable Länge 162
    - zugehörigkeit 160
  - Switch 39, 238
    - Stackable 240
  - Switch-Architektur
    - Bus 247
    - Matrix 247
    - Shared Memory 247
  - Switching 103
  - Switching-Verfahren 242
  - SYN 212
  - Synchronisation der Sequenznummer 212
  - Synchronität 36, 73
  - SYN-Cookie 223
  - SYN-Flood-Attacke 221
  - SYN-Flooding 310
  - Syntax-Notation 302
  - syslog 307
  - Systemmanagement 297
- T
- Tag-Controll-Feld 76
  - Tag Protocol Identifier 76
  - TCP 207
  - TCP/IP 123
  - Teilstreckennetz 14
  - Three-Way-Handshake 213
  - Time Exceeded 139
  - Timestamp 132
    - Reply 140
    - Request 140
  - Time to Live 127
  - Token Bucket 229
  - Top-Level-Domain 145
  - Topologie 6
    - Bus- 6
    - logische 8
    - physikalische 8
    - Ring- 6
    - Stern- 7
  - ToS 126
  - TP-Kabel 56
  - Traceroute 140, 289
  - Traffic Shaping 228
  - Transceiver 86
  - Transmission Control Protocol 207f.
  - Transport-Modus 185
  - Transportprotokoll 207
  - Transportschicht 25

Triggered Updates 282

Trunk 257

TTL 127

TUBA 176

Tunneling 193

Tunnel-Modus 185

Twisted-Pair 55

- -Kabeltypen 56

Type of Service 126

## U

Übertragung

- analog 32

- digital 32

Übertragungsfrequenz 47

Übertragungskapazität 15

Übertragungsrate 45

UDP 207

Unicast 15

Urgent-Zeiger 212

User Datagram Protocol 207, 220

- Header 220

UTP-Kabel 56, 62

## V

Verbindung

- kupferbasiert 105

- Monomode 105

- Multimode 105

Verbindungsabbau 214

Verbindungsaufbau 25, 213

Verfügbarkeitsverbund 4

Verkabelung 3, 37

- Glasfaser- 41

- Kupfer- 55

- Primär- 37

- Sekundär- 37

- Tertiär- 38

- Twisted-Pair- 55

Verschlüsselung 26, 185

Verzögerung 9

Virtual-Carrier-Sense-Konzept 334

Virtual-Router-Redundancy-Protokoll

272

VLAN 255

- Typen 256

VLAN Trunk Protocol 258

VLSM 162

Vollader 51

Vollduplex 15

VRRP 272

VTP 258

## W

Wegewahl 6, 14, 277

Weighted Fair Queuing 231

- Class-Based - 233

Wellenlänge 42

Well-Known-Port 212

Well-Known-Service 212

WEP 342

WFQ 231

Wide Area Network 5

Widerstand 56

Wi-Fi 6 319

Wi-Fi Protected Access 340, 343

Wi-Fi Protected Access 2 344

Wi-Fi Protected Access 3 344

Windowgröße 212

Wireless Local Area Network 319, 328

- Header 336

Wires Equivalent Privacy 342

Wire-Speed 245

Wiring Closet 59

WLAN 319

WPA 340

WPA2 344

WPA3 344