

# HANSER



## Leseprobe

zu

## Rechnernetze

von Wolfgang Riggert und Ralf Lübben

Print-ISBN: 978-3-446-47280-8

E-Book-ISBN: 978-3-446-47382-9

E-Pub-ISBN: 978-3-446-47383-6

Weitere Informationen und Bestellungen unter

<https://www.hanser-kundencenter.de/fachbuch/artikel/9783446472808>

sowie im Buchhandel

© Carl Hanser Verlag, München

# Vorwort zur 7. 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.hanserfachbuch.de](http://plus.hanserfachbuch.de) zur Verfügung. Online ist auf HanserPlus umfangreiches Zusatzmaterial erhältlich: Quizzes, Linksammlungen und die Lösungen zu den Aufgaben.

# Inhalt

<b>Vorwort zur 7. 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 .....	20
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	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	Gigabit-Ethernet .....	104
4.2.1	Physikalische Grundlagen .....	105
4.2.2	Varianten .....	106
4.2.3	Besonderheiten .....	109
4.3	10G-Ethernet und darüber hinaus .....	111
4.3.1	Eigenschaften .....	111
4.3.2	Vorteile .....	115
4.4	Technologische Trends .....	117
4.5	Zusammenfassung .....	120
4.6	Wissensüberprüfung .....	121
<b>5</b>	<b>IP-Protokollfamilie .....</b>	<b>123</b>
5.1	IP - Internet Protocol .....	126
5.1.1	Fragmentierung .....	131
5.1.2	Routing-Optionen .....	132
5.1.3	Routing .....	133

5.2	ARP – Address Resolution Protocol .....	135
5.3	ICMP – Internet Control Message Protocol .....	138
5.4	Dynamic Host Configuration Protocol & Domain Name System ..	141
5.4.1	Dynamic Host Configuration Protocol .....	142
5.4.2	Domain Name System .....	146
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	IPv6-Adressmanagement .....	191
7.4.5	Begleitprotokolle .....	193
7.5	Migrationswege .....	196

7.5.1	Tunneling	197
7.5.2	Dual-IP-Stack	198
7.6	Mobile IPv6	199
7.6.1	Kommunikationsablauf	199
7.6.2	Technischer Hintergrund	200
7.7	Überlegungen zur Sicherheit	203
7.8	Zusammenfassung	207
7.9	Übungen	209
7.10	Wissensüberprüfung	210
<b>8</b>	<b>TCP/UDP-Protokoll</b>	<b>211</b>
8.1	TCP im Detail	212
8.1.1	Besonderheiten	213
8.1.2	Merkmale	213
8.1.3	Verbindungsmanagement	217
8.1.4	Fehlervermeidungsmechanismen	219
8.2	UDP – User Datagram Protocol	224
8.3	Überlegungen zur Sicherheit	225
8.4	QoS – Quality-of-Service	228
8.4.1	Klassifikation	231
8.4.2	Congestion Avoidance	232
8.4.3	Congestion Management	234
8.5	Netzneutralität	237
8.6	Zusammenfassung	239
8.7	Wissensüberprüfung	240
<b>9</b>	<b>Layer 2 – Geräte, Protokolle und Konzepte</b>	<b>241</b>
9.1	Switches	242
9.1.1	Eigenschaften	242
9.1.2	Arbeitsweise	244
9.1.3	Switching-Verfahren	246
9.1.4	Erweiterungsmöglichkeiten	249
9.1.5	Kapazitätssteigerung	250
9.1.6	Switch-Architekturen	251
9.2	Spanning-Tree	253
9.3	Virtuelle LANs	259
9.3.1	VLAN-Typen	260
9.3.2	Trunk	261

9.3.3	VLAN-Management .....	262
9.3.4	Link-Aggregation, Spanning-Tree und VLAN .....	263
9.4	Überlegungen zur Sicherheit .....	264
9.4.1	Angriffsziel: STP-Bridge .....	264
9.4.2	Angriffsziel: STP-Parameter .....	265
9.4.3	Angriffsziel: MAC-Tabelle .....	267
9.5	Zusammenfassung .....	269
9.6	Übungen .....	270
9.7	Wissensüberprüfung .....	270
<b>10</b>	<b>Layer 3 – Geräte, Protokolle und Konzepte .....</b>	<b>271</b>
10.1	Router .....	271
10.1.1	Bedeutung .....	272
10.1.2	Routing-Ablauf .....	274
10.1.3	Routing-Methoden .....	277
10.1.4	Unterschiede zwischen Routern und Switches .....	279
10.2	Routing .....	281
10.2.1	Bedeutung .....	282
10.2.2	Routing-Protokolle – allgemeine Klassifizierung .....	282
10.3	Routing-Protokolle .....	287
10.3.1	RIP – Routing Information Protocol .....	287
10.3.2	OSPF – Open Shortest Path First .....	290
10.4	Routing-Probleme .....	293
10.5	Einsatzaspekte von Switches und Routern .....	294
10.6	Überlegungen zur Sicherheit .....	296
10.7	Zusammenfassung .....	297
10.8	Wissensüberprüfung .....	298
<b>11</b>	<b>Verwaltung von Netzwerken .....</b>	<b>299</b>
11.1	Netzwerkmanagement .....	300
11.1.1	Netzwerkstatistiken .....	302
11.1.2	FCAPS-Modell .....	304
11.1.3	SNMP .....	305
11.1.4	syslog .....	311
11.2	Überlegungen zur Sicherheit .....	312
11.2.1	Allgemeine Bedrohungen .....	312
11.2.2	Fehleranalyse .....	315
11.2.3	Übungen .....	325



11.3 Zusammenfassung .....	326
11.4 Wissensüberprüfung .....	327
<b>12 Wireless Local Area Networks .....</b>	<b>329</b>
12.1 IEEE 802.11-Standards .....	331
12.2 Wireless-Architekturen .....	337
12.3 Modulationsverfahren und Kanäle .....	339
12.4 Zugriffsmethoden: CSMA/CA .....	342
12.5 Rahmentypen .....	346
12.6 Anmeldeverfahren .....	350
12.7 Sicherheit .....	351
12.8 Zusammenfassung .....	357
12.9 Wissensüberprüfung .....	357
<b>13 Literatur .....</b>	<b>359</b>
<b>Index .....</b>	<b>365</b>

**Ergänzendes Material auf <https://plus.hanser-fachbuch.de>**

Lösungen zu den Kapitelfragen

Die Abbildungen des Buches

Mind Maps

Quizzes auf Basis von Kahoot!

# 1

# Netzwerkgrundlagen und -architektur

## Lernziele

Nach der Beendigung dieses Kapitels sollte der Leser in der Lage sein, folgende Fragen zu beantworten:

- Wie sind Netzwerke hinsichtlich ihrer Topologie aufgebaut?
- Aus welchen Basiskomponenten bestehen Netzwerke?
- Wie ist der Netzzugang geregelt?
- Was sind die Vorteile eines Schichtenmodells?
- Welche Funktionalität ist auf welcher Ebene des Schichtenmodells angesiedelt?

## Kapiteleinführung

Netzwerke schlagen ein neues Kapitel in der Informationsverarbeitung auf. In vielen Unternehmen bilden sie heute das Rückgrat der Informationsinfrastruktur. Angefangen von Netzwerken, die nur fünf Rechner verbinden, reicht das Spektrum moderner Lösungen bis hin zu weltweiten Verbänden, in denen viele Rechnerwelten eine integrative Einheit mit größtmöglicher Produktivität bilden. Triebfeder für die fortschreitende Vernetzung ist das Internet. Als leistungsfähige Werbeplattform und Vertriebskanal für viele Arten von Produkten und Dienstleistungen überwindet es traditionelle Marktgrenzen mit Geschäftsmodellen wie E-Commerce. Infolge dieses Booms werden leistungsfähige Netzwerke, die eine Vielzahl von Nutzern innerhalb akzeptabler Antwortzeiten bedienen, eine notwendige Voraussetzung.

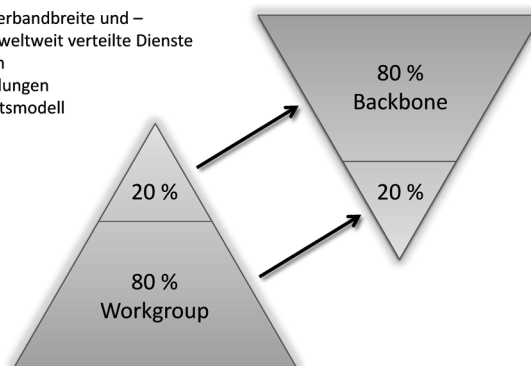
Im Vordergrund für den Betrieb und den Ausbau von Netzwerken stehen drei Anforderungen:

- Die Geschwindigkeit muss für die Partner des Datenaustausches zufriedenstellend ausfallen, ohne dass große Schwankungen in der Antwortzeit, selbst zu Spitzenlastzeiten, auftreten.
- Das Management der Netzkomponenten und der Endstationen muss einfach sein.
- Die Kosten des Betriebes müssen in vertretbarem Rahmen liegen.

Getrost der Prämisse „*Nichts ist so beständig wie der Wandel*“ fällt es zunehmend schwerer, Leitlinien für eine zukunftssichere Netzplanung aufzustellen. In einer Welt, in der sich die Innovationszyklen ständig verkürzen, Produkte innerhalb eines Quartals veralten und das Internet alle Geschäftsbereiche umwälzt, bleiben auch die Netzwerktechnologie und ihre Prinzipien kaum ausgespart. Dennoch lassen sich einige Trends erkennen:

- Zukünftige Anwendungen verlangen die Übertragung großer Datenmengen. Dazu zählen Augmented- und Virtual-Reality-Anwendungen, Streaming-Dienste mit hohen Datenraten für Full-HD-Videos oder Cloud-Gaming-Dienste, bei denen Video- und Kontrolldaten in Echtzeit übertragen werden. Aber auch die Übermittlung von Röntgenbildern hoher Auflösung zwischen medizinischen Einrichtungen oder gar die Übertragung des Operationsgeschehens zwischen Krankenhäusern ist keineswegs nur Vision, sondern schon Realität.
- Die Zukunft zeigt eine Applikationslandschaft, die hohe Ansprüche an Antwortzeit und Güte der Übertragung stellen wird. Den durch die neuen Anwendungen dramatisch wachsenden Ansprüchen an die Bandbreite gesellt sich eine revolutionäre Veränderung des Verkehrsmusters hinzu. Die alte 80/20-Regel, nach der 80% der Datenlast im Segment oder dem Unternehmen verbleiben und nur 20% die Segmentgrenze überschreiten, wird durch Client/Server-Architekturen, das Internet und die VLAN-Bildung regelrecht auf den Kopf gestellt. Dieser Wandel, gekoppelt mit der Dezentralisierung der Datenquellen allgemein, macht die Datenflüsse eines Netzes unvorhersehbar und hochdynamisch.
- Die Veränderungen in den Anwendungen, in der Zahl der Netzbenutzer und im Verkehrsmuster machen verständlich, warum Organisationen gezwungen sind, permanent Teile ihres Netzes neu zu strukturieren und auf Technologien mit höherer Bandbreite umzustellen.

- Steigerung von Serverbandbreite und –geschwindigkeit für weltweit verteilte Dienste
- Latenzzeit-Reduktion
- Multimedia-Anwendungen
- Zero-Trust-Sicherheitsmodell



**Bild 1.1** Veränderte 80/20-Regel

Dennoch existieren auch in diesem Meer von Unwägbarkeiten einige Fixpunkte. Diese Begriffe bilden praktisch die unverrückbaren Säulen des Netzgebäudes, um die sich alle neuen Entwicklungen ranken und an denen sie sich orientieren. Zu den Grundprinzipien gehören Aspekte wie:

- Kommunikationsrichtung und Anzahl der Kommunikationspartner,
- Topologie/Architektur und Ausdehnung,
- Protokolle und Dienste,
- Signalcodierung und Übertragungsmedium,
- Fehlerbehandlung und Datenflusskontrolle,
- Wegewahl/Routing.

Netzwerke bieten mehr als nur die Befreiung des PCs aus seinem isolierten Wirkungsbereich. Häufig fallen in diesem Zusammenhang Begriffe wie Server, Netzwerkbetriebssysteme oder Adapter sowie der Verweis auf zahlreiche Vorteile wie Kostenreduzierung oder Produktivitätssteigerung.

## ■ 1.1 Basiselemente eines Netzwerkes

Eine Netzstruktur basiert auf vier Elementen:

- den **Rechnern oder Knoten**, die verbunden werden sollen,
- den **Infrastrukturkomponenten**, die den Anschluss und die Kopplung der Rechner im Gesamtkontext leisten. Zu ihren Aufgaben gehört es, Datensignale zu regenerieren und dann zu übertragen (Signalisierung), Informationen über die möglichen Wege im Netzwerk bereitzustellen, andere Geräte über Fehler im Netz zu informieren, Datenverkehr gemäß den Dienstgüteanforderungen zu klassifizieren oder Datenströme anhand von Sicherheitsrichtlinien zu erlauben oder zu unterbinden,
- der **Verkabelung**, die die physikalische Verbindung der einzelnen Elemente sicherstellt. Neben der kabelgebundenen Möglichkeit existiert die Anbindung von Endgeräten an die Netzwerkinfrastruktur über drahtlose Alternativen,
- dem **Protokoll**, das die Regeln für einen Nachrichtenaustausch festlegt. Dazu gehört die Definition von Nachrichtentypen und der Übertragungseinheit, d. h. des Datenpaketes, seines Inhaltes und seiner Größe und Struktur, sowie den Austauschprinzipien zwischen den Netzteilnehmern.

Damit sich der Netzwerkzug in Bewegung setzen kann, fehlen noch die Schienen, die Weichen und der Fahrplan:

- **Netzwerkkarte:** In jedem in das Netzwerk zu integrierenden Rechner muss eine Netzwerkkarte installiert sein. Erst über diese Weiche kann der Teilnehmer an den Leistungen des Verbundes partizipieren. Jede Anfrage oder Mitteilung an andere Teilnehmer wird über dieses Medium in das Netzwerk eingespeist. Die Netzwerkkarte ist zuständig für die Übertragung und den Empfang aller Nachrichten.
- **Verbindung:** Die Verbindung zwischen den Netzwerkkarten und damit zwischen den einzelnen Teilnehmern in Form der Schienen wird über Netzkabel oder drahtlos hergestellt. Für kabelgebundene Verbindungen stehen zwei Typen zur Auswahl: Twisted-Pair-Kabel oder Glasfaserkabel. Sie unterscheiden sich hinsichtlich der zulässigen Geschwindigkeit und technischer Parameter des Übertragungsmediums: elektrischer oder Lichtimpuls.
- **Netzwerkfähiges Betriebssystem:** Für die Kommunikation müssen die Teilnehmer eines Netzwerkes dieselbe Sprache sprechen, diese Regeln werden in Protokollen beschrieben und müssen letztendlich in Software umgesetzt werden. Heutzutage implementieren nahezu alle Betriebssysteme diese Softwarekomponenten, um über Netzwerke miteinander zu kommunizieren. Weiterhin benötigen die Betriebssysteme passende Treiber, um Hardware zur Kommunikation wie Netzwerkkarten zu unterstützen. Der Weg dahin führte aber über spezielle Varianten wie Novell Netware, das zu Spitzenzeiten einen Marktanteil von 80 % besaß.

Die Vorteile eines Netzwerkes erstrecken sich auf unterschiedliche Bereiche:

- **Datenverbund** gewährt den Zugriff auf räumlich verteilte Daten.
- **Lastverbund** gestattet eine optimale Prozessorauslastung. Damit kann eine Verteilung der Rechenlast zu Spitzenzeiten erreicht werden.
- **Funktionsverbund** erweitert die lokale Funktionalität durch den Zugriff auf gemeinschaftlich netzwerkweit genutzte Ressourcen.
- **Leistungsverbund** ermöglicht im Falle einer algorithmischen Zerlegung eines Problems die Verteilung der Rechenlast auf mehrere Knoten. Ein typisches Beispiel hierfür ist die Berechnung von Schlüsseln der symmetrischen Verschlüsselungsalgorithmen.
- **Verfügbarkeitsverbund** stellt eine Mindestleistung bei Ausfall einzelner Komponenten zur Verfügung. Fällt ein Netzknoten aus, kann der Anwender im Idealfall einen Nachbarrechner nutzen, ohne auf die netzweiten Ressourcen verzichten zu müssen. Lediglich die lokalen Anwendungen bleiben von der Bearbeitung ausgeschlossen. Damit wächst die Verfügbarkeit des Gesamtsystems.

Die Leistungsfähigkeit eines Netzwerkes lässt sich anhand dreier Faktoren beurteilen:

- **Bandbreite:** Sie ist der Ausdruck für die Kapazität, die das Medium bewältigen kann. Sie misst das Informationsvolumen, das von einem zu einem anderen Ort in einer gegebenen Zeitspanne übertragen werden kann. Die übliche Maßeinheit ist Bit/s.
- **Durchsatz:** Er gibt die aktuell transportierte Menge an Daten an und spiegelt damit die augenblickliche Verkehrssituation und kein theoretisches Maximum wider.
- **Goodput:** Er ist das Maß für die übertragenen Nutzdaten, d.h. der reinen Nettodaten ohne den verwaltungsmäßig notwendigen Protokolloverhead.

## ■ 1.2 Netzwerkkategorien

Netzwerke werden zur besseren Systematisierung, zur einfacheren Verwaltung und zur übersichtlicheren Fehlersuche in Kategorien eingeteilt. Eine gängige Typisierung unterscheidet nach:

- Personal Area Network (PAN),
- Reichweite,
- administrativer Verantwortung,
- Topologie,
- Technologie.

Der geografische Bereich, den ein Netzwerk abdeckt, wird aufgeteilt in:

- Personal Area Network (PAN),
- Local Area Network (LAN),
- Metropolitan Area Network (MAN),
- Wide Area Network (WAN).

**PANs** sind Netze mit geringer Reichweite, die das Umfeld einer Person abdecken, z.B. zur Kommunikation von Computern, Smartphones und Wearables. Häufig wird hierzu Bluetooth als drahtlose Funktechnologie verwendet.

**LANs** sind Netzwerke von Unternehmen. Jedes Unternehmen hat ein starkes Interesse daran, diese Infrastruktur unter eigener Kontrolle zu betreiben und zu warten, um das Herzstück der Informationstechnologie autonom zu halten. Es ist dabei auf das Firmen- oder Campusgelände und in seiner Ausdehnung ohne Zusatzmaßnahmen auf 500 m beschränkt.



Die eingesetzte Technologie und der verwendete Kabeltyp bestimmen wesentlich die exakten Entfernungsrestriktionen und die Anzahl der Knoten, die ein LAN bilden.

Unter einem **MAN** ist ein Regionalnetz mit einem Ausdehnungsradius von ca. 100 km zu verstehen. Ein **WAN** hingegen ist keiner geographischen Beschränkung unterworfen.

**MANs** bilden häufig Verbindungsnetze zwischen Institutionen. Ihr Hauptaugenmerk liegt auf der Bildung von Kommunikationsverbänden jenseits der geographischen Unternehmensgrenzen unter eigener Administration und Kontrolle.

**WANs** verbinden die unterschiedlichen LANs der Unternehmen über eine gesonderte Infrastruktur, die sich im Besitz spezialisierter Dienstleister befindet. Ähnlich wie das Autobahnnetz, das Orte nicht direkt verbindet, besitzt ein WAN keine explizit angebotenen Teilnehmerstationen. Benutzer sind also immer Teil eines LANs oder MANs, die entweder regional begrenzt verbunden oder aber unter Zuhilfenahme eines WANs räumlich unbegrenzt gekoppelt werden.



WANs sind Netzwerke, die Routing-Protokolle zur Wegewahl der zu übertragenden Informationen nutzen. LANs hingegen beruhen in der Regel auf dem Broadcast-Prinzip, wie es vom Rundfunk her bekannt ist.

Ein flexibler, zukunftsfähiger Netzaufbau setzt ein entsprechendes Design voraus. Der Topologie kommt große Bedeutung zu, denn schließlich bildet sie das Rückgrat des Netzes, das nur mit großem Aufwand verändert werden kann. Eine Topologie lässt sich hinsichtlich dreier Merkmale beurteilen:

- **Skalierung:** Wie verhält sich der Aufbau bei einer Erweiterung oder Reduzierung von Stationen?
- **Fehlertoleranz:** Wie reagiert das Netz auf den Ausfall einer Station oder einer Verbindung zwischen Rechnern?
- **Verkabelungsaufwand:** Welcher Aufwand entsteht, um alle Stationen anzuschließen?

Unter Berücksichtigung dieser Fragestellungen lassen sich mehrere Grundformen beschreiben sowie eine Kombination dieser:

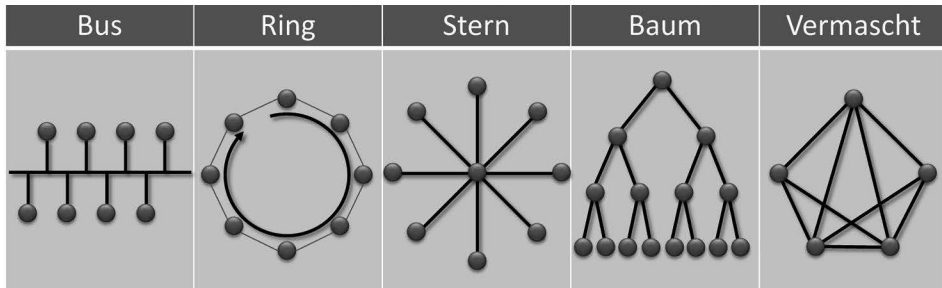
- **Bus:** Dieser Aufbau verwendet ein zentrales Kabel. Die einzelnen Rechner müssen sich vergleichbar den Haltestellen einer Buslinie gesondert an dieses Medium anschließen. Dazu ist ein eigenes Anschlusskabel für jeden Rechner notwendig. Die Enden der Buslinie müssen durch einen Abschlusswiderstand ordnungsgemäß terminiert werden. Bei dieser Topologie wird nur sehr wenig Kabel benötigt. Rechner können sehr einfach am Netzverkehr teilnehmen, aber

auch durch Lösen der Verbindung zum zentralen Kabel wieder zu Kommunikationsinseln werden. Sobald aber das Buskabel unterbrochen wird, kommt das gesamte Netzwerk zum Erliegen.

- **Ring:** Jede Station besitzt genau einen linken und einen rechten Nachbarn. Der Ring ist gerichtet, d. h. die Nachrichten werden in definierter Weise weitergeleitet. Diese Tatsache birgt allerdings das Problem, dass bei Ausfall einer Station der Ring unterbrochen ist, d. h. dass Signale diese Stelle nicht passieren können und demzufolge das Gesamtnetz seine Funktionsfähigkeit verliert. In der Praxis werden durch einen zweiten entgegen gerichteten Ring entsprechende Vorkehrungen getroffen, um immer einen geschlossenen Ring zu gewährleisten. Als Vorteil zeichnen diese Struktur die einfache Erweiterbarkeit und der geringe Kabelbedarf aus.
- **Stern:** Bei diesem Aufbau besitzt jeder Rechner eine eigene Verbindung zu einer zentralen Verteilereinheit. Zwar wird deutlich mehr Kabel als bei der busförmigen Variante benötigt, jedoch sind bei einem Ausfall eines Netzkabels keine anderen Rechner betroffen. Herausragendes Merkmal eines Sterns ist seine leichte Ausbaufähigkeit und seine Ausfallsicherheit. Einziger Schwachpunkt ist die zentrale Verteilerstelle, deren Ausfall nicht kompensiert werden kann.
- **Baum:** Ausgehend von einem Wurzelknoten verzweigt sich das Netzwerk in mehrere Äste. Die Wurzel und Knoten stellen hierbei Infrastrukturkomponenten zur Weiterleitung von Daten dar. Die Knoten am Ende sind Endgeräte wie PCs und Laptops. Kommt es zu Ausfällen an der Wurzel oder in den mittleren Schichten, werden Äste voneinander getrennt.
- **(Voll-)Vermascht:** Knoten haben eine oder mehrere Verbindungen zu weiteren Knoten. Ist jeder Knoten mit jedem anderen verbunden, wird dies als vollvermascht bezeichnet. Die Vollvermaschung bietet einen hohen Schutz gegenüber Ausfällen von Knoten und Verbindungen, erfordert aber einen hohen Aufwand bei der Verkabelung. Deswegen haben häufig nur Knoten mit zentraler Funktion viele Verbindungen, so dass beim Ausfall von Verbindungen alternative Wege möglich sind. Prominentestes Beispiel ist das Internet. Dieses besteht aus einer Vermaschung von vielen wiederum vermaschten Netzen.

Derzeit hat sich der Stern und als dessen Erweiterung der Baum als „State of the Art“ im LAN durchgesetzt. Im Kernbereich von Netzen werden häufig zentrale Elemente redundant ausgelegt und miteinander vermascht, sodass Ausfälle einzelner Infrastrukturkomponenten nicht zum Gesamtausfall oder zur Segmentierung des Netzwerkes führen. Typisch ist diese Topologie für die Vernetzung im Bereich der LANs auf Basis von Ethernet.





**Bild 1.2** Netzwerktopologien

**Tabelle 1.1** Topologievergleich

	Bus	Ring	Stern	Baum	Vermascht
Verkabelungsaufwand	++	+	-	+	-
Skalierbarkeit	+	++	++	++	++
Fehlertoleranz	+	-	+	+	++



Die physikalische Topologie beschreibt den Aufbau des Netzwerkes, d. h. die Form, in der die Kabel verlegt sind. Die logische Topologie verweist auf den Pfad, den die Daten von der Quelle zum Ziel nehmen. Beide Formen können übereinstimmen (Ethernet), müssen es aber nicht (Token Ring).

Ein weiterer Ansatz, ein Netzwerk zu beschreiben, legt seine verwendete Technologie zugrunde. Dabei werden Merkmale wie Topologie, Kabeltyp, Entfernungseinschränkungen, Kontrollinformationen oder Adressen beleuchtet.

## ■ 1.3 Netzwerkarchitekturen

Die Gestaltung und der Aufbau betrieblicher Anwendungssysteme sind stark mit den IT-technischen Möglichkeiten verwoben. Dies zeigt sich in mehreren Paradigmenwechseln, die sich im Laufe der Evolution der Informationstechnologie und der sie begleitenden Option der Verteilung der Ressourcen vollzogen haben.

Stand mit dem Aufkommen von Rechner zunächst die Verarbeitung von Massendaten und die Bewältigung von Routinetätigkeiten im Vordergrund, so hat sich dieses Bild zu einer flexiblen Nutzung der vielfältigsten Aufgaben durch mobile Geräte gewandelt. Drei Entwicklungslinien lassen sich ausmachen:

- monolithische Anwendungssysteme,
- Client/Server-Architekturen,
- Cloud-Computing.

### Monolithische Anwendungssysteme

Das charakteristische Merkmal dieser Form der Datenverarbeitung ist ein zentraler Rechner (Mainframe) mit angebotenen Terminals, die selbst über keine Rechenkapazität verfügen und folglich nur als reine Präsentationsgeräte genutzt werden können. Diese Architektur verbindet Funktionalität und Datenverwaltung als untrennbare Einheit. Die Verbindung mit anderen Rechensystemen ist schwierig bis unmöglich, sodass diese Konstellation denkbar integrationsfeindlich ist. Aber nicht nur die mangelnde Integrationsmöglichkeit stellt eine Hürde dar. Weitere Probleme:

- die Unterstützung neuer Anforderungen verlangt stets neue Systeme,
- die schneller als der Leistungszuwachs steigenden Kosten,
- die teure Pflege und Wartung,
- die mangelhafte Skalierbarkeit.

### Peer-to-Peer- und Client/Server-Architekturen

Mit dem Aufkommen der PCs als kleine preiswerte Recheneinheiten Mitte der 1980er-Jahre und der gleichzeitigen Möglichkeit der Vernetzung dieses neuen Gerätetyps, ergab sich das Potenzial der räumlichen begrenzten Verteilung von Rechenkapazität. Diesem Gedanken folgend sind heutige Anwendungssysteme verteilte Systeme, deren Funktionalität und Datenbestand als kooperierende Elemente betrachtet werden. Die Verteilung kennt zwei Ausprägungen, die sich danach richtet, wer und durch wen die Ressourcen betreut werden:

- In einer **Peer-to-Peer-Umgebung** arbeitet jeder Rechner gleichberechtigt und jeder Nutzer administriert seine eigenen Betriebsmittel.
- In einer **Client/Server-Architektur** werden Anwendungen und Datenbestände auf verschiedene Rechner im Netz verteilt. Aus Sicht des Anwenders erscheint das verteilte System aber als integrierter Dienst.

Dem letzten Gedanken folgend lassen sich Rechner grundsätzlich in zwei verschiedene Gruppen einteilen: Server und Clients. Server sind Rechner, die ihre Ressourcen und Dienste der Allgemeinheit zur Verfügung stellen, Clients sind Leistungsnehmer. Diese Art der Gruppierung ist das heute vorherrschende Verarbeitungsprinzip und wird als Client/Server-Architektur bezeichnet. Es beschreibt die Vorstellung, dass die Kooperation einem Grundschema folgt:

- Die Initiative einer Zusammenarbeit geht vom Client aus, indem er Aufträge an einen Dienstleister, den Server, schickt, der seine Bereitschaft bekundet hat, für bestimmte Dienste verfügbar zu sein. Dabei gilt eine „1 : n-Beziehung“ in beide Richtungen. Der Client kann im Laufe der Verarbeitung auf mehrere Server zugreifen und ein Server kann verschiedene Clients bedienen. Aus der Sicht des Servers – also des Empfängers einer Anforderung – heißt diese Ver-

teilung, er bietet nur bestimmte Dienste an, sodass ihn keine beliebigen überraschenden Nachrichten erreichen können. Auch nimmt er Anforderungen nur entgegen, wenn er „frei“ ist.

Dennoch kann die Auslastung nur prognostiziert werden, sodass Unsicherheit darüber besteht, welche Kapazität er vorhalten muss, um für alle Anwendungsfälle gewappnet zu sein. Dieser Informationsmangel kann zur Verschwendung von Ressourcen führen, wenn keine gleichmäßige Auslastung vorliegt und Lastspitzen mit der gleichen Performance wie ein unterdurchschnittlicher Verkehr bedient werden sollen.



Welche Auswirkungen eine Vernetzung dezentraler Knoten auf einzelne Nutzer hat, zeigen folgende drei Aspekte:

- **Räumliche Trennung:** Ressourcen in einem Netz haben zu ihrem Kommunikationspartner eine räumliche Distanz. Daraus ergibt sich eine Verzögerung der Signale, die sich letztlich in der Übertragungsdauer niederschlägt. Dem Nutzer begegnet dieser Aspekt durch die Antwortzeit. Aber auch die verfügbare Bandbreite, die Verzögerung von Sendungen oder die Fehlerrate des Mediums können den Nutzer beeinträchtigen.
- **Unabhängigkeit der Knoten:** Die einzelnen Rechner eines Netzes handeln autonom, d. h. sie unterliegen keinem Abstimmungsmechanismus hinsichtlich anderer Teilnehmer. Die Entscheidung zum Senden einer Nachricht treffen die Rechnerknoten ohne Rücksicht auf den Zustand des Netzes und seiner Elemente.
- **Heterogenität der Knoten:** Die Knoten des Netzes unterscheiden sich hinsichtlich Hardware, Betriebssystem und Anwendung. Zur Teilnahme am Netzbetrieb bestehen keine Voraussetzungen hinsichtlich bestimmter Ausstattungsmerkmale. Zum Datenaustausch zwischen den Knoten ist damit keine Kenntnis der genauen Konfiguration eines Partners erforderlich.

**Tabelle 1.2** Vor- und Nachteile von Peer-to-Peer- und Client/Server-Netzwerken

Vorteile Peer-to-Peer	Vorteile Client/Server
preiswerte Implementierung	zentralisierte Administration – alle Daten können zentral gesichert werden
kein Netzwerkadministrator notwendig	Skalierbarkeit und flexible Architektur verbesserte Sicherheit
Nachteile Peer-to-Peer	Nachteile Client/Server
geringe Skalierbarkeit, wenn die Kommunikationsbeziehungen mit Anzahl der Knoten steigt	Server verlangen höherwertige Ausstattung
Sicherheitsprobleme	Administrator notwendig
jeder Nutzer benötigt bedingt Administrationskenntnisse	Single Point of Failure in Form des Servers

# Index

## Symbole

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

## A

Access Control List 296, 351  
Access-Point 330  
ACK 214  
Acknowledgement 143, 214  
– -Nummer 215  
ACL 296  
ACR 57  
Address Mask  
– Reply 141  
– Request 141  
Address Resolution Protocol 135  
– Cache 135  
– Reply 136  
– Request 136  
Adresskonfiguration  
– automatisch 178  
Advanced Encryption Standard 354  
AES 354  
Aging-Timer 244  
Alohanet 68  
Antivirus-Software 314

Anwendungsklasse 59  
Anwendungsschicht 26  
Anycast 16, 178  
AP 330  
Applikationsmanagement 301  
ARP 135  
ARPANet 123  
ARP-Cache-Poisoning 267  
asynchron 36  
Attempt Limit 79  
Attenuation to Crosstalk Ratio 57  
Autodiscovery 301  
Autokonfiguration 19  
Auto-Negotiation 81, 101  
Autosensing 64  
Autotopology 301

## B

Backbone  
– Collapsed- 40  
– Distributed- 39  
Backoff 344  
Bandbreite 5, 47  
Bandbreitenreservierung 178  
Base 71  
baseline 326  
Basic Service Set 337  
Basisband 84  
Basisdatentransfer 213  
Beacon Frame 346  
Beamforming 336  
Begleitprotokoll 193, 211

- Berners-Lee, Tim 123
  - Best-Effort-Service 230
  - Betriebssystem 4
  - Biegeradius 58
  - Bitfolge 24
  - Bitrate 58
  - Bitübertragungsschicht 23
  - Block Acknowledgement 345
  - Border Gateway Protocol 285
  - Botnetz 225
  - BPDU 255
  - Break-Out-Kabel 52
  - Brechungsindex 44, 46
  - Bridge 242
  - Bridge Protocol Data Unit 255
  - Broadcast 16
    - -adresse 157
    - -Domäne 76
    - -Netz 15
  - Brute-Force 313
  - BSS 337
  - BSS Coloring 346
  - Bündelader 52
  - Busy Waiting 77
- C**
- Cache-Poisoning 148
  - Carrier Extension 109
  - Carrier Sense 77
  - Category 59
  - CATNIP 176
  - CBWFQ 237
  - 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 221, 229, 232
    - -Collapse 221
    - -Management 229, 234
  - Converged Interface Adapters 118
  - Core 43
  - Crosstalk 62
    - Alien- 63, 113
  - CSMA/CA 342
  - CSMA/CD-Verfahren 76, 82
  - Cut-Through 246
- D**
- DAD 203
  - Dämpfung 47, 56
  - Darstellungsschicht 25
  - Datenaustausch 32
  - Datenflusskontrolle 81, 214, 219
  - Datenkompression 26
  - Datenverbund 4
  - DCF 342
  - Defaultroute 276, 278
  - Deferring 77
  - Delay Skew 63, 108
  - Denial of Service 225, 268, 314
  - Destination-Adresse 74
  - Deutsches Network Information Center 129
  - DHCP 141
  - Dienstgüte 127, 177
  - DiffServ 128, 230
  - Diffusionsnetz 15
  - Direct Sequence Spread Spectrum 339
  - Distributed Coordination Function 342
  - DNS 141
  - Domain Name System 141, 146
  - DoS 225
  - Drei-Schichten-Modell 11
  - DS-Byte 128

- DSSS 339
  - Dual-IP 197
    - -Stack 198
  - Duplicate Address-Detection 203
  - Durchsatz 5
  - Dynamic Host Configuration Protocol 141f.
- E**
- Echo 139
    - Reply 139
  - EDIFACT 26
  - Einkopplungswinkel 44
  - Electronic Data Interchange for Administration, Commerce and Transport 26
  - Elektromagnetische Verträglichkeit 42, 62
  - Encapsulation 21, 197
  - Ende-zu-Ende verschlüsselte Protokolle 320
  - Energy Efficient-Ethernet 119
  - Ethernet 68
    - Distanz 82
    - Namenskonvention 71
    - Paket 71
    - Paketfelder 72
  - EUI-64 Interface-ID 191
  - Eventhandling 301
- F**
- Fast-Ethernet 95
  - FCAPS-Modell 304
  - FEXT 63
  - FHSS 339
  - Fibre Channel 105
  - FIFO 235
  - File Transfer Protocol 26
  - Firewall 314
  - First-in-First-out 235
  - Flag 128, 215
  - Flooding 245f.
  - Flow Control 179
  - Flow Label 178, 181
  - Flusskontrolle 110
  - Forwarding 184
  - Fragmentation Offset 128
  - Fragment Free 248
  - Fragmentierung 14, 131, 179, 184
  - Fragment Offset 185
  - Fragmentprüfung 80
  - Frame 14, 25
  - Frame Aggregation 345
  - Frame Check Sequence 91
  - Frequency Hopping Spread Spectrum 339
  - Fresnel-Verlust 48
  - FTP 26
  - Funktionsverbund 4
- G**
- Gerätehärtung 314
  - Ghost 91
  - Gigabit-Ethernet 62, 104, 109
  - Glasfaser 41
    - -Kabelarten 51
    - -Steckverbindungen 52
    - -Typen 49
  - Goodput 5
- H**
- Halbduplex 15
  - Hardwareadresse 73
  - Header
    - ARP- 136
    - Authentication 185
    - Destination Options- 183
    - Encapsulation 185
    - -Erweiterung 182
    - Fragment- 184
    - Hop-by-Hop Options- 183
    - IP 126
    - IPv6- 179
    - Routing- 184
    - TCP-Protokoll 214
  - Hello-Paket 284, 290
  - Hello-Timer 256

Helper Address 144  
 Hidden Node 344  
 Hohlander 52  
 Hold Down Timer 286  
 Hop Count 281  
 Hop-Count-Limit 286  
 Hop-Limit 179, 182  
 Hostadresse 152  
 HTTP 26  
 Hub 88  
 Hypertext Markup Language 125  
 Hyper Text Transfer Protocol 26

**I**

IANA 187  
 ICMP 138  
 Idle 77  
 IEEE 67  
 IEEE 802.3 68, 70  
 IEEE 802.11 331  
 IMP 124  
 Induktivität 57  
 Initialisierungsvektor 352  
 Integritätsprüfung 81  
 Interface Identifier 188  
 Interframe Gap 77, 84  
 Internet Architecture Board 125  
 Internet Control Message Protocol 138  
 Internetprotokoll 126  
 – IPv4 175  
 – IPv6 175  
 Internet Society 125  
 Int-Serv 230  
 IP 126  
 – -Adressierung 151  
 – Adressklasse 153  
 IPv6-Adresstyp  
 – link-lokale Adresse 189  
 – solicited Node Multicast-Adresse 190  
 – Unicastadresse, global 187  
 – unique-loal-Adresse 188  
 ISO/OSI-Referenzmodell 20, 126

**J**

Jabber 91  
 JAM-Signal 78  
 Jitter 230  
 Jumbo-Frame 92  
 Jumbograms 179

**K**

Kahn, Robert 123  
 Kanal 36  
 Kapazität 5, 57  
 Kaskadierung 88  
 – von Switches 250  
 Kern 43  
 Keystream 352  
 Klasse 60  
 Kleinrock, Leonard 123  
 Kollision 78  
 – Early- 80, 90  
 – Late- 80, 90  
 Kollisions-Domäne 76  
 Kollisionserkennung 78

**L**

LAN 5  
 Laser 46  
 Lastverbund 4  
 Latenz 230  
 Layer 2 241  
 Layer 3 271  
 Learn-and-Stay-Verfahren 245  
 Least Significant Byte 25  
 LED 46  
 Leistungsverbund 4  
 Leistungsverlust 47  
 Leitungsvermittlung 16  
 Lichtwellenleiter 37, 44  
 Lifetime 201  
 Link Aggregation 82, 250  
 LLC 24  
 Local Area Network 5  
 Logical Link Control 24

Long Wave 106

Loopback 156

## M

MAC 24

– -Adresse 73, 151

– -Flooding 267

– -Schicht 98

Malware 314

MAN 5

Managed Devices 305

Management Information Base 305,  
308

Man-in-the-Middle 203, 267, 314

Maximum Transfer Unit 180

Maximum Transmission Unit 126

MBZ 128

Media Access Control 24

Media Independent Interface 97

Metrik 273, 288

Metropolitan Area Network 5

MIB 305

MII 97

MII-Schicht 98

MIMO 336

MLT-3-Verfahren 34

Mobile IP 199

Mode 46

Modendispersion 47

Modulation

– Amplituden- 32

– Frequenz- 32

– Phasen- 32

Modulationsverfahren 339

Monomodefaser 49

Most Significant Byte 25

MTU 126

Multicast 16

Multicasting 178

Multicast Listener Discovery Protocol  
193

Multimode-Gradientenfaser 50

Multimode-Stufenfaser 49

Multiple Access 76, 78

Multiple Input Multiple Output 336

Multiplexing 35, 214, 216

– Frequenz- 36

– Zeit- 36

Multiprotokoll 198

Multi-User-MIMO 336

## N

Nameserver 146

NAT 166

Nebensprechen 57

– Fernnebensprechdämpfung (FEXT) 63

– Nahnebensprechdämpfung (NEXT) 57

Neighbor advertisement 194

Neighbor discovery 195

Neighbor Discovery Protocol 192f.

Neighbor-Discovery-Protokoll (NDP) 194

Neighbor solicitation 194

netstat 302

Network Address Translation 166

Network Slicing 239

Netzkennung 152, 156

Netzneutralität 237

Netzpräfix 152

Netzwerk 3

– -adresse 152

– -architektur 8

– -kabel 4

– -karte 4

– -management 170, 300

– -schicht 24

– virtuelles lokales 249, 259, 294

Netzwerkpräfix 201

NEXT 57

Next Header 179, 181

Non-Blocking 249

NRZI-Verfahren 34

Numerische Apertur 48

## O

OFDM 339

OFDMA 339

Open Shortest Path First 128



Open-Shortest-Path-First-Protokoll 283, 290  
Open-System-Authentifizierung 350  
Orthogonal Frequency Division Multiple Access 339  
Orthogonal Frequency Division Multiplexing 339  
OSI-Schichten 22  
OSPF 128, 283

## P

Packet Bursting 109  
Padding 131  
Paket 14, 25  
Paketvermittlung 16  
PAN 5  
Patchpanel 65  
Payload-Length 179  
PDU 20  
Personal Area Network 5  
PHY-Spezifikation 98, 108, 114  
PHY-Typen 116  
Pigtail 46  
ping 141, 293, 302  
PLCP-Header 346  
Polling 301  
Port 110, 244  
Port Security 145  
Power-over-Ethernet (PoE) 119  
Präambel 72, 346  
Priorität 179  
Priority Queuing 235  
Propagation Delay 62  
Protocol Data Unit 20  
Protokoll 3  
Prüfsumme 24, 74, 129, 179, 216  
Punkt-zu-Punkt-Verbindung 16, 261

## Q

QoS 228, 238  
Quality-of-Service 228, 238

## R

Random Early Detection 233  
RARP 138  
Rayleigh-Streuung 47  
Reassemblierung 132  
RED 233  
Redirect 194  
Reflexion 48  
Registrierungsprozess 202  
Repeater 83, 85  
– Klasse 1 102  
– Klasse 2 102  
Resource Reservation Protocol 181  
Ressourcenreservierung 230  
Retransmission 17  
Reverse Address Resolution Protocol 138  
RIP 161, 283  
RIPE 188  
RJ-45-Stecker 60, 88  
Roaming 350  
Rogue Device 203  
Root-Bridge 255  
Route Poisoning 286  
Router 271  
Router-Advertisement 192, 194  
Router-Solicitation 194  
Route-Tag-Feld 290  
Routing 25, 281  
– indirekt 133  
– Loose-Source 132  
– Methoden 277  
– Recorded 133  
– Strict-Source 133  
Routing-Algorithmus 281  
Routing Information Protocol 161, 169, 283, 287  
Routing-Protokoll 282, 287  
– Classful 284  
– Classless 285  
– Distance-Vector 283  
– Exterior-Gateway 282  
– Interior-Gateway 283  
– Link-State 284

- Routing-Schleife 286
  - Routing-Tabelle 273, 278, 281
  - RSVP 181
  - Rückflusssdämpfung 56, 62, 108
- S**
- Scanning
    - aktiv 350
    - passiv 350
  - Schichtenmodell 23
  - Second-Level-Domain 146
  - Segment 25, 212
  - Sequenznummer 139, 215, 217
  - Server 9
  - Service Set Identifier 337, 351
  - Short Frame 91
  - Short Wave 106
  - Sicherheitspolitik 313
  - Sicherungsschicht 24
  - Signalcodierung 72
  - Signalisierung 3, 32
  - Simple Internet Protocol Plus 176
  - Simple Mail Transfer Protocol 26
  - Simple Network Management Protocol 305
    - Befehle 307
  - Simplex 15
  - Sitzungsschicht 25
  - Skalierbarkeit 19
  - Sliding Window 214
  - Slot-Time 79
  - SMI 306
  - SMTP 26
  - SNMP 305
  - Snooping
    - DHCP- 145
  - Socket 214, 216
  - Solicitation Request 192
  - Source-Adresse 74
  - Spanning-Tree 253
  - Split Horizon 286
  - Spoofing 144
    - DNS- 148
  - SSID 337
  - Stabilität 19
  - Stack 22
  - Starvation 144
  - Stateful 193
  - Stateless 193
    - -Autoconfiguration 192
  - Staukontrolle 214, 221, 234
  - Store and Forward 247
  - Store-and-Forward-Netz 14
  - Structure of Management Information 306, 310
  - Subnetz 158
    - -Adresse 152
    - -Identifikator 160
    - -Strukturierung 164
    - -variable Länge 162
    - -zugehörigkeit 160
  - Subnetz-ID 187
  - Switch 39, 242
    - Stackable 244
  - Switch-Architektur
    - Bus 251
    - Matrix 251
    - Shared Memory 251
  - Switching 103
  - Switching-Verfahren 246
  - SYN 216
  - Synchronisation der Sequenznummer 216
  - Synchronität 36
  - SYN-Cookie 227
  - SYN-Flood-Attacke 225
  - SYN-Flooding 314
  - Syntax-Notation 306
  - syslog 311
  - Systemmanagement 301
- T**
- Tag-Control-Feld 75
  - Tag Protocol Identifier 75
  - TCP 211
  - Teilstreckennetz 14
  - Three-Way-Handshake 217
  - Time Exceeded 140

Timestamp 133  
– Reply 141  
– Request 141  
Time to Live 129  
Token Bucket 233  
Top-Level-Domain 146  
Topologie 6  
– Bus- 6  
– logische 8  
– physikalische 8  
– Ring- 7  
– Stern- 7  
ToS 127  
TP-Kabel 56  
Traceroute 141, 293  
Traffic Shaping 232  
Transceiver 86  
Transmission Control Protocol 211, 212  
Transport Layer Security Protokoll (TLS)  
321  
Transport-Modus 185  
Transportprotokoll 211  
Transportschicht 25  
Triggered Updates 286  
Trunk 261  
TTL 129  
TUBA 176  
Tunneling 197  
Tunnel-Modus 185  
Twisted-Pair 55  
– -Kabeltypen 56  
Type of Service 127

## U

Übertragung  
– analog 32  
– digital 32  
Übertragungsfrequenz 47  
Übertragungskapazität 15  
Übertragungsrage 45  
UDP 211  
Unicast 16  
Universal Resource Identifier 125  
Urgent-Zeiger 216

User Datagram Protocol 211, 224  
– Header 224  
UTP-Kabel 56, 62

## V

Verbindung  
– kupferbasiert 105  
– Monomode 105  
– Multimode 105  
Verbindungsabbau 218  
Verbindungsaufbau 25, 217  
Verfügbarkeitsverbund 4  
Verkabelung 3, 37  
– Glasfaser- 41  
– Kupfer- 55  
– Primär- 37  
– Sekundär- 37  
– Tertiär- 38  
– Twisted-Pair- 55  
Verschlüsselung 26, 185  
Verzögerung 10  
Virtual-Carrier-Sense-Konzept 344  
Virtual-Router-Redundancy-Protokoll  
276  
VLAN 259  
– Typen 260  
VLAN Trunk Protocol 262  
VLSM 162  
Vollader 51  
Voll duplex 15  
VRRP 276  
VTP 262

## W

Wegewahl 6, 14, 281  
Weighted Fair Queuing 235  
– Class-Based - 237  
Wellenlänge 42  
Well-Known-Port 216  
Well-Known-Service 216  
WEP 352  
WFQ 235  
Wide Area Network 5

- Widerstand 56
- Wi-Fi 6 329
- Wi-Fi Protected Access 350, 353
- Wi-Fi Protected Access 2 354
- Wi-Fi Protected Access 3 354
- Windowgröße 216
- Wireless Local Area Network 329, 338
  - Header 346
- Wires Equivalent Privacy 352
- Wireshark 320
- Wire-Speed 249
- Wiring Closet 59
- WLAN 329
- WPA 350
- WPA2 354
- WPA3 354