

INFORMATIK

DEPARTMENT FÜR ANGEWANDTE INFORMATIK

INTERNET-TECHNOLOGIEN

Grundlagen

Die Autorinnen danken für jedes konstruktive Feedback. Verbesserungsvorschläge und Korrekturen von Anwenderinnen werden nach Möglichkeit zeitnah nach Bekanntwerden umgesetzt, d.h.:

„Bei der Generierung aktueller Versionen - automatische Generierung - werden die aktuellen Änderungen berücksichtigt.“

© 2011-2023, neo Lernhilfen, Graz, AUSTRIA

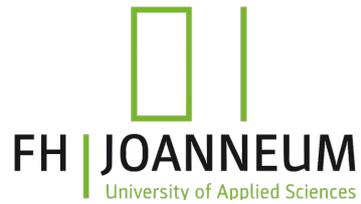
Urheberrecht:

An den übergebenen/präsentierten Unterlagen und den darin enthaltenen Werken und Leistungen, insbesondere an darin enthaltene Grafiken, Text, Textangaben, Rechenbeispielen, udgl (folgend kurz „Werke“ genannt) stehen die ausschließlichen Urheberrechte und Nutzungsrechte Herrn DI Edgar Neuherz unbeschränkt zu; jede - auch auszugsweise - Nutzung der Werke, insbesondere in Vorträgen, als Schulungs- und Unterrichtsmaterial bedarf daher zuvor einer schriftlichen Vereinbarungen mit Herrn DI Neuherz; in jedem Fall ist die Namensnennung durch den Hinweis © DI Edgar Neuherz einzuhalten.

Alle Angaben erfolgen ohne Gewähr: Eine Haftung der Autorinnen ist ausgeschlossen.

E-Mail: office@neo-lernhilfen.at

(Version: 2023-10-30 11:00)



INTERNET-TECHNOLOGIEN

Grundlagen

Studienjahr 2023/24

2023-10-30

v1.00

(Version: 2023-10-30 11:00)



(Download)

Verantwortlich für den Inhalt:

DI G. Mittenecker & DI E. Neuherz, Graz

Historische Entwicklung	1
1 Das Internet	3
1.1 Einführung	3
1.1.1 Offene Systemarchitektur	3
1.1.2 Internetstandards	3
1.1.3 Request for Comments	3
1.2 Vom ARPANET zum INTERNET	4
1.2.1 Die ARPA	4
1.2.2 Das ARPANET	4
1.2.3 TCP-Protokoll	4
1.2.4 Ethernet-Technologie	5
1.3 Geburtsstunde des Internets	5
1.3.1 Öffentliche Demonstration	5
1.3.2 Entwicklung von UNIX	5
1.3.3 Internetworking	5
1.3.4 Erster Internetwurm	5
2 Das WWW	7
2.1 Einführung	7
2.1.1 Hypertext	7
2.1.2 Hypermedia	7
2.1.3 Hyperlink	7
2.2 Das World Wide Web	8
2.2.1 Übersicht	8
2.2.2 Erster WWW-Server	8
2.2.3 HTTP-Standards	8
2.2.4 WWW-Browser	8
2.2.5 HTML-Standards	8
3 ISO/OSI Referenzmodell	9
3.1 Begriffe	10
3.1.1 Schichtenmodell	10
3.1.2 OSI-Modell	10
3.1.3 7 Schichten	10
3.1.4 Protokoll	10
3.1.5 Schnittstellen	10
3.1.6 Protokollstapel	10
3.2 OSI Referenzmodell	11
3.2.1 Bitübertragungsschicht (Schicht 1)	11
3.2.2 Sicherungsschicht (Schicht 2)	11
3.2.3 Vermittlungsschicht (Schicht 3)	11
3.2.4 Transportschicht (Schicht 4)	11
3.2.5 Sitzungsschicht (Schicht 5)	11
3.2.6 Darstellungsschicht (Schicht 6)	11
3.2.7 Anwendungsschicht (Schicht 7)	11
3.3 TCP/IP Referenzmodell	12
3.3.1 Netzzugangsschicht (OSI 1-2)	12
3.3.2 Internetschicht (OSI-Schicht 3)	12
3.3.3 Transportschicht (OSI 4)	12

Basistechnologien

13

4 Rechnernetze

15

- 4.1 Übersicht 15
- 4.2 Übertragungstechniken 16
 - 4.2.1 Übertragungsrichtung 16
 - 4.2.2 Kommunikationsformen 16
 - 4.2.3 Punkt-zu-Punkt Netze 16
- 4.3 Physikalische Netztopologien 17
 - 4.3.1 Punkt-zu-Punkt Netzwerk 17
 - 4.3.2 Teilvermaschtes Netz 17
 - 4.3.3 Ring 17
 - 4.3.4 Bus 17
 - 4.3.5 Stern 17
 - 4.3.6 Hybride Sterntopologie 17
- 4.4 Netzwerkbezeichnungen 18
 - 4.4.1 PAN 18
 - 4.4.2 LAN 18
 - 4.4.3 MAN 18
 - 4.4.4 WAN 18
 - 4.4.5 GAN 18
 - 4.4.6 Internetworks 18

5 Datencodierung

19

- 5.1 Digitale Datencodierung 19
 - 5.1.1 Binärdatendarstellung 19
 - 5.1.2 Signalübertragung 19
 - 5.1.3 Datenübertragungsrate 19
- 5.2 Codierungstechniken 20
 - 5.2.1 Übersicht 20
 - 5.2.2 NRZ-L-Kodierung 20
 - 5.2.3 NRZI-Kodierung 20
 - 5.2.4 Manchester Kodierung 20
 - 5.2.5 MLT-3 Kodierung 20
- 5.3 Zusammengesetzte Codierverfahren 20
 - 5.3.1 4B5B 20

6 Datenübertragung

21

- 6.1 Nachrichtentechnik Grundlagen 22
 - 6.1.1 Periodische Funktionen 22
 - 6.1.2 Harmonische Schwingung 22
 - 6.1.3 Fourier Transformation 22
 - 6.1.4 Rechteckimpuls 22
- 6.2 Übersicht der Übertragungsmedien 23
 - 6.2.1 Kupferkabel 23
 - 6.2.2 Lichtwellenleiter 23
 - 6.2.3 Drahtlose Übertragung 23
- 6.3 Physikalische Grundlagen 24
 - 6.3.1 Physikalische Größe 24

6.3.2	SI-Einheitensystem	24
6.4	Kennwerte	25
6.4.1	Das Bel (dBel)	25
6.4.2	Impedanz	25
6.4.3	Signaldämpfung	25
6.4.4	Nebensprechdämpfung	25

7 Übertragungsmedien 26

7.1	Kupferkabel-Technologie	27
7.1.1	Twisted Pair Kabel	27
7.1.2	RJ-Steckverbindung	27
7.1.3	Kabel-Kategorien	27
7.1.4	Verbreitete Kabeltypen	27
7.1.5	TP-Ethernet Vernetzung	27
7.1.6	Ethernet Kabellängen	27
7.2	Glasfaser-Technologie	28
7.2.1	Optische Übertragung	28
7.3	Drahtlos-Technologien	29
7.3.1	Implementierung von WLANs	29
7.3.2	Roaming in WLANs	29
7.3.3	Richtfunktechnologie	29
7.3.4	Wi-Fi Generationen	29

Internetdienste und Anwendungen 31

8 Internettechnologien 33

8.1	Organisationen	34
8.1.1	RIPE NCC	34
8.1.2	ISOC	34
8.1.3	IANA	34
8.1.4	IAB	34
8.2	Der Standardisierungsprozeß	35
8.2.1	Request for Comments (RFC)	35
8.2.2	Entwicklungsprozeß	35
8.3	Internet Protocol (IPv4)	36
8.3.1	Grundbegriffe	36
8.3.2	IP-Adress-Klassen	37
8.3.3	Spezielle IP-Adressen (Broadcast, Loopback, ...)	38
8.3.4	Subnetz-Adressierung	39
8.4	Internet Protocol Version 6 (IPv6)	40
8.4.1	IPv6-Adressen	40
8.5	Domain Name System	42
8.5.1	Namens- und Verzeichnisdienste	42
8.5.2	Domain Name System	42
8.5.3	Fully Qualified Name	42
8.5.4	Domains und Subdomains	42
8.5.5	DNS Server	43
8.6	Routing	44
8.6.1	Routing Tabellen	44
8.6.2	IP Forwarding	44
8.6.3	IPv4 Datagramm	44
8.6.4	NAT und Masquerading	45

8.6.5	ICMP, Traceroute	45
8.7	Transportprotokolle	46
8.7.1	TCP	46
8.7.2	UDP	49
8.7.3	HTTP/3 (mit UDP statt TCP)	49

9 Netzwerkkomponenten 51

9.1	Einteilung	51
9.1.1	Passive Netzwerkkomponenten	51
9.1.2	Aktive Netzwerkkomponenten	51
9.1.3	Übersicht	52
9.2	Netzwerkkarten	52
9.2.1	MS Windows (NDIS)	52
9.2.2	MS-Windows NT 4.0	52
9.2.3	MS-Windows Vista, Windows 7	52
9.3	Repeaters/Hubs	53
9.3.1	Topologie	53
9.3.2	Funktionen	53
9.3.3	Kaskadierung von Hubs	53
9.3.4	Einsatz	53
9.3.5	Direkter Vergleich	53
9.4	Bridges	54
9.4.1	Weiterleitung und Filterung	54
9.4.2	Selbstlernende Bridges	54
9.4.3	Schleifenbildung durch Bridging	55
9.4.4	Spanning-Tree	55
9.4.5	Übersetzende Bridges	55
9.5	Switches	56
9.5.1	Port-Tabellen von Switches	56
9.5.2	Arbeitsweise von Switches	56
9.5.3	VLAN	57
9.6	Routers	58
9.6.1	Routing-Tabellen	58
9.6.2	Routing-Algorithmen	59
9.6.3	Routing-Protokolle	60
9.7	Firewalls	61

10 Internetdienste 63

10.1	Electronic Mail Service	64
10.1.1	Email	64
10.1.2	Basisfunktionen	64

Anhang 65

11 Personenregister 66

11.1	Pioniere des Internet	66
11.1.1	Vannevar Bush	66
11.1.2	J. C. R. Licklider	66
11.1.3	Charles Herzfeld	67
11.1.4	Paul Baran	67
11.1.5	Theodor Holm Nelson	67

11.1.6	Leonard Kleinrock	67
11.1.7	Lawrence Roberts	68
11.1.8	Steve Crocker	68
11.1.9	Jon Postel	68
11.1.10	Vinton G. Cerf	68
11.1.11	Robert E. Kahn	69
11.1.12	Ray Tomlinson	69
11.1.13	Robert Metcalfe	69

Abbildungsverzeichnis

1.1	Pioniere des Internets	4
1.2	ARPANET in December 1969	4
2.1	ein Hypertextsystem von 1969	7
2.2	Kommerzialisierung des Internets	8
3.1	IPv4-Header	12
3.2	IPv6-Header	12
3.3	TCP-Header	12
4.1	Übersicht Rechnernetze	15
4.2	Übersicht Übertragungstechniken	16
5.1	Übersicht der Kodierungsarten	20
5.2	NRZ-L codierte Datenfolge	20
5.3	NRZI codierte Datenfolge	20
5.4	Manchester codierte Datenfolge	20
5.5	MLT-3 codierte Datenfolge	20
6.1	Darstellung Rechteckimpuls durch Fourierreihe	22
6.2	Sinus 1. und 3. Ordnung	22
6.3	Koaxialkabel	23
6.4	Twisted Pair Kabel	23
6.5	Lichtwellenleiter	23
6.6	Funk-LAN	23
6.7	Richtfunk	23
6.8	Physikalische Größe	24
6.9	NEXT und FEXT	25
6.10	Signaldämpfung	25
7.1	Unshielded Twisted Pair	27
7.2	Shielded Twisted Pair	27
7.3	RJ45 Stecker	27
7.4	Aufbau Singlemode und Multimode Glasfaser-Kabel	28
7.5	WLAN - Handover (Roaming)	29
7.6	WLAN	29
7.7	WLAN - Handover (Roaming)	29
7.8	Richtfunk	29
8.1	Regionale Registries	34
8.2	Beispiel einer IP-Adresse	37
8.3	Adressbereich der 32-Bit-IP-Adresse	37
8.4	Primäre Adress-Klassen A, B und C	37
8.5	speziellen Klassen D und E	37
8.6	Limited Broadcast	38
8.7	Loop-Back-Adresse	38
8.8	Beispiel einer privaten Netz-ID	38
8.9	Beispiel einer Multicast Adresse	38
8.10	Beispiel einer Subnetz-Adressierung	39
8.11	Beispiel einer Subnetzmaske	39
8.12	Default Masken für die Klassen A, B und C	39
8.13	Klassenlose Notation	39
8.14	Anzahl von möglichen IPv6 Adressen	40
8.15	Beispiel einer IPv6-Adresse	40
8.16	Beispiel mit unterdrückten Nullen	40
8.17	Alternative Schreibweisen	40
8.18	IPv6 URL-Notation	40
8.19	IPv6 URL-Notation (inkl. Portnummer)	40
8.20	IPv6 Netz-Notation	40
8.21	Loop-Back-Adresse	41

8.22	Nicht spezifizierte IPv6-Adresse	41
8.23	Link-Local-Unicast-Adresse	41
8.24	DNS Adressraum Hierarchie	42
8.25	Beispiel einer FQDN	42
8.26	Beispiele für FQHN	42
8.27	FQDN der Subdomain peanut	42
8.28	Beispiel zu Routingtabellen	44
8.29	IPv4 Datagramm Header	44
8.30	TCP-Header	46
8.31	TCP/IP Socket	47
8.32	Zwei TCP Verbindungen	47
8.33	TCP Verbindungsaufbau	47
8.34	Zustandsübergangs-Diagramm	48
8.35	TCP Verbindungsabbau	48
8.36	Bestätigungsmechanismus in TCP	48
9.1	Beispiele aktiver Netzwerkkomponenten	52
9.2	NDIS-Multiprotokollstapel	52
9.3	Dual IP Layer TCP/IP Protocol Stack	52
9.4	Next Generation TCP/IP Stack	52
9.5	Topologie eines Multiport Repeaters	53
9.6	Selbstlernende Bridges - Funktionsweise	54
9.7	Verbindung von LAN-Segmenten	54
9.8	Spanning Tree Protocol (STP)	55
9.9	Schleifenbildung durch Bridging	55
9.10	Übersetzende Bridges	55
9.11	Source Address Table (SAT) von Switches	56
9.12	Store and Forward Switching	56
9.13	Cut Through Switching	56
9.14	VLAN auf Basis von Organisationseinheiten	57
9.15	Routing Tabellen (Next Hop)	58
9.16	Netzwerke mit Router	58
9.17	Routing Tabellen mit Default Routen	58
9.18	Einteilung der Routing-Algorithmen	59
9.19	Routenwahl durch Hopminimierung	59
9.20	Routenwahl durch Kostenminimierung	60
9.21	Autonomes System	60
10.1	Funktionsweise eines Email-System	64
10.2	Analogie Brief zu Email	64
10.3	Funktionsweise eines Email-System	64
11.1	Vannevar Bush	66
11.2	J. C. R. Licklider	66
11.3	Charles Maria Herzfeld	67
11.4	Paul Baran	67
11.5	Theodor Holm Nelson	67
11.6	Leonard Kleinrock	67
11.7	Lawrence Roberts	68
11.8	Steve Crocker	68
11.9	Jon Postel	68
11.10	Vinton G. Cerf	68
11.11	Robert E. Kahn	69
11.12	Ray Tomlinson	69
11.13	Robert Metcalfe	69

Tabellenverzeichnis

5.1	Binäre Einheiten	19
5.2	4B5B Codegruppen	20
6.1	SI-Basisgrößen	24
6.2	SI-Einheiten der Mechanik	24
6.3	SI-Einheiten der Kinematik	24
6.4	dB-Werte	25
6.5	Kennwerte der Signaldämpfung	25
6.6	Kennwerte der Nebensprechdämpfung	25
7.1	Kabeltypen	27
7.2	Ethernet Vernetzung	27
7.3	Längen für Kupfer-Doppelader	27
7.4	Wi-Fi Generationen	29
8.1	Eigenschaften der IP-Adress-Klassen	37
8.2	Private Adressbereiche	38
9.1	Vergleich Hub mit Switch	53
9.2	Port Zustände eines Switches	55

Historische Entwicklung

Inhaltsangabe

1.1	Einführung	3
1.1.1	Offene Systemarchitektur	3
1.1.2	Internetstandards	3
1.1.3	Request for Comments	3
1.2	Vom ARPANET zum INTERNET	4
1.2.1	Die ARPA	4
1.2.2	Das ARPANET	4
1.2.3	TCP-Protokoll	4
1.2.4	Ethernet-Technologie	5
1.3	Geburtsstunde des Internets	5
1.3.1	Öffentliche Demonstration	5
1.3.2	Entwicklung von UNIX	5
1.3.3	Internetworking	5
1.3.4	Erster Internetwurm	5

1.1 Einführung

Das Internet, im Alltag oft fälschlicherweise mit dem **World Wide Web** selbst identifiziert, ist mittlerweile durch Smart-Phones immer erreichbar und versorgt uns mit Informationen aus allen nur denkbaren Bereichen.

Das **Internet** ist der Zusammenschluss aus vielen miteinander verbundenen Netzwerken.

Definition 1.1

Sehr oft wird dieser Begriff fälschlicherweise mit dem **World Wide Web** (WWW) gleichgesetzt welches aber nur einen Dienst des Internets darstellt.

1.1.1 Offene Systemarchitektur

Durch ein festes Regelwerk (Kommunikationsprotokolle) ist es möglich verschiedene Hardwarekomponenten (Netz-Hardware) unabhängig von ihrer technologischen Umsetzung zu verbinden.

Ein **Kommunikationsprotokoll** (Protokoll) ist eine Sammlung von Regeln und Vorschriften, die Datenformat und Übertragungsart einer Nachricht festlegt (wie z. B. Verbindungsauf-, abbau, etc.).

Definition 1.2

1.1.2 Internetstandards

Die erfolgreiche Verbreitung des Internets ist vor allem der offenen Systemarchitektur zu verdanken, d.h. alle notwendigen Spezifikationen sind öffentlich verfügbar und für jeden zugänglich.

Die **Internetstandards** werden in Form eines öffentlichen Standardisierungsprozess verabschiedet, der es prinzipiell jedem Benutzer ermöglicht zu einem zukünftigen Standard Stellung zu beziehen (**RFC**) und sich so an der Entwicklung des Internets zu beteiligen.

Definition 1.3

Weiters sind die Internet-Kommunikationsprotokolle darauf ausgelegt unterschiedliche Computer, Betriebssysteme und Anwendungen miteinander zu verbinden.

1.1.3 Request for Comments

Neue Technologien im Internet entstehen durch Diskussionen von Experten in den sogenannten **RFC**¹

Definition 1.4

Daraus entstand eine durchnummerierte Sammlung von Internet-Dokumenten in den Technologien, Standards und Sonstiges dokumentiert und standardisiert wurde.



Internet



RFC

¹englisch: **RFC** = Request for Comments

1.2 Vom ARPANET zum INTERNET

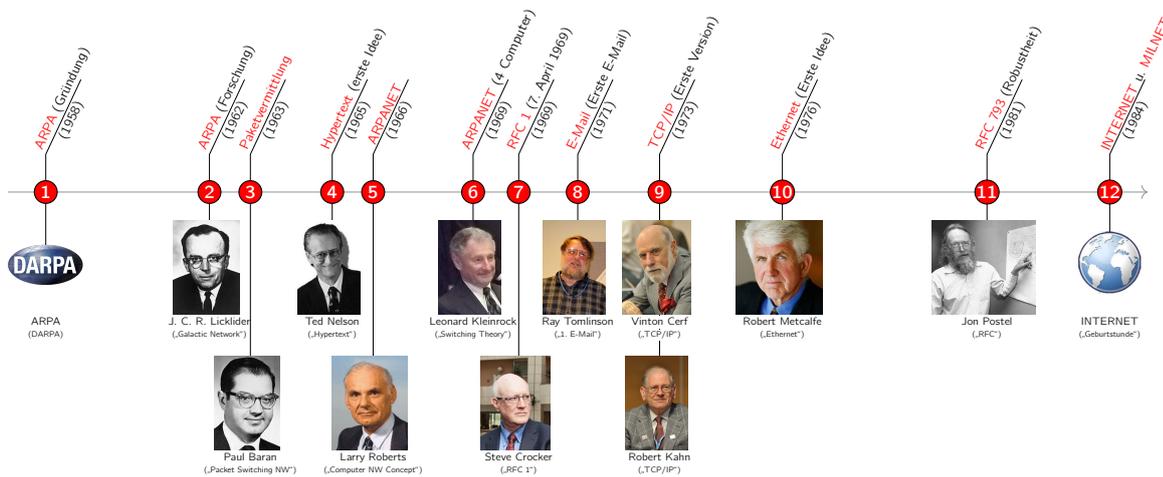


Abb. 1.1: Pioniere des Internets

1.2.1 Die ARPA

Am 4. Oktober 1957 startete die Sowjetunion den ersten russischen Satelliten Sputnik.

Der sogenannte **Sputnik-Schock** bezeichnet die politischen und gesellschaftlichen Reaktionen in der Westlichen Welt (insbesondere der USA) auf den Start des ersten künstlichen Erdsatelliten **Sputnik 1** durch die **Sowjetunion**.

Definition 1.1

Durch dieses Ereignis wurde die Entwicklung von Militär- und Raumfahrttechnologien intensiviert und im November 1957 im Kongress ein Konzept für die ARPA präsentiert.

Die **ARPA**² bezeichnet eine Behörde des Verteidigungsministeriums der Vereinigten Staaten, die Forschungsprojekte im Auftrag des Militärs durchführt und am 7. Februar 1958 gegründet wurde.

Definition 1.2

Die ARPA beschäftigte weder Wissenschaftler noch besaß sie Forschungseinrichtungen oder Laboratorien.

Sie umfasste nur ein kleines Büro und ein schmales Budget (Pentagon-Standards).

Ihre Aufgabe bestand darin Forschungsgelder und Aufträge an Unternehmen und Universitäten zu verteilen, deren Ideen vielversprechend erschienen.

Sie diente als Koordinationsstelle für private und universitäre Forschungsprojekte.

Zwar wurden die Projekte durch das Militär gefördert, aber die Ergebnisse unterlagen keiner strengen Geheimhaltung, wurden von Forschern und Unternehmen öffentlich publiziert und auf Kongressen vorgestellt (wie z. B. BSD-Unix, TCP/IP, etc.).

1.2.2 Das ARPANET

Mit Sputnik stieg auch die Gefahr eines nuklearen Erstschlags der UDSSR und der Aufbau eines Kommunikationssystems, das in der Lage war, einen solchen Angriff zu überleben, gewann an Bedeutung.



Abb. 1.2: ARPANET in December 1969

Das ARPANET entwickelte sich wie folgt:

- **Dezember 1969:** 4 Hosts
- **April 1971:** 23 Hosts über 15 Knotenpunkte
- **Januar 1973:** 35 Knoten
- **ab Mitte 1973:** erste internat. Knoten (UK,NO)
- **ab 1975:** Satellitenverbindung (UK,NO)
- **ab 1977:** erste öffentliche Demonstration
- **ab 1983:** über 500 Hosts
- **ab 1983:** Aufspaltung in zivilen und militärischen Teilbereich (MILNET)

1.2.3 TCP-Protokoll

1983 wurde die Kommunikationssoftware aller angeschlossenen Rechensysteme vom alten **NCP**³ auf das 1973 unter der Leitung von Vinton Cerf und Robert Kahn entwickelte **TCP/IP**⁴ umgestellt.

Die Umstellung auf das **TCP/IP**-Protokoll wurde notwendig, da es unter **NCP** nur bedingt möglich war, eine Kommunikation über heterogene Netzwerke hinweg zu gewährleisten.

Dies war für die erfolgreiche, weltweite Verbreitung für das Netz der Netze entscheidend.

³englisch: **NCP** = Network Control Protocol

⁴englisch: **TCP/IP** = Transmission Control Protocol/Internet Protocol

²englisch: **ARPA** = Advanced Research Projects Agency

1.2.4 Ethernet-Technologie

Durch einen Konferenzbeitrag 1970 von Norman Abramson von der Universität Hawaii über das paketvermittelte Funknetzwerk ALOHANET angeregt, entwickelte Robert Metcalfe die Idee des Ethernet.

Metcalfe zeigte in seiner Studienabschlußarbeit daß unter Verwendung der mathematischen Warteschlangentheorie eine Effizienz von bis zu 90 % der theoretischen Maximalkapazität erreicht werden kann, ohne daß das System durch Paket-Kollisionen blockiert wird.

Er präsentierte seine Idee auf der National Computer Conference im Juni 1976.

1.3 Geburtsstunde des Internets

Zwei Gründe leisteten einen wesentlichen Beitrag für den Erfolg des Internets:

- Öffnung des neuen Mediums für die Allgemeinheit
- Bereitstellung einfacher Benutzerschnittstelle

Am 1. Januar 1983 wurde das ARPANET von NCP auf die neue Protokollfamilie **TCP/IP** und ihren drei Basisprotokollen umgestellt:

- **IP**⁵
- **TCP**⁶
- **ICMP**⁷

Dadurch wurde erstmals eine gemeinsame Zusammenschaltung unterschiedlicher Netzwerktechnologien auf einfache und effiziente Weise möglich.

1.3.1 Öffentliche Demonstration

Im Oktober 1972 sollte in Washington eine Tagung der **ICCC**⁸ mit einer ersten öffentlichen Demonstration des **ARPANET** stattfinden.

Robert Kahn als verantwortlicher Leiter der Demonstration benötigte ein knappes Jahr, um eine Hand voll Applikationen im ARPANET wirklich soweit stabil und lauffähig zu entwickeln, damit die geplante Demonstration erfolgreich verlaufen konnte.

Im Erdgeschoß des Washington Hilton Hotels konnte die Öffentlichkeit einen direkten Zugang zum **ARPANET** nutzen, von wo aus Anwendungen verteilt über die gesamte USA gestartet werden konnten. [4, S 30]

Die Demonstration war ein großer Erfolg, und Wissenschaftler aus der ganzen Welt erhielten einen ersten Einblick in die Möglichkeiten, die das ARPANET bot.

Eine der bekanntesten Demonstrationen zeigte eine Unterhaltung mit ELIZA⁹, einem Programm am Massachusetts Institute of Technology.

⁵englisch: **IP** = Internet Protocol

⁶englisch: **TCP** = Transmission Control Protocol

⁷englisch: **ICMP** = Internet Control Message Protocol

⁸englisch: **ICCC** = International Conference on Computer Communications

⁹einem Programm Joseph Weizenbaums, das das Verhalten eines Psychiaters nachahmte

1.3.2 Entwicklung von UNIX

Die Entwicklung des Betriebssystem UNIX¹⁰ leistete einen wichtigen Anteil an der Verbreitung von **TCP/IP** und der Popularität des Internet.

BSD-UNIX wurde an vielen amerikanischen Universitäten verwendet.

ARPA unterstützte dabei parallel:

- **Bolt, Beranek, Newman** (BBN) bei der zügigen Implementierung der **TCPIIP**-Protokolle.
- **Berkeley** bei der Integration der **TCP/IP**-Protokolle in deren Betriebssystem-Distribution.

Damit gelang es der ARPA zur rechten Zeit, über 90 % der Informatik-Abteilungen der amerikanischen Universitäten zu erreichen.

Die BSD-UNIX Distribution gewann sehr große Popularität, da sie neben den Standard **TCP/IP**-Anwendungsprogrammen zusätzliche Netzwerk-Management-Programme zur Verfügung stellte.

Durch die Implementierung von Sockets in der BSD-Distribution konnten Anwendungsprogramme direkt auf die Kommunikationsprotokolle zugreifen.

Die Verwendung von Sockets war unkompliziert und ermöglichte es vielen Wissenschaftlern, selbst mit **TCP/IP** zu experimentieren.

Bereits 1976 waren die **TCP/IP** Protokolle vollständig in BSD-UNIX integriert.

1.3.3 Internetworking

1977 fand erstmalig eine öffentliche Demonstration des Internetworking, eine Kommunikation über verschiedene, nicht kompatible Computernetzwerke, statt.

Dabei zeigten Vinton Cerf und Robert Kahn einen über **TCP** verbundenen Zusammenschluß aus Packet Radio Net, SATNET und ARPANET.

Aus einem Lieferwagen an der Westküste der USA wurden Datenpakete über die USA hinweg an das University College in London via Satellit gesendet, dann zurück nach Virginia und schließlich an die University of Southern California.

1.3.4 Erster Internetwurm

Am Abend des 2. November 1988 legte der erste Internetwurm, ein sich selbst reproduzierendes Programm, sagenhafte 10 % der damals 60.000 an das Internet angeschlossenen Rechner lahm und erregte damit großes Aufsehen in der Öffentlichkeit.

Innerhalb weniger Stunden hatte sich das Programm über das Gebiet der gesamten USA ausgebreitet, hatte Tausende von Computern befallen und diese, auf Grund der Systemlast, die seine Aktivität erzeugte, außer Betrieb gesetzt.

¹⁰insbesondere das frei verfügbare Betriebssystem BSD-UNIX an der University of California in Berkeley



Internet



ICCC 1972

2

Das WWW

Inhaltsangabe

2.1	Einführung	7
2.1.1	Hypertext	7
2.1.2	Hypermedia	7
2.1.3	Hyperlink	7
2.2	Das World Wide Web	8
2.2.1	Übersicht	8
2.2.2	Erster WWW-Server	8
2.2.3	HTTP-Standards	8
2.2.4	WWW-Browser	8
2.2.5	HTML-Standards	8

2.1 Einführung

2.1.1 Hypertext



Quelle: [1]

Abb. 2.1: ein Hypertextsystem von 1969

Ein **Hypertext** ist ein Text mit einer netzförmigen, dynamischen Struktur, die die gewohnte lineare Ordnung statisch gedruckter Publikationen aufbricht.

Definition 2.1

Hypertexte sind nicht vorgesehen wie ein Buch von Anfang bis Ende zu lesen.

Er wird in Auszeichnungssprachen geschrieben, die neben für den Leser nicht sichtbaren Gestaltungsanweisungen auch Hyperlinks enthalten, also Querverweise zu entfernten Textpassagen oder anderen Dokumenten im Netzwerk.

Die gebräuchlichste Auszeichnungssprache für Internetdokumente ist die Hypertext Markup Language (HTML), die in der Gegenwart allgegenwärtig ist.

Ein Hypertext kann informatisch als Netzwerk aus Hypertext-Knoten beschrieben werden, die durch Hyperlink-Kanten verbunden sind.

2.1.2 Hypermedia

Ted Nelson prägt 1965 bei einer ACM¹-Jahreskonferenz das Wort Hypertext und Hypermedia.

Hypermedia sind elektronische, multimediale Dokumente, die Verbindungen (Hyperlinks) zu anderen Dokumenten/Informationen enthalten und umfassen neben Texte auch andere Medien.

Definition 2.2



Hypermedia

Fälschlicherweise wird Hypermedia oftmals mit Multimedia gleichgesetzt oder verwechselt. Viele Autoren benutzen die Begriffe Hypertext und Hypermedia synonym.

Das derzeit größte existierende Hypermedium ist das World Wide Web.

2.1.3 Hyperlink

Ein **Hyperlink** ist ein Verweis auf eine andere Textstelle im aktuellen oder einem anderen Hypermedia-Dokument, der zur nicht-linearen Vernetzung von Informationen in Dokumenten dient.

Definition 2.3



Hyperlink



Hyperlink

Im Allgemeinen wird der Begriff auf das World Wide Web bezogen, in dem Hyperlinks ein Kernbestandteil sind; hierzu ist auch der Begriff Weblink einschlägig.

Durch das Hypertextsystem können auch Dateien anderen Typs, die im selben System vorliegen oder daran angeschlossen sind, aufgerufen werden.

So können Hyperlinks genutzt werden, um beispielsweise Filme, Bilder und Animationen zu erreichen oder Dateien auf einen Computer herunterzuladen.

¹englisch: ACM = Association for Computing Machinery (erste wissenschaftliche Gesellschaft für Informatik, gegründet 1947)

2.2 Das World Wide Web

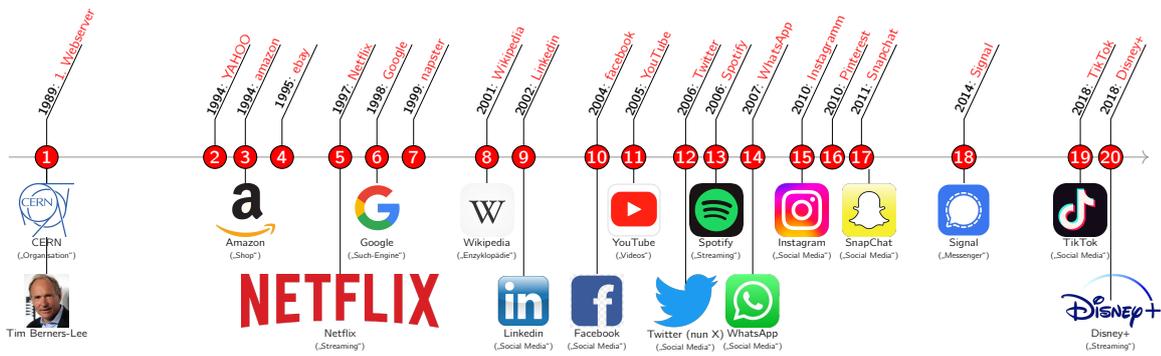


Abb. 2.2: Kommerzialisierung des Internets

2.2.1 Übersicht

Der Erfolg des Internets ist vor allem der einfachen Benutzung zu verdanken, d.h. auch ein Nichtfachmann kann durch einen Webbrowser auf verschiedene, durch Hyperlinks verknüpfte, Webseiten zugreifen.

Das **WWW**² bezeichnet eine Technologie, mit der man einfach auf ein verteiltes Hypermedia-Dokumentenmodell zugreifen kann.

Definition 2.1

2.2.2 Erster WWW-Server

Am 12. März 1989 präsentierte Tim Berners Lee im Schweizer Kernforschungsinstitut (CERN) einen Vorschlag für ein verteiltes Hypertext-basierendes Dokumenten-Managementsystem.

„The WorldWideWeb (W3) is a wide-area hypermedia information retrieval initiative aiming to give universal access to a large universe of documents.“
(Tim Berners-Lee)

Zitat 2.1

Im Folgejahr entwickelte er zusammen mit Robert Cailliau den ersten WWW-Server und WWW-Browser. Zu Weihnachten 1990 wurde auf Berners-Lees NeXT-Rechner die erste Website in Betrieb genommen.

2.2.3 HTTP-Standards

HTTP³ ist ein Protokoll für die Kommunikation zwischen Browsern und WWW-Servern.

Definition 2.2

HTTP wurde von der **IETF**⁴ und dem **W3C**⁵ standardisiert und die aktuelle Version HTTP/3 im Juni 2022 als RFC 9114 veröffentlicht.

HTTPS⁶ ist ein Kommunikationsprotokoll im World Wide Web, mit dem Daten abhörsicher übertragen werden können.

Definition 2.3

² englisch: **WWW** = World Wide Web

³ englisch: **HTTP** = Hypertext Transfer Protocol

⁴ englisch: **IETF** = Internet Engineering Task Force

⁵ englisch: **W3C** = World Wide Web Consortium

⁶ englisch: **HTTPS** = Hypertext Transfer Protocol Secure (sicheres Hypertext-Übertragungsprotokoll)

2.2.4 WWW-Browser

Ein **Browser** ist ein spezielles Programm welches auf Dokumente, die von einem Web-Server zur Verfügung gestellt werden, zugreifen und ihre Inhalte darstellen kann.

Definition 2.4

Anfänge des WWW

Anfang der 1990er Jahre erschien mit dem Netscape Navigator von Netscape Communications als Nachfolger des NCSA Mosaic ein neuartiger Browser.

Als 1995 die Benutzung des World Wide Webs populär wurde, hatte der Netscape Navigator einen Marktanteil von weltweit über 80 Prozent.

Browserkrieg

Als **Browserkrieg** wird ein von 1995 bis 1998 andauernder Verdrängungswettbewerb zwischen den Unternehmen Microsoft und Netscape um die Vorherrschaft ihrer Webbrowser bezeichnet.

Definition 2.5

Microsoft konnte sich am Ende mit seinem Produkt Internet Explorer gegen das Konkurrenzprodukt Netscape Navigator durchsetzen.

Die Entwicklung ab 2004, in denen Mozilla Firefox und andere alternative Browser dem Internet Explorer wieder Marktanteile abnehmen konnten, wird zuweilen als „zweiter Browserkrieg“ bezeichnet.

2.2.5 HTML-Standards

HTML⁷ ist ein Dokumentenformat und dient zur Darstellung von verschiedenen Medien in einem Browser.

Definition 2.6

HTML dient als Auszeichnungssprache dazu, einen Text semantisch zu strukturieren, nicht aber zu formatieren.

Die visuelle Darstellung ist nicht Teil der HTML-Spezifikationen und wird durch den Webbrowser und Gestaltungsvorlagen wie **CSS**⁸ bestimmt.

⁷ englisch: **HTML** = Hypertext Markup Language (Hypertext-Auszeichnungssprache)

⁸ englisch: **CSS** = Cascading Style Sheets („gestufte Gestaltungsbögen“)

3

ISO/OSI Referenzmodell

Inhaltsangabe

3.1	Begriffe	10
3.1.1	Schichtenmodell	10
3.1.2	OSI-Modell	10
3.1.3	7 Schichten	10
3.1.4	Protokoll	10
3.1.5	Schnittstellen	10
3.1.6	Protokollstapel	10
3.2	OSI Referenzmodell	11
3.2.1	Bitübertragungsschicht (Schicht 1)	11
3.2.2	Sicherungsschicht (Schicht 2)	11
3.2.3	Vermittlungsschicht (Schicht 3)	11
3.2.4	Transportschicht (Schicht 4)	11
3.2.5	Sitzungsschicht (Schicht 5)	11
3.2.6	Darstellungsschicht (Schicht 6)	11
3.2.7	Anwendungsschicht (Schicht 7)	11
3.3	TCP/IP Referenzmodell	12
3.3.1	Netzzugangsschicht (OSI 1-2)	12
3.3.2	Internetschicht (OSI-Schicht 3)	12
3.3.3	Transportschicht (OSI 4)	12
3.3.4	Anwendungsschicht (OSI 5-7)	12

3.1 Begriffe

3.1.1 Schichtenmodell

Eine Schichtenmodell (Schichtenarchitektur) ist ein häufig angewandtes Strukturierungsprinzip für die Architektur von Softwaresystemen.

Bei einem **Schichtenmodell** werden einzelne Aspekte des Softwaresystems konzeptionell einer Schicht (**layer**) zugeordnet.

Definition 3.1

3.1.2 OSI-Modell

Das **ISO/OSI-Referenzmodell**¹ ist ein Referenzmodell für **Netzwerkprotokolle** als **Schichtenarchitektur**.

Definition 3.2

Es wird seit 1983 von der **ITU**² und seit 1984 auch von der **ISO**³ als Standard veröffentlicht. Seine Entwicklung begann im Jahr 1977

Zweck des **OSI-Modells** ist es, Kommunikation über unterschiedlichste technische Systeme hinweg zu beschreiben und die Weiterentwicklung zu begünstigen.

3.1.3 7 Schichten

Dieses Modell definiert sieben aufeinanderfolgende Schichten (**layers**) mit jeweils eng begrenzten Aufgaben.

In der gleichen Schicht mit klaren Schnittstellen definierte Netzwerkprotokolle sind einfach untereinander austauschbar, selbst wenn sie wie das **Internet Protocol** eine zentrale Funktion haben.

¹englisch: **OSI** = **Open Systems Interconnection model**

²englisch: **ITU** = **International Telecommunication Union**

³englisch: **ISO** = **International Organization for Standardization**

3.1.4 Protokoll

Im **OSI-Modell** sind die Kommunikationsabläufe in sieben Schichten aufgeteilt.

Dabei werden auf jeder einzelnen Schicht die Anforderungen separat umgesetzt.

Je Schicht müssen Sender- und Empfängerseite nach festgelegten Regeln arbeiten, diese werden als **Protokoll** bezeichnet und bildet eine logische, horizontale Verbindung zwischen zwei Instanzen derselben Schicht.

Definition 3.3

3.1.5 Schnittstellen

Als **Schnittstelle** bezeichnet man Dienste, die eine Schicht von der direkt darunterliegenden Schicht nutzen kann.

Definition 3.4

Der reale Datenfluss erfolgt beim Schichtenmodell vertikal über die Schnittstellen.

Die Instanzen einer Schicht sind genau dann austauschbar, wenn sie sowohl beim Empfänger als auch beim Sender ausgetauscht werden können.

3.1.6 Protokollstapel

Ein **Protokollstapel** oder Protokollturm ist in der Datenübertragung eine konzeptuelle Architektur von Kommunikationsprotokollen. Die einzelnen Protokolle sind dabei als fortlaufend nummerierte Schichten (**layers**) eines Stapels (**stacks**) übereinander angeordnet.

Definition 3.5

Jede Schicht benutzt dabei zur Erfüllung ihrer speziellen Aufgabe die jeweils tiefere Schicht im Protokollstapel, indem sie diese über deren **Service Access Point** anspricht.



Schichtenmodell



Protokoll



OSI-Modell



Protokollstapel

3.2 OSI Referenzmodell

3.2.1 Bitübertragungsschicht (Schicht 1)

Die **Bitübertragungsschicht** definiert **physikalische** und **technische Eigenschaften** des Übertragungsmediums (Übertragungskanal).

Definition 3.1

Dazu zählen z. B. die verwendeten Übertragungsverfahren (z. B. Manchester-Kodierung), sowie Bauform und Belegung von Steckverbindungen mit ihren mechanischen und elektrisch/optischen Parametern.

3.2.2 Sicherungsschicht (Schicht 2)

Die **Sicherungsschicht** gewährleistet, daß entlang einer Punkt-zu-Punkt Verbindung trotz gelegentlicher Fehler eine **zuverlässige Übertragung** stattfinden kann.

Definition 3.2

Zu den auf der Sicherungsschicht zu bewältigenden Aufgaben zählen z. B. die Organisation von Daten in Datenpakete (Fragmentierung), die Übertragung von Datenpaketen und das Bitstopfen.

Als **Bitstopfen** wird das Einfügen eines oder mehrerer Füllbits in einer Datenübertragung bezeichnet, um **Signalinformationen**⁴ an den Empfänger zu übermitteln.

Definition 3.3

Eine zuverlässige Übertragung wird durch einfache Fehler-Erkennungsverfahren, wie z. B. die Prüfsummenberechnung, ermöglicht.

3.2.3 Vermittlungsschicht (Schicht 3)

Die **Vermittlungsschicht** übernimmt die Zuweisung von Adressen und sorgt für die Weiterleitung von Datenpaketen.

Definition 3.4

Sie ermöglicht damit auch die Verknüpfung einzelner Netzwerke (**Internetworking**) und stellt eine Verbindung zwischen Endsystemen her.

⁴d.h. keine Nutzdaten im eigentlichen Sinne

3.2.4 Transportschicht (Schicht 4)

Die **Transportschicht** stellt sicher, daß Datenpakete fehlerfrei, vollständig und in der richtigen Reihenfolge vom Sender zum Empfänger gelangt.

Definition 3.5

Auf der Transportschicht erfolgt ebenfalls die Abbildung von Netzwerkadressen auf logische Namen.

3.2.5 Sitzungsschicht (Schicht 5)

Die **Sitzungsschicht** dient der Einrichtung einer Übertragungssitzung zu einem entfernten Rechnersystem, wie z. B. Sicherheitsmechanismen wie Authentifikation über Passwort-Verfahren

Definition 3.6

Die Sitzungsschicht wird auch als Kommunikationssteuerungsschicht bezeichnet.

3.2.6 Darstellungsschicht (Schicht 6)

Die **Darstellungsschicht** übersetzt verschiedene Datenformate, die auf den verbundenen Rechnersystemen eingesetzt werden und sorgt für eine korrekte Interpretation der übertragenen Daten.

Definition 3.7

Zu den Aufgaben dieser Schicht gehören zusätzlich die Datenkomprimierung und die Verschlüsselung .

3.2.7 Anwendungsschicht (Schicht 7)

Die **Anwendungsschicht** bietet eine Schnittstelle für Anwendungsprogramme, die das Netzwerk für ihre Zwecke nutzen wollen.

Definition 3.8

Hier werden einfach nutzbare Dienste zur Verfügung gestellt, die die netzwerkinternen Details vor dem Anwender oder dem Programmierer des Anwendungsprogrammes verbergen.

3.3 TCP/IP Referenzmodell

Für das Internet und die Internetprotokollfamilie ist die Gliederung nach dem sogenannten **TCP/IP**-Referenzmodell maßgebend. Dieses ist auf die Internet-Protokolle (TCP, IP) zugeschnitten, die den Datenaustausch über die Grenzen lokaler Netze hinaus ermöglicht.

3.3.1 Netzzugangsschicht (OSI 1-2)

Die **Netzzugangsschicht** ist zwar im **TCP/IP**-Referenzmodell spezifiziert, enthält aber keine Protokolle.

Definition 3.1

Sie dient als Platzhalter für verschiedene Techniken zur Punkt-zu-Punkt Datenübertragung.

3.3.2 Internetschicht (OSI-Schicht 3)

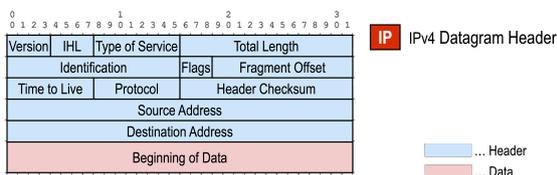


Abb. 3.1: IPv4-Header

Die **Internetschicht** ist für die Weitervermittlung und Wegwahl (Routing) von Paketen zuständig.

Definition 3.2

Kern dieser Schicht ist das Internet Protokoll (IPv4 o. IPv6), das einen Paketauslieferungsdienst bereitstellt.

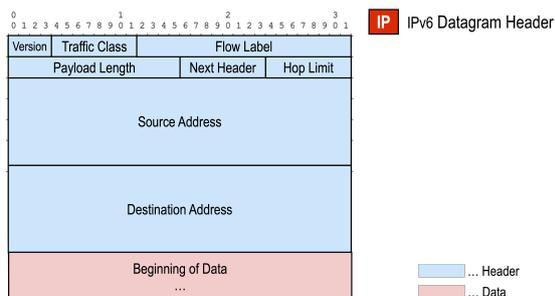


Abb. 3.2: IPv6-Header

3.3.3 Transportschicht (OSI 4)

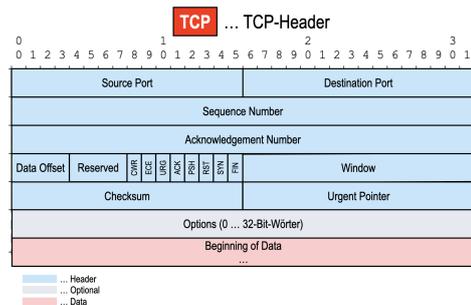


Abb. 3.3: TCP-Header

Die **Transportschicht** ermöglicht eine Ende-zu-Ende-Kommunikation.

Definition 3.3

Sie übernimmt die Einrichtung einer Kommunikationsverbindung zweier im Netz verteilter Anwendungsprogramme und sorgt dafür, dass Daten fehlerfrei und in richtiger Reihenfolge beim Empfänger ankommen.

Das wichtigste Protokoll dieser Schicht ist das **Transmission Control Protocol (TCP)**.

3.3.4 Anwendungsschicht (OSI 5-7)

Die **Anwendungsschicht** umfasst alle Protokolle, die mit Anwendungsprogrammen zusammenarbeiten.

Definition 3.4

Diese Schicht dient als Schnittstelle zu den Anwendungsprogrammen, die über das Netzwerk kommunizieren wollen.

Die Anwendungen selbst befinden sich dabei außerhalb dieser Schicht und des **TCP/IP**-Referenzmodells.

Basistechnologien

4

Rechnernetze

Inhaltsangabe

4.1	Übersicht	15
4.2	Übertragungstechniken	16
4.2.1	Übertragungsrichtung	16
4.2.2	Kommunikationsformen	16
4.2.3	Punkt-zu-Punkt Netze	16
4.3	Physikalische Netztopologien	17
4.3.1	Punkt-zu-Punkt Netzwerk	17
4.3.2	Teilvermaschtes Netz	17
4.3.3	Ring	17
4.3.4	Bus	17
4.3.5	Stern	17
4.3.6	Hybride Sterntopologie	17
4.4	Netzwerkbezeichnungen	18
4.4.1	PAN	18
4.4.2	LAN	18
4.4.3	MAN	18
4.4.4	WAN	18
4.4.5	GAN	18
4.4.6	Internetworks	18

4.1 Übersicht

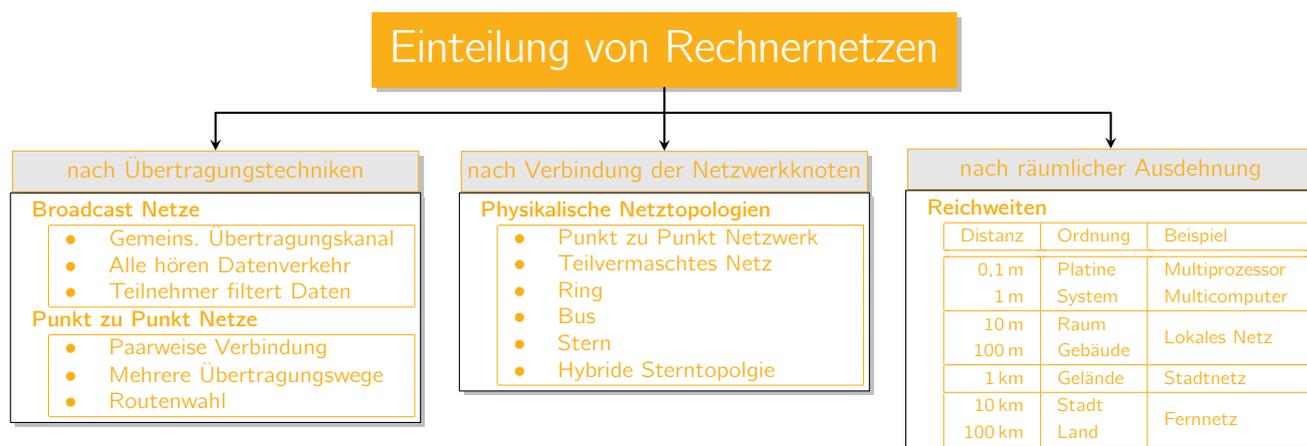


Abb. 4.1: Übersicht Rechnernetze

4.2 Übertragungstechniken

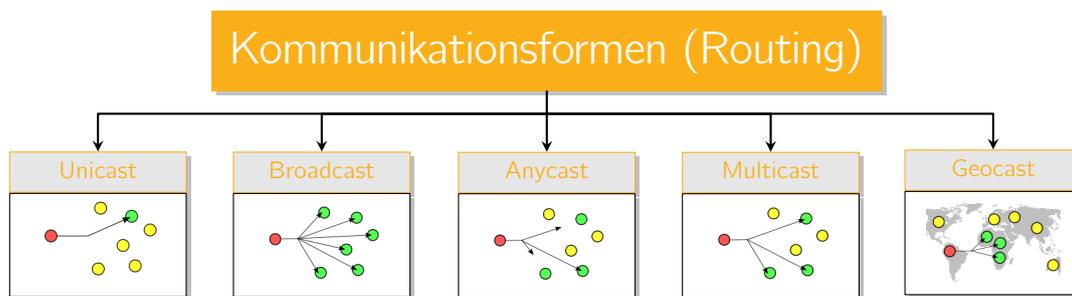


Abb. 4.2: Übersicht Übertragungstechniken

4.2.1 Übertragungsrichtung

Bidirektional

Bei einer **bidirektionalen** Datenübertragung erfolgt die Übertragung der Daten in beiden Richtungen, d.h. Sender und Empfänger können sowohl Daten senden als auch empfangen.

Definition 4.1

Beim Vollduplex-Verfahren erfolgt die Datenübertragung in beiden Richtungen gleichzeitig.

Beim Halbduplex-Verfahren ist eine Übertragung nur in eine Richtung zur gleichen Zeit möglich.

Unidirektional

Bei einer **unidirektionalen** Datenübertragung erfolgt die Übertragung der Daten nur in eine Richtung, d.h. Sender sendet und Empfänger empfängt die Daten.

Definition 4.2

Daraus folgt, dass dem Empfänger kein Rückkanal zur Verfügung steht und damit der Empfänger dem Sender nicht mitteilen kann ob die Nachricht einwandfrei übertragen wurde.

4.2.2 Kommunikationsformen

Unicast Netze

Bei einem **Unicast** erfolgt die Adressierung einer Nachricht nur an einen einzigen Empfänger.

Definition 4.3

Dieser Begriff lässt keine Rückschlüsse darauf zu, ob es sich um eine bidirektionale Verbindung handelt, oder ob die jeweiligen Daten nur in eine Richtung übertragen werden.

Broadcast Netze

Bei einem **Broadcast** werden von einem Punkt aus Daten an **alle Teilnehmer** übertragen.

Definition 4.4

Bei einigen Anwendungen (wie z. B. Wetterberichte, Verteilung von Börsenkurse, Übertragung von Radiosendungen) müssen Hosts Nachrichten an viele oder sogar alle anderen Hosts versenden.

Anycast Netze

Bei einem **Anycast** wird einer Gruppe eine gemeinsame Adresse zugeteilt, aber nur der Knoten mit der kürzesten Route empfängt die Nachricht.

Definition 4.5

Multicast Netze

Bei einem **Multicast** werden von einem Punkt aus Daten an **eine Gruppe** übertragen.

Definition 4.6

Bei manchen Anwendungen, wie z. B. bei einer Liveübertragung eines Sportereignisses, das an vielen Standorten betrachtet wird, werden Daten zu mehreren Empfänger gesendet.

Falls die Gruppe nicht sehr klein ist, ist das Senden zu jedem Empfänger teuer, und Broadcasting Verschwendung.

Beim Multicast wird eine Nachricht gezielt an eine bestimmte Gruppe gesendet, die zwar viele Mitglieder haben kann, aber im Vergleich zum Gesamtnetz klein ist.

Geocast Netze

Geocast ist eine spezielle Form des Multicast, d.h. Daten werden nur an ein räumlich abgegrenztes Gebiet übertragen.

Definition 4.7

4.2.3 Punkt-zu-Punkt Netze

Eine **Punkt-zu-Punkt-Verbindung** (Direktverbindung) in der Informations- und Kommunikationstechnik (IKT) ist eine direkte, unmittelbare Verbindung zwischen zwei Punkten oder Orten.

Definition 4.8



Direktverbindung

Man unterscheidet zwischen

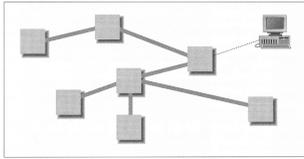
- Client-Server-Modell
- Peer-to-Peer-Modell (P2P)



Broadcast

4.3 Physikalische Netztopologien

4.3.1 Punkt-zu-Punkt Netzwerk

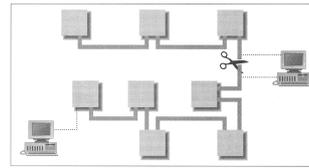


Bei einem **Punkt-zu-Punkt Netzwerk** existiert zw. zwei Knoten nur ein Verbindungsweg.

Definition 4.1

Vorteile	Nachteile
bietet jedem Knoten volle Bandbreite	Keine Redundanz: wird ein Link unterbrochen, existiert kein Ersatzweg.
Vorhersagbare Übertragungsraten, kein Routing benötigt	
Leicht erweiterbar und verständlich, Leichte Fehlersuche	

4.3.4 Bus

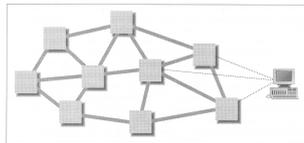


Bei einem **Bus** hat jeder Knoten (bis auf die Endknoten) genau zwei Nachbarn. Jeder Knoten ist an ein gemeinsames Medium angeschlossen.

Definition 4.4

Vorteile	Nachteile
Geringe Kosten (geringe Kabelmenge)	Datenübertragung kann leicht abgehört werden
Einfache Verkabelung	Ein Störung blockiert gesamten Strang
Garantierte Bandbreite	Es sendet immer nur eine Station (andere Sender sind blockiert)
Gute Skalierung, Kostengünstig	Langsame Übertragung bei vielen Knoten

4.3.2 Teilvermaschtes Netz

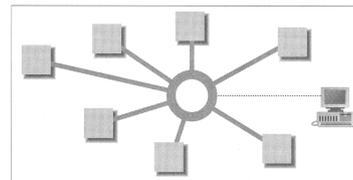


Bei einem **teilvermaschten Netz** sind zwischen zwei Knoten mehrere Verbindungswege möglich.

Definition 4.2

Vorteile	Nachteile
Sicherste Variante eines Rechnernetzes	Aufwendig da viele Kabel nötig
Ausfall eines Knotens kein Einfluß auf das Netz	Aufwendiges Routing, Hoher Energieverbrauch
Sehr leistungsfähig	Übertragung kann leicht abgehört werden
Gute Skalierung, Kostengünstig	Langsame Übertragung bei vielen Knoten

4.3.5 Stern

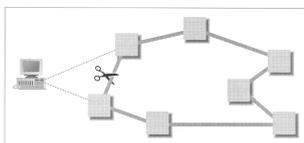


Bei einem **Stern** sind alle Knoten mit einem Zentralknoten verbunden.

Definition 4.5

Vorteile	Nachteile
Ausfall eines Knotens hat keinen Einfluß auf den Rest des Netzes	Bei Ausfall des Verteilers wird Netzverkehr unmöglich
Hohe, verschiedene Übertragungsraten möglich	
Leicht erweiterbar und verständlich, Leichte Fehlersuche	
Einfaches Routing im Sternverteiler	

4.3.3 Ring

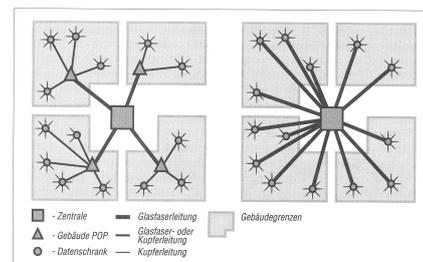


Bei einem **Ring** ist jeder Knoten mit einem linken und einem rechten Nachbarknoten verbunden.

Definition 4.3

Vorteile	Nachteile
Ausfall eines Knotens hat keinen Einfluß auf den Rest des Netzes	Bei Ausfall eines Knotens kann Netzkommunikation unterbrechen
Alle Stationen arbeiten als Verstärker	Übertragung kann leicht abgehört werden
Alle Knoten haben gleichen Zugriff	Langsame Übertragung bei vielen Knoten
Garantierte Bandbreite, Kostengünstig, Gute Skalierung	Relativ hoher Energieaufwand

4.3.6 Hybride Sterntopologie



4.4 Netzwerkbezeichnungen

4.4.1 PAN

Unter einem **PAN**¹ versteht man ein Netz, das von Kleingeräten wie PDAs oder Mobiltelefonen ad hoc auf- und abgebaut werden kann.

Definition 4.6

Dabei werden sowohl drahtgebundene (z. B. USB, FireWire) als auch drahtlose Übertragungstechniken verwendet. Die Reichweite beträgt gewöhnlich nur wenige Meter.

Bei der drahtlosen Übertragungstechnik können folgende Kurzstreckenfunk-Technologien eingesetzt werden:

- **IrDA**
- **Bluetooth**: z. B. Tastaturen, Maus
- **RFID**: z. B. Smartcards

Bluetooth ist ein Industriestandard für Datenübertragung zwischen Geräten über kurze Distanz per Funktechnik.

Definition 4.7

Bluetooth bildet eine Schnittstelle, über die sowohl mobile Kleingeräte wie Mobiltelefone und PDAs als auch Computer und Peripheriegeräte miteinander kommunizieren können.

Der Prozess des Verbindens zweier Geräte über Bluetooth heißt **Koppeln** oder **Pairing** (engl.), die Geräte sind nach dessen Erfolg gekoppelt.

Definition 4.8

4.4.2 LAN

Ein **LAN**² ist ein Rechnernetz, das die Ausdehnung von **PAN** übertrifft, aber die von **MAN**, **WAN** und **GAN** nicht erreicht.

Definition 4.9

Drahtlose **LANs** (**WLANs**) sind heute weit verbreitet, besonders in Privathaushalten, älteren Bürogebäuden, Cafeterias und anderen Orten, wo es zu aufwendig wäre Kabel zu verlegen.

Verkabelte **LANs** benutzen meistens Kupferkabel, aber auch Glasfaserkabeln.

Als Topologie wird meist eine Punkt-zu-Punkt-Verbindung mit Ethernet aufgebaut.

4.4.3 MAN

Ein **MAN**³ ist ein breitbandiges Telekommunikationsnetz, welches zahlreiche LANs über Backbone-Technologien verbindet.

Definition 4.10

Ein Stadtnetz erstreckt sich über ein Gebiet von der Größe einer Stadt, wie z. B. das Kabelfernsehnetz in vielen Städten.

MANs werden oft von international tätigen Telekommunikationsfirmen aufgebaut, die per MAN verkabelte Metropolen wiederum in einem Wide Area Network (WAN) national oder in einem Global Area Network (GAN) international vernetzen.

Ein MAN kann eine Ausdehnung von bis zu 100 Kilometern haben.

4.4.4 WAN

Ein **WAN**⁴ ist ein Rechnernetz, das sich im Unterschied zu einem **LAN** oder **MAN** über einen sehr großen geografischen Bereich erstreckt.

Definition 4.11

Ein Fernnetz erstreckt sich über ein großes geografisches Gebiet, zumeist ein Land oder Kontinent.

Im Unterschied zu LANs gehören bei einem WAN die Hosts und Subnetze unterschiedlichen Personen und werden von unterschiedlichen Personen bedient.

Die meisten Unternehmer besitzen keine eigenen WAN-Übertragungsleitungen sondern mieten diese von Network Provider-Firmen.

Ein Mobilfunknetz ist ein Beispiel für ein drahtloses WAN.

4.4.5 GAN

Unter einem **GAN**⁵ versteht man ein Netz, das über unbegrenzte geographische Entfernungen mehrere Wide Area Networks verbinden kann. Dies kann zum Beispiel die Vernetzung weltweiter Standorte eines internationalen Unternehmens sein.

Definition 4.12

Oft wird bei einem **GAN** Satelliten- oder Glasfaserübertragung eingesetzt.

Der Begriff **GAN** wird im Vergleich zu **LAN** und **WAN** eher selten verwendet.

GAN ist nicht die direkte Bezeichnung für das Internet! So ist das Internet ein **GAN**, aber nicht jedes **GAN** wird Internet genannt.

4.4.6 Internetworks

Eine Gruppe miteinander verbundene Netze wird als **Internetwork** oder **Internet** (nicht zu verwechseln mit dem weltweiten Netz).

Definition 4.13

Diese Begriffe werden nicht nur zur Bezeichnung des weltweiten Internets benutzt, sondern hier im allgemeinen Sinn.

¹englisch: **PAN** = Personal Area Network

²englisch: **LAN** = Local Area Network

³englisch: **MAN** = Metropolitan Area Network

⁴englisch: **WAN** = Wide Area Network

⁵englisch: **GAN** = Global Area Network



WAN



GAN



MAN

5

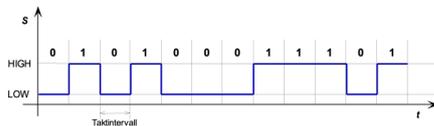
Datencodierung

Inhaltsangabe

5.1	Digitale Datencodierung	19
5.1.1	Binärdatendarstellung	19
5.1.2	Signalübertragung	19
5.1.3	Datenübertragungsrate	19
5.2	Codierungstechniken	20
5.2.1	Übersicht	20
5.2.2	NRZ-L-Kodierung	20
5.2.3	NRZI-Kodierung	20
5.2.4	Manchester Kodierung	20
5.2.5	MLT-3 Kodierung	20
5.3	Zusammengesetzte Codierverfahren	20
5.3.1	4B5B	20

5.1 Digitale Datencodierung

5.1.1 Binärdatendarstellung



Ein **Binärcode** ist ein Code, in dem Informationen durch Sequenzen von zwei verschiedenen Symbolen (z. B. 1/0) dargestellt werden.

Definition 5.1

5.1.2 Signalübertragung

Die Benutzung eines Taktsignals (kurz **Takt**) ist ein Verfahren, den richtigen zeitlichen Ablauf einer elektronischen Schaltung sicherzustellen.

Definition 5.2

5.1.3 Datenübertragungsrate

Die **Datenübertragungsrate** (kurz Datenrate) ist die Übertragungsgeschwindigkeit, mit der eine bestimmte Datenmenge innerhalb eines Zeitintervalls über einen Übertragungskanal übertragen wird.

Definition 5.3

In einem digitalen Netz werden für die Datenmenge folgende SI- bzw. Binär-Einheiten verwendet:

SI-Einheit	Präfix	Byte	Binär	Präfix	Byte	Differenz
Kilobyte	kB	10^3	Kibibyte	KiB	2^{10}	2,4 %
Megabyte	MB	10^6	Mebibyte	MiB	2^{20}	4,9 %
Gigabyte	GB	10^9	Gibibyte	GiB	2^{30}	7,4 %
Terabyte	TB	10^{12}	Tebibyte	TiB	2^{40}	10 %
Petabyte	PB	10^{15}	Pebibyte	PiB	2^{50}	12,6 %
Exabyte	EB	10^{18}	Exbibyte	EiB	2^{60}	15,3 %
Zettabyte	ZB	10^{21}	Zebibyte	ZiB	2^{70}	18,1 %
Yottabyte	YB	10^{24}	Yobibyte	YiB	2^{80}	20,9 %

Tab. 5.1: Binäre Einheiten



Binärcode



Taktsignal



Datenübertragungsrate

5.2 Codierungstechniken

5.2.1 Übersicht

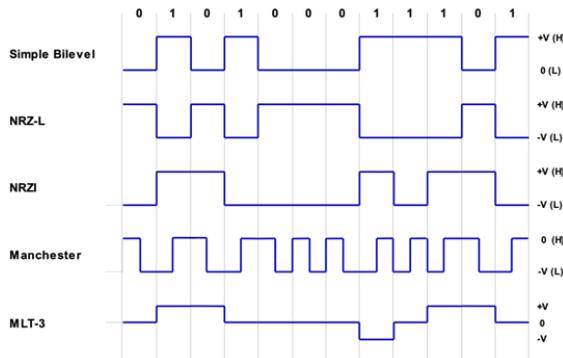


Abb. 5.1: Übersicht der Codierungsarten

5.2.2 NRZ-L-Kodierung

Die **NRZ** Codierung hat im Gegensatz zum RZ-Code keinen dritten Spannungswert. Beide binäre Symbole bestehen aus konstanten Leitungszuständen (meist Spannungen).

Der **NRZ**¹-Code ordnet direkt jedem Bit-Wert einen Leitungszustand zu.

Definition 5.1

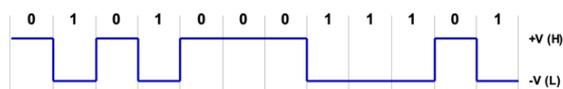


Abb. 5.2: NRZ-L codierte Datenfolge

5.2.3 NRZI-Kodierung

Die **NRZI**²-Kodierung ordnet einem der beiden Bit-Werte den bereits anliegenden Leitungszustand zu, dem anderen Bit-Wert einen Zustandswechsel (Inversion).

Definition 5.2

Daraus ergibt sich unmittelbar die Polaritätsfreiheit: Ein Verpolen der Übertragungsleitung ändert nicht die Bitfolge.

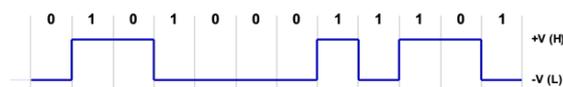


Abb. 5.3: NRZI codierte Datenfolge

5.2.4 Manchester Kodierung

Der Manchester-Code ist ein Leitungscode, der bei der Kodierung das Taktsignal erhält.

Definition 5.3

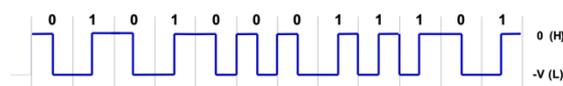


Abb. 5.4: Manchester codierte Datenfolge

5.2.5 MLT-3 Kodierung

MLT-3³ Kodierung verwendet drei Spannungsniveaus bezeichnet mit den Symbolen (+, 0, -).

Definition 5.4

Durch seine drei Stufen zählt die gebildete Signalform zu den ternären Signalen.

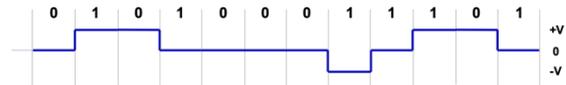
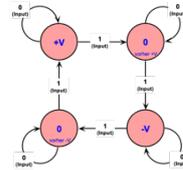


Abb. 5.5: MLT-3 codierte Datenfolge

5.3 Zusammengesetzte Codierverfahren

5.3.1 4B5B

	4B	5B	Funktion
0	0000	11110	Hex data 0
1	0001	01001	Hex data 1
2	0010	10100	Hex data 2
3	0011	10101	Hex data 3
4	0100	01010	Hex data 4
5	0101	01011	Hex data 5
6	0110	01110	Hex data 6
7	0111	01111	Hex data 7
8	1000	10010	Hex data 8
9	1001	10011	Hex data 9
A	1010	10110	Hex data A
B	1011	10111	Hex data B

	4B	5B	Funktion
C	1100	11010	Hex data C
D	1101	11011	Hex data D
E	1110	11100	Hex data E
F	1111	11101	Hex data F
Q	-	00000	Quit (Signalverlust)
I	-	11111	Idle (Pause)
J	-	11000	Start
K	-	10001	Start
T	-	01101	End
R	-	00111	Reset
S	-	11001	Set
H	-	00100	Halt

Tab. 5.2: 4B5B Codegruppen

4B5B-Code ist ein Leitungscode, der eindeutig umkehrbar vier Nutzdatenbits auf fünf Codebits abbildet.

Dieser Code wird z. B. bei Fast Ethernet 100BASE-TX in Kombination mit einer MLT-3-Leitungscodierung bei Kupferkabeln verwendet.

Zusätzlich zu den Datensymbolen zur Übertragung der Nutzdaten gibt es damit auch SteuerCodes zur Verwaltung der Verbindung, z. B. um Anfang und Ende der Frames oder Fehler erkennen zu können.

Der Nachteil dabei ist, dass durch das Einfügen eines weiteren Bits die codierte Bitrate gegenüber der Nutzdatenbitrate um 25 % erhöht werden muss.

¹englisch: **NRZ** = Non return To Zero

²englisch: **NRZI** = Non return To Zero Inverted

³englisch: **MLT** = Multilevel Transition



MLT-3



NRZ, NRZI



Manchester



4B5B-Code

6

Datenübertragung

Inhaltsangabe

6.1	Nachrichtentechnik Grundlagen	22
6.1.1	Periodische Funktionen	22
6.1.2	Harmonische Schwingung	22
6.1.3	Fourier Transformation	22
6.1.4	Rechteckimpuls	22
6.2	Übersicht der Übertragungsmedien	23
6.2.1	Kupferkabel	23
6.2.2	Lichtwellenleiter	23
6.2.3	Drahtlose Übertragung	23
6.3	Physikalische Grundlagen	24
6.3.1	Physikalische Größe	24
6.3.2	SI-Einheitensystem	24
6.4	Kennwerte	25
6.4.1	Das Bel (dBel)	25
6.4.2	Impedanz	25
6.4.3	Signaldämpfung	25
6.4.4	Nebensprechdämpfung	25

6.1 Nachrichtentechnik Grundlagen

Abb. 6.1: Darstellung Rechteckimpuls durch Fourierreihe

6.1.1 Periodische Funktionen

Die Funktionswerte einer **periodischen Funktion** wiederholen sich in regelmäßigen Abständen. Die Abstände zwischen gleichen Funktionswerte werden **Periode** genannt.

Definition 6.1

Die bekanntesten periodischen Funktionen sind Sinus- und Cosinus-Funktionen mit der Periode 2π .

Viele reelle Funktion können in Potenzreihen entwickelt werden. Unter gewissen Voraussetzungen, können periodische Funktion als Reihe von Sinus- und Kosinus-Funktionen entwickeln werden (Fourier-Reihe).

6.1.2 Harmonische Schwingung

Die **Harmonische Schwingung** ist als Funktion der Zeit eine rein **sinusförmige Schwingung**.

Definition 6.2

$$f(t) = A \cdot \sin(\omega \cdot t)$$

Die Harmonische kann mit $\omega = 2\pi \cdot f$ bzw. mit $\omega = f \cdot 2\pi$ auch in Abhängigkeit der Frequenz f dargestellt werden.

$$f(t) = A \cdot \sin(f \cdot 2\pi \cdot t)$$

Beispiele

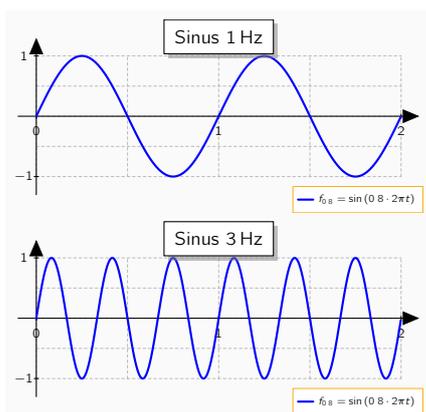


Abb. 6.2: Sinus 1. und 3. Ordnung

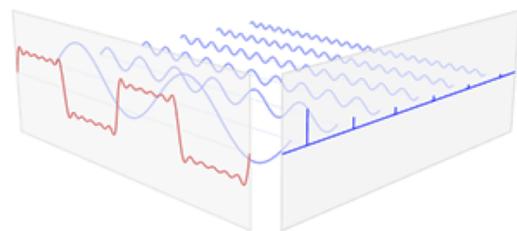
6.1.3 Fourier Transformation

Die Theorie der Fourier-Reihen und Fourier-Integrale reichen bis in das 18. Jahrhundert zurück. Benannt ist sie nach dem französischen Mathematiker Jean Baptiste Joseph Forier.

Als **Fourier-Reihe** bezeichnet man die Reihenentwicklung einer periodischen, abschnittsweise stetigen Funktion in eine Funktionenreihe aus Sinus- und Kosinusfunktionen..

Definition 6.3

6.1.4 Rechteckimpuls



6.2 Übersicht der Übertragungsmedien

6.2.1 Kupferkabel



Abb. 6.3: Koaxialkabel

Koaxialkabel (Koaxkabel) sind zweipolige Kabel mit konzentrischem Aufbau, mit einem Innenleiter (Seele) umgeben von einem hohlzylindrischen Außenleiter.

Definition 6.1

Der Zwischenraum ist ein Isolator bzw. Dielektrikum. Das Dielektrikum kann anteilig oder vollständig aus Luft bestehen (siehe Luftleitung).

Als **Dielektrikum** (Mehrzahl: Dielektrika) wird eine elektrisch schwach- oder nichtleitende Substanz bezeichnet, in der die vorhandenen Ladungsträger nicht frei beweglich sind.

Definition 6.2

Der Außenleiter ist meist durch einen isolierenden, korrosionsfesten und wasserdichten Mantel nach außen hin geschützt und schirmt den Innenleiter vor Störstrahlung ab.

Der mechanische Aufbau und insbesondere das Dielektrikum des Kabels bestimmt den Leitungswellenwiderstand sowie die von der Frequenz abhängige Dämpfung der Kabel.

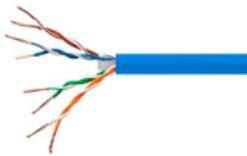


Abb. 6.4: Twisted Pair Kabel

Als **Twisted-Pair-Kabel** bezeichnet man Kabeltypen, in denen die Adern paarweise miteinander verdreht sind.

Definition 6.3

Verdrillte Adernpaare bieten gegenüber parallel geführten Adern einen besseren Schutz gegenüber elektrischen und magnetischen Störfeldern.

Durch Verdrillen der Adernpaare heben sich Beeinflussungen durch äußere Felder größtenteils gegenseitig auf.

Ein elektrisch leitender Schirm, oft aus Aluminiumfolie und/oder Metallgeflecht oder aus Kupfer ausgeführt, bietet zusätzlich Schutz gegen störende äußere elektromagnetische Felder.

Twisted-Pair-Kabel ohne Schirm werden als **Unshielded Twisted Pair (UTP)** bezeichnet.

Definition 6.4

6.2.2 Lichtwellenleiter



Abb. 6.5: Lichtwellenleiter

Lichtwellenleiter sind aus Lichtleitern bestehende, teilweise mit Steckverbindern konfektionierte Kabel zur Übertragung von Licht.

Definition 6.5

Das Licht wird dabei in Fasern aus Quarzglas oder Kunststoff (polymere optische Faser) geführt.

Sie werden häufig auch als Glasfaserkabel bezeichnet, wobei in diesen typischerweise mehrere Lichtwellenleiter gebündelt werden, die zudem zum Schutz und zur Stabilisierung der einzelnen Fasern noch mechanisch verstärkt sind.

6.2.3 Drahtlose Übertragung



Abb. 6.6: Funk-LAN

Ein **Wireless Accesspoint** (Basisstation), ist ein elektronisches Gerät, das als Schnittstelle für kabellose Kommunikationsgeräte fungiert.

Definition 6.6

Für gewöhnlich verbinden **Wireless Accesspoints** Notebooks und andere mobile Endgeräte mit eingebautem **Wireless Adapter** über ein WLAN mit einem LAN oder einem anderen kabelgebundenen Datennetz (Telefonnetz, Kabelfernsehtz).

Ein **WLAN**¹ (oder Wireless LAN) bezeichnet ein lokales Funknetz.

Definition 6.7



Abb. 6.7: Richtfunk

Als **Richtfunk** bezeichnet man eine drahtlose Übertragung, die von einem Ausgangspunkt auf einen definierten Zielpunkt gerichtet ist.

Definition 6.8

Die Richtwirkung dieser Funkanwendung ergibt sich durch Einsatz von Richtantennen (energiebündelnder Antennen), die die elektromagnetische Energieübertragung weitgehend auf die gewünschte Richtung beschränken.

¹englisch: **WLAN** = **Wireless Local Area Network**

6.3 Physikalische Grundlagen

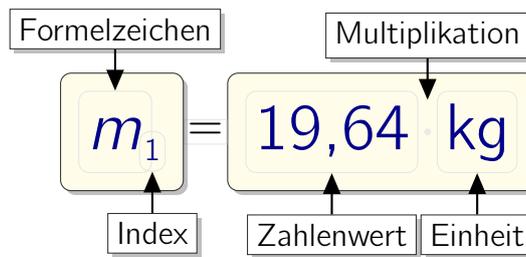


Abb. 6.8: Physikalische Größe

6.3.1 Physikalische Größe

Jede **physikalische Größe** wird als Produkt von einem **Zahlenwert (Maßzahl)** mit einer **Maßeinheit** (kurz **Einheit**) angegeben. Bei vektoriellen Größen wird zusätzlich auch eine Richtung angegeben.

Zahlenwert

Der Zahlenwert einer physikalischen Größe ist üblicherweise eine reelle Zahl, kann aber - wie z.B. in der Elektrotechnik - auch eine komplexe Zahl sein.

Die **Maßzahl** einer physikalischen Größe ist ihr Zahlenwert.

Definition 6.1

Einheit

Die Einheiten in der Physik (Mechanik) sind willkürlich gewählt und haben im Verlauf der Geschichte auch viele Änderungen erfahren.

Die **Maßeinheit** kurz **Einheit** ist die durch Gesetz oder Konvention festgelegte Definition einer physikalischen Größe.

Definition 6.2

Es gibt auch physikalische Größen ohne bestimmte Einheit.

Eine physikalischen Größe, die durch eine **reine Zahl** angegeben werden kann ist eine Größe der **Dimensionszahl**.

Definition 6.3

Die Benennung **dimensionslose Größe** ist veraltet² und sollte nicht mehr verwendet werden

Formelzeichen

Sinnvollerweise wird einer physikalischen Größe in mathematischen Gleichungen ein Formelzeichen zugeordnet.

Formelzeichen (Größensymbole) sind Symbole, die zur Bezeichnung einer physikalischen Größe verwendet werden.

Definition 6.4

Einheitenzeichen

Für mathematische Gleichungen und Berechnungen wird für Einheiten eine verkürzte Form zur Darstellung der Einheit verwendet.

Einheitenzeichen werden stellvertretend für die Einheitenamen verwendet.

Definition 6.5

6.3.2 SI-Einheitensystem

Das **Internationale Einheitensystem** oder **SI³** ist das verbreitetste Einheitensystem für physikalische Größen.

SI-Einheiten sind die durch das SI definierte Einheiten.

Definition 6.6

SI-Basisgrößen

Das SI beruht auf sieben Basisgrößen, aus die alle anderen physikalischen Größen abgeleitet werden können.

Eine **SI-Basisgröße** kann nicht von einer anderen SI-Basisgröße abgeleitet werden.

Definition 6.7

Basisgröße	Symbol	Basiseinheit	Zeichen
Zeit	t	Sekunde	s
Länge	l	Meter	m
Masse	m	Kilogramm	kg
el. Stromstärke	I	Ampere	A
abs. Temperatur	T	Kelvin	K
Stoffmenge	n	Mol	mol
Lichtstärke	I_V	Candela	cd

Tab. 6.1: SI-Basisgrößen

SI-Einheiten der Mechanik

Nachfolgend sind auszugsweise physikalische Größen der Mechanik aufgezählt.

Phys. Größe	Symbol	SI-Einheit	Zeichen
Masse	m	Kilogramm	kg
Kraft	F	Newton	N
Gewichtskraft	F_G	Newton	N
Drehmoment	M	Newtonmeter	N m
Dichte	ρ		kg/m ³
Druck	p	Pascal	Pa
Zug-/Druckspannung	σ	Pascal	Pa

Tab. 6.2: SI-Einheiten der Mechanik

SI-Einheiten der Kinematik

Phys. Größe	Symbol	SI-Einheit	Zeichen
Geschwindigkeit	v		m/s
Beschleunigung	a		m/s ²
Fallbeschleunigung	g		m/s ²

Tab. 6.3: SI-Einheiten der Kinematik

²EN ISO 80000

³Système international d'unités

6.4 Kennwerte

6.4.1 Das Bel (dBel)

Das **Bel (dBel)** ist eine Hilfsmaßeinheit zur Berechnung des Verhältnisses zweier Größen mit Hilfe des dekadischen Logarithmus.

Definition 6.8

Erstrecken sich die Verhältnisse zweier Größen über mehrere 10-er Potenzen dann wird durch Verwendung des dekadischen Logarithmus das Ergebnis lesbarer.

Beispiele

$$A = 10 \cdot \log_{10} \frac{P_1}{P_2} \quad \text{in [dB]}$$

dB	$P_1/P_2 > 0$	dB	$P_1/P_2 < 0$
0 dB	1		
3 dB	≈ 2	-3 dB	$\approx 0,5$
10 dB	10	-10 dB	0,1
20 dB	100	-20 dB	0,01
30 dB	1000	-30 dB	0,001
60 dB	1 000 000	-30 dB	0,000 001
90 dB	1 000 000 000	-90 dB	0,000 000 001

Tab. 6.4: dB-Werte

Häufig werden in der Praxis negative dB-Werte als Kehrwert der positiven Werte verwendet.

Beispiel: -90 dB bedeutet $1/1\,000\,000\,000$ oder „eine Abschwächung des Signals auf ein Milliardstel“ (häufig z. B. bei Funksignalen am Handy verwendet).

6.4.2 Impedanz

Die **Impedanz** (der Wellenwiderstand) ist eine Eigenschaft eines Mediums, in dem sich eine Welle ausbreitet.

Definition 6.9

Koaxialkabel der Kommunikationstechnik besitzen einen definierten Wellenwiderstand.

6.4.3 Signaldämpfung

$$a_v = 10 \cdot \log_{10} \frac{P_i}{P_o}$$

Symbol	Interpretation	Bemerkung
a_v	Dämpfung	in Dezibel
P_i	Signaleingangsleistung	„Senden“
P_o	gemessene Signalausgangsleistung	„Empfangen“

Tab. 6.5: Kennwerte der Signaldämpfung

6.4.4 Nebensprechdämpfung

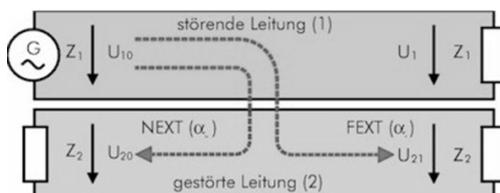


Abb. 6.9: NEXT und FEXT

Nebensprechen (Übersprechen) ist ein Begriff aus der Telefonie und bezeichnete ursprünglich einen Effekt, durch den man am Telefon ein anderes Gespräch leise mithören kann.

Definition 6.10



Übersprechen

Beim elektrischen Übersprechen⁴ wird ein Signal von einem Adernpaar auf ein anderes Adernpaar induktiv, kapazitiv oder galvanisch eingekoppelt.



Einheit Bel

Glasfaser sind gegen Übersprechen unempfindlich.

Nahnebensprechdämpfung

Als **Nahübersprechen (Nahnebensprechen)** bezeichnet man das Störsignal, das am nahen Ende (auf Seite des Senders) empfangen wird.

Definition 6.11

$$a_n = 10 \cdot \log_{10} \frac{P_i}{P_o}$$

Symbol	Interpretation
a_n	Nahnebensprechdämpfung in Dezibel
P_i	Signal-Eingangsleistung Paar 1
P_o	gemessene Signal-Ausgangsleistung Paar 2

Tab. 6.6: Kennwerte der Nebensprechdämpfung

Der Störsignal-Pegel ist bei NEXT größer als bei FEXT

Fernebensprechdämpfung

Als **Fernübersprechen** oder **Fernebensprechnung** ist die Einkopplung durch einen störenden Sender am fernen Ende (auf Seite des Empfängers)

Definition 6.12

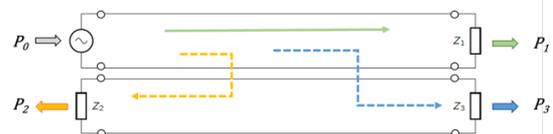


Abb. 6.10: Signaldämpfung

Symbol	Berechnung	Bemerkung
a_{loss}	$10 \cdot \log_{10} (P_0/P_1)$ [dB]	Signaldämpfung (Signal Loss)
a_{NEXT}	$10 \cdot \log_{10} (P_0/P_2)$ [dB]	NEXT-Wert
a_{FEXT}	$10 \cdot \log_{10} (P_0/P_3)$ [dB]	FEXT-Wert
a_{ACR}	$a_{NEXT} - a_{loss}$ [dB]	ACR-Wert

Attenuation To Crosstalk Ratio (ACR), auch Übersprechdämpfung, ist das Verhältnis von Signaldämpfung (Signal Loss) zu Übersprechen (NEXT) der Übertragungsstrecke.

Definition 6.13

$$ACR = a_n - a_v$$

Symbol	Interpretation
ACR	Verhältnis Nutzsignal zu anliegendem Störsignal
a_n	Nahnebensprechdämpfung in Dezibel
a_v	(Signal-) Dämpfung in Dezibel



Koaxialkabel



Übersprechdämpfung

⁴englisch: *crosstalk* = abgekürzt XT

7

Übertragungsmedien

Inhaltsangabe

7.1	Kupferkabel-Technologie	27
7.1.1	Twisted Pair Kabel	27
7.1.2	RJ-Steckverbindung	27
7.1.3	Kabel-Kategorien	27
7.1.4	Verbreitete Kabeltypen	27
7.1.5	TP-Ethernet Vernetzung	27
7.1.6	Ethernet Kabellängen	27
7.2	Glasfaser-Technologie	28
7.2.1	Optische Übertragung	28
7.3	Drahtlos-Technologien	29
7.3.1	Implementierung von WLANs	29
7.3.2	Roaming in WLANs	29
7.3.3	Richtfunktechnologie	29
7.3.4	Wi-Fi Generationen	29

7.1 Kupferkabel-Technologie

7.1.1 Twisted Pair Kabel



Abb. 7.1: Unshielded Twisted Pair

UTP (Unshielded Twisted Pair) ist eine Bezeichnung nach ISO/IEC 11801: U/UTP Kabel mit ungeschirmten Paaren, ohne Gesamtschirm.

Definition 7.1

Weltweit sind dies die meistverwendeten Kabel für Ethernet-LANs (mehr als 90 Prozent).

Erst für zukünftige Techniken werden geschirmte Kabel benötigt (10-Gigabit-Ethernet).



Abb. 7.2: Shielded Twisted Pair

STP (Shielded Twisted Pair): veraltete allgemeine Bezeichnung für Kabel mit Schirmung, ohne auf Art der Schirmung (Drahtgeflecht/Folie, einzelne Paare/Gesamtschirmung) einzugehen.

Definition 7.2

Im Weiteren auch Teil der Bezeichnung für Kabel mit Drahtgeflecht als Paarschirm:

- **S/STP (screened shielded twisted pair)** (Drahtgeflecht als Paar- und Gesamtschirm)
- **F/STP (foiled shielded twisted pair)** (Drahtgeflecht als Paar-, Folie als Gesamtschirm)

FTP (Foiled Twisted Pair): ungenaue, veraltete Bezeichnung für Kabel mit Folienschirmung, ohne auf die Art der Schirmung (einzelnen Paare oder Gesamtschirmung) einzugehen.

Definition 7.3

Die Aderpaare sind mit einem metallischen Schirm (meist aluminiumkaschierte Kunststoffolie) umgeben.

7.1.2 RJ-Steckverbindung

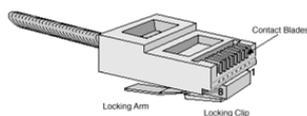


Abb. 7.3: RJ45 Stecker

RJ¹-Steckverbindungen sind genormte Steckverbindungen für Telekommunikations-Verkabelungen gemäß **CFR Part 68²**.

Definition 7.4

Die Standards beschreiben die Bauformen von Steckern, Buchsen und deren Kontaktbelegungen.

¹englisch: **RJ** = **Registered Jack**, eingetragene Steckverbindung

²englisch: **CFR** = **US-amerikanischen Code of Federal Regulations**

7.1.3 Kabel-Kategorien

Die Leistungsfähigkeit einer Übertragungsstrecke, bestehend aus Leitung, Stecker und weiteren Netzwerkkomponenten, wird nach der ISO/IEC 11801 bzw. der EN 50173 in Klassen, die einer Einzelkomponente in Kategorien eingestuft.

Die Kategorien/Klassen sind abwärtskompatibel, das bedeutet, dass höhere Kategorien/Klassen automatisch die darunterliegenden mit abdecken.

Die **Klasse der Übertragungsstrecke** definiert sich durch die Komponente mit der **geringsten Kategorie**.

Definition 7.5

Die Zusammenschaltung von z. B. einem Kategorie-5-Kabel mit Kategorie-6-Anschlusskomponenten reduziert die Klasse von theoretisch E auf D.

Die Kategorien 1 und 2 sind nur informell definiert; die Kategorien 3 und 4 sind kommerziell nicht mehr relevant (in Altinstallationen aber weiter anzutreffen).

7.1.4 Verbreitete Kabeltypen

Kat.	Kl.	Typ	Bandbr.	Geschw.	Anwendung
Cat 5	D	UTP	100 MHz	100 Mbit/s	100BASE-TX
Cat 5e	D	UTP	100 MHz	1 Gbit/s	1000BASE-T 2.5GBASE-T 5GBASE-T@<75m
Cat 6	E	UTP	250 MHz	1 Gbit/s	5GBASE-T 10GBASE-T@<55m
Cat 6A	E _A	STP	500 MHz	10 Gbit/s	10GBASE-T
Cat 7	F	S/FTP	600 MHz	10 Gbit/s	CCTV
Cat 7a	F _A	S/FTP	1000 MHz	10 Gbit/s	-
Cat 8.1	G	S/FTP	2000 MHz	40 Gbit/s	5GBASE-T
Cat 8.2	G	S/FTP	2000 MHz	40 Gbit/s	40GBASE-T

Tab. 7.1: Kabeltypen

7.1.5 TP-Ethernet Vernetzung

Anwendung	Bemerkung
10BASE-T	Ethernet
100BASE-TX	Fast Ethernet
100BASE-T	Gigabit Ethernet
10GBASE-T	10 Gigabit Ethernet
40GBASE-T	40 Gigabit Ethernet

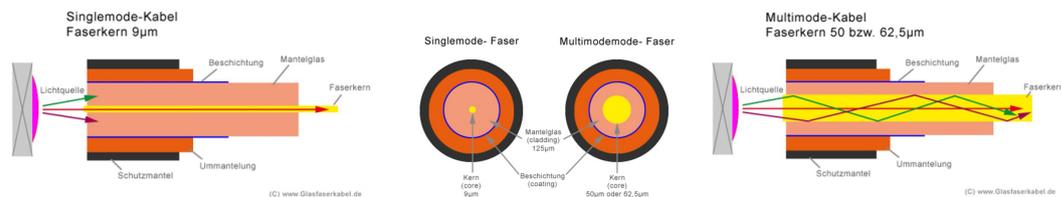
Tab. 7.2: Ethernet Vernetzung

7.1.6 Ethernet Kabellängen

Kabelkategorie	Übertragungs-klasse (nach ISO/EN)	Standard	Linklänge	Übertragungs-frequenz	Kabel genormt bis (nach TIA/EIA 568 und EN 50288)
Cat-3	Klasse C	10BASE-T, 100BASE-VG		2 × 10 MHz	16 MHz
Cat-5	-	100BASE-TX	100 m	2 × 31,25 MHz	100 MHz
Cat-5	-	1000BASE-T		4 × 62,5 MHz	100 MHz
Cat-5e	Klasse D		*) 45...7 m		100 MHz
Cat-5e, ungeschirmt					100 MHz
Cat-5e, geschirmt			über 45 m		100 MHz
Cat-6, ungeschirmt	Klasse E	10GBASE-T	*) 55... 100 m	4 × 417 MHz	250 MHz
Cat-6, geschirmt					250 MHz
Cat-6A	Klasse E _A		100 m		500 MHz
Cat-7	Klasse F				600 MHz
Cat-8		40GBASE-T	30 m		1600 MHz

Tab. 7.3: Längen für Kupfer-Doppelader

7.2 Glasfaser-Technologie



Quelle: [5]

Abb. 7.4: Aufbau Singlemode und Multimode Glasfaser-Kabel

7.2.1 Optische Übertragung

Modenübertragung

Multimodefasern, in denen sich mehrere tausend Moden ausbreiten können, werden (bzw. wurden) vor allem für kurze Entfernungen (z. B. in LANs, max. wenige hundert Meter) eingesetzt.

In **Single Mode Fiber**³, die einen sehr kleinen Kerndurchmesser (9 µm) haben, kann sich nur die sogenannte Grundmode ausbreiten.

Die Anzahl der auftretenden Moden beeinflusst die Signalübertragung, da jede Mode einen unterschiedlich langen Lichtweg nimmt.

Deshalb zeigen Multimodefasern mit zunehmender Länge eine stärkere Signalverfälschung (Modendispersion) als Monomodefasern, die somit zur Signalübertragung über weite Strecken besser geeignet sind.



Lichtwellenleiter

Sie werden auch über hunderte oder sogar tausende Kilometer (z. B. bei interkontinentalen Seekabeln) aber inzwischen auch für Campus-Netze oder Rechenzentren eingesetzt.

³englisch: *Single Mode Fiber* = Singlemode-, Monomodefaser

7.3 Drahtlos-Technologien

Abb. 7.5: WLAN - Handover (Roaming)

7.3.1 Implementierung von WLANs

Funk-/Radiowellen sind leicht zu erzeugen, legen große Entfernungen zurück und durchdringen mühelos Gebäude. Deshalb ist die Funkübertragung heute sehr weit verbreitet.

Mit **WIFI** wird der Standard **IEEE 802.11** der Funkübertragungstechnik bezeichnet.

Definition 7.1

Ein IEEE-802.11-Netz besteht aus **Clients** (Laptops, Mobiltelefone) und einem **Zugangspunkt** (**Access Point**).

Ein **Access Point** (**AP, Basisstation**) stellt eine Verbindung zum verkabelten Netzwerk her.

Definition 7.2

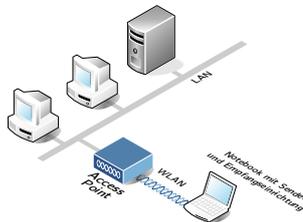


Abb. 7.6: WLAN

WLANs dienen in den meisten Firmen- und Privatnetzen zum drahtlosen Zugang zum LAN und über einen Router weiter zum Internet.

7.3.2 Roaming in WLANs

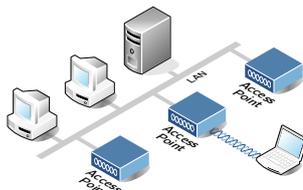


Abb. 7.7: WLAN - Handover (Roaming)

Der Wechsel von einem WLAN-Gerät (Access Point) zu einem anderen wird als **Roaming** oder **Handover** bezeichnet.

Definition 7.3

7.3.3 Richtfunktechnologie

Als **Richtfunk** wird eine drahtlose Nachrichtenübertragung bezeichnet, die vom Ausgangspunkt auf einen definierten Zielpunkt gerichtet ist.

Definition 7.4

Die Richtwirkung ergibt sich aus dem Einsatz von Richtantennen, die die Übertragung auf die gewünschte Richtung beschränken.

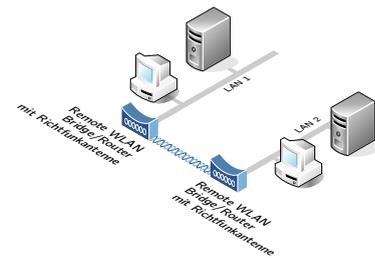


Abb. 7.8: Richtfunk

7.3.4 Wi-Fi Generationen

Der Kunstbegriff **Wi-Fi**⁴, als Wortspiel analog zu „Hi-Fi“, wird seit 1999 kommerziell genutzt.

Wi-Fi bezeichnet auch die WiFi-Alliance und wird auch bei der Zertifizierung von WLAN-Geräten verwendet.

Definition 7.5

Bezeichnung	IEEE Standard	Maximale Linkrate
Wi-Fi 4	802.11n	72 – 600Mbit/s
Wi-Fi 5	802.11ac	433 – 6933Mbit/s
Wi-Fi 6	802.11ax	600 – 9608Mbit/s
Wi-Fi 6E	802.11ax	600 – 9608Mbit/s
Wi-Fi 7	802.11be	
Wi-Fi 8		

Tab. 7.4: Wi-Fi Generationen

Die aktuellen WLAN-Standards sind Wi-Fi 6, Wi-Fi 6E und Wi-Fi 7, die auf kurze Entfernungen (ca. 30-50 m) viele gleichzeitige Verbindungen und hohe Datenraten (einige hundert MBit/s) unterstützen.



IEEE 802.11

⁴englisch: **Wi-Fi** = **Wireless Fidelity** (Drahtlose Zuverlässigkeit)

Internetdienste und Anwendungen

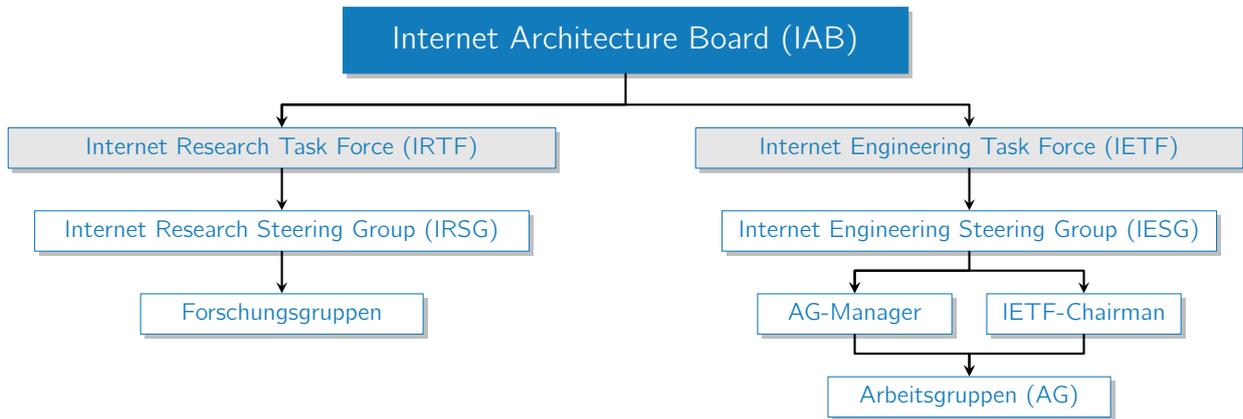
8

Internettechnologien

Inhaltsangabe

8.1	Organisationen	34
8.1.1	RIPE NCC	34
8.1.2	ISOC	34
8.1.3	IANA	34
8.1.4	IAB	34
8.2	Der Standardisierungsprozeß	35
8.2.1	Request for Comments (RFC)	35
8.2.2	Entwicklungsprozeß	35
8.3	Internet Protocol (IPv4)	36
8.3.1	Grundbegriffe	36
8.3.2	IP-Adress-Klassen	37
8.3.3	Spezielle IP-Adressen (Broadcast, Loopback, ...)	38
8.3.4	Subnetz-Adressierung	39
8.4	Internet Protocol Version 6 (IPv6)	40
8.4.1	IPv6-Adressen	40
8.5	Domain Name System	42
8.5.1	Namens- und Verzeichnisdienste	42
8.5.2	Domain Name System	42
8.5.3	Fully Qualified Name	42
8.5.4	Domains und Subdomains	42
8.5.5	DNS Server	43
8.6	Routing	44
8.6.1	Routing Tabellen	44
8.6.2	IP Forwarding	44
8.6.3	IPv4 Datagramm	44
8.6.4	NAT und Masquerading	45
8.6.5	ICMP, Traceroute	45
8.7	Transportprotokolle	46
8.7.1	TCP	46
8.7.2	UDP	49
8.7.3	HTTP/3 (mit UDP statt TCP)	49

8.1 Organisationen



8.1.1 RIPE NCC

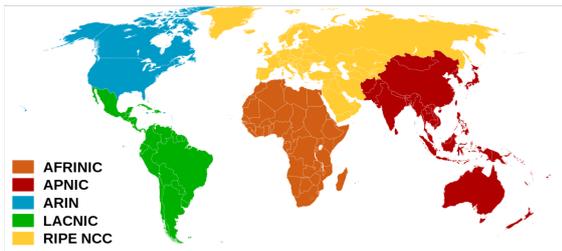


Abb. 8.1: Regionale Registries

Eine **RIR**¹ ist eine regional mit der Verwaltung und Zuteilung von Internet-Ressourcen betraute Organisation.

Definition 8.1

Weltweit gibt es fünf aktive regionale Registries.

Die Zuständigkeit der **RIR** umfasst die Verwaltung von IP-Adressen (IPv4 und IPv6) sowie AS-Nummern.

Die **RIPE**² sind eine Arbeitsgemeinschaft in Amsterdam zur Koordination des Internets.

Definition 8.2

Die RIPE, gegründet am 16. Mai 2014, entstand aus der Kooperation der Betreiber von Rechnernetzen zwecks Schaffung eines gesamteuropäischen Netzes.

Die RIPE beschließt im Konsens von Arbeitsgruppen Empfehlungen an das RIPE NCC.

RIPE NCC³ ist eine RIR zuständig für Europa, den Nahen Osten und Teile von Zentralasien.

Definition 8.3

8.1.2 ISOC

Die **ISOC**⁴ ist eine professionelle Gesellschaft, deren Hauptaufgabe die Sorge für das weitere Wachstum und die Weiterentwicklung des weltweiten Internets ist.

Definition 8.4

Die Festlegung von neuen Standards ist die Hauptaufgabe der **ISOC**.

¹englisch: **RIR** = Regional Internet Registry

²französisch: **RIPE** = Réseaux IP Européens

³französisch: **RIPE NCC** = Réseaux IP Européens Network Coordination Centre

⁴englisch: **ISOC** = Internet Society

Dazu zählt auch die Behandlung der Fragen, in welcher Weise das Internet genutzt wird oder nach den dadurch ausgelösten Folgen im sozialen, politischen oder technischen Bereich.

Das **ISOC** Board of Trustees bestätigt Nominierungen für das **IAB**, die vom **IETF** Nominierungskomitee getroffen werden.

8.1.3 IANA

Defacto lag bis 1998 die Kontrolle über die Internet-Adressen bei **IANA** in der Hand von Jon Postel, einem der Gründervater des Internet, der von Anfang an als Editor der **RFCs** fungierte.

Nach seinem Tod ging die Gewalt über die Adressvergabe an die **ICANN**⁵ über.

8.1.4 IAB

Das **IAB**⁶ ist ein Komitee, welches den Überblick über die Architekturen der Standardisierungsaktivitäten der **IETF** wahrt und die **ISOC** beratend unterstützt.

Definition 8.5

Das **IAB** unterstützt und organisiert die **IRTF** und lädt zu Arbeitstreffen (**IAB Workshops**) ein, die bestimmte Themen von Internetarchitekturen detailliert behandeln.

IRTF

Die **IRTF**⁷, eine von zwei Arbeitsgruppen des **IAB**, wurde 1986 gegründet um Forschung und Entwicklung von Netzwerktechniken zu fördern.

Definition 8.6

Die **IRTF** besteht aus Forschungsgruppen, die sich unter anderem mit folgenden Themen befassen:

- End-to-End
- Information Infrastructure Architecture
- Privacy and Security
- Internet Resource Discovery
- Routing
- Services Management
- Reliable Multicast
- Internet Congestion Control



IRTF
RFC 2014

⁵englisch: **ICANN** = Internet Corporation for Assigned Names and Numbers

⁶englisch: **IAB** = Internet Architecture Board

⁷englisch: **IRTF** = Internet Research Task Force (Internetforschung-Arbeitsgruppe)

IRSG

Die **IRSG**⁸ leitet und koordiniert die Forschungsarbeiten der IRTF.

Definition 8.7

Dabei kommt es mitunter zu Schnittstellen mit den Arbeiten der **IETF**. Sogar bei den Mitgliedern der Gruppen gibt es Überschneidungen.

IETF

Die **IETF**⁹ befasst sich mit der Entwicklung von Internetstandards und Best Practices um die Funktionsweise des Internets zu verbessern.

Definition 8.8

Im Gegensatz zur forschungsorientierten Internet Research Task Force (**IRTF**) kümmert sich die **IETF** um die technische Entwicklung und Standardisierung von Internetprotokollen.

Die **IETF** veröffentlicht in der Dokumentenreihe **RFC** etablierte Internetprotokollstandards, experimentelle Neuentwicklungen und Dokumente mit informativen Charakter.

Zurzeit gliedert sich die **IETF** in sieben Arbeitsgruppen mit einem dieser Bereiche:

- **Applications and Real-Time (ART)**¹⁰
- **General (GEN)**¹¹
- **Internet (INT)**¹²
- **Operations and Management (OPS)**¹³
- **Routing (RTG)**
- **Security (SEC)**¹⁴
- **Transport Services (TSV)**¹⁵

IESG

Die **IESG**¹⁶ ist verantwortlich für die Leitung der **IETF** und der Internet-Standardisierungsprozesse

Definition 8.9

Die **IESG**, ein Teil der **ISOC**, kümmert sich um das technische Management der **IETF**-Aktivitäten und des Internet-Standardisierungsprozesses.

Die Hauptverantwortung der **IESG** liegt bei allen Aktivitäten, die den Eintritt neuer und den Fortschritt bereits in der Bearbeitung befindlicher Standardisierungsvorschläge betreffen.

Die **IESG** ist die letzte Instanz zur Verabschiedung eines offiziellen Internet-Standards. Sie setzt sich aus den Arbeitsgruppen-Managern der **IETF** zusammen.

⁸englisch: **IRSG** = Internet Research Steering Group (Internet-Forschungslenkungsausschuss)

⁹englisch: **IETF** = Internet Engineering Task Force (Internettechnik-Arbeitsgruppe)

¹⁰englisch: **ART** = Applications and Real-Time (Anwendungen und Echtzeit)

¹¹englisch: **GEN** = General (Allgemeines)

¹²englisch: **INT** = Internet (Internet-Dienste)

¹³englisch: **OPS** = Operations and Management (Betrieb und Netzmanagement)

¹⁴englisch: **SEC** = Security (Sicherheit)

¹⁵englisch: **TSV** = Transport Services (Transportdienste)

¹⁶englisch: **IESG** = Internet Engineering Steering Group (Internettechnik-Lenkungsausschuss)

8.2 Der Standardisierungsprozess

8.2.1 Request for Comments (RFC)

Spezifikationen eines späteren Internet-Standards, Vorschläge für neue oder Revision bestehender Standards werden zunächst als technische Berichte, sogenannte **RFCs**¹⁷ durch **IESG** oder **IAB** veröffentlicht.

Definition 8.10



RFC-Editor

Schon die Namensgebung weist darauf hin, daß der eingereichte Spezifikationsvorschlag Gegenstand öffentlicher Diskussion sein soll.

Die Veröffentlichung neuer **RFCs** obliegt der Verantwortlichkeit des **RFC**-Editors und unterliegt der generellen Richtungsweisung des **IAB**.

Die Serie der **RFCs** wird fortlaufend und chronologisch durchnummeriert. Jeder neue **RFC** bzw. dessen Revision erhält eine eigene Nummer.

Der Status der neuen Standards wird periodisch veröffentlicht und zeigt den Fortschritt auf dem Weg zum Internet-Standard.

8.2.2 Entwicklungsprozess

Die **IETF** fungiert im Internet-Standardisierungsprozess als Dreh- und Angelpunkt. Ein Großteil aller technischer Beiträge wird von ihr initiiert und sie wirkt als Integrationspunkt für andere Standards, die außerhalb des Internet-Standardisierungsprozesses definiert wurden. (siehe Abb. 1.22).

Eine Spezifikation, die einmal als Internet-Standard veröffentlicht werden soll, durchläuft dann einen fest vorgegebenen Entwicklungsprozess mit unterschiedlichen Reifegraden.

- **Proposed Standard**
Eine neue Spezifikation, die bereits von der Internet-Gemeinde begutachtet wurde. Eine zügige Implementation ist erwünscht, um dabei gewonnenen Erfahrungen in die weitere Ausgestaltung der Spezifikation miteinbeziehen zu können.
- **Draft Standard**
Ein Proposed Standard, mit mindestens zwei unabhängigen Implementierungen, kann erst nach Ablauf von 6 Monaten auf dieses Level gehoben werden. Der Draft Standard wird bereits als endgültige Spezifikation betrachtet, die nur noch verändert wird, falls unvorhergesehene Probleme auftreten, die das erzwingen.
- **Internet Official Protocol Standard**
Wurden für einen Draft Standard bereits ausreichend Einsatzerfahrungen gewonnen, so kann dieser in den Status eines offiziellen Internet Standards erhoben werden. Er zeigt bereits einen hohen Grad an technischer Ausgereiftheit und man rechnet damit einen signifikanten Beitrag für das Internet und seine Benutzer zu leisten.

Zusätzlich zum **RFC**-Status, legt das **IAB** einen Protocol Status für die betreffende **TCP/IP**-HW fest:

- **Required**: dieses Protokoll muß unterstützt werden
- **Recommended**: Unterstützung dieses Protokolls empfohlen
- **Elective**: eine Unterstützung ist freiwillig
- **Limited Use**: nur für Testgruppen
- **Not Recommended**: Unterstützung unerwünscht (z. B. veraltet)

¹⁷englisch: **RFC** = Request for Comments

8.3 Internet Protocol (IPv4)

8.3.1 Grundbegriffe

Aus Sicht der Netzwerkschicht des **TCP/IP**-Referenzmodells kann das Internet als eine über Multiprotokoll-Router miteinander verbundene, riesige Sammlung einzelner autonomer Systeme (Subnetze) betrachtet werden.

Alle miteinander verbundene Netzwerke nutzen das Internet-Protokoll (IP-Protokoll), das dafür sorgt, daß Datenpakete stets ihren Weg vom Sender zum dezierten Empfänger finden.

Gemäß RCF 1009 und RCF 1122 gelten folgende Grundbegriffe:

Eine **Nachricht (Segment)** ist eine via TCP zu übertragende Dateneinheit, bestehend aus einem TCP-Header und Nutzdaten.

Definition 8.11

Ein **Paket (Datagramm)** ist eine zwischen zwei IP-Instanzen ausgetauschte Dateneinheit, bestehend aus einem IP-Header und Nutzdaten.

Definition 8.12

Ein **Frame (Rahmen)** ist eine zwischen zwei Instanzen der Bitübertragungsschicht (Schicht 2) des **TCP/IP** Referenzmodells ausgetauschte Dateneinheit, bestehend aus einem Header, den Nutzdaten und einem abschließenden Trailer.

Definition 8.13

Ein **Host** bezeichnet ein Rechensystem, an dem die/der Nutzer:in eines Internetdienstes (Client) arbeitet.

Definition 8.14

Ein **Router (Gateway)** bezeichnet ein Zwischensystem, welches zwischen verschiedenen Netzwerk-Segmenten vermittelt.

Definition 8.15

Ein **IGP**¹⁸ bezeichnet ein Routingverfahren, das innerhalb eines Autonomen Systems zum Einsatz kommt.

Definition 8.16

Ein **EGP**¹⁹ bezeichnet ein Routingverfahren, das zwischen einzelnen autonomen Systemen zum Einsatz kommt.

Definition 8.17

Dank des IP-Adressierungsschema erscheint das globale Internet dem Nutzer tatsächlich als ein einziges homogenes und universelles Netzwerk. Damit bleiben viele Details der Einzelnetze des Internets dem Anwender verborgen.

Tatsächlich bleiben - durch Verwendung von hierarchisch aufgebaute, logische Namen (**DNS**) - auch die numerische IP-Adressen dem Anwender verborgen.

¹⁸ **englisch:** *IGP* = Interior Gateway Protocol

¹⁹ **englisch:** *EGP* = Exterior Gateway Protocol

IP-Adresse

Eine **IP-Adresse** ist eine Adresse in Computernetzen, die - wie das Internet - auf dem Internetprotokoll (IP) basieren.

Definition 8.18

AS-Nummer

Jedem autonomen System wird eine eindeutige **AS-Nummer** (Autonomous System Number) als 32-Bit-Ganzzahl (RFC 6996) zugewiesen.

Definition 8.19

Autonomes System

Ein **autonomes System (AS)** ist ein System, das sich anderen AS so präsentiert, als hätte es nur einen einzigen inneren Routing-Plan

moderne Definition 8.20

Autonome Systeme sind untereinander verbunden und bilden so das Internet.

Ein AS wird gewöhnlich von einem Internet-Serviceprovider (ISP) verwaltet, und besteht aus mehreren Routern und den damit verbundenen Netzwerken.

Durch die Verwendung von ASs vereinfacht sich der Routing-Aufwand zwischen den Millionen Netzwerken.



AS

8.3.2 IP-Adress-Klassen

Klasse	Bits	Anzahl		Anzahl Bits		Adressraum		
		Netze	max.	Hosts	max.	Netz	Hosts	von - bis
A	0	126	$= 2^7 - 2$	16 777 214	$= 2^{24} - 2$	8	24	1.0.0.0 - 126.0.0.0
B	10	16 384	$= 2^{14} - 2$	65 534	$= 2^{16} - 2$	16	16	128.1.0.0 - 191.254.0.0
C	110	2 097 152	$= 2^{21} - 2$	254	$= 2^8 - 2$	24	8	192.0.0.0 - 223.255.254.0
D	1110							224.0.0.0 - 239.255.255.255
E	1111							240.0.0.0 - 254.255.255.255

Tab. 8.1: Eigenschaften der IP-Adress-Klassen

Eine **Internet-Adresse (IP-Adresse)** besteht aus 4 Byte (4 Oktetten) zu je 8 Bit, das sind insgesamt 32 Bits.

Definition 8.1

Die IP-Adresse wird meist als Punkt-Dezimal-Notation²⁰, eine Folge von vier vorzeichenlosen, ganzzahligen, durch Dezimalpunkte getrennten Dezimalzahlen, angegeben.



Abb. 8.2: Beispiel einer IP-Adresse

Der gesamte, theoretisch verfügbare Adressbereich umfasst in Dezimaldarstellung den Bereich:



Abb. 8.3: Adressbereich der 32-Bit-IP-Adresse

Logisch gliedert sich eine IP-Adresse in zwei Teile: ein Adresspräfix und ein Adresssuffix.

Das **Adresspräfix** oder auch **Netz-ID**²¹ identifiziert das **physikalische Netzwerk**, an das der betreffende Rechner angeschlossen ist.

Definition 8.2

Dieses Schema der Adresshierarchie unterstützt eine globale Verwaltung der Netz-IDs

Das **Adresssuffix** oder auch **Host-ID**²² identifiziert einen bestimmten **Rechner** in dem durch die Netz-ID bestimmten Netzwerk.

Definition 8.3

Die Verwaltung der Host-IDs erfolgt in der Regel durch den jeweiligen Netzwerk-Administrator.

Der IP-Adressraum wurde historisch in drei verschiedene Adress-Klassen unterteilt, die sich in Länge des Präfix und Suffix unterscheiden.

Primäre Adress-Klassen

Aus den ersten ein bis vier Bits einer IP-Adresse ergibt sich die jeweils vorliegende Adressklasse und damit die Aufteilung der Adresse in Adresspräfix und Adresssuffix.

Die Klassen A, B und C werden als **Primäre Adress-Klassen** bezeichnet.

Definition 8.4



Abb. 8.4: Primäre Adress-Klassen A, B und C

Spezielle Adress-Klassen

Die speziellen Klassen D und E sind für **Multicast-Adressen** (Klasse D) und experimentelle Zwecke (Klasse E) reserviert.

Definition 8.5

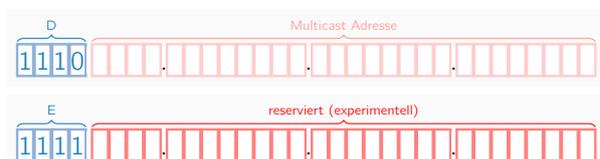


Abb. 8.5: speziellen Klassen D und E

²⁰ englisch: *Dotted Decimal Notation* = Punkt-Dezimal-Notation

²¹ englisch: *NetId* = Network Identification

²² englisch: *Host-ID* = Host Identifier

8.3.3 Spezielle IP-Adressen (Broadcast, Loopback, ...)

Klasse	Anzahl				Adressraum	
	Bits	Netze	Hosts	max.	von	- bis
A	0	1	16 777 214	= 2 ²⁴	10.0.0.0	- 10.255.255.255
B	10	16	1 048 576	= 2 ²⁰	172.16.0.0	- 172.31.255.255
C	110	256	65 536	= 2 ¹⁶	192.168.0.0	- 192.168.255.255

Tab. 8.2: Private Adressbereiche

Broadcast-Adressen

Über eine **Broadcast-Adresse** können **alle** Rechner in einem durch die Netz-ID identifizierten Netzwerk gleichzeitig adressiert werden.

Definition 8.1

Bei der Broadcast-Adresse werden alle Bits der betreffenden Host-ID auf 1 gesetzt, damit ist die höchste / letzte Adresse in jedem Subnetz die Broadcastadresse.

Ein IP-Datenpaket mit der Broadcast-Adresse wird solange durch das lokale Netzwerk weitergereicht, bis es von allen Rechnern des Netzes empfangen worden ist.

Loopback-Adressen

Bei der **Loop-Back-Adresse (Local Host Adresse)**, die Netz-ID 127 der Klasse A, erhält ein sendender Rechner ausgesendete Datenpakete wieder zurück.

Definition 8.4

Obwohl dabei die Host-ID nicht relevant ist, wird gemäß der Konvention die Host-ID 1 verwendet.

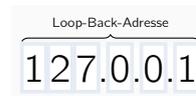


Abb. 8.7: Loop-Back-Adresse

Private Adressen

Als **Private IP-Adressen** werden speziell reservierte IP-Adressen genannt, die im globalen Internet nicht weitervermittelt werden (RFC 1597).

Definition 8.5

Das oben angegebenen Beispiel wird auch als „**Directed Broadcast**“ bezeichnet:

Das Ziel sind die Teilnehmer eines bestimmten Netzes. Die Adresse wird durch die Kombination aus Zielnetz und dem Setzen aller Hostbits auf 1 angeben.

Limited Broadcast

Bei einem **Limited Broadcast** wird als Ziel die IP-Adresse 255.255.255.255 angegeben. Dieses Ziel liegt immer im eigenen lokalen Netz und wird direkt in einen Ethernet-Broadcast umgesetzt.

Definition 8.2

Ein **Limited Broadcast** wird von einem Router nicht weitergeleitet.



Abb. 8.6: Limited Broadcast

Netzwerk-Adressen

Wird als Host-ID der Wert 0 verwendet, so ist das die Adresse des durch die **Netz-ID** angegebenen Netzwerks und nicht die eines speziellen, an dieses Netzwerk angeschlossenen Rechners.

Definition 8.3

Ebenso bezieht sich eine Adresse mit der Netz-ID 0 stets auf das eigene, lokale Netzwerk.



Abb. 8.8: Beispiel einer privaten Netz-ID

Multicast-Adressen

Mit einer **Multicast-Adresse** kann eine Gruppe zusammengehöriger Rechner adressiert werden.

Definition 8.6

Jede Rechnergruppe erhält zu diesem Zweck eine IP-Adresse der Klasse D, die diese Gruppe eindeutig adressiert.

Es existieren feste Multicast-Adressen, die dauerhaft für spezielle Gruppen eingerichtet sind, und temporäre, die für die private Nutzung zur Verfügung stehen.

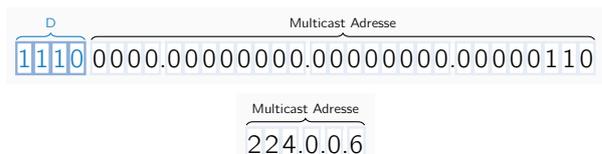


Abb. 8.9: Beispiel einer Multicast Adresse

8.3.4 Subnetz-Adressierung

Subnetz-ID

Einen möglicher Ansatz zur flexiblen Aufteilung des Adressraums bietet die Subnetz-Adressierung²³.

Bei der **Subnetz-Adressierung** wird eine bestimmte Anteil der Host-ID als **Subnetz** reserviert der übrige Anteil weiterhin als **Host-ID** verwendet.

Definition 8.1

Zu diesem Zweck wird eine bestimmte Anzahl Bits von der Host-ID für eine Subnetz-ID reserviert,

So kann z. B. ein Netzwerk der Klasse B, dessen Host-ID 16 Bits umfasst, in eine 6 Bit lange Subnetz-ID und eine neue 10 Bit lange Host-ID unterteilt werden.

Damit ist eine Adressierung von 62 Subnetzen mit jeweils 1022 verfügbaren Host-IDs möglich.

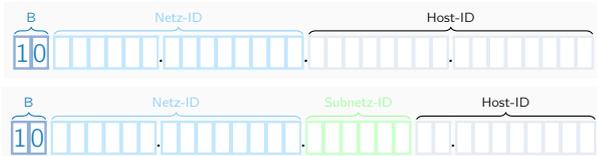


Abb. 8.10: Beispiel einer Subnetz-Adressierung

Von außen ist diese Aufteilung in Subnetzwerke nicht erkennbar und daher nicht nachvollziehbar.

Sie kann ohne Mitwirkung der regulierenden Behörde zur Adressvergabe (ICANN) erfolgen und obliegt allein der Verantwortung des Inhabers der betreffenden Netz-ID.

Subnet-Masks

Zur Unterscheidung der Host- von der Netzadresse (Netz-ID, Subnetz-ID) wird eine Subnetzmaske verwendet .

Bei der **Subnetzmaske** wird der **Bereich der Netzadresse** durch 1-Bits und der **Bereich der Host-ID** durch 0-Bits markiert.

Definition 8.2

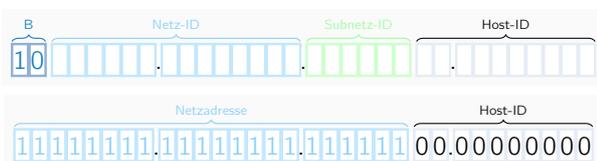


Abb. 8.11: Beispiel einer Subnetzmaske

Default Subnetzmasken

Für die Klassen A, B und C sind folgende Default Subnetzmasken definiert:

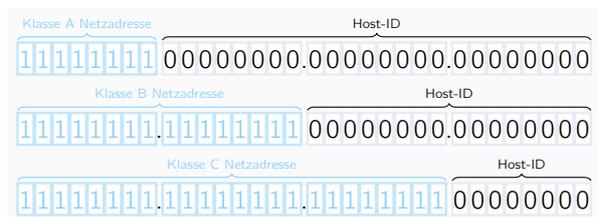


Abb. 8.12: Default Masken für die Klassen A, B und C

Klassenlose Notation von IP-Adressen

CIDR²⁴ beschreibt ein Verfahren zur effizienteren Nutzung des bestehenden 32-Bit-IP-Adress-Raumes für IPv4.

Definition 8.3



CIDR

CIDR wurde 1993 eingeführt²⁵, um die Größe von Routingtabellen zu reduzieren und um die verfügbaren Adressbereiche besser auszunutzen.

Bei CIDR führte man sogenannte Suffixe ein, welche die Anzahl der 1-Bits in der Netzmaske angibt.

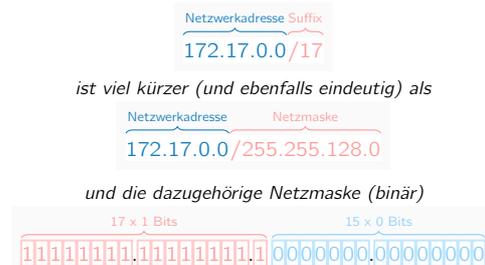


Abb. 8.13: Klassenlose Notation

²³ englisch: *Subnetting* = Subnetz-Adressierung

²⁴ englisch: *CIDR* = *Classless Inter-Domain Routing*

²⁵ siehe auch RFC 1518, RFC 1519, RFC 4632

8.4 Internet Protocol Version 6 (IPv6)

Bei der Einführung des Protokollstandards IPv4 (Internet Protocol Version 4) erwies sich dieser, allen aktuellen Problemen zum Trotz, jedoch als äußerst langlebig und erfolgreich.

Dank des ausgeklügelten Designs überlebte das IP-Protokoll ebenfalls eine Reihe von Hardware-Generationen, was sicher in seinem hohen Grad an Skalierbarkeit und seiner Flexibilität begründet liegt.

8.4.1 IPv6-Adressen

Adress-Notation

Bei der Entwicklung konnte niemand ahnen, dass das Internet exponentiell wachsen würde und eine Überarbeitung des IP wurde notwendig.

Eine **IPv6-Adresse** besteht aus 8 vierstelligen, durch Doppelpunkte voneinander getrennten Hexadezimalzahlen.

Definition 8.1

Mit 128 Bit zur Darstellung von IPv6-Adressen sind $2^{128} = 3,4 \cdot 10^{38}$ verschiedene Adressen verfügbar, das sind:

340.282.366.920.938.463.463.374.607.431.768.211.456

Abb. 8.14: Anzahl von möglichen IPv6 Adressen



Anzahl IPv6

Gäbe in jeder der ca. 2 Billionen Galaxien des bekannten Universums 100 Milliarden Planetensysteme mit je einem bewohnten Planeten (in Erdgröße), dann könnte man je Planet $1,7 \cdot 10^{15}$ IP-Adressen, das wären etwa 3 Adressen je m^2 der Planetenoberfläche, vergeben.

Die IPv6-Adresse wird als Folge von 8 vierstelligen, durch Doppelpunkte, analog zum Punkt bei IPv4, getrennte Hexadezimalzahlen, angegeben.

1. 2. 3. 4. 5. 6. 7. 8.
2001:0db8:85a3:08d3:1319:8a2e:0370:7344

Abb. 8.15: Beispiel einer IPv6-Adresse



IPv6 Notation

Ein oder mehrere aufeinander folgende Blöcke, deren Wert 0 beträgt, dürfen ausgelassen und durch zwei aufeinanderfolgende Doppelpunkte angezeigt werden.

1. 2. 3. bis 6. 7. 8.
2001:0db8:0:0:0:0:1428:57ab

1. 2. 7. 8.
2001:0db8::1428:57ab

Abb. 8.16: Beispiel mit unterdrückten Nullen

Die Reduktion darf nur einmal durchgeführt, d.h. höchstens eine Gruppe aus Null-Blöcken ersetzt, werden.

2001:0db8:0:0:08d3:0:0:0
2001:0db8::08d3:0:0:0
2001:0db8:0:0:08d3::

Abb. 8.17: Alternative Schreibweisen

Führende Nullen im Vierblock können auch weg gelassen werden. Damit vereinfacht sich obiges Beispiel zu:

2001:db8:0:0:8d3::

URL-Notation

In einer **URL**²⁶ wird die IPv6-Adresse in eckige Klammern eingeschlossen, z. B.:

HTTP IPv6 URL
http://[2001:0db8:85a3:08d3::0370:7344]/

Abb. 8.18: IPv6 URL-Notation



URL Notation

Diese Notation verhindert die fälschliche Interpretation von Portnummern als Teil der IPv6-Adresse:

HTTP IPv6 URL Portnummer
http://[2001:0db8:85a3:08d3::0370:7344]:8080/

Abb. 8.19: IPv6 URL-Notation (inkl. Portnummer)

Netz-Notation

IPv6-Netzwerke werden in CIDR-Notation aufgeschrieben, d.h. Netzadresse (Präfix) und Suffix (Präfixlänge in Bits) durch einen Schrägstrich getrennt notiert.

Ein Netzwerk mit

Netzadresse (Präfix) Suffix
2001:0db8:1234::/48

ergibt einen Adressraum von

Netzadresse Suffix
2001:0db8:1234:0000:0000:0000:0000:0000

bis

Netzadresse Suffix
2001:0db8:1234:ffff:ffff:ffff:ffff:ffff



Netznotation

Abb. 8.20: IPv6 Netz-Notation

²⁶englisch: URL = Uniform Resource Locator

Loopback-Adresse

Die IPv6-Loop-Back-Adresse ist wie folgt definiert:

Loop-Back-Adresse
::1/128

Abb. 8.21: Loop-Back-Adresse

Nicht spezifizierte IPv6-Adresse

Folgende Darstellung zeigt das Fehlen einer (nicht spezifizierten) Adresse an:

Nicht spezifiziert
::/128

Abb. 8.22: Nicht spezifizierte IPv6-Adresse

Link Local Unicast-Adresse

Eine **Link-Local-Unicast-Adresse** ist nur innerhalb eines abgeschlossenen Netzwerkes-Segmentes, d.h. bis zum ersten Router, gültig.

Definition 8.2

Link-Local-Unicast-Adresse
fe80::/10

Abb. 8.23: Link-Local-Unicast-Adresse

8.5 Domain Name System

8.5.1 Namens- und Verzeichnisdienste

Um auf einen entfernten Rechner über das Internet zu greifen zu können, muß der Zielrechner über seine weltweit eindeutige IP-Adresse identifiziert werden.

Für Anwender ist die 32 Bit lange IPv4-Adresse nur schwer im Gedächtnis zu behalten.

Stattdessen nutzt der Anwender z. B. einen symbolischen Namen (E-Mail-Adresse) oder eine URL (Uniform Resource Locators) im World Wide Web.

Ein Dienst, der Ressourcen eindeutig spezifiziert und diese über das Internet verfügbar macht, wird allgemein als **Verzeichnisdienst** bezeichnet.

Definition 8.1

Die Übersetzung verläuft automatisch und ist für die Anwendung bzw. für den Nutzer nicht wahrnehmbar.

Mit dem explosionsartigen Wachstum des Internets war eine zentrale Verwaltung einer Namens-Adresszuordnung im großen Maßstab nicht mehr sinnvoll.

8.5.2 Domain Name System

Das **Domain Name System**²⁷ (**DNS**) als eine verteilte Datenbankanwendung dient dazu, symbolischen Namen binäre IP-Adressen zuzuordnen.

Definition 8.2

Host Sub Domäne Top Level
pc064.ima.fh-joanneum.at

Abb. 8.24: DNS Adressraum Hierarchie

Der DNS-Adressraum ist hierarchisch strukturiert und den verschiedenen Abschnitten ist jeweils ein eigener DNS-Server zugeordnet, die das Mapping im betreffenden Adressraumabschnitt übernehmen.

Durch den hierarchischen Aufbau in sogenannte Domänen²⁸ wird weltweit eine eindeutige Identifikation einer Adresse gewährleistet.

8.5.3 Fully Qualified Name

Fully Qualified Domain Name

Der vollständige Name einer **Domain** wird als **Fully Qualified Domain Name (FQDN)** bezeichnet.

Definition 8.3

3rd-level 2nd-level top-level root
www.example.com.

Abb. 8.25: Beispiel einer FQDN

Da das Root-Label immer leer ist (leere Zeichenkette), wird bei den meisten Benutzer-Anwendungen (Browsern) auf die Eingabe des Punktes zwischen dem Label der Top Level Domain und dem root-label verzichtet.

²⁷siehe auch RFCs 1034 und 1035

²⁸englisch: *domains* = Domänen, analog zur Gliederung einer Postanschrift (Name, Straße, Postleitzahl, Wohnort, Land)

Streng genommen handelt es sich bei dieser Schreibweise nicht mehr um eine absolute, sondern um eine relative Adresse und damit nicht mehr um einen FQDN.

Fully-Qualified Host Name

Der vollständige Name eines Rechners, entweder als FQDN oder IP-Adresse, wird als **Fully Qualified Host Name (FQHN)** bezeichnet.

Definition 8.4

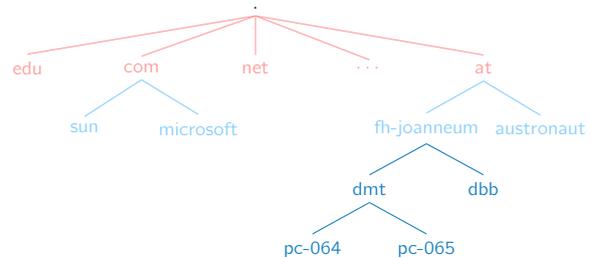


Abb. 8.26: Beispiele für FQHN

Resource Records

Ein **Resource Record (RR)** ist die grundlegende Informationseinheit in einem Domain Name System (DNS).

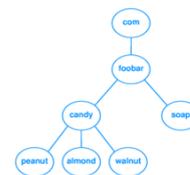
Definition 8.5

Der Resource Record tritt in Zonendateien (ASCII-Darstellung) oder in DNS-Transport-Paketen oder DNS-Caches (komprimierter Form) auf.

Bei der Angabe in **Resource Records** auf Nameservern muss zwingend der FQDN, d.h. der volle Name mit Punkt angegeben werden.

Definition 8.6

8.5.4 Domains und Subdomains

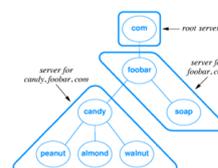


peanut.candy.foobar.com

Abb. 8.27: FQDN der Subdomain peanut

Dabei übernimmt der DNS-Server folgende Aufgaben:

- FQNs/IP-Adressen Mapping
- DNS Server-Hierarchie (Domains / Subdomains)
- Top-Level-Domain-/untergeordnete DNS Server



Name Server

Ein **Nameserver** ist ein Server, der symbolischen Namen von Rechnern bzw. Diensten eine numerische IP-Adresse zuordnet (**Namensauflösung**).

Definition 8.1

Nameserver sind Programme, die Anfragen zum Domain-Namensraum beantworten. Teilweise werden auch die Rechner, auf denen diese Programme laufen, als Nameserver bezeichnet.

Man unterscheidet zwischen autoritativen und nicht-autoritativen Nameservern.

Autoritativer Server

Für jede Zone existiert mindestens ein verantwortlicher Nameserver (**autoritativer Server**), dieser wird als **Primary Nameserver** bezeichnet.

Definition 8.2

Aus Redundanz- und Lastverteilungsgründen werden autoritative Nameserver fast immer als Server-Cluster realisiert, wobei die Zonendaten identisch auf einem oder mehreren Secondary Nameservern liegen.

Nicht-autoritativer Server

Ein **nicht-autoritativer** Nameserver bezieht Informationen über seine Zone von anderen Nameservern sozusagen aus zweiter oder dritter Hand.

Definition 8.3

Da sich DNS-Daten normalerweise nur sehr selten ändern, speichern nicht-autoritative Nameserver die einmal von einem Resolver angefragten Informationen im lokalen RAM (Cache) ab, damit diese bei einer erneuten Anfrage schneller vorliegen.

Jeder Eintrag im Cache besitzt ein **Verfallsdatum (TTL²⁹)**. Läuft dieses Datum ab, wird der Eintrag aus dem Cache gelöscht.

Definition 8.4

Die TTL wird durch einen autoritativen Nameserver für diesen Eintrag festgelegt und wird nach der Änderungswahrscheinlichkeit des Eintrages bestimmt (sich häufig ändernde DNS-Daten erhalten eine niedrige TTL). Das

kann unter Umständen bedeuten, dass der Nameserver in dieser Zeit falsche Informationen liefert, wenn sich die Daten zwischenzeitlich geändert haben.

Ein Spezialfall ist der **Caching Only Nameserver**. In diesem Fall ist der Nameserver für keine Zone verantwortlich und muss alle eintreffenden Anfragen über weitere Nameserver (**Forwarder**) auflösen.

Resolver

Resolver sind einfache **Software-Module**, die im Hintergrund für eine Anwendung Informationen von Nameservern abrufen können.

Definition 8.5

Der Resolver übernimmt die Anfrage einer Anwendung, ergänzt sie (FQDN) und übermittelt sie an einen normalerweise fest zugeordneten Nameserver. Ein Resolver arbeitet entweder rekursiv oder iterativ.

Die so gewonnene Antwort übergibt der Resolver an das Programm, das die Daten angefordert hat, beispielsweise an den Webbrowser.

Im **rekursiven** Modus schickt der Resolver **eine** Anfrage an den ihm zugeordneten Nameserver, der diese, wenn nötig, rekursiv weiterleitet.

Definition 8.6

Hat dieser die gewünschte Information nicht im eigenen Datenbestand, so kontaktiert der Nameserver weitere Server – und zwar solange, bis er eine Antwort erhält; entweder positive, oder von einem autoritativen Server eine negative. Rekursiv arbeitende Resolver überlassen also die Arbeit zur vollständigen Auflösung ihrem Nameserver.

Im **iterativen** Modus kontaktiert der Resolver **sukzessive** selbst **mehrmals** verschiedene Nameserver bis er eine verbindliche Antwort erhält.

Definition 8.7

Nameserver besitzen in der Regel eigene Resolver. Diese arbeiten gewöhnlich iterativ.

Bekanntere Programme zur Überprüfung der Namensauflösung sind nslookup, host und dig.



Nameserver

²⁹englisch: **TTL = Time To Live**

8.6 Routing

Abb. 8.28: Beispiel zu Routingtabellen

Das **Routing**³⁰ bezeichnet allgemein in Rechnernetzen das Festlegen von Wegen für Nachrichtenströme bei der Nachrichtenübermittlung

Definition 8.1

In paketvermittelten Datennetzen ist zwischen den beiden verschiedenen Prozessen Routing und Forwarding zu unterscheiden:

8.6.1 Routing Tabellen

Eine **Routingtabelle** gibt Aufschluss darüber, auf welchem Weg (Route) sich ein netzwerkfähiges Gerät (z. B. Rechner, Router) mit anderen Netzwerken und deren Teilnehmern zu verbinden hat.

Definition 8.2

Ein Eintrag weist einem Adressbereich eines Netzwerkziels eine Angabe zu, über welchen Router und welche Schnittstelle die Daten als Paketstrom zu leiten sind.

Jeder Eintrag in einer Routingtabelle besitzt mindestens folgende Informationen:

- **Netzadresse und Subnetzmaske**
Beide Angaben bestimmen den IP-Adresspräfix eines Zielnetzes und damit das Ziel, auf welches sich dieser Tabelleneintrag bezieht.
- **Next Hop (Gateway)**
Nächste Routeradresse (Nachbar-Router), an welche ein Paket weitergeleitet werden muss.
- **Metrik**
Enthält Informationen über Gewichtung/Präferenz der Nutzung der Leitweginformation, wenn mehrere über dasselbe Routing-Protokoll gelernte Routen für dasselbe Zielnetz existieren. Die beste Route ist diejenige mit dem kleinsten Metrik-Wert.

8.6.2 IP Forwarding

Das Durchsuchen mehrerer Routingtabellen mit Hilfe des **Longest Prefix Match** wäre sehr rechenaufwändig.

Beim **IP-Forwarding** wird aus vielen Routingeinträgen, -tabellen eine einzige Tabelle³¹ erstellt, welche eine effiziente Verarbeitung weiterzuleitender Pakete ermöglicht.

Definition 8.3

Obwohl die hardwarenahe Forwarding-Tabelle aus der softwarebasierten Routing-Tabelle generiert wird, werden beide häufig unter dem Begriff Routingtabelle subsumiert.

8.6.3 IPv4 Datagramm

Ein **Datagramm** ist eine in sich geschlossene, unabhängige Dateneinheit, die ohne weitere Verbindungssicherung zwischen zwei Endpunkten (Peer-to-Peer) verschickt wird.

Definition 8.4

Ein Datagramm zeichnet sich durch geringen Protokoll-Overhead aus und enthält im Wesentlichen die Empfänger-, Absenderadresse und Nutzdaten.

Abb. 8.29: IPv4 Datagramm Header

³⁰ **englisch:** *routing* = Vermittlung, senden, steuern

³¹ Forwardingtabelle oder auch **Forwarding Information Base**, kurz **FIB**

8.6.4 NAT und Masquerading

Network Address Translation (NAT), Netzwerk-adressübersetzung) ist in Rechnernetzen der Sammelbegriff bei Änderungen von Adressen im IP-Header von IP-Paketen (Schicht 3 des ISO/OSI-Modells).

Definition 8.5

Port Address Translation (PAT) wird gemeinsam mit NAT eingesetzt und dann auch als NAT/PAT, NATPT oder „IP Masquerading“ bezeichnet.

IP Masquerading ermöglicht unter anderem die gleichzeitige Verwendung einer einzigen öffentlichen Adresse (vgl. private IP-Adressen) durch mehrere Hosts.

Üblicherweise übernimmt der Router im Netzwerk die NAT, der die Verbindung zum Internet herstellt (daher ist in der Regel dieser Router das Default-Gateway eines Hosts).

8.6.5 ICMP, Traceroute

Internet Control Message Protocol (ICMP) ist ein Hilfsprotokoll für das Internet Protocol (IP) und muss von allen IP-Routern und IP-Endgeräten unterstützt werden.

Definition 8.6

Mit ICMP werden vor allem Informations- und Fehlermeldungen über das Internet Protocol ausgetauscht.

ICMP und das TTL-Feld im IP-Header werden auch genutzt, um einen ganzen Verbindungsweg zwischen zwei Endsystemen (der über viele Router führen kann) ermitteln und anzeigen zu können (**traceroute**).



Forwarding



ICMP



traceroute

8.7 Transportprotokolle

Die Transportschicht, zwischen Anwendung- und Vermittlungsschicht, erfüllt die wichtigste Rolle bei der direkten Bereitstellung von Kommunikationsdiensten für die Anwendungsprozesse.

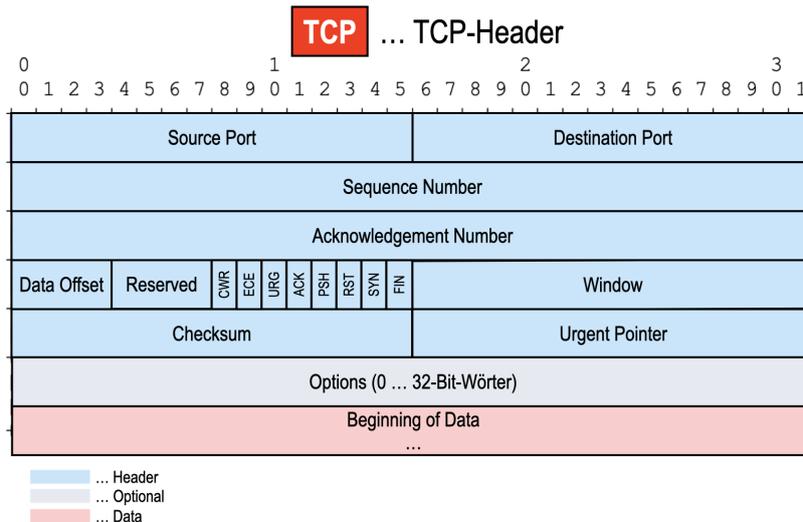


Abb. 8.30: TCP-Header

8.7.1 TCP

Das **Transmission Control Protocol (TCP)** ist ein zuverlässiges, verbindungsorientiertes, paketvermittelndes Transportprotokoll, das definiert, auf welche Art und Weise Daten zwischen Netzwerkkomponenten ausgetauscht werden soll.

Definition 8.1

Aufbau des TCP-Header

- **Source Port**
Portnummer der Senderseite
- **Destination Port**
Portnummer der Empfängerseite
- **Sequence Number**
Dient zur Sortierung nach Übertragung, wenn Pakete in unterschiedlicher Reihenfolge ankommen.
- **Acknowledge Number**
Die Sequenznummer, die der Absender als Nächstes erwartet (nur gültig wenn ACK-Flag gesetzt).
- **Data Offset**
Länge des TCP-Headers in 32-Bit-Blöcken (ohne Nutzdaten) und Startadresse der Nutzdaten.
- **Reserved**
Für zukünftige Anwendungen reserviert.
- **Control Flags**
Signalisiert zwei mögliche Zustände und wird für die Weiterverarbeitung der Daten benötigt werden.
- **Receive Window**
Ergibt, nach Berechnung, Anzahl der Daten-Objekts, die der Sender bereit ist zu empfangen.
- **Checksum**
Prüfsumme (über TCP-Header, Daten und Pseude-Header), zur Erkennung von Übertragungsfehlern.
- **Urgent Pointer**
Ergibt mit der Sequenz-Nummer die Position des ersten Bytes nach den Urgent-Daten an.

- **Options**
Enthält Zusatzinformationen und kann bis zu 40 Byte lang sein.

Bedeutung der Kontrollflags

- **CWR,ECE**
für **ECN**³². Mit **ECE**-Bit³³ teilt der Empfänger dem Sender mit, dass das Netzwerk überlastet ist. Sender bestätigt dies mit **CWR**-Bit³⁴.
- **URG**³⁵
Daten nach dem Header werden sofort von der Anwendung bearbeitet. Wird äußerst selten benutzt.
- **ACK**³⁶
Bestätigt in Kombination mit der **Acknowledge**-Number den Empfang von TCP-Segmenten.
- **PSH**³⁷
Augehende und eingehende Puffer werden übergangen
- **RST**³⁸
Die Verbindung wird abgebrochen, z. B. bei technischen Problemen oder Abweisung unerwünschter Verbindungen.
- **SYN**
Initialisiert Verbindung und wird vom Empfänger beim erfolgreichen Verbindungsaufbau mit mit **SYN + ACK** bestätigt.
- **FIN**³⁹
Signalisiert dass keine weitere Daten vom Sender kommen und gibt Verbindung frei.

³² **englisch:** ECN = Explicit Congestion Notification

³³ **englisch:** ECE = ECN-Echo

³⁴ **englisch:** CWR = Congestion Window-Reduces

³⁵ **englisch:** URG = Urgent

³⁶ **englisch:** ACK = Acknowledge

³⁷ **englisch:** PSH = Push

³⁸ **englisch:** RST = Reset

³⁹ **englisch:** FIN = Finish

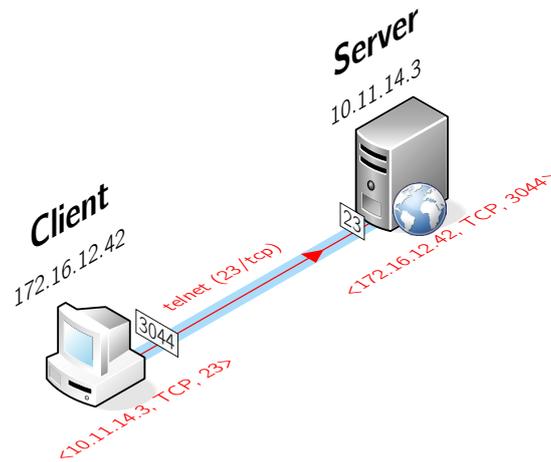


Abb. 8.31: TCP/IP Socket

Ein **Socket** (Kombination aus IP-Adresse, Transportprotokoll, Portnummer) kann einen einzelnen Netzwerkprozess **eindeutig** identifizieren. Definition 8.1

Man unterscheidet zwei Arten von Portnummern:

- **well-known ports**⁴⁰ standardisierte Portnummern über die ein fremder Rechner einen bestimmten Netzwerkdienst gezielt ansprechen kann.
- **dynamically allocated ports**⁴¹ werden erst vergeben wenn ein Prozeß eine Portnummer benötigt.

Durch **zwei Sockets**, einer für den Ausgangsrechner und einer für den Zielrechner, wird eine **TCP-Verbindung** eindeutig definiert. Definition 8.2

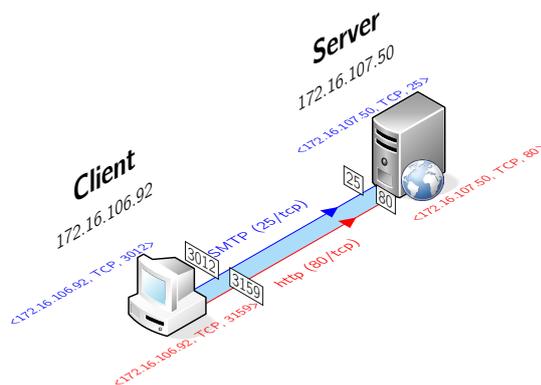


Abb. 8.32: Zwei TCP Verbindungen

3-Way-Handshake

Beim Aufbau einer TCP-Verbindung werden nur drei Nachrichten ausgetauscht. Dieses Verfahren wird als **3-Way-Handshake**⁴² bezeichnet. Definition 8.3

Das **3-Way-Handshake** erfüllt zwei wichtige Aufgaben:

- **Sender und Empfänger** garantieren Bereitschaft für einen Datenaustausch.
- **Initialisierung der Sequenznummern** zum Start des Datentransfers.

TCP Verbindungsaufbau

TCP verlangt von Sender und Empfänger eine Vereinbarung über die aufzubauende Verbindung.

Eventuelle Duplikatpakete aus früheren Verbindungen können so ignoriert werden.

Abb. 8.33: TCP Verbindungsaufbau

Verbindungsaufbau in drei Schritten:

1. Client initialisiert Sequenz-NR x, sendet **SYN**⁴³ und starten den Verbindungsaufbau.
2. Server bestätigt empfangene Sequenz-NR x mit **SYN ACK**⁴⁴ und eigener Sequenz-NR y.
3. Client bestätigt mit **ACK**⁴⁵ Empfang des **SYN-ACK-Segment** mit Sequenz-NR y.

Mit dem Empfang dieser Sender-Bestätigung ist das Drei-Wege-Handshake Protokoll abgeschlossen .

⁴⁰ englisch: *well-known ports* = reservierte Ports

⁴¹ englisch: *dynamically allocated ports* = dynamisch zugewiesene Ports

⁴² englisch: *3-Way-Handshake* = Drei-Wege-Handshake

⁴³ Segment mit gesetztem SYN-Bit

⁴⁴ Segment mit gesetztem SYN- und ACK-Bit

⁴⁵ Segment mit gesetztem ACK-Bit

TCP Varianten

Es existieren zahlreiche Varianten von **TCP** mit unterschiedlichen Verbesserungen und Erweiterungen, die aber untereinander „kompatibel“ bleiben müssen, dh. es können bei der Kommunikation von Partner mit verschiedenen Versionen eventuell nicht alle Möglichkeiten genutzt werden.

8.7.2 UDP

Das **User Datagram Protocol (UDP)** ist ein minimales, verbindungsloses Netzwerkprotokoll, das zur Transportschicht der Internetprotokollfamilie gehört und ermöglicht Anwendungen den Versand von Datagrammen in IP-basierten Rechnernetzen.

Definition 8.2

Funktionsweise

UDP verwendet Ports, um versendete Daten dem richtigen Programm auf dem Zielrechner zukommen zu lassen.

Dazu enthält jedes Datagramm die Prot Nummer des Dienstes, der die Daten erhalten soll.

Optional kann bei **UDP** eine Prüfsummen mitgesendet werden um fehlerhaft übertragene Datagramme zu erkennen und zu verwerfen.

UDP ist ein verbindungsloses, nicht-zuverlässiges und ungesichertes wie auch ungeschütztes Übertragungsprotokoll.

Das bedeutet, es gibt keine Garantie, dass ein einmal gesendetes Paket auch ankommt, dass Pakete in der gleichen Reihenfolge ankommen, in der sie gesendet wurden, oder dass ein Paket nur einmal beim Empfänger eintrifft.

Es gibt auch keine Gewähr dafür, dass die Daten unverfälscht oder unzugänglich für Dritte beim Empfänger eintreffen.

Eine Anwendung, die **UDP** nutzt, muss daher gegenüber verlorengegangenen und unsortierten Paketen unempfindlich sein oder selbst entsprechende Korrekturmaßnahmen und ggf. auch Sicherungsmaßnahmen vorsehen.

Da vor Übertragungsbeginn nicht erst eine Verbindung aufgebaut werden muss, kann ein Partner oder können beide Partner schneller mit dem Datenaustausch beginnen.

Das fällt vor allem bei Anwendungen ins Gewicht, bei denen nur kleine Datenmengen ausgetauscht werden müssen.

Einfache Frage-Antwort-Protokolle wie **DNS** (das Domain Name System) verwenden zur Namensauflösung hauptsächlich **UDP**, um die Netzwerkbelastung gering zu halten und damit den Datendurchsatz zu erhöhen.

Ein Drei-Wege-Handschlag wie bei **TCP** (dem Transmission Control Protocol) für den Aufbau der Verbindung würde in diesem Fall unnötigen Overhead erzeugen.

8.7.3 HTTP/3 (mit UDP statt TCP)

HTTP bis Version 2 stützt sich auf das **Transmission Control Protocol (TCP)** als Transportprotokoll.

TCP bestätigt den Erhalt jedes Datenpakets. Dies führt dazu, dass im Falle eines Paketverlustes alle anderen Pakete auf die erneute Übertragung des verloren gegangenen warten müssen (**Head-of-Line Blocking**).

Für mehrere Verbesserungen und Modernisierung der Übertragung von Webseiten und Webservices wurden die meisten Mechanismen von **TCP** jetzt in **HTTP/3** integriert und verbessert.

HTTP/3 wird daher nur noch in „einfachen“ **UDP**-Datagrammen verschickt und **TCP** wurde für einen großen Teil des Internet-Verkehrs unnötig.

9

Netzwerkcomponenten

Inhaltsangabe

9.1	Einteilung	51
9.1.1	Passive Netzwerkcomponenten	51
9.1.2	Aktive Netzwerkcomponenten	51
9.1.3	Übersicht	52
9.2	Netzwerkcomponenten	52
9.2.1	MS Windows (NDIS)	52
9.2.2	MS-Windows NT 4.0	52
9.2.3	MS-Windows Vista, Windows 7	52
9.3	Repeaters/Hubs	53
9.3.1	Topologie	53
9.3.2	Funktionen	53
9.3.3	Kaskadierung von Hubs	53
9.3.4	Einsatz	53
9.3.5	Direkter Vergleich	53
9.4	Bridges	54
9.4.1	Weiterleitung und Filterung	54
9.4.2	Selbstlernende Bridges	54
9.4.3	Schleifenbildung durch Bridging	55
9.4.4	Spanning-Tree	55
9.4.5	Übersetzende Bridges	55
9.5	Switches	56
9.5.1	Port-Tabellen von Switches	56
9.5.2	Arbeitsweise von Switches	56
9.5.3	VLAN	57
9.6	Routers	58
9.6.1	Routing-Tabellen	58
9.6.2	Routing-Algorithmen	59
9.6.3	Routing-Protokolle	60
9.7	Firewalls	61

9.1 Einteilung

9.1.1 Passive Netzwerkcomponenten

Als **passive Netzwerkcomponenten** werden all jene Materialien bezeichnet, die ohne Stromversorgung auskommen.

Definition 9.1

Zu den passiven Netzwerkcomponenten gehören z. B. Leitungen, Kabel, Stecker, Buchsen, Anschlussdosen.

9.1.2 Aktive Netzwerkcomponenten

Alle Geräte, die aktiv Signale verarbeiten bzw. verstärken können, werden als **aktive Netzwerkcomponenten (Netzwerkgeräte)** bezeichnet.

Definition 9.2

Aktive Netzwerkcomponenten benötigen für die korrekte Arbeitsweise eine Stromversorgung.



Netzwerkcomponenten

9.1.3 Übersicht

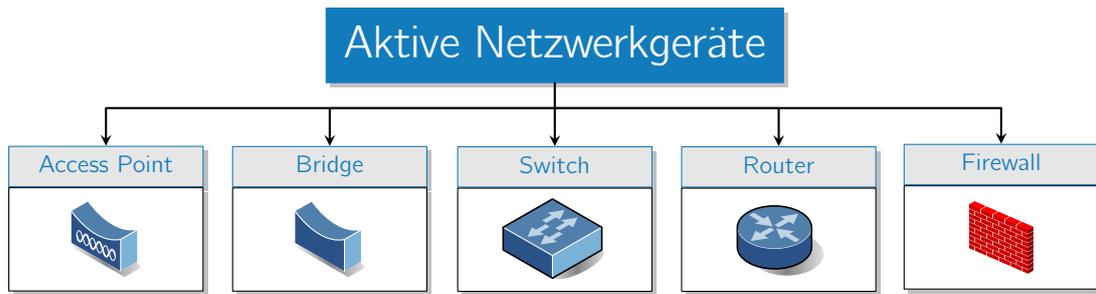


Abb. 9.1: Beispiele aktiver Netzwerkkomponenten

9.2 Netzwerkkarten

9.2.1 MS Windows (NDIS)

Eine **Netzwerkkarte** oder **Network Interface Card (NIC¹)** ist der Teil eines Computers, welche diesen mit einem lokalen Netzwerk verbindet.

Definition 9.1

Früher oft auf Steckkarten (Erweiterungssteckplatz), ist sie heute auf den meisten Hauptplatinen integriert.

NDIS-Multiprotokollstapel

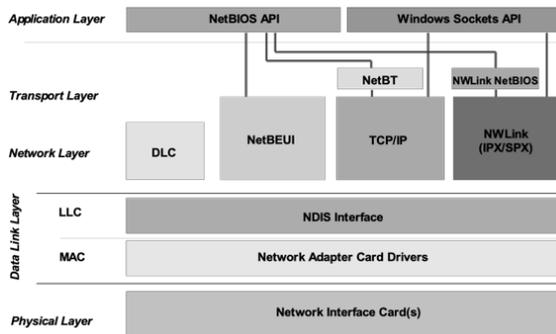


Abb. 9.2: NDIS-Multiprotokollstapel

Die **Network Driver Interface Specification (NDIS)** ist ein von Microsoft und 3Com entwickelter Standard zur Einbindung von Netzwerkkarten.

Definition 9.2

Sie erlaubt in einem PC den Betrieb von mehreren Karten und je Netzwerkkarte den Einsatz mehrerer Protokolle.

NDIS wird, im Gegensatz zu ODI für Apple, unter Windows verwendet.

Unter Linux und FreeBSD ist es möglich mit Hilfe eines Wrappers die Windows-Treiber zum Betrieb von Netzwerkkarten zu nutzen.

CoNDIS stellt eine Weiterentwicklung des NDIS-Treibers dar und soll in allen zukünftigen MS-Betriebssystemen die NDIS-Treiber ersetzen.

Definition 9.3

9.2.2 MS-Windows NT 4.0

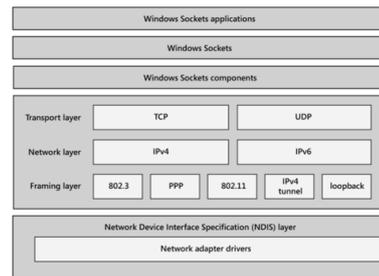


Abb. 9.3: Dual IP Layer TCP/IP Protocol Stack

Protokollstapel

- **NetBEUI** (NetBIOS Extended User Interface)
- **TCP/IP** (Internet Protocol Suite)
- **NWLink (IPX/SPX)** (Novell NetWare)
- **DLC** (Data Link Control)

Application Layer

- **APIs** (Application Programming Interfaces)
- **NetBIOS API**
- **Winsock (Windows Sockets API)**

9.2.3 MS-Windows Vista, Windows 7

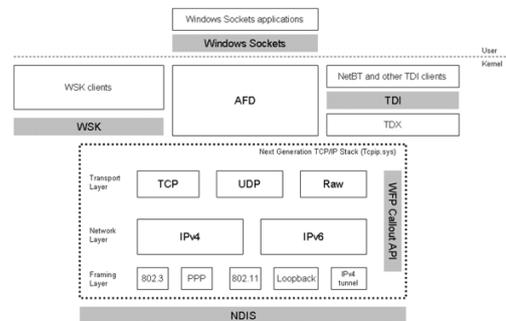


Abb. 9.4: Next Generation TCP/IP Stack

¹englisch: **NIC** = Network Interface Card



NW-Karte



NDIS

9.3 Repeaters/Hubs

9.3.1 Topologie

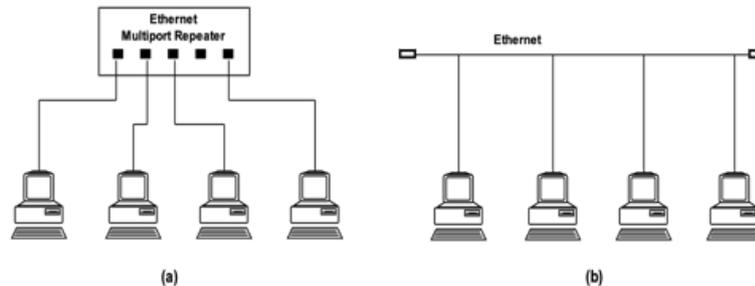


Abb. 9.5: Topologie eines Multiport Repeaters

Eine Verkabelungsart topologisch als Stern entspricht auf Ethernet-Ebene logisch einem Bus.

Die einfachste Möglichkeit mehrere LANs zu verbinden ist die Verwendung von Hubs. Sie sind Geräte der Bitübertragungsschicht.

Wenn ein Bit an einer Hub-Schnittstelle ankommt, sendet der Hub das Bit einfach rundum an alle anderen Schnittstellen [2, S 425].

Ein **Repeater** (**repeater**²) ist ein Signalverstärker zur Vergrößerung der Reichweite eines Signals.

Definition 9.1

Repeater sind Bestandteil der Bitübertragungsschicht (Schicht 1 des OSI-Modells) und dienen der Erweiterung von Netzwerksegmenten.

Als **Hub** (**hub**³) oder auch **Multiportrepeater** werden Geräte bezeichnet, die Netzwerkknoten sternförmig verbinden.

Definition 9.2

Beim Hub wird das Signal eines Netzwerkteilnehmers nicht analysiert, sondern nur die übertragene Bitebene wird regeneriert.

Am Anschluss eines Hubs kann man den Datenverkehr zwischen Netzwerkteilnehmern mit Netzwerkniffern analysieren und mitschneiden.

Da Repeater keine Rahmen zwischenspeichern, können sie auch keine LAN-Segmente mit unterschiedlichen Datenraten (z. B. 10 Mbit/s und 100 Mbit/s) verbinden.

9.3.2 Funktionen

- Wiederherstellung der Präambel
- Weiterleitung von Jam-Signalen
- Wiederherstellung der Signalamplituden
- Wiederherstellung des Signal Timings
- Wiederherstellung der Signalsymmetrie
- Fragment Extension
- Automatische Partitionierung

²englisch: *repeat* = wiederholen

³englisch: *hub* = Knotenpunkt

9.3.3 Kaskadierung von Hubs

Repeating Hubs können in einem Ethernet nicht beliebig kaskadiert werden, um eine größere Netzausdehnung zu erreichen.

Die **Round-Trip-Delay-Time (RTDT)** ist die Zeit, die ein Datenframe benötigt, um von einem Ende des Netzwerkes zum weitest entfernten andere Ende des Netzwerkes und wieder zurück zu gelangen.

Definition 9.3



Repeater

Eine für jede Datenübertragungsrate spezifische maximale **RTDT** darf nicht überschritten werden.

Wird das Netz zu groß, also die **RTDT** zu hoch, steigt die Anzahl der Kollisionen und unerkannter Kollisionen und beeinträchtigt damit die Netzwerkqualität.

9.3.4 Einsatz

Hubs sind eine veraltete und für Sicherheitslücken anfällige Technologie.

Aus diesen Gründen werden Hubs heute kaum verwendet und vor allem für die Erweiterung älterer Netzwerke eingesetzt.

Ausnahme: Einsatz bei Netzwerkanalysen, damit sämtliche Daten des Netzwerkes an allen Ports zur Verfügung stehen und damit kein zusätzlicher Mirror-Port benötigt wird.



Hub

9.3.5 Direkter Vergleich

Nachfolgend sind Funktionsweise und Fähigkeiten von Hub und Switch im direkten Vergleich dargestellt:

	Hub	Switch
Limitierte Bandbreite	Ja	Nein
Versand/Empfang gleichzeitig	Nein	Ja
Auswahl einzelner Endgeräte	Nein	Ja
Broadcast	Ja	Ja
Netzanalyse ohne Mirror-Port	Ja	Nein
OSI-Schichtmodell	Schicht 1	Schicht 2
Ports für Collision Domain	alle	einzelne

Tab. 9.1: Vergleich Hub mit Switch

9.4 Bridges

- 1 Bridge bootet (leere Tabelle)
- 2 S sendet an R
- 3 T sendet an R
- 4 Z sendet Broadcast
- 5 X sendet an T
- 6 X sendet an Y
- 7 Y sendet an X
- 8 R sendet an Z

Abb. 9.6: Selbstlernende Bridges - Funktionsweise

Eine **Bridge** (**bridge**⁴) ist ein Netzwerkgeräte, das zwei Segmente auf der Schicht 2 (Sicherheitsschicht) verbindet.

Definition 9.1

Die Ports aller Bridge-Arten arbeiten im **Promiscuous Mode**⁵, d.h. empfangene Pakete werden überprüft (Checksum) und nur korrekte Frames werden weitergesendet.

9.4.1 Weiterleitung und Filterung

Unter **Filterung** versteht man die Fähigkeit einer Bridge, festzustellen, ob ein Rahmen an eine Schnittstelle weitergeleitet oder einfach verworfen werden soll.

Definition 9.2

Das Filtern und Weiterleiten einer Bridge erfolgt anhand einer Bridge-Tabelle.

Weiterleitung ist die Fähigkeit, jene Schnittstelle zu ermitteln, an die ein Rahmen zu senden (weiterzuleiten) ist.

Definition 9.3

Die Bridge-Tabelle enthält für jeden Knoten:

- **LAN-Adresse** eines Knotens
- Bridge-**Schnittstelle** zum Knoten
- **Zeit** der Eintragung

9.4.2 Selbstlernende Bridges

Eine Bridge ist selbstlernend, d.h. sie erzeugt ihre Tabellen automatisch, dynamisch, und autonom.

Es ist weder ein Konfigurationsprotokoll noch der Eingriff eines Netzwerkadministrators notwendig [2, S 428].

Verbinden von LAN-Segmenten

Im folgenden Beispiel werden zwei Bridges mit jeweils zwei Schnittstellen verwendet.



Bridge

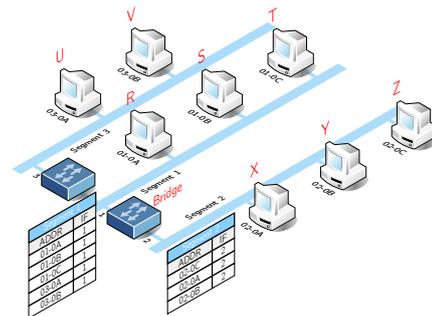


Abb. 9.7: Verbindung von LAN-Segmenten

Das Netzwerk im dargestellten Beispiel hat für die Kommunikation zwischen Segment 2 und Segment 3 zwei entscheidende Nachteile:

1. Bei **Ausfall von Segment 1** ist keine Kommunikation mehr möglich
2. Es erfolgt der **gesamte Datenverkehr über Segment 1** (Überlastungsgefahr).

Ein Problem beim rein hierarchischen Design für zusammengeschlossene LAN-Segmente ist: fällt ein Hub oder eine Bridge nahe dem oberen Ende der Hierarchie aus, dann sind Teile der darunterliegenden LANs vom Netzwerk getrennt.

Deshalb ist es wünschenswert, Netzwerke mit mehreren Pfaden zwischen LAN-Segmenten aufzubauen (Redundanz).

⁴ englisch: *bridge* = Brücke

⁵ englisch: *promiscuous mode* = freizügiger Modus

9.4.3 Schleifenbildung durch Bridging

- 1 **Alle Bridges:**
Einschalten (Power-On)
- 2 **Alle Bridges:**
Ports → „Blocking“
- 3 **Alle Bridges:**
senden „BPDU“^as
- 4 **LAN:**
Bestimmung der Root-Bridge
- 5 **Root-Bridge:**
sendet Konfigurations-BPDUs
- 6 **Alle Bridges:**
bestimmen Root-Port
- 7 **LAN:**
bestimmt Designated-Ports

^aenglisch: **BPDU** = Bridge Protocol Data Unit

Abb. 9.8: Spanning Tree Protocol (STP)

Mehrere redundante Pfade zwischen LAN-Segmenten haben einen schwerwiegenden Nachteil: Innerhalb dieses zusammenschlossenen LAN können Rahmen kreisen und sich vermehren.

Beim Start sind die Tabellen aller Bridges leer. Sendet ein Host einen Rahmen, dann erzeugt die verbundenen Bridges eine Kopie und sendet diese auf den anderen Interfaces zu den benachbarten Bridges.

Der **Spanning-Tree-Algorithmus** stellt sicher, dass zwischen zwei Rechnern nur ein Datenpfad existiert und verhindert dadurch unerwünscht kreisende Pakete.

Definition 9.1



Spanning Tree

In jeder Bridge sind 5 Zustände der Ports definiert:

Status	Typ	Verarbeitet	Weiterleitung von		Lernen von	
LED	Name	BDUs	BDUs	Frames	MAC-Adr.	
●	Blocking	Stable	ja	nein	nein	nein
●	Listening	Transitional	ja	ja	nein	nein
●	Learning	Transitional	ja	ja	nein	ja
●	Forwarding	Stable	ja	ja	ja	ja
○	Disabled	Stable	nein	nein	nein	nein

Tab. 9.2: Port Zustände eines Switches

Abb. 9.9: Schleifenbildung durch Bridging

Der Zielhost muss zuerst einen Rahmen erzeugen, damit seine Adresse in den Bridge-Tabellen aufscheint. Da dieser Zielhost unbekannt ist, wiederholt sich diese Vorgangsweise für jede beteiligte Bridge.

Dieses Multiplizieren von Kopien kann sich unendlich fortsetzen und die Anzahl der Kopien wächst exponentiell und kann das gesamte Netzwerk zum Absturz bringen (Broadcast-Stürme).

MAC-Bridges nutzt man, um die Last in großen Netzen zu mindern, denn jeder Strang erhält nur die Pakete, die für ihn bestimmt sind.

Definition 9.2

Mit **LLC-Bridges** verbindet man Teilnetze mit unterschiedlichen Zugriffsverfahren.

Definition 9.3

In einer **LLC-Bridge** werden die Parameter zwischen den Netzwerksträngen angepasst und übersetzt.

9.4.4 Spanning-Tree

Der Spanning-Tree Algorithmus⁶ identifiziert Mehrfachwege, indem er Topologien mit redundanten Wegen durch eine logische Blockierung bestimmter Pfade in eine Baumtopologie ohne Schleifen überführt.

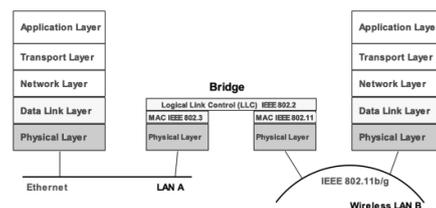


Abb. 9.10: Übersetzende Bridges

⁶entworfen von Radia Perlman und 1990 als IEEE 802.1D standardisiert

⁷englisch: **LLC** = Logical Link Control

9.5 Switches

Abb. 9.11: Source Address Table (SAT) von Switches

Switch (**switch**⁸) oder Multiport-Bridge bezeichnet ein Kopplungselement das Netzwerksegmente miteinander verbinden und dafür sorgt dass die Datenpakete an ihr Ziel kommen.

Definition 9.1

Es gibt in der Fachliteratur keine eindeutige Differenzierung zwischen Bridges und Switches.

Switches arbeiten als transparente Bridges, haben jedoch eine höhere Durchsatzleistung und mehr Ports. Switches wurden viel später entwickelt als Bridges.

9.5.1 Port-Tabellen von Switches

Einfache Switches arbeiten ausschließlich auf der Schicht 2 (Sicherheitsschicht) des OSI-Modells.

Beim Erhalt eines Frames legt ein Switch einen Eintrag in die **Source-Address-Table (SAT)** von der 48 Bit langen MAC-Adresse und des physischen Ports, an dem dieser empfangen wurde, an.

Definition 9.2

Im Unterschied zum Hub werden Frames anschließend nur noch an den Port weitergeleitet, der für die entsprechende Zieladresse in der SAT gelistet ist.

Ist der Weg zur Zieladresse unbekannt (Lernphase), leitet der Switch den Frame an alle anderen aktiven Ports.

9.5.2 Arbeitsweise von Switches

Ein Paket kommt beim Switch auf der Eingangsleitung an und verlässt ihn über **eine** Ausgangsleitung.

Store and Forward Switching

Ist die sicherste, aber auch langsamste Switching-Methode mit der größten Latenzzeit.

Bei **Store and Forward**⁹ empfängt und speichert der Switch zunächst das ganze Frame, berechnet die Prüfsumme und trifft dann seine Weiterleitungsentscheidung anhand der Ziel-MAC-Adresse.

Definition 9.3

Ergeben sich bei der Berechnung der Prüfsumme Differenzen, wird der Frame verworfen.

Dadurch verbreiten sich keine fehlerhaften Frames im lokalen Netzwerk.



Switch

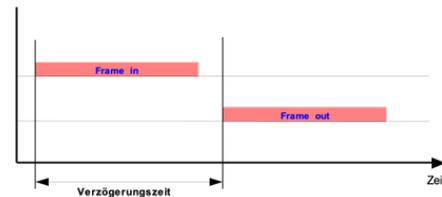


Abb. 9.12: Store and Forward Switching

Cut Through Switching

Eine sehr schnelle Methode, hauptsächlich von besseren Switches implementiert.

Bei **Cut Through**¹⁰ trifft der Switch beim Eintreffen des Frame direkt nach der Ziel-MAC-Adresse eine Weiterleitungsentscheidung und schickt der Frame weiter, während es noch empfangen wird.

Definition 9.4

Die Verzögerungszeit setzt sich wie folgt zusammen:

- Längen der Präambel (8 Byte)
- Längen der Ziel-MAC-Adresse (6 Byte)
- Reaktionszeit des Switches

Durch die frühestmögliche Weiterleitung kann der Frame aber nicht auf Fehlerfreiheit geprüft werden.

Damit leitet der Switch auch eventuell beschädigte Frames weiter.

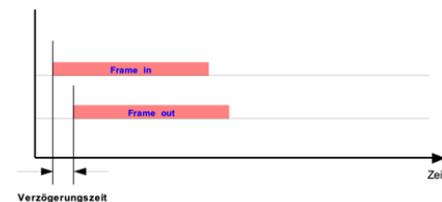


Abb. 9.13: Cut Through Switching



Store and Forward

⁸englisch: *switch* = Umschalter, Weiche

⁹englisch: *store and forward* = speichern und weiterreichen

¹⁰englisch: *store and forward* = speichern und weiterreichen

Adaptive Switching

Adaptive Switching bezeichnet die Kombination aus den Vorteilen der beiden Verfahren **Store and Forward** und **Cut Through**.

Definition 9.5

Ein adaptiver Switch ist ein Netzwerk-Switch, der normalerweise im Cut-Through-Modus arbeitet.

Wenn die Fehlerrate eines Ports jedoch zu hoch ansteigt, konfiguriert der Switch diesen Port automatisch so, dass er im Store-and-Forward-Modus läuft.

Dadurch wird die Leistung des Switches optimiert, indem bei niedrigen Fehlerraten eine schnellere Cut-Through-Schaltung, bei hohen Fehlerraten jedoch eine Store-and-Forward-Schaltung mit höherem Durchsatz ermöglicht wird, bei der fehlerhafte Frames nicht weiter geleitet sondern verworfen werden.

9.5.3 VLAN

Ein **Virtual Local Area Network (VLAN)** ist ein logisches Teilnetz innerhalb eines Switches bzw. gesamten physischen Netzes. Es kann sich über mehrere Switches hinweg ausdehnen.

Definition 9.6

Lokale Netze werden heute üblicherweise mit Hilfe von aktiven Komponenten (in der Regel Switches) aufgebaut (OSI-Schicht 2).

Die heute gängigen Switch-Implementierungen können die Anschlüsse üblicherweise im Vollduplex-Modus betreiben und kollisionsfrei arbeiten.

Damit können auch sehr große, aber dennoch performante LANs mit einigen hundert oder tausend Stationen aufgebaut werden.

Aufteilung in Teilnetze

Eine Unterteilung solcher Netze bietet grundsätzlich folgende Vorteile:

- **Flexibilität**
Zuordnung von Endgeräten zu Netzsegmenten, unabhängig vom Standort der Basisstation (logische Gruppen).
- **Performance**
z. B. Verkleinerung der Broadcast-Domänen (damit sich Broadcasts nicht über das gesamte Netz ausbreiten).
- **Sicherheit**
VLANs können Netze gegen Ausspionieren und Abhören besser absichern als Switch-basierte Netze.

Aufteilung in Organisationseinheiten

Ein VLAN trennt physische Netze in Teilnetze auf, indem es dafür sorgt, dass VLAN-fähige Switches Frames (Datenpakete) nicht in ein anderes VLAN weiterleiten (obwohl die Teilnetze an gemeinsamen Switches angeschlossen sein können).

Für nachfolgende Grafik gilt für die Organisationseinheiten folgende farbliche Zuordnung:

- **rot**: Marketing (M)
- **grün**: Produktion (P)
- **blau**: Forschung und Entwicklung (F&E)

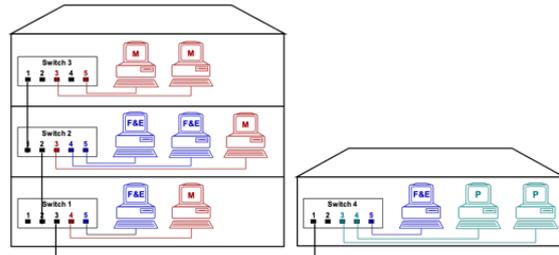


Abb. 9.14: VLAN auf Basis von Organisationseinheiten



VLAN

Im Beispiel in Abb. 9.14 sind Computer der „F&E“-Abteilung (blau) an verschiedene Switches in verschiedenen Stockwerken und sogar verschiedenen Gebäuden angeschlossen.

Wenn alle „blauen“ Switch-Ports in ein eigenes VLAN konfiguriert werden, können auf Layer 2 nur alle „blauen“ Geräte miteinander kommunizieren.

Ein **Broadcast-Frame** von einem der blauen Geräte wird auch nur von allen Ports verschickt, die in dieses VLAN konfiguriert sind.

Wird ein Frame, der von einem bestimmten VLAN Port kommt, zu einem anderen Switch weitergeleitet (schwarze Ports und schwarze Leitungen), muss der erste Switch vor dem Weiterleiten ein **VLAN Tag** (eine Info, zu welcher VLAN-Nummer der Frame gehört) einfügen, damit der nächste Switch weiß, an welche Ports (=an welches VLAN) dieser Frame weitergeleitet werden darf.

VLAN Tags dürfen nur auf den Verbindungen zwischen Switches (**Trunk Links** genannt) verwendet werden, vor der Zustellung an ein Endgerät muss das **VLAN Tag** wieder entfernt werden.

Meist wird bei der VLAN-Konfiguration der weltweit verbreitete IEEE 802.1Q Standard für die **VLAN Tags** verwendet, der von vielen Switch-Herstellern unterstützt wird.

9.6 Router

Abb. 9.15: Routing Tabellen (Next Hop)

Router (**router**¹¹) sind Netzwerkgeräte, die Datenpakete zwischen mehreren Rechnernetzen weiterleiten können.

Definition 9.1

Router treffen ihre Weiterleitungsentscheidung anhand von Informationen aus der Netzwerk-Schicht 3 (IP-Adresse).

Dazu bedienen sie sich einer lokal vorhandenen Routingtabelle, die angibt, welches Netz

- über welchen Anschluss des Routers (Netzwerkinterface <Netz-ID,Host-ID>)
- lokal oder über entfernten Router (lokal oder Next Hop)

erreichbar ist.

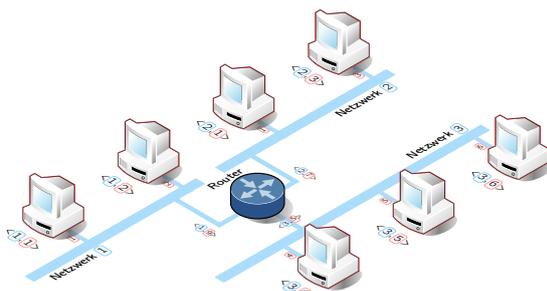


Abb. 9.16: Netzwerke mit Router

9.6.1 Routing-Tabellen

Eine **Routingtabelle** enthält zu jedem potentiellen Ziel eine Angabe, über welchen Port das Datenpaket den Router wieder verlassen muß.

Definition 9.2

Da die Routingtabelle jeweils nur Angaben über die nächste Station eines Datenpakets auf seinem Weg enthält, wird sie auch als Next-Hop-Tabelle bezeichnet.

Die hierarchische Adressierung (Netz-ID,Host-ID) erweist sich für die Routing-Tabelle als sehr vorteilhaft: Alle Datenpakete, die an ein bestimmtes Subnetz gerichtet sind, verlassen den Router über denselben Port.



Router

Falls das Ziel sich nicht im selben Subnetz befindet wie der Router, muß für eine korrekte Weiterleitung nur der erste Teil der Zieladresse überprüft werden.

Routing-Tabellen (Default)

Ersetzt man eine Reihe von Einträgen mit identischen Next-Hop-Wert durch einen einzelnen Eintrag (Vorgabe Routing), erhält man die **Default-Routing-Tabelle**.

Definition 9.3

Durch Default-Routing läßt sich die Routingtabelle entsprechend verkleinern und damit der Berechnungsaufwand zur Weiterleitung der Datenpakete deutlich verringert.

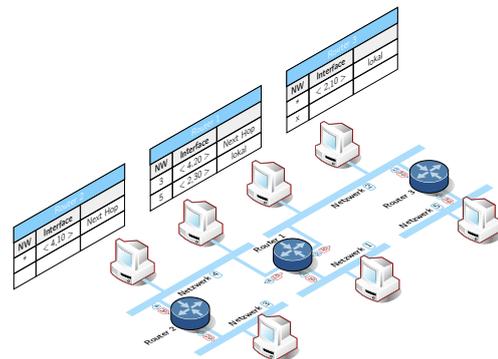


Abb. 9.17: Routing Tabellen mit Default Routen

Wird in der Routingtabelle für ein bestimmtes Ziel kein expliziter Eintrag gefunden, wird das Datenpaket an die im Vorgaberouting festgelegte Route (Default Route) weitergeleitet.

¹¹englisch: **routing** = Steuerung, Festlegen der Route

9.6.2 Routing-Algorithmen

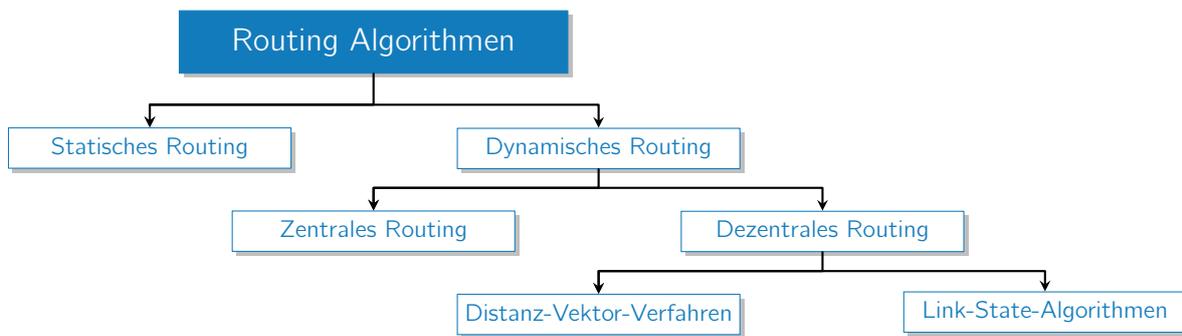


Abb. 9.18: Einteilung der Routing-Algorithmen

Routingmetrik

Die **Routingmetrik (Metrik)** oder auch **Kosten**, ist ein numerisches Maß für die Güte einer bestimmten Route einer Verbindung.

Definition 9.1

Die Metrik kann durch Bewertung oder durch Messung bestimmt sein.

Statische Routing-Algorithmen

Beim **statischen Routing** wird die Routingtabelle einmal bei der Inbetriebnahme des Routers erstellt und danach nicht mehr verändert.

Definition 9.2

Statische Routing ist ein sehr einfaches Verfahren und erfordert nur geringen Berechnungsoverhead.

Dynamische Routing-Algorithmen

Beim **Dynamischen Routing** passt sich die Routingtabelle an veränderte Strukturen im Netz an und wird bei Bedarf aktualisiert.

Definition 9.3

Netzverkehr sowie der Zustand der Netzwerkhardware werden permanent überwacht. Netzwerkprobleme können automatisch behoben und Routen entsprechend umgeleitet werden.

Zentrale Routing-Algorithmen

Beim **Zentralem Routing** berechnet die Routingtabelle eine **zentrale Instanz**, die über den Zustand des Netzes informiert ist und Routingentscheidungen treffen kann.

Definition 9.4

Nachteile des Zentralen Routings [2, S 394]:

- **Lange Reaktionszeiten** bei Veränderungen der Netzwerkstruktur
- **Ausfall des Rechners** gefährdet Netzwerkbetrieb
- **Verminderung der Übertragungsleistung** bei Unterdimensionierung

Aufgrund dieser Nachteile werden in der Praxis meist dezentrale, verteilte Routingverfahren verwendet.

Dezentrale Routing-Algorithmen

Beim **Dezentralen Routing** berechnet jeder Router seine Routingtabelle lokal und versendet dann Routinginformation an benachbarte Router.

Definition 9.5



Metrik

Der Router versendet die Routinginformation periodisch, so daß nach einer kurzen Anlaufzeit jeder Router die besten Wege zu allen Zielen erfaßt hat.

Fällt eine Netzwerkverbindung aus, erhält ein Router über diese Verbindung keine weiteren Updates.

Existiert eine Ausweichroute, wird die Routingtabelle angepasst um ausgefallene Netzhardware zu umgehen.

Distance Vector Routing (DV)

Beim **Distanz-Vektor-Routing**¹² (**DVR**¹³) wird für jeden Router in der Tabelle als Kostenmaß (Metrik) die Distanz¹⁴ zum Router verwendet.

Definition 9.6

Abb. 9.19: Routenwahl durch Hopminimierung

Ein Distanzvektor-Protokoll war das erste Routingverfahren, das im ARPANET zum Einsatz kam.

Es wurde im Internet als Routing Information Protocol (RIP) in RFC 1058 (RIPv2 in RFC 1723) standardisiert.

¹²oftmals auch als Bellman-Ford- oder Ford-Fulkerson-Algorithmus bezeichnet, nach Wissenschaftlern die dieses Verfahren entwickelt haben.

¹³englisch: *distance vector routing* = abgekürzt DVR

¹⁴die Anzahl der notwendigen Hops, die Warteschlangenlänge oder die Übertragungszeit

Ein **Hop** bezeichnet jeweils eine Teilstrecke zwischen zwei benachbarten Routern.

Definition 9.7

Wird die Anzahl der benötigten Hops als Metrik gewählt, dann beträgt der Abstand zu den jeweiligen Nachbarn trivialerweise einen Hop.

Link State Routing (DV)

Da das Distanzvektor-Routingverfahren die Bandbreiten nicht berücksichtigt wurde es durch das Link-State-Routing ersetzt, welches die Bandbreiten der Verbindungen (durch Gewichtung) berücksichtigt und damit effizientere Routingergebnisse liefert.

Beim **Link-Status-Routing (LSR¹⁵)** wird in jedem Router eine interne Topologie-Datenbank mit aktueller Netzwerk-Informationen (Netzwerkgraph, „Landkarte“) verwaltet.

Definition 9.8

Abb. 9.20: Routenwahl durch Kostenminimierung

Statt einer kompletten Routingtabelle beinhalten die zwischen den Routern ausgetauschte Nachrichten nur den Status einer bestimmten Verbindung.

- **Nachrichtenaustausch**
Nachrichten werden über einen Broadcast an alle Router des Netzwerks geschickt.
- **Jeder Router**
des Netzwerks erhält eine vollständige das gesamte Netzwerk betreffende Statusinformation.
- **Jeder Knoten**
kann mit Hilfe dieser Information einen eigenen Netzwerkgraphen (Landkarte) erstellen und seine Routingtabelle selbst berechnen.
- **Optimale Route**
Berechnung des kürzesten Pfades (z. B. durch den Dijkstra Algorithmus).

Das Link-State-Routingverfahren kann auf Änderungen in der Topologie und der Auslastung des Netzes viel schneller als das Link-State-Routing reagieren, da alle Knoten hier gleichzeitig über eine Statusänderung informiert werden.

¹⁵englisch: LSR = link state routing

9.6.3 Routing-Protokolle

Autonomes System

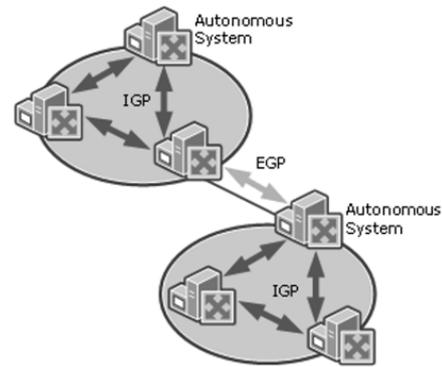


Abb. 9.21: Autonomes System

Ein **autonomes System (AS)** ist eine Menge von Routern mit einem gemeinsamen inneren Gateway-Protokoll (IGP), unter einer einzigen technischen Verwaltung (Administration).

Definition 9.9



AS

Autonome Systeme sind untereinander verbunden und bilden so das Internet.

Interne Routingprotokolle

Als **IGP¹⁶** werden Routingprotokolle bezeichnet, die innerhalb von autonomen Systemen eingesetzt werden (Intradomain-Routing).

Definition 9.10



IGP

Im Gegensatz zu Exterior-Gateway-Protokollen (EGP) zeichnen sie sich durch besondere Fähigkeiten im Umgang mit komplizierten Netzwerktopologien aus.

Exterior Gateway Protocols (EGPs)

Ein **EGP¹⁷** dient dazu, Erreichbarkeitsinformationen zwischen autonomen Systemen (AS) auszutauschen, d.h. Informationen darüber, welche Netze erreichbar sind.

Definition 9.11



EGP

Die Router der autonomen Systeme setzen diese Daten dann in interne Routing-Informationen für Intradomain-Routingprotokolle wie **OSPF¹⁸** oder **RIP¹⁹** um.

Ein EGP hat drei wesentliche Funktionen:

- **Nachbarn festlegen:**
Zwei Router aus zwei verschiedenen AS verständigen sich miteinander, ob sie EGP-Partner werden wollen.
- **Erreichbarkeit der Nachbarn:**
In bestimmten Zeitintervallen wird überprüft, ob die EGP-Partner noch erreichbar sind.
- **Hauptaufgabe: Erreichbarkeit von Netzwerken:**
EGP-Partner erhalten auf Anfrage eine Liste von erreichbaren Netzwerken in den autonomen Systemen der Nachbarn.

¹⁶englisch: IGP = Interior Gateway Protocol

¹⁷englisch: EGP = Exterior-Gateway-Protokoll

¹⁸englisch: OSPF = Open Shortest Path First

¹⁹englisch: RIP = Routing Information Protocol

9.7 Firewalls

Eine **Firewall** (**firewall**²⁰) ist ein Sicherungssystem, das ein Rechnernetz oder einzelne Computer vor unerwünschten NW-Zugriffen schützt.

Definition 9.12

Es wird zwischen Personal Firewall und externen Firewall unterschieden. Man unterscheidet prinzipiell zwischen folgenden Varianten:

- **Personal Firewall** (Desktop Firewall)
bezeichnet eine lokal auf dem Computer installierte Firewall-Software.
- **Externe Firewall** (Netzwerk-Firewall)
arbeitet auf einem separaten Gerät, das Netzwerke oder Netzsegmente miteinander verbindet.



Firewall

²⁰englisch: *firewall* = Brandmauer

10

Internetdienste

Inhaltsangabe

10.1 Electronic Mail Service	64
10.1.1 Email	64
10.1.2 Basisfunktionen	64

10.1 Electronic Mail Service

Der älteste und populärste Dienst im Internet ist die elektronische Post, der sogenannte Electronic Mail Service (Email). Die ersten Email-Systeme existierten bereits kurz nach dem Start des ARPANET.

Abb. 10.1: Funktionsweise eines Email-System

10.1.1 Email

Als **E-Mail**¹ wird ein **computerbasiertes System** zur Verwaltung/Übertragung von Nachrichten, sehr oft auch die **Nachricht** selbst, bezeichnet.

Definition 10.1

Bei der Veröffentlichung der ersten Protokolle für E-Mail 1982, hat sich ein nicht-kommerzieller Vorschlag von Informatik-Studenten gegen einen von der **ITU-T**² durchgesetzt. „Email“ ist eine Nachbildung der Briefpost auf Basis moderner, digitaler Kommunikationsmittel.

Für gewöhnlich laufen MTAs als Prozesse im Hintergrund die der Anwender gar nicht aktiv wahrnimmt.



E-Mail

Abb. 10.2: Analogie Brief zu Email

Der Email-Dienst als Message Handling Systeme (MHS) besitzt zwei grundlegende Komponenten:

User Agents (UA)

Als **User Agents (UA)** werden Systeme bezeichnet, mit denen der Anwender in der Lage ist, Nachrichten zu erzeugen, editieren, lesen, senden und empfangen.

Definition 10.2

UAs sind lokale Anwendungsprogramme, die dem Nutzer eine Schnittstelle zur Benutzung des Nachrichtendienstes zur Verfügung stellen.

Message Transfer Agents (MTA)

Die **Message Transfer Agents (MTA)** sind für den Transport der Nachrichten vom Sender zum Empfänger verantwortlich.

Definition 10.3

Abb. 10.3: Funktionsweise eines Email-System

10.1.2 Basisfunktionen

Ein Email-System hat fünf Basisfunktionen zu erfüllen:

- 1. Erzeugen einer Nachricht**
Erstellen des Nachrichteninhalts und der notwendigen Header-Elemente der Nachricht mit Hilfe eines Texteditors (Mailclient).
- 2. Zustellen einer Nachricht**
Verbindungsaufbau/Zustellung, zum Zwischensystem oder direkt zum Empfänger, erfolgt im Hintergrund ohne direkte Beteiligung des Anwenders.
- 3. Statusmeldung der Zustellung**
Statusmeldung an Sender ob Nachricht erfolgreich zugestellt wurde oder an welchen Gründen die Zustellung gescheitert ist.
- 4. Darstellung einer Nachricht**
Aktuelle E-Mail-Programme kodieren Text/Dateianhänge automatisch. Abweichungen vom Standard³ müssen im Header deklariert werden⁴.
- 5. Ablegen einer Nachricht**
Nach erfolgreicher Zustellung wird die Nachricht weiter verarbeitet (Löschen, Speichern, etc.).

¹englisch: *E-Mail* = **electronic mail**, „elektronische Post“

²englisch: *ITU-T* = **ITU Telecommunication Standardization Sector**

³RFC 5322: Verwendung des 7-Bit-ASCII-Zeichensatzes

⁴RFC 2045: als Erweiterung von RFC 5322, MIME und Base64

Anhang

11

Personenregister

Inhaltsangabe

11.1 Pioniere des Internet	66
11.1.1 Vannevar Bush	66
11.1.2 J. C. R. Licklider	66
11.1.3 Charles Herzfeld	67
11.1.4 Paul Baran	67
11.1.5 Theodor Holm Nelson	67
11.1.6 Leonard Kleinrock	67
11.1.7 Lawrence Roberts	68
11.1.8 Steve Crocker	68
11.1.9 Jon Postel	68
11.1.10 Vinton G. Cerf	68
11.1.11 Robert E. Kahn	69
11.1.12 Ray Tomlinson	69
11.1.13 Robert Metcalfe	69

11.1 Pioniere des Internet

11.1.1 Vannevar Bush



Quelle: [19]

Abb. 11.1: Vannevar Bush



V. Bush

Vannevar Bush (1890-1974) war ein US-amerikanischer Ingenieur und Analogrechner-Pionier.

Bush entwickelte in seinem 1945 publizierten Essay *As We May Think* das Konzept des Memex (Memory Extender), der als ein Vorläufer des Personal Computers und des Hypertextes gilt.

Bush zählt zu den Begründern der Kooperation zwischen Militär, Universitäten und privater Unternehmer.

„Kein Amerikaner hat größeren Einfluss auf die Entwicklung von Wissenschaft und Technologie gehabt als Vannevar Bush. [7]“

(Jerome Wiesner, Präsident MIT)

Zitat 11.1

11.1.2 J. C. R. Licklider



Quelle: [9]

Abb. 11.2: J. C. R. Licklider



Licklider

Joseph Carl Robnett Licklider (1915-1990), besser bekannt als J.C.R. Licklider oder unter seinem Spitznamen „Lick“, war ein amerikanischer Psychologie-Professor.

Er prägte die Frühzeit der amerikanischen Informatik, indem er in leitenden Positionen neue Richtungen bei der Hardware- und Software-Entwicklung aufzeigte.

Er gilt als Gründerfigur der Künstlichen Intelligenz, moderner Interaktions-Konzepte für Computer sowie des Time-Sharings und des Internets.

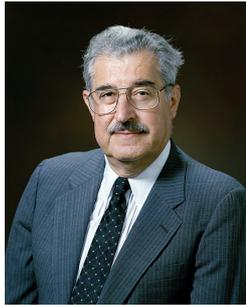
„Als Medium für die Darstellung von Informationen ist die gedruckte Seite unübertroffen. Sie bietet genügend Auflösung, um dem Auge Genüge zu tun. Sie präsentiert genügend Informationen, um den Leser für eine angenehme Zeitspanne zu beschäftigen. Sie bietet hohe Flexibilität in Bezug auf Schriftart und Formatierung. Sie lässt den Leser Art und Geschwindigkeit der Betrachtung selbst bestimmen. Sie ist klein, leicht, beweglich, replizierbar, entsorgbar und kostengünstig, lässt sich schneiden, heften und kleben. [3, S. 4]“
 (J. C. R. Licklider)

Zitat 11.2

„Das Internet ist das Werk von Tausenden von Menschen. Es wird in den nächsten Jahren von Hunderten neuer Ideen fortentwickelt. Es ist wie eine Kathedrale. Irgendwann kommt ein Historiker und fragt, wer denn die Kathedrale gebaut hat. Wenn man nicht aufpasst und die Arbeit der anderen nicht achtet, kann man sich selbst täuschen und glauben, der Erbauer zu sein“
 (Paul Baran, 2001)

Zitat 11.3

11.1.3 Charles Herzfeld



Quelle: [8]

Abb. 11.3: Charles Maria Herzfeld



Herzfeld

Charles Maria Herzfeld (1925-2017) war ein österreichisch-amerikanischer Wissenschaftler und Manager.

Als Direktor der Defense Advanced Research Projects Agency (DARPA) startete er die Entwicklung des Arpanets, Vorläufer des Internets.

11.1.4 Paul Baran



Quelle: [13]

Abb. 11.4: Paul Baran



Paul Baran

Paul Baran (1926-2011) war ein US-amerikanischer Informatiker polnischer Abstammung.

Seine 1964 veröffentlichte elfteilige Arbeit On Distributed Communication gilt als einer der Grundsteine zur Entwicklung des Internets.

Darin präsentierte Baran erstmals die Idee, Informationen durch so genannte Paketvermittlung in einem Netzwerk mit hochgradig vernetzten Knoten zu übertragen.

11.1.5 Theodor Holm Nelson



Quelle: [18]

Abb. 11.5: Theodor Holm Nelson



Nelson

Theodor „Ted“ Holm Nelson (* 1937 in Chicago) ist ein US-amerikanischer Philosoph und Informationstechniker.

Nelson prägte 1965 die Begriffe Hypertext und Hypermedia. Seine Devise ist:

„Eine Benutzeroberfläche sollte so einfach sein, dass ein Anfänger sie in einem Notfall innerhalb von zehn Sekunden verstehen kann.“
 (Theodor Holm Nelson)

Zitat 11.4

11.1.6 Leonard Kleinrock



Quelle: [12]

Abb. 11.6: Leonard Kleinrock



Kleinrock

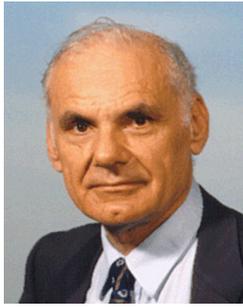
Leonard Kleinrock (* 13. Juni 1934 in New York City) ist ein US-amerikanischer Elektroingenieur und Informatiker, der fundamentale Beiträge zur Theorie von Computernetzwerken und des Internets leistete.

Er leistete sowohl Beiträge zur mathematischen Theorie von Computer-Netzwerken als auch die Spezifikation der Paketvermittlung (Packet Switching), der Grundlage der Internet Technologie.

Sein Beitrag dazu geht bis auf seine Dissertation von 1962 zurück. Er wandte diese Ideen in der Entwicklung des ARPANET an, dessen erste Knoten in Form von Interface Message Processors (IMP) 1969 bei Kleinrock

an der UCLA und Douglas Engelbart bei SRI International waren.

11.1.7 Lawrence Roberts



Quelle: [11]

Abb. 11.7: Lawrence Roberts

Lawrence „Larry“ Gilman Roberts (1937-2018) war ein US-amerikanischer Elektrotechniker und Informatiker, der fundamentale Beiträge zur Theorie von Computer-Netzwerken und des Internets leistete.

Während seiner Zeit als Programmleiter und Büroleiter der Advanced Research Project Agency entwickelte Roberts mit seinem Team die Paketvermittlung und das ARPANET, einen Vorgänger des heutigen Internets.

11.1.8 Steve Crocker



Quelle: [17]

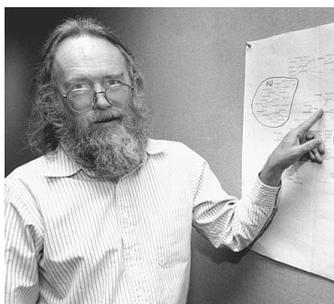
Abb. 11.8: Steve Crocker

Stephen David Crocker (* 15. Oktober 1944 in Pasadena (Kalifornien)) ist ein US-amerikanischer Informatiker und Internetpionier.

Ende der 1960er Jahre arbeitete er – unter anderem mit Vinton Cerf und Jon Postel – in dem Forscherteam, das die Netzwerkprotokolle für das Arpanet entwickelte, den Vorläufer des Internets.

Crocker schrieb den ersten RFC – worin in der Folge die Internetstandards definiert wurden –, der am 7. April 1969 veröffentlicht wurde.

11.1.9 Jon Postel



Quelle: [10]

Abb. 11.9: Jon Postel

Jonathan „Jon“ Bruce Postel (1943-1998) war ein US-amerikanischer Informatiker und Wegbereiter des Internets.

Postel war fast dreißig Jahre als Herausgeber der Requests for Comments (RFC) tätig.

Während dieser Zeit verfasste er selbst über 200 RFC, unter anderem so grundlegende wie RFC 791 bis RFC 793 (IP, ICMP und TCP) und RFC 2223 (Instructions to RFC Authors).

Sein vielleicht bekanntestes Vermächtnis stammt aus RFC 793, welches das Robustheitsprinzip enthält und oft als Postels Gesetz bezeichnet wird: „be conservative in what you do, be liberal in what you accept from others“ („sei konservativ in dem, was Du tust, sei tolerant in dem, was Du von anderen akzeptierst“, oft formuliert als „sei konservativ in dem, was Du sendest, sei tolerant in dem, was Du empfängst“).

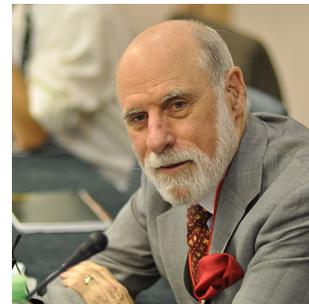
„Sei konservativ in dem, was Du tust, sei tolerant in dem, was Du von anderen akzeptierst“
(Theodor Holm Nelson, RFC 793)

Zitat 11.5

Postel war Gründungsmitglied des Internet Architecture Board (IAB), erstes Einzelmitglied der Internet Society und Teil dessen Board of Trustees.

Ebenso initiierte er die Internet Assigned Numbers Authority (IANA) und stand ihr von Beginn an bis zu seinem Tode als Direktor vor.

11.1.10 Vinton G. Cerf



Quelle: [20]

Abb. 11.10: Vinton G. Cerf

Vinton Gray „Vint“ Cerf (* 23. Juni 1943 in New Haven, Connecticut) ist ein US-amerikanischer Informatiker, der zusammen mit anderen als „Vater des Internets“ bezeichnet wird. 2004 wurde ihm der Turing-Preis verliehen, 2008 der Japan-Preis, 2023 die IEEE Medal of Honor.

Cerf spielte eine Schlüsselrolle in der Entwicklung des Internets und der im Internet verwendeten Verbindungsprotokolle.

Cerf und Crocker wurden über Leonard Kleinrocks Network Measurement Center in die Installation des schließlich von Bolt Beranek and Newman unter Führung von Bob Kahn realisierten Arpanets eingebunden, und waren unter Aufsicht von Lawrence Roberts an der Spezifikation der Arpanet-Host-Protokolle beteiligt.

Als Assistenzprofessor für Elektrotechnik und Informatik in Stanford, unterstützte die Gruppe um Kahn bei der

Koordination zur öffentlichen Demonstration des Arpanets und entwickelte im Anschluss an diese mit seinen Studenten und Kahn das Transmission Control Protocol (TCP) und das Internet Protocol (IP).

Im September 1973 präsentierten sie eine erste Version von **TCP/IP**, die im Mai 1974 auch veröffentlicht wurde. In seiner Zeit in Stanford leitete Cerf auch die International Network Working Group, die später in die IFIP aufging.

11.1.11 Robert E. Kahn



Quelle: [15]

Abb. 11.11: Robert E. Kahn



Kahn

Robert „Bob“ Elliot Kahn (* 23. Dezember 1938 in New York City) ist ein US-amerikanischer Informatiker, der zusammen mit anderen als „Vater des Internets“ bezeichnet wird.

Er hat zusammen mit Vint Cerf das Transmission Control Protocol (TCP) und das Internet Protocol (IP) entwickelt.

Kahn war zuständig für das Systemdesign des Arpanets. Darüber hinaus war er der Kommunikationstheoretiker beim Design des Interface Message Processors.

1972 holte ihn Arpanet-Projektleiter Lawrence „Larry“ Roberts zur nun DARPA (Defense Advanced Research Projects Agency) umbenannten ARPA.

Im Oktober desselben Jahres präsentierte er auf der International Computer Communication Conference (ICCC) das Arpanet mit 40 verbundenen Computern der Öffentlichkeit.

Als er bei DARPA an Projekten zur paketvermittelten Datenübertragung per Satellit und per Funk arbeitete, kam er auf grundlegende Ideen für das Transmission Control Protocol.

Er erkannte auch die Notwendigkeit offener Netzwerkarchitekturen, damit unterschiedliche Netzwerke - unabhängig von der eingesetzten Hard- und Software - miteinander zu kommunizieren können.

Ab Frühling 1973 unterstützte ihn Vinton G. Cerf bei dem Projekt TCP. Bei der Entwicklung diente ihnen das ohne Mitwirkung Kahns für das ursprüngliche Arpanet entworfene Network Control Program (NCP) als Grundlage.

Im September 1973 präsentierten sie eine erste Version, die im Mai 1974 auch veröffentlicht wurde, und die bereits zwischen TCP und IP unterschied.

Als Cerf 1976 zur DARPA kam, übernahm dieser von Kahn bis 1982 die Führungsrolle im Internet-Projekt und leitete die Weiterentwicklung von TCP.

1980 wurde **TCP/IP** vom amerikanischen Verteidigungsministerium als Standard anerkannt, und am 1. Januar 1983 wurde das Arpanets (nun Internet) auf **TCP/IP** umgeschaltet.

11.1.12 Ray Tomlinson



Quelle: [14]

Abb. 11.12: Ray Tomlinson



Tomlinson

Raymond Samuel „Ray“ Tomlinson (1941-2016) war ein US-amerikanischer Informatiker.

Er gilt als Erfinder der E-Mail. Mit dem Anti-Computerwurm Reaper entwickelte er auch das erste bekannte Programm gegen Malware.

Während Tomlinson sein E-Mail-Nachrichtensystem entwickelte, wurde der heutige Nutzen von niemandem erkannt, seine Arbeit wurde eher als Spielerei gesehen. Als Tomlinson sein System einem Kollegen demonstrierte, bemerkte dieser scherzhaft:

„Sag das niemandem! Das ist nicht das, woran wir arbeiten sollen.“

(Ray Tomlinson)

Zitat 11.6

1971 präsentierte Tomlinson seinen Mitarbeitern das Programm und versandte die erste E-Mail. Deren genauer Inhalt ist unbekannt; Tomlinson konnte sich nur noch daran erinnern, dass er darin unter anderem die Verwendung des @-Symbols erklärte.

11.1.13 Robert Metcalfe



Quelle: [16]

Abb. 11.13: Robert Metcalfe

Robert Melancton Metcalfe (* 7. April 1946 in Brooklyn, New York) ist ein US-amerikanischer Elektroingenieur und gilt als der Erfinder des Ethernet.



Metcalfe

Literatur

- [1] Wikimedia Commons. Hypertext — Wikimedia Commons, the free media repository. Online; Stand 24. Oktober 2023. 2023. URL: <https://commons.wikimedia.org/w/index.php?title=File:HypertextEditingSystemConsoleBrownUniv1969.jpg&oldid=775858578>.
- [2] James F. Kurose und Keith W. Ross. Computernetzwerke. Ein Top-Down Ansatz mit Schwerpunkt Internet. Addison-Wesley, 2002.
- [3] J. C. R. Licklider. Libraries of the Future. A Biographical Memoir. National Academy of Sciences, Washington D.C., 1979.
- [4] Harald Meinel Christoph und Sack. WWW. Kommunikation, Internetworking, Web-Technologien. Springer-Verlag Berlin Heidelberg, 2004.
- [5] ServiceNet. Der Unterschied: Singlemode und Multimode LWL-Kabel. Online; Stand 24. Oktober 2023. 2023. URL: https://www.glasfaserkabel.de/Der-Unterschied-zwischen-Singlemode-und-Multimode-LWL-Kabeln:_:13.html.
- [6] Tripp-Lite. Shielded vs Unshielded Cable Explained. Online; Stand 24. Oktober 2023. 2019. URL: <https://blog.triplite.com/what-is-the-difference-between-shielded-and-unshielded-network-cables>.
- [7] Jerome B. Wiesner. Vannevar Bush 1890—1974. A Biographical Memoir. National Academy of Sciences, Washington D.C., 1979.
- [8] Wikipedia. Charles Herzfeld — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2022. URL: https://de.wikipedia.org/w/index.php?title=Charles_Herzfeld&oldid=221017511.
- [9] Wikipedia. J. C. R. Licklider — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2022. URL: https://de.wikipedia.org/w/index.php?title=J._C._R._Licklider&oldid=229344085.
- [10] Wikipedia. Jon Postel — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Jon_Postel&oldid=237958585.
- [11] Wikipedia. Lawrence Roberts (Ingenieur) — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: [https://de.wikipedia.org/w/index.php?title=Lawrence_Roberts_\(Ingenieur\)&oldid=231151221](https://de.wikipedia.org/w/index.php?title=Lawrence_Roberts_(Ingenieur)&oldid=231151221).
- [12] Wikipedia. Leonard Kleinrock — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Leonard_Kleinrock&oldid=234013736.
- [13] Wikipedia. Paul Baran — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Paul_Baran&oldid=233434034.
- [14] Wikipedia. Ray Tomlinson — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Ray_Tomlinson&oldid=237468446.
- [15] Wikipedia. Robert E. Kahn — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Robert_E._Kahn&oldid=236257401.
- [16] Wikipedia. Robert Metcalfe — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Robert_Metcalfe&oldid=232075495.
- [17] Wikipedia. Steve Crocker — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Steve_Crocker&oldid=234749026.
- [18] Wikipedia. Theodor Holm Nelson — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2021. URL: https://de.wikipedia.org/w/index.php?title=Theodor_Holm_Nelson&oldid=213913128.
- [19] Wikipedia. Vannevar Bush — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Vannevar_Bush&oldid=237062613.
- [20] Wikipedia. Vinton G. Cerf — Wikipedia, die freie Enzyklopädie. Online; Stand 24. Oktober 2023. 2023. URL: https://de.wikipedia.org/w/index.php?title=Vinton_G._Cerf&oldid=236301718.