

Rüdiger SCHREINER  
Oliver P. WALDHORST

# COMPUTER- NETZWERKE

8. Auflage



VON DEN GRUNDLAGEN  
ZUR FUNKTION  
UND ANWENDUNG

HANSER





**Blieben Sie auf dem Laufenden!**

Hanser Newsletter informieren Sie regelmäßig über neue Bücher und Termine aus den verschiedenen Bereichen der Technik. Profitieren Sie auch von Gewinnspielen und exklusiven Leseproben. Gleich anmelden unter

**[www.hanser-fachbuch.de/newsletter](http://www.hanser-fachbuch.de/newsletter)**



Rüdiger Schreiner  
Oliver P. Waldhorst

# Computernetzwerke

Von den Grundlagen zur  
Funktion und Anwendung

8., aktualisierte Auflage

HANSER

Die Autoren:  
Rüdiger Schreiner, Schopfheim  
Prof. Dr. Oliver P. Waldhorst, Offenburg

Alle in diesem Werk enthaltenen Informationen, Verfahren und Darstellungen wurden nach bestem Wissen zusammengestellt und mit Sorgfalt getestet. Dennoch sind Fehler nicht ganz auszuschließen. Aus diesem Grund sind die im vorliegenden Werk enthaltenen Informationen mit keiner Verpflichtung oder Garantie irgendeiner Art verbunden. Autoren und Verlag übernehmen infolgedessen keine juristische Verantwortung und werden keine daraus folgende oder sonstige Haftung übernehmen, die auf irgendeine Art aus der Benutzung dieser Informationen – oder Teilen davon – entsteht. Ebenso wenig übernehmen Autoren und Verlag die Gewähr dafür, dass die beschriebenen Verfahren usw. frei von Schutzrechten Dritter sind. Die Wiedergabe von Gebrauchsnamen, Handelsnamen, Warenbezeichnungen usw. in diesem Werk berechtigt also auch ohne besondere Kennzeichnung nicht zu der Annahme, dass solche Namen im Sinne der Warenzeichen- und Markenschutz-Gesetzgebung als frei zu betrachten wären und daher von jedermann benutzt werden dürften.

Die endgültige Entscheidung über die Eignung der Informationen für die vorgesehene Verwendung in einer bestimmten Anwendung liegt in der alleinigen Verantwortung des Nutzers.

Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.

Bibliografische Information der Deutschen Nationalbibliothek:

Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

Dieses Werk ist urheberrechtlich geschützt.

Alle Rechte, auch die der Übersetzung, des Nachdruckes und der Vervielfältigung des Buches, oder Teilen daraus, vorbehalten. Kein Teil des Werkes darf ohne schriftliche Genehmigung des Verlages in irgendeiner Form (Fotokopie, Mikrofilm oder ein anderes Verfahren) – auch nicht für Zwecke der Unterrichtsgestaltung – mit Ausnahme der in den §§ 53, 54 URG genannten Sonderfälle –, reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

© 2023 Carl Hanser Verlag München, <http://www.hanser-fachbuch.de>

Lektorat: Sylvia Hasselbach

Copy editing: Sandra Gottmann, Wasserburg

Umschlagdesign: Marc Müller-Bremer, [www.rebranding.de](http://www.rebranding.de), München

Umschlagrealisation: Max Kostopoulos

Satz: Eberl & Koesel Studio, Kempten

Druck und Bindung: Hubert & Co. GmbH & Co. KG BuchPartner, Göttingen

Printed in Germany

Print-ISBN 978-3-446-47415-4

E-Book-ISBN 978-3-446-47472-7

E-Pub-ISBN 978-3-446-48004-9

# Inhalt

<b>Vorwort</b>	<b>XV</b>
<b>1 Zur Geschichte der Netzwerke</b>	<b>1</b>
1.1 Netzwerke – der Beginn	1
1.2 Definition eines Netzwerkes	3
1.3 Das OSI-Modell	3
1.4 Übersicht über das OSI-Modell	4
1.4.1 Layer I – die physikalische Schicht (Physical)	4
1.4.2 Layer II – die Sicherungsschicht (Data Link)	5
1.4.3 Layer III – die Vermittlungsschicht (Network)	5
1.4.4 Layer IV – die Transportschicht (Transport Layer)	5
1.4.5 Layer V – die Kommunikations-/Sitzungsschicht (Session)	6
1.4.6 Layer VI – die Darstellungsschicht (Presentation)	6
1.4.7 Layer VII – die Anwendungsschicht (Application)	6
1.5 Übertragungswege im OSI-Modell	7
1.6 Allgemeine Bemerkungen	8
1.7 Zum Weiterlesen	10
<b>2 Layer I des OSI-Modells</b>	<b>11</b>
2.1 Die Medien	11
2.2 Historische Verkabelung: Thin-Wire (Koaxialkabel)	12
2.3 Die universelle Gebäudeverkabelung (UGV)	14
2.3.1 Kabeltypen Twisted Pair	15
2.3.2 Verlegung der universellen Gebäudeverkabelung und Geräteverbindungen	16
2.4 Glasfaser	17
2.4.1 Exkurs in die Physik – Glasfasertypen, Lichtwellenleiter, Effekte	18
2.4.2 Lichtleitung in der Faser	18
2.4.3 Die Stufenindexfaser	19
2.4.4 Längenbeschränkung und Grenzen/Dispersion	20
2.4.5 Die Gradientenindexfaser	22
2.4.6 Qualitäten und Längenbeschränkung	23

2.4.7	Die Mono- oder Singlemode-Faser .....	23
2.4.8	Verlegung und Handhabung .....	24
2.4.9	Laser sind gefährlich .....	25
2.4.10	High-Speed-Verfahren .....	25
2.5	Die Gesamtverkabelung .....	26
2.5.1	Gebäude/Büro .....	26
2.5.2	Geschwindigkeit .....	27
2.5.3	Miniswitches .....	28
2.5.4	Fiber-to-the-Desk .....	29
2.6	Kabeltypen/Dateneinspeisung/Entnahme .....	29
2.6.1	Kabeltypen .....	29
2.6.2	Kabelkategorien .....	32
2.7	Transceiver .....	33
2.8	Zugriffsverfahren .....	34
2.8.1	CSMA/CD .....	35
2.8.2	Andere Verfahren – kollisionsfreie Verfahren .....	37
2.9	Zum Weiterlesen .....	38
<b>3</b>	<b>Layer II – die Sicherungsschicht .....</b>	<b>39</b>
3.1	Adressen .....	39
3.1.1	Adressermittlung/ARP .....	40
3.2	Kollisionsbereiche und Bridges .....	41
3.3	Store and Forward-Bridging .....	42
3.4	Switches .....	44
3.4.1	Geswitchte Topologien .....	45
3.5	Keine Kollisionen – keine Detection, Duplex .....	46
3.6	Loops – das Netzwerk bricht zusammen .....	47
3.6.1	Loops – verwirrte Bridges .....	47
3.6.2	Spanning Tree, Loops werden abgefangen .....	48
3.6.3	Probleme mit dem Spanning Tree .....	49
3.7	Layer II-Pakete .....	50
3.8	Anmerkungen zu den Geräten .....	51
3.9	Zum Weiterlesen .....	52
<b>4</b>	<b>Layer III – die Vermittlungsschicht .....</b>	<b>53</b>
4.1	Neue Adressen .....	53
4.1.1	Adressklassen .....	54
4.1.2	Subnetze .....	56
4.1.3	Besondere Adressen .....	57
4.2	Segmentierung der Netze .....	57
4.2.1	Wer gehört zu welchem (Sub-)Netz? .....	58
4.2.2	Kommunikation in und zwischen LANs .....	58



4.2.3	Die Subnetzmaske .....	58
4.2.4	Asymmetrische Segmentierung .....	61
4.2.5	Ermittlung des Netzes/Subnetzes .....	62
4.3	Der Router, Weiterleitung auf Layer III .....	64
4.3.1	Das Spiel mit den Layer II-Adressen .....	66
4.3.2	Router-Loopback-Adressen .....	69
4.4	Reservierte und spezielle Adressen .....	69
4.4.1	Multicast-Adressen/Testadressen .....	70
4.4.2	Private Adressen .....	70
4.4.3	APIPA – Automatic Private IP Addressing .....	70
4.4.4	Superprivate Adressen .....	71
4.5	Das IP-Paket .....	71
4.5.1	Das Verfallsdatum TTL .....	73
4.5.2	Fragmentierung von IP-Paketen, MTU .....	73
4.6	Routing – die weltweite Wegfindung .....	74
4.6.1	Distance Vector und Link State .....	74
4.6.2	Statisches und dynamisches Routing, nah und fern .....	75
4.6.3	Beeinflussung der Routen, Failover .....	76
4.7	QoS – Quality of Service .....	77
4.8	Das Domain Name System (DNS) .....	78
4.8.1	Zuordnung von Namen zu Adressen .....	79
4.8.2	Auflösung der Adressen, Forward Lookup .....	80
4.8.3	Auflösung der Namen, Reverse Lookup .....	81
4.8.4	Namen auflösen, nslookup .....	82
4.8.5	Automatische Vergabe von Adressen, DHCP .....	83
4.8.6	DHCP-Relay .....	84
4.8.7	Windows-Namen .....	85
4.9	Uni-, Broad- und Multicast .....	87
4.9.1	Broad- und Multicast auf Layer II und III .....	88
4.10	PING und TRACEROUTE – die kleinen Helfer .....	93
4.11	Zum Weiterlesen .....	94
<b>5</b>	<b>Layer IV – die Transportschicht .....</b>	<b>96</b>
5.1	Ports und Sockets .....	96
5.2	Das Transmission Control Protocol .....	98
5.2.1	Das TCP-Segment .....	98
5.2.2	TCP-Verbindungen .....	100
5.3	Das User Datagram Protocol .....	102
5.3.1	Das UDP-Datagramm .....	103
5.4	Security auf Layer III und IV, Router und Firewall .....	103
5.4.1	Unterschiede zwischen Router und Firewall .....	104
5.4.2	Zonen einer Firewall .....	104

5.4.3	Mehr Intelligenz bei der Weiterleitung/DMZ .....	105
5.4.4	Firewall-Philosophien .....	106
5.5	NAT, PAT und Masquerading .....	108
5.6	Zum Weiterlesen .....	110
<b>6</b>	<b>Virtuelle Netze und Geräte .....</b>	<b>111</b>
6.1	VLANs – virtuelle Netze .....	111
6.1.1	VLAN-Kennung, Tags .....	113
6.1.2	Trunks .....	114
6.1.3	Verkehr zwischen VLANs .....	115
6.1.4	VLAN-Transport, Trunk zum Router .....	117
6.1.5	Vorteile der VLANs .....	118
6.1.6	Grenzen der VLANs .....	119
6.1.7	Bemerkungen zu VLANs .....	119
6.1.8	Erweiterungen der VLAN-Umgebungen .....	121
6.1.9	Spanning-Tree .....	121
6.1.10	Pruning .....	121
6.1.11	Eigene IP-Adresse für Switches .....	122
6.1.12	Lernfähige Umgebungen .....	123
6.1.13	Delegation der VLAN-Verwaltung .....	124
6.1.14	Default/Native VLAN .....	124
6.1.15	Fazit .....	125
6.2	Virtuelle Geräte .....	126
6.2.1	Virtuelle Switches .....	126
6.2.2	Virtuelle Router und virtuelle Firewalls .....	127
6.3	Software defined Networks (SDN) .....	127
6.4	Cloud, Microsegmentation, volle Virtualität .....	128
6.5	Zum Weiterlesen .....	129
<b>7</b>	<b>VPN – virtuelle private Netzwerke .....</b>	<b>130</b>
7.1	Tunnel .....	130
7.1.1	Absicherung der Verbindung .....	132
7.1.2	Mechanismus .....	133
7.1.3	Split oder Closed Tunnel .....	133
7.1.4	Modi der Datenverschlüsselung .....	134
7.1.5	VPN durch Firewalls .....	134
7.1.6	Andere Tunneltechniken .....	134
7.2	Verschlüsselung .....	135
7.2.1	Symmetrische Verschlüsselung .....	135
7.2.2	Asymmetrische Verschlüsselung .....	136
7.2.3	Hybrid-Verschlüsselung .....	137
7.3	Zum Weiterlesen .....	138

<b>8</b>	<b>Wireless LAN</b>	<b>139</b>
8.1	Access-Points und Antennen, Anschlüsse	139
8.2	Störungen	140
8.2.1	Interferenzen, Mehrwegeausbreitung	140
8.2.2	Versteckte Endgeräte	141
8.2.3	Entstörung	141
8.3	Die Funkzelle und die Kanäle	142
8.4	Betriebsmodi	142
8.5	Namen, das Beacon	143
8.6	Verschlüsselung	144
8.7	Aufbau eines Infrastruktur-WLAN	144
8.8	Stromversorgung der Sender	146
8.9	Mesh	147
8.10	Wi-Fi und Proprietäres	148
8.11	Standards und Parameter	148
8.11.1	802.11	149
8.11.2	Bandspreizung	149
8.11.2.1	DSSS, Direct Sequence Spread Spectrum	150
8.11.2.2	FHSS	153
8.11.3	802.11b	153
8.11.4	802.11a	153
8.11.4.1	OFDM	154
8.11.5	802.11 h	154
8.11.6	802.11 g	155
8.11.7	802.11n, Wi-Fi 4	155
8.11.7.1	Antenna-Diversity	155
8.11.7.2	Gruppengewinn	156
8.11.7.3	MIMO, Multiple Input Multiple Output	156
8.11.7.4	Beamforming	157
8.11.7.5	Packet-Aggregation	157
8.11.8	802.11ac, Wi-Fi 5	157
8.11.9	802.11ax, Wi-Fi 6	158
8.11.10	802.11be, Wi-Fi 7	158
8.11.11	802.11ad	158
8.11.12	802.11ay	158
8.12	Powerline – eine Alternative	158
8.13	Zum Weiterlesen	159
<b>9</b>	<b>Netzzugang, Szenarien</b>	<b>161</b>
9.1	DSL/ADSL/VDSL	161
9.2	Breitbandkabel	162
9.3	Stand- oder Mietleitungen	162
9.3.1	Fiber to the Home	164

9.4	Satellit .....	164
9.5	Mobilfunk – das Handy-Netz .....	165
9.6	Gebäudeverbindungen .....	166
9.6.1	Richtfunkverbindungen .....	166
9.6.2	Richtlaser .....	166
9.7	Hardware .....	167
9.8	Zum Weiterlesen .....	168
<b>10</b>	<b>IP Version 6 (IPv6) .....</b>	<b>169</b>
10.1	Die IPv6-Adresse .....	169
10.2	Adressierung .....	171
10.2.1	Unicast-Adressen .....	171
10.2.1.1	Link Local Unicast-Adresse .....	171
10.2.1.2	Global Unicast-Adresse .....	172
10.2.1.3	Unique Local Unicast-Adresse .....	172
10.2.1.4	Unspecified-Adresse .....	172
10.2.1.5	Loopback .....	172
10.2.1.6	IPv4-kompatible Adressen .....	172
10.2.1.7	IPv4-Mapped-Adressen .....	172
10.2.2	Multicast-Adressen .....	173
10.2.2.1	Solicited-Node Multicast-Adresse .....	173
10.2.3	Anycast-Adressen .....	174
10.3	Adress-Zoo – welche sind notwendig? .....	174
10.4	Interface-ID .....	175
10.5	Privacy-Extension .....	176
10.6	ICMPV6 .....	176
10.6.1	Nachbarermittlung, NDP .....	177
10.6.1.1	Router Advertisements und Solicitation .....	177
10.6.1.2	Neighbor Advertisements und Solicitation .....	178
10.6.2	Adress-Caches .....	179
10.6.2.1	Neighbor-Cache .....	179
10.6.2.2	Destination-Cache .....	179
10.7	Zusammenfassung der IPv6-Adressen .....	179
10.8	Adressvergabe .....	180
10.8.1	Feste Konfiguration .....	180
10.8.2	DHCPv6, Stateful Autoconfiguration .....	180
10.8.3	Autokonfiguration, Stateless Autoconfiguration .....	180
10.8.3.1	Automatische Adressvergabe .....	180
10.8.3.2	DAD, Duplicate Address Detection .....	180
10.8.4	Adresszustand .....	181
10.9	Umnummerierung eines Netzes .....	181
10.10	MTU .....	181

10.11	Router-Redirection .....	182
10.12	Das IPv6-Paket .....	182
10.13	VPN in IPv6 .....	183
10.14	Quality of Service .....	183
10.15	Kommunikation beider Welten .....	184
10.15.1	Encapsulierung .....	184
10.15.2	Fixe und dynamische Tunnel .....	184
10.15.3	Fix, Gateway-to-Gateway-Tunneling .....	185
10.15.4	Automatische Tunnel .....	185
10.15.4.1	6to4 .....	185
10.15.4.2	ISATAP .....	186
10.15.4.3	Teredo .....	186
10.16	DNS in IPv6 .....	188
10.17	DHCPv6 .....	188
10.18	Zusammenfassung .....	189
10.19	Zum Weiterlesen .....	189
<b>11</b>	<b>Netzwerkspeicher .....</b>	<b>191</b>
11.1	Dateiübertragung, TFTP und FTP .....	191
11.1.1	TFTP – Trivial File Transfer Protocol .....	192
11.1.2	FTP – File Transfer Protocol .....	192
11.2	Filesharing .....	195
11.2.1	DAS – Direct Attached Storage .....	195
11.2.2	NAS – Network Attached Storage .....	195
11.2.2.1	NFS – Network File System .....	196
11.2.2.2	SMB – Server Message Block .....	196
11.2.3	WebDAV .....	198
11.3	SAN – Storage Area Network .....	199
11.4	Zum Weiterlesen .....	202
<b>12</b>	<b>Repetitorium und Verständnisfragen .....</b>	<b>203</b>
12.1	Einführung .....	203
12.2	Layer I .....	204
12.3	Layer II .....	207
12.4	Layer III .....	209
12.5	Layer IV .....	213
12.6	Allgemeines .....	215
12.7	IP Version 6 .....	217
<b>13</b>	<b>Praxis/Übungen .....</b>	<b>219</b>
13.1	ARP-Requests .....	220
13.2	Kommunikation auf Layer III .....	224

13.3	Layer II-Loop-Probleme .....	225
13.4	Die Subnetzmaske .....	227
13.5	Das Default Gateway .....	229
13.6	Nameserver .....	232
13.7	Routen prüfen .....	235
13.8	Prüfen der Verbindungen auf Layer IV .....	236
13.9	APIPA-Adressierung .....	240
13.10	Das Kernel-Routing .....	240
13.10.1	Die Routing-Tabelle .....	240
13.10.2	Beeinflussen des Routings .....	242
13.10.3	Mehrere Netzwerkadapter .....	243
13.11	Genau hineingesehen – der Network Analyzer .....	246
13.11.1	ARP-Request .....	247
13.11.2	Telnet-Session .....	248
13.12	IPv6 .....	250
<b>Anhang .....</b>		<b>255</b>
<b>14</b>	<b>Exkurse .....</b>	<b>257</b>
14.1	Exkurs in die Zahlensysteme: Bit, Byte, binär .....	257
14.1.1	Binär ist nicht digital .....	257
14.1.2	Bit und Byte .....	258
14.2	Zahlensysteme in der Computerwelt .....	258
14.2.1	Das Dezimalsystem .....	258
14.2.2	Das Binärsystem .....	259
14.2.3	Das Hexadezimalsystem .....	259
14.2.4	Umrechnung der Systeme .....	260
14.3	Beispiel eines Routing-Vorganges .....	263
14.4	PXE .....	266
14.5	Voice over IP .....	268
14.5.1	VoIP im Privatbereich .....	268
14.5.2	VoIP im Firmenbereich .....	269
<b>15</b>	<b>Szenarien, Planung, Beispiele .....</b>	<b>271</b>
15.1	Netzwerke im privaten Bereich .....	271
15.2	Büros und Kleinfirmen .....	273
15.3	Mittlere und größere Firmen .....	274
15.4	Planung eines Netzwerkes .....	275
15.4.1	Verkabelung .....	275
15.5	Der Strom .....	278
15.6	Klima .....	279
15.7	Impressionen .....	279

<b>16</b>	<b>Steckertypen</b>	<b>291</b>
16.1	Thin-Wire	291
16.2	UGV	292
16.3	Glasfaser	293
16.3.1	ST-Stecker (Straight Tip)	293
16.3.2	SC-Stecker	294
16.3.3	MT-RJ-Stecker	295
16.3.4	LC-Stecker	295
16.3.5	E2000-Stecker	295
16.4	Bemerkungen zu Steckertypen	296
16.5	Schutz der Patchkabel und Dosen	296
<b>17</b>	<b>Fehleranalyse</b>	<b>298</b>
17.1	Ein Rechner oder mehrere sind nicht am Netz	298
17.2	Alle Rechner sind nicht am Netz	300
17.3	Router prüfen	301
17.4	Einige Rechner ohne Internet	301
17.5	Netzwerk ist langsam	302
	<b>Abkürzungsverzeichnis</b>	<b>303</b>
	<b>Index</b>	<b>307</b>





# Vorwort

Noch ein Buch über Netzwerke? In jeder Buchhandlung gibt es sie bereits meterweise. Aber dieses Buch unterscheidet sich von den anderen und hat eine besondere Geschichte. Der beste Aspekt daran ist, dass es nicht geplant war. Beruflich arbeite ich sehr viel mit Computerbetreuern zusammen, in allen Schattierungen der Ausbildung und des Wissensstandes, von Hilfsassistenten ohne Computererfahrung bis hin zu professionell ausgebildeten Fachkräften.

Wenn diese Probleme haben, die sie nicht lösen können oder Beratung brauchen, wenden sie sich an mich. Und dies in einer völlig inhomogenen Umgebung, mit Windows, Linux, MacIntosh, Sun, etc. Die Fluktuation ist sehr groß, in großen Teilen der Umgebung muss das Rad ständig neu erfunden werden.

Im Laufe der Jahre fiel mir auf, dass immer wieder dieselben Fragen, immer wieder Verständnisprobleme an denselben Stellen auftreten. Weshalb? Netzwerke sind heute eine unglaublich komplexe Angelegenheit. Aber wie der Computer selbst, finden sie immer mehr Einzug auch in Privathaushalte. Längst ist die Zeit vorbei, in der es zu Hause nur wenige Rechner gab. Längst sind wir so weit, dass viele Haushalte mehrere Computer besitzen und untereinander Daten austauschen und ans Internet wollen. Viele Spiele sind netzwerkfähig geworden, Drucker, Faxgeräte und Scanner werden gemeinsam genutzt. Oft ist es kein Problem, ein paar Rechner zusammenzuhängen und ein kleines Netzwerk zum Laufen zu bekommen. Aber wenn es Probleme gibt, sind die meisten verloren.

Ebenso ist in kleineren und mittleren Unternehmen (oft durch die Aufgabentrennung in großen Unternehmen ebenso) das IT-Personal meist auf die Betreuung der Rechner und Server ausgerichtet. Das Netzwerk wird meist eingekauft und als Black-Box betrieben. Netzwerke sind oft ein „Buch mit sieben Siegeln“ und eine Infrastruktur, die wie das Telefon behandelt wird. Jeder verlässt sich darauf, aber wenn es nicht funktioniert, ist die Katastrophe da. Oft wird „gebastelt“, bis es irgendwie funktioniert, ohne darüber nachzudenken, dass es noch viel besser sein könnte, performanter und stabiler und nicht nur einfach funktionieren kann.

Im Bereich Netzwerk gibt es eine unheimliche Grauzone des Halbwissens. Ähnliches sieht man bei den Betriebssystemen. CD rein, Setup angeklickt, 15mal „OK“ gedrückt und der Rechner läuft – solange, bis es Probleme gibt.

Viele sind sehr interessiert am Thema Netzwerk. Der Einstieg aber ist schwer, das Thema ist keine Wochenendsache und meist fehlen die Ansprechpartner. Beklagt wird von den meisten, dass es auf dem Markt entweder Bücher gibt, die nur sehr oberflächlich sind, oder aber sofort auf einen Level gehen, in dem der Einsteiger verloren ist. Weiter sind sehr viele

Bücher zu einem hochspeziellen Thema geschrieben worden und erlauben so nur den Einstieg in kleine Teilbereiche. Oft ist die Sicht der Lehrbücher herstellerbezogen. Linux-Netzwerke, Windows-Netzwerke, meist Nebenskapitel in Büchern über die Betriebssysteme selbst. Oder es sind Bücher von Herstellern der Netzwerkgeräte, die detailliert das Feature-set und die Konfiguration beschreiben.

Sicher sind diese Bücher sehr gut – aber nicht für einen Einstieg geeignet. Sie behandeln speziell die Konfigurationen und Möglichkeiten ihrer Geräte und Umgebungen – und nicht der Standards. Auch sind sie nicht für einen Heimanwender geeignet, der mehr verstehen will, und ebenso nicht für eine Firmenleitung oder IT-Abteilung kleiner und mittlerer Umgebungen, die strategisch entscheiden müssen, welchen Weg sie im Bereich Netz gehen wollen.

Dieselbe Erfahrung musste ich selbst machen, als ich erstmalig mit dem Thema Netzwerke konfrontiert wurde. Es gibt viele gute Kurse und Ausbildungen, meist von den Herstellern der Geräte. Eine Privatperson oder kleine Firma kann aber nicht tausende Euro bezahlen, aus einfachem Interesse. Immer wieder erkläre ich dasselbe neu. Und oft hörte ich: „Kannst Du mir nicht ein Buch empfehlen, das wirklich einen Einstieg erlaubt? Das soviel Grundwissen vermittelt, dass man versteht, wie das alles funktioniert, aber auf einer für jedermann verständlichen Basis? Ohne aber nur oberflächlich zu sein? Das ein breites Spektrum des „Wie“ bietet, verstehen lässt und den „Aha-Effekt“ auslöst?“

Ein Bekannter, der gutes Computer-, aber kein Netzwerk-Know-how hatte, bat mich, ihn ins Thema Netzwerke einzuweisen. Wir trafen uns eine Weile regelmäßig und ich überlegte mir, wie ich ihn an das Thema heranbringen kann. Aus diesen Notizen, „Schmierzetteln“ und Zeichnungen stellte ich eine kleine Fibel zusammen. Weiter fand ich Interesse in einem Computer-Verein, baute die Unterlagen aus und hielt den ersten „Netzwerkkurs“. Die Resonanz war enorm. Nie hätte ich gedacht, dass so viele Interesse haben. Vom Schüler, der seine PCs zum Spielen vernetzen will, über den KMU-Besitzer, der Entscheidungsgrundlagen sucht, bis zum IT-Spezialist, der über den Tellerrand schauen wollte, war alles vertreten.

Die Teilnehmer brachten mich auf die Idee, aus den Unterlagen ein Buch zu machen. Dies ist die Geschichte dieses Buches. Das Ziel ist, dem Leser zu ermöglichen, Netzwerke wirklich zu verstehen, egal ob in großen Umgebungen oder zu Hause. Das Ziel ist, soviel Know-how zu erarbeiten, dass der Interessierte versteht, wie es funktioniert und aufbauen kann, und der Einsteiger, der in Richtung Netz gehen will, das Handwerkszeug bekommt, um tiefer einzusteigen und sich an die „dicken Wälzer“ zu wagen. Gezeigt wird, wie es wirklich funktioniert, wie es strukturiert ist und welche großen Stolperfallen es gibt. Genauso soll der Leser in der Terminologie firm werden.

Ein interessierter Einsteiger will nicht 200 Seiten Kommandozeile eines Routers lesen, sondern verstehen, was ein Router wirklich ist. Ist es sein Job oder Interesse, soll er dann nach der Lektüre dieses Buches in der Lage sein, die Erklärungen dieser Kommandozeile sofort zu verstehen. Das Hauptziel dieses Buches sind die Grundlagen und ihr Verständnis. Wer die Grundlagen verstanden hat, dem fügt sich alles wie ein Puzzle zusammen. Leider wird darauf in der Literatur zu wenig eingegangen. Diese Lücke will das Buch schließen. Ein gutes Fundament, Verständnis und „wirklich verstehen“ ist der Leitfaden. Am Ende soll der Leser qualitativ, aber nicht oberflächlich, alle Informationen und Zusammenhänge kennen, wird arbeitsfähig sein, in der Terminologie firm und bereit für den nächsten Schritt. Die Grundlagen werden mit Absicht ziemlich tief behandelt, denn ein Verstehen der Basis ist

immer Voraussetzung für ein fundiertes Wissen. Dies ist in jedem komplexen Thema so. Daher gibt es einige Exkurse in die Physik und Mathematik. Das hört sich abschreckend an, sie sind aber, so hoffe ich, für jeden verständlich gehalten.

Das Buch wurde bewusst als ein Buch zum Lesen geschrieben. Trockene Theorie, die manchen bekannt ist, manchen nicht, habe ich als Exkurse an das Ende des Buches ausgelagert, um den Fluss nicht zu stören. Wer diese Grundlagen nicht hat, ist gebeten, sich die Mühe zu machen, diese Exkurse zur richtigen Zeit zu lesen; es wird im Text jeweils darauf verwiesen. Ich rate dazu, das Buch nicht einfach wie einen Roman zu lesen, sondern sehr bewusst und kapitelweise. Es stecken viele Informationen in sehr kompakter Form darin. Man ist leicht versucht, es in einem Zug zu lesen, doch wird dabei eine Menge untergehen. Ein Repetitorium und Fallbeispiele geben am Ende die Möglichkeit, mit dem Erlernten umzugehen.

Zum Schluss möchte ich nicht versäumen, einigen Personen zu danken, die einen großen Anteil am Entstehen der Unterlagen beziehungsweise des Buches hatten: Herrn Prof. Dr. F. Rösler für die Chancen und die Möglichkeit der Weiterbildungen; Herrn Dr. H. Schwedes für die Korrekturlesung und die wertvollen Anregungen; der Linux Usergroup Lörrach e. V. für das tolle Feedback; Herrn H. Volz für die akribische fachliche Korrekturlesung und seine Anmerkungen; Herrn Dr. P. Zimak für die stets offene Türe und die vielen beantworteten Fragen in den letzten Jahren; und nicht zuletzt ganz besonders meiner Familie für die gestohlene Zeit.

Das Buch ist aus den Erfahrungen in Jahren der Praxis entstanden – es ist ein Buch der Praxis und ein dynamisches Buch, das aus ständigem Feedback gewachsen ist. In diesem Sinne wünsche ich Ihnen möglichst großen Gewinn und viel Spaß bei seiner Lektüre. Eines haben mir die bislang abgehaltenen Netzwerkurse und Diskussionen gezeigt: Ein so trockenes Thema wie Netzwerke kann auch Spaß machen! Interessant ist es allemal.

*Lörrach, im Oktober 2005*

*Rüdiger Schreiner*

## **Vorwort zur achten Auflage**

„Computernetzwerke“ von Rüdiger Schreiner – ein Buch, das Generationen von Auszubildenden und Studierenden einen einfachen Einstieg in die Welt der Netzwerke ermöglicht hat und daher durchaus als Standardwerk bezeichnet werden darf. Umso mehr fühle ich mich geehrt, dass man mir das Vertrauen geschenkt hat, das Buch für die achte Auflage zu aktualisieren.

Seit der ersten Auflage sind fast 18 Jahre vergangen. Im Zeitalter der Computernetzwerke sind das Jahrhunderte! Kaum ein Gebiet ist einem so schnellen Wandel unterworfen. Und so ist es in der Geschichte des Buches nicht selten vorgekommen, dass Technologien und Trends, die in einer Auflage als „die Zukunft“ angekündigt wurden, beim Erscheinen der nächsten Auflage bereits Standard oder gar veraltet waren.

Ein Überblick über die historische Entwicklung der Computernetze mit allen jemals relevanten Technologien hat sicherlich seinen eigenen Wert. In einer zu großen Häufung werden Ausführungen zu historischen Technologien aber schnell als Ballast empfunden – gerade in einem Buch, das in die Materie einführen soll. Aus diesem Grund habe ich mich von manchen Themen getrennt.

Bei der Aktualisierung anderer Themen habe ich darauf geachtet, die für eine Einführung in die Materie wesentlichen Aspekte hervorzuheben. Damit erfüllt das Buch weiterhin seinen Zweck, einen niederschweligen Einstieg in die Thematik zu bieten. Spezialliteratur zu einzelnen Themen findet sich an anderer Stelle. Auf diese wird in den zentralen Kapiteln des Buches verwiesen.

Den Lesern der Voraufgaben danke ich für ihre Hinweise und Korrekturen. Allen Lesern der 8. Auflage wünsche ich viel Freude bei der Lektüre und würde mich natürlich über erneutes Feedback freuen.

*Offenburg, im Juli 2023*

*Oliver P. Waldhorst*

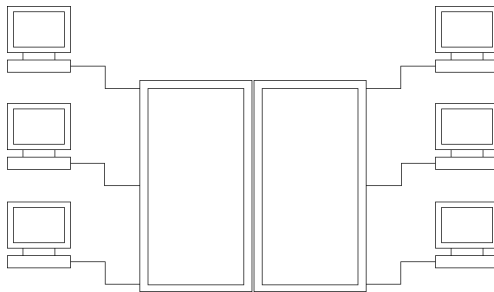
# 1

# Zur Geschichte der Netzwerke

## ■ 1.1 Netzwerke – der Beginn

In der Anfangszeit der Datenverarbeitung standen zentrale Rechner im Mittelpunkt, die von wenigen Spezialisten betrieben werden konnten. In Firmen, Institutionen und Universitäten wurden die Daten auf- und vorbereitet und dann zentral im Großrechner verarbeitet. Meist waren die Systeme und Programme proprietär, der Weg der Daten war denkbar umständlich. Die meisten Daten mussten in Form von Papier oder mobilen Datenträgern zur Zentraleinheit gebracht, eingegeben und die Ergebnisse nach der Verarbeitung ebenso wieder abgeholt werden.

Die Programme zur Verarbeitung der Daten wurden meist selbst geschrieben und auf Lochkarten, Lochstreifen, etc. encodiert und jeweils vor der Verarbeitung der Datensätze in das System eingelesen.



**Bild 1.1** Ein Terminalsystem: An einer großen Zentraleinheit, welche die gesamte „Intelligenz“ beherbergte, waren Terminals ohne eigene Intelligenz angeschlossen. Somit hatte jeder Zugriff auf die vom Großrechner gebotenen Ressourcen.

Eine erste Abhilfe brachten Terminalsysteme. Hier wurden Terminals (im Prinzip nur ein Monitor und eine Tastatur) ohne eigene Intelligenz an Großrechner angeschlossen und boten so einen Zugriff auf die Ressourcen bis hin zum Arbeitsplatz an (zum Beispiel IBM, Digital und Siemens).

Mit der beginnenden Entwicklung der Personal Computer (PC) kam die eigene Verarbeitungskapazität bis an den Arbeitsplatz heran.

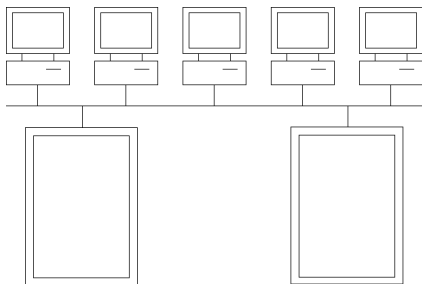
Vor allem aus Kostengründen wurde sofort die Frage nach einer gemeinsamen Nutzung von Ressourcen laut (ein Laserdrucker kostete 1985 noch über DM 20 000). Auch war es relativ umständlich, die Daten auf einem PC zu erzeugen und dann per Diskette oder als Ausdruck weiterzugeben.

Dazu kommt noch, dass nun Dinge wie die Datensicherung, die Benutzerverwaltung und die Systempflege auf jedem Rechner einzeln durchgeführt werden mussten, was einen sehr großen Aufwand an Administration darstellte. Was früher zentral am Großrechner administriert wurde, musste nun an jedem Arbeitsplatz einzeln bewältigt werden. Die Lösung war die Vernetzung. Sie bot Datenaustausch und -sicherung, Ressourcenteilung, zentralisierte Userverwaltung und -authentifizierung in einem an.

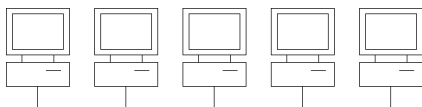
Mit der zunehmenden Kommunikationsfähigkeit und Leistungskapazität der PCs wurde ein Ende der zentralen Großrechner vorausgesagt. Heute ist jedoch der gängige Zustand eine Koexistenz beider. Im Netzwerk untereinander erreichbar bieten Großrechner enorme Rechenkapazitäten, Fileserver zentrale Datenhaltung und -sicherung sowie Printserver, Faxserver etc. eine gemeinsame Ressourcennutzung an. Die Arbeitsplatzstationen als Ersatz der „dummen“ Terminals bieten dabei aber genug „Intelligenz“ für die täglichen Anwendungen vor Ort ohne Belastung des Zentralsystems an.

Das frühere Sternsystem, Zentraleinheit und sternförmig angeschlossene Datenterminals und das Peer-to-Peer-Netzwerk, ein vermaschter Netzwerkverbund von gleichwertigen Stationen, sind in heutigen Client-Server-Umgebungen zusammengefloßen.

In vielen Fällen tendiert man heute wieder dazu, Dienste auf Servern zu konsolidieren. Die Leistungsfähigkeit der Server ist enorm gestiegen, Terminalsysteme sind heute fast für alle Betriebssysteme erhältlich.



**Bild 1.2** Ein heterogenes Netzwerk: Hier sind Clients und Server miteinander vernetzt. Die Server bieten spezielle Dienste an, die von allen genutzt werden können.



**Bild 1.3** Ein Peer-to-Peer-Netzwerk. Gleichwertige Stationen sind untereinander vernetzt.

Im Laufe der Jahre wurden immer mehr dieser isolierten Netzwerke (Intranets) an das weltweite Internet angeschlossen. Ein Austausch von Daten ist daher weltweit möglich. Mehr zum Thema Internet folgt weiter unten.

## ■ 1.2 Definition eines Netzwerkes

Was ist denn nun ein Netzwerk? Der Begriff Netzwerk umfasst nicht nur die Welt der Computer. Das weltweite Telefonnetz, das ISDN, der Verbund der Bankautomaten etc. sind ebenfalls Informationsnetzwerke.

Generell lässt sich daher definieren:

*Ein Netzwerk ist eine Infrastruktur, die Datenendgeräten die Kommunikation, den Datenaustausch und die Nutzung gemeinsamer Ressourcen transparent ermöglicht.*

Transparent bedeutet, der Endbenutzer muss sich nicht darum kümmern, mithilfe welcher Verfahren, Geräte und Medien die Informationen transportiert werden.

Hier in diesem Buch wollen wir uns mit Computernetzwerken beschäftigen, obwohl durchaus Überschneidungen auftreten, zum Beispiel bei PPP (Point to Point Protocol, siehe unten), dem Netzwerkzugang über den Telefonanschluss und ein Modem. Hier benutzt das Computernetzwerk die Infrastruktur des Telefonienetzwerkes zur Datenübertragung.

Was muss beachtet werden, um eine bestehende Netzwerkinfrastruktur ausnutzen zu können? Welche verschiedenen Geräte und Medien sind im Einsatz, und was muss dabei berücksichtigt werden? Die Technik, die Geräte, die Verkabelung und die Softwareparameter, die im alltäglichen Gebrauch verwendet werden, stehen im Vordergrund dieser Einführung. Ebenso die Terminologie. Es gilt, in den gängigen Fachbegriffen firm zu werden. Das Ziel ist es, einen Einstieg in die Materie Netzwerk zu bekommen, der es ermöglicht, je nach Interesse, in die vielen verschiedenen Facetten des Themas tiefer einzusteigen. Die Frage „Wie funktioniert es?“ steht im Vordergrund, ebenso und vor allem auch das Verstehen der Grundlagen.

Im Laufe der Jahre wurden nun viele Typen von Netzwerken entwickelt, meist isoliert und herstellerabhängig. Mit der Einführung der (welt-)weiten Verbindungen mussten Standards ausgearbeitet werden, die entweder eine weltweite Konvergenz herbeiführten oder eine Übersetzung der Verfahren ermöglichten. Dies gilt für den physikalischen Aufbau (Netzwerkgeräte, Verkabelung etc.) genauso wie für die Datenformate.

## ■ 1.3 Das OSI-Modell

1984 entwickelte die ISO (International Standardization Organisation) ein umfassendes Modell für die Kommunikation unter Computern, das OSI-Referenzmodell (Open Systems Interconnection). In diesem wird die Kommunikation zwischen Rechnern in sieben in sich abgeschlossene Schichten aufgeteilt. Jede Schicht kann somit einzeln weiterentwickelt werden, ohne die gesamte Kommunikation zu beeinflussen.

**Tabelle 1.1** Das OSI-Modell in der Übersicht: Jede Zeile beschreibt einen Layer des Modells.

Layer VII	Anwendungsschicht	(Application)
Layer VI	Darstellungsschicht	(Presentation)
Layer V	Kommunikationsschicht	(Session)
Layer IV	Transportschicht	(Transport)
Layer III	Vermittlungsschicht	(Network)
Layer II	Sicherungsschicht	(Data Link)
Layer I	Physikalische Schicht	(Physical)

Für den Netzwerker sind die Schichten eins bis vier essenziell. Sie regeln die Datenübertragung an sich, die Schichten fünf bis sieben sind anwendungsbezogen. Pro Schicht sind viele verschiedene Standards implementiert.

Wichtig ist im OSI-Modell, dass die Kommunikation zwischen Rechnern und zwischen den Schichten geregelt ist. Ob PC 1 nun eine andere Implementierung von Layer I benutzt als PC 2, muss für die anderen Schichten bedeutungslos sein. Genauso muss es egal sein, ob die Maschinen Unix, Mac OS, Windows oder ein anderes Betriebssystem benutzen.

## ■ 1.4 Übersicht über das OSI-Modell

Zu Beginn ein kleiner Vorgriff. Der Leitfaden für den Einstieg in das Netzwerk wird das OSI-Modell sein, Layer für Layer. Daher ein kurzer Überblick. Einige Parameter sind sicher bekannt. Wie sie zusammenhängen, werden wir Schritt für Schritt erarbeiten.

Das OSI-Modell ist sehr wichtig. Im Umfeld der Netzwerker ist es eine Arbeitsschablone. Netzwerker reden von „Layer II-Problemen“, „Layer III-Grenzen“ etc. Man sollte daher auf jeden Fall in diesem Modell firm sein. Aber genauso muss man immer bedenken, dass das OSI-Modell ist, was sein Name besagt – ein Modell. Es ist nirgends genau implementiert, es gibt etliche Abweichungen und Ausnahmen.

Es hilft uns aber, die Zusammenhänge zu verstehen, und wir begehen keinen Fehler, zuerst einmal anzunehmen, alles würde OSI-konform verlaufen.

### 1.4.1 Layer I – die physikalische Schicht (Physical)

Hier sind, wie schon der Name sagt, die physikalischen Parameter definiert. Dazu gehören die Kabeltypen, die Anschlüsse, die Streckenlängen, die elektrischen Eckdaten wie Spannungen, Frequenzen etc. Getrennt wird hier in drei Bereiche:

- Der Nahbereich (LAN, Lokal Area Network, meist in einem Gebäude),
- mittlere Entfernungen (MAN, Metropolitan Area Network, meist Gebäudeverbindungen) und
- die Fernverbindungen (WAN, Wide Area Network, Fernstrecken bis weltweit).





Beispiele für die Standards im Layer I sind zum Beispiel verschiedene Übertragungsmedien wie Kupferkabel, Glasfaser, Richtfunk, Signalform und Frequenzen im Medium.

### 1.4.2 Layer II – die Sicherungsschicht (Data Link)

Die Sicherungsschicht ist für eine zuverlässige Übertragung der Daten zuständig. Sie regelt die Flusssteuerung, regelt den Zugriff, verhindert eine Überlastung des Empfängers und ist für die physikalische Adressierung innerhalb eines Netzsegmentes (siehe unten) auf dieser Schicht verantwortlich. Hier ist die erste Fehlererkennung implementiert. Die Topologie eines Netzwerkes ist stark von dieser Schicht abhängig, sie definiert die Art und Weise, wie die Rechner und Netzwerkgeräte miteinander verbunden sind.



Ein Beispiel im Layer II sind Hardwareadressen.

### 1.4.3 Layer III – die Vermittlungsschicht (Network)

In Schicht drei des OSI-Modells wird die logische Adressierung (segmentübergreifend bis weltweit) der Geräte definiert. Die Routing-Protokolle dieser Schicht ermöglichen die Wegfindung in großen (bis weltweiten) Netzwerken und redundante Wege ohne Konflikte. Routing-Protokolle sorgen ebenfalls dafür, dass die Ressourcen in vermaschten Netzen mit vielen redundanten Wegen bei dem Ausfall einer Verbindung weiterhin benutzt werden können.



Quality of Service (QoS), Routing und das IP-Protokoll sind Beispiele im Layer III.

### 1.4.4 Layer IV – die Transportschicht (Transport Layer)

Die Transportschicht beschreibt Mechanismen für den Datentransport zwischen Anwendungen und Prozessen auf verschiedenen Endgeräten. Die Schicht vier regelt das Datenmultiplexing und die Flusskontrolle, das heißt, mehrere Anwendungen höherer Protokolle können gleichzeitig Daten über eine Netzwerkverbindung transportieren. In der Transportschicht sind verbindungslose und verbindungsorientierte Dienste implementiert. Der Begriff Verbindung bezieht sich dabei auf eine logische Verbindung zwischen zwei Anwendungen bzw. Prozessen. Verbindungsorientierte Dienste können einen zuverlässigen Datenaustausch durchführen. Der Sender und der Empfänger kontrollieren ihre Möglichkeiten der Kommunikation (Aufbau einer logischen Verbindung), die Daten werden erst nach dieser Prüfung versandt. Eine weitgehende Fehlerkontrolle prüft die Daten und for-

dert entweder verlorene oder korruptierte Daten zur erneuten Übersendung an. Am Ende der Kommunikation wird die Verbindung gezielt und kontrolliert wieder abgebaut. Verbindungslose Dienste verzichten auf den Verbindungsaufbau und -abbau sowie auf die Wiederholung der Übertragung verlorener oder korruptierter Pakete. In der Regel führen sie dennoch eine Fehlerkontrolle durch. Dabei werden fehlerhafte Daten nicht erneut angefordert, sondern stillschweigend verworfen und nicht an höhere Schichten weitergegeben. Im Layer IV wird nach definierten Anwendungen unterschieden. Hier beginnt die Kommunikation zwischen dem Netzwerk und der Anwendung.



Beispiele im Layer IV sind etwa das TCP- oder das UDP-Protokoll.

### 1.4.5 Layer V – die Kommunikations-/Sitzungsschicht (Session)

Die Kommunikationsschicht ist hauptsächlich eine „Serviceschicht“ für die bidirektionale Kommunikation von Anwendungen in verschiedenen Endgeräten. Sitzungen und Datenströme werden angefordert, aufgebaut, kontrolliert und koordiniert. Meist bedienen sich die Services der Schicht V dabei der Dienstangebote der Schicht IV.



Ein Beispiel im Layer V ist unter anderem das SMB-Protokoll zum Drucken und zum Verbinden mit Windows-Freigaben.

### 1.4.6 Layer VI – die Darstellungsschicht (Presentation)

Die Darstellungsschicht sorgt dafür, dass die Daten so bearbeitet werden, dass sie optimal ausgetauscht und verarbeitet werden können. Hierfür gibt es etliche standardisierte Kodierungs-, Konvertierungs- und Kompressionsverfahren, zum Beispiel für Verschlüsselungsroutinen, Zeichendarstellungen, Video- und Audioübertragungen.



Beispiele im Layer VI sind Standards wie MPEG, TIFF, GIF und ASCII.

### 1.4.7 Layer VII – die Anwendungsschicht (Application)

Die Anwendungsschicht interagiert direkt mit der Software (Anwendung), die eine Netzwerkübertragung anfordert. Sie ermittelt, ob die Möglichkeit einer Verbindung besteht, und identifiziert und sucht Ressourcen.

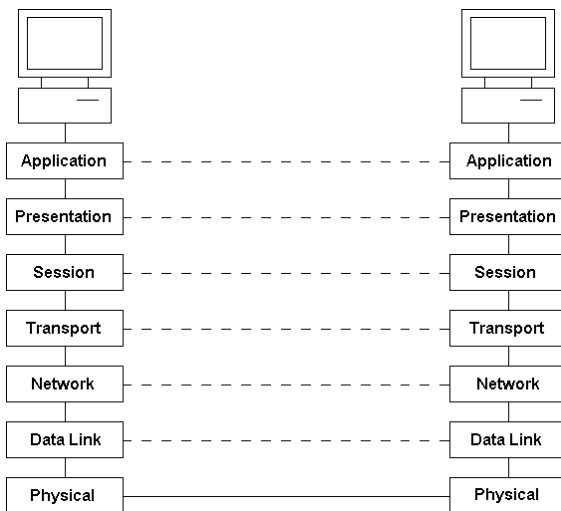


Beispiele im Layer VII sind verteilt arbeitende Server-Client-Lösungen sowie Kontroll- und User-Interfaces.

## ■ 1.5 Übertragungswege im OSI-Modell

Das OSI-Modell selbst bietet natürlich keine Möglichkeit, Daten auszutauschen, sondern liefert die Rahmenbedingungen, mit denen ein Datenaustausch unter den verschiedensten Systemen reglementiert wird. Die Datenübertragung wird von den Implementierungen der Regeln durch die Hersteller innerhalb der Schichten mittels Protokollen vorgenommen.

Ein Protokoll ist also nichts anderes als eine Aufstellung von definierten Regeln zur Kommunikation. Dabei kommuniziert eine Schicht virtuell mit derselben Schicht (Anwendung/Protokoll) auf dem Kommunikationspartner. Der wirkliche Weg der Daten ist von oben durch die Schichten bis nach unten auf Layer I, dann die Übertragung über das Medium und beim Empfänger wieder vertikal nach oben.



**Bild 1.4** Die virtuelle (gestrichelt) und die echte Kommunikation: Jede Schicht kommuniziert scheinbar mit derselben auf dem Partner. In Wirklichkeit aber verläuft die Kommunikation vertikal durch alle Schichten nach unten, die Daten werden über die physikalischen Medien versendet und nehmen ihren Weg dann wieder vertikal bis zum Ziel.

Der große Vorteil ist, sofern sich die Hersteller an die Standards und Schichtung halten, dass jeder, der einen Dolmetscher für seine eigene Art der Implementierung eines Layers anbietet, mit allen anderen kommunikationsfähig bleibt.

So ist es möglich, dass Apple-Computer, Intel-basierte Computer unter Windows oder Linux, Unix-Computer unter Solaris, DEC-Unix etc. untereinander kommunizieren, Daten austauschen und gemeinsame Ressourcen anbieten und nutzen können.

Jede Schicht verpackt das Datenpaket, das sie von einer höheren zur Weiterverarbeitung bekommt, in ein eigenes „Kuvert“ und reicht es eine Schicht weiter.

Beim Empfänger läuft es genau andersherum. Jede Schicht entfernt ihr Kuvert und reicht das Paket nach oben weiter. Schicht vier zum Beispiel ist dabei absolut uninteressiert daran, was vorher für eine Verpackung um das Paket war und über welches Medium es transportiert wurde. Sie interessiert es auch nicht, was als Inhalt im Paket ist, lediglich das „Kuvert Schicht vier“ ist für sie von Bedeutung. So wird deutlich, wie die Interkommunikation unter den verschiedensten Plattformen und Systemen möglich wird. Sind die Protokolle korrekt implementiert, steht der Kommunikation nichts mehr im Wege.

Sind zwei völlig inkompatible Netze zu verbinden, muss ein Gerät dazwischengeschaltet werden, das eine Übersetzung vornimmt, bis zu der Schicht, die wieder gleich implementiert ist. Ein Beispiel auf Layer I ist ein Medienkonverter, der z.B. ein Kupfer- mit einem Glasfasernetz verbindet. Ein Beispiel auf Layer II ist ein Access Point, der ein WLAN-Netz mit Ethernet verbindet.

Ab dieser Übersetzung ist der Weg wieder völlig gleich. Die höheren Schichten bekommen von dieser Übersetzung nichts mit (ebenso der Anwender/User). Aber nochmals sei betont, das OSI-Modell ist ein Modell und so gut wie nirgends absolut starr implementiert. Es ist unser Leitfaden und eine Vorgabe für die Hersteller.

Als Beispiel kann der Brief verschiedener Bittsteller an den Präsidenten der Vereinigten Staaten gelten. Einmal kommt er von einer einsamen Insel, einmal aus einer Großstadt. Der Großstädter schreibt seinen Brief und wirft ihn frankiert in den nächsten Postkasten. Die Post befördert ihn über diverse Sortier- und Verteilerstellen per Bahn, LKW oder Flugzeug nach Washington und liefert ihn aus. Die Antwort des Präsidenten nimmt denselben Weg in die andere Richtung.

Der Inselbewohner geht dann zum örtlichen Telegrafenamts, von wo aus die Nachricht per Morsezeichen und Funk an die Küste übermittelt wird. Dort wird sie niedergeschrieben und per Fax nach Amerika geschickt. Der Kontaktmann des Volkes bringt das Fax zum Dolmetscher, der es übersetzt und danach als Brief weiterschickt. Auch hier nimmt die Antwort denselben Weg zurück.

Weder der Präsident noch die beiden Absender haben eine Ahnung vom Transport. Der Präsident bekommt zwei Briefe. Vom unterschiedlichen Weg, den der Inhalt genommen hat, muss er dabei nichts wissen. Ebenso ist es den Absendern egal, ob der eine morst und der andere schreibt. Beide Nachrichten finden ihren Weg hin und zurück, trotz der unterschiedlichen Wege. Der Inselbewohner sendet Morsesignale und erhält auf diese Weise auch die Antwort. Er braucht von allem anderen nichts zu wissen, virtuell hat ihm der Präsident per Morsezeichen geantwortet.

Der andere Bittsteller versendet einen Brief – und bekommt einen solchen zurück. Er hat keine Kenntnis davon, dass ein anderer Bittsteller Morsezeichen verwendet hat.

Beide haben aber ihr Ziel erreicht, sie haben kommuniziert. Sie könnten dies auch untereinander tun, auf dieselbe Art und Weise, ohne zu bemerken, dass sie lokal andere Methoden benutzen. Dies ist nicht das Ziel eines weltweiten Netzwerkes. Ziel ist, dass jeder mit jedem kommunizieren kann und sich keine Gedanken machen muss, wie seine Daten transportiert werden.

## ■ 1.6 Allgemeine Bemerkungen

Was ist nun wichtig zu wissen, um einen Betrieb aufrechtzuerhalten? Was muss man über die Implementierung der Hersteller in den Schichten wissen, um einen Betrieb zu garantieren?

Die Layer I bis IV sind sehr netzwerkbezogen, die Layer V bis VII darstellungs- und anwendungsbezogen.

Im Verlauf dieser Einführung werden wir die Layer I bis IV schrittweise und realitätsbezogen kennenlernen. Die Layer V bis VII überlassen wir den Anwendern und Anwendungsentwicklern!

Dementsprechend ist der Hauptteil dieses Buches (Kapitel 2 bis 13) den Layern I bis IV gewidmet. Diese werden in den Kapiteln 2 bis 5 aufeinander aufbauend behandelt. Kapitel 6 geht auf neue Aspekte in diesen Layern ein, die sich aus dem immer stärker werdenden Trend zur Virtualisierung von Hardware ergeben.

Die Kapitel 7 bis 9 behandeln den Zugang zum Netzwerk und dem Internet. Kapitel 7 befasst sich mit dem Netzwerkzugang von entfernten Standorten aus über Virtual Private Networks (VPN), während es in Kapitel 8 um den lokalen drahtlosen Zugang über Wireless LAN geht. Verschiedene Szenarien für die Anbindung eines Netzwerks an das Internet werden in Kapitel 9 vorgestellt.

Einer der wichtigsten Technologiewechsel im Internet ist die Umstellung des Layer III von IPv4 auf IPv6. Während Kapitel 4 hauptsächlich auf IPv4 basiert, wird IPv6 in Kapitel 10 behandelt.

Netzwerkspeicher sind ein wichtiger Bestandteil heutiger Netzwerkkumgebungen. Obwohl diese teilweise auf Layer VII Protokollen basieren, werden sie im Hauptteil des Buches in Kapitel 11 beschrieben.

Ein Repetitorium mit Wiederholungsfragen sowie praktischen Übungen schließen den Hauptteil des Buches in Kapitel 12 bzw. 13 ab.

Im Anhang finden sich in Kapitel 14 vertiefende Exkurse, die bewusst aus dem Hauptteil ausgelagert wurden. Darüber hinaus enthält Kapitel 15 Beispiele für die Netzwerkplanung in verschiedenen Szenarien unter Verwendung von Bausteinen aus dem Hauptteil. Eine Übersicht über gängige Steckertypen findet sich in Kapitel 16. Kapitel 17 gibt praktische Hinweise zur Fehleranalyse. Der Anhang schließt mit einem Abkürzungsverzeichnis und dem Stichwortverzeichnis.

Wir werden sehen, dass sich die verschiedenen Implementierungen der Layer und die Protokolle nicht absolut genau an das OSI-Modell halten. Es ist auch kein starres Gesetz, sondern ein Kommunikationsmodell. Leichte Abweichungen, die sich die Hersteller erlauben, sind ohne Bedeutung, solange sie irgendwann wieder an der Grenze der Schichten korrigiert werden. Ab dieser Schicht ist wieder eine native (OSI-konforme) Kommunikation möglich. Die Protokolle, die auf den verschiedenen Schichten angesiedelt sind, sind nichts Anderes als festgelegte Regeln, nach denen verfahren werden muss. Benutzen alle dieselben Protokolle oder gibt es Protokollübersetzer, steht dem Datenaustausch nichts mehr im Wege.

Das OSI-Modell ist ein essenzielles Werkzeug im Netzwerkbereich. Jeder, der in diesem Gebiet tätig ist, sollte die Layer und ihre Bedeutung genau kennen. Nochmals sei betont, das OSI-Modell ist ein Modell. Wir werden es als festes Modell betrachten und mit ihm arbeiten. Aber wir müssen immer im Hinterkopf behalten, dass es nirgends so implementiert ist, wie wir hier annehmen. Trotzdem begehen wir keinen Fehler, wenn wir uns an ihm orientieren.

## ■ 1.7 Zum Weiterlesen

In der Welt der Computernetzwerke ist vieles standardisiert, das bedeutet, dass in offiziell verabschiedeten Dokumenten festgelegt ist, wie die Dinge funktionieren. Dies ist dringend notwendig, da wir in der Regel Geräte verschiedener Hersteller über das Netzwerk miteinander verbinden und alles reibungslos funktionieren soll. Wir werden im Laufe des Buches immer wieder auf Standards verweisen, in denen der interessierte Leser weitere Details finden kann. Es ist immer lohnenswert, einen Blick hineinzuworfen.

Es gibt zahlreiche Organisationen, die sich mit der Standardisierung befassen. Die erste Organisation, die in diesem Buch genannt wurde, ist die Internationale Organisation für Normung (ISO). Interessierten Lesern empfehlen wir einen Blick in den offiziellen Standard [ISO1994], der das ISO/OSI-Modell detailliert beschreibt.

### Literatur

[ISO1994] International Organization for Standardization (ISO): ISO/IEC 7498-1:1994 – Information Technology – Open Systems Interconnection – Basic Reference Model: The Basic Model. International Organization for Standardization, 1994. Zugriffen am 18.07.2023. [https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269\\_ISO\\_IEC\\_7498-1\\_1994\(E\).zip](https://standards.iso.org/ittf/PubliclyAvailableStandards/s020269_ISO_IEC_7498-1_1994(E).zip)