Nr. **152**/Februar 2017 € 5,00 ISSN 1022-1611

news

CLUBCOMPUTER · DIGITAL SOCIETY

CLUBSYSTEM

Smart-TV und AAL

Netzwerktechnik

Grundlagen
Datenübertragung
Kabelgebundene Übertragung
Netzwerk Hardware
Verkabelung
Strukturierte Verkabelung

CLUBMETA

Der kleine unendliche Urlaub

P.b.b. 16Z040679 M ClubComputer, Siccardsburggasse 4/1/22 1100 Wien

Bilder aus pixaby.com

Inhalt

Liebe Leserinnen und Leser!

Franz Fiala

Ich habe mir ein High-Speed-Modem gekauft. Der Beipacktext beschrieb eine Konfiguration, die nicht der Geräte-Einstellung entsprochen hat. Da war nix mit Plug-And-Play.

Man stelle sich einen typischen Enduser ohne weiter gehende Netzwerkkenntnisse vor. Für den ist hier Endstation. Er verflucht die Firma und bringt das Gerät zurück.

Aber schon mit den Inhalten der vorliegenden Ausgabe kann man sich in einem solchen Fall weiter helfen.

PCNEWS-152

Kenntnisse über Netzwerke sind heute ebenso wichtig wie solche über den PC. Und daher präsentiert Euch **Christian Zahler** in dieser und in den kommenden Ausgaben einen systematischen Einblick in die Netzwerktechnik am neuesten Stand der Technik.

Franz Fiala

Wir versenden in diesen Tagen Zahlscheine für den Mitgliedsbeitrag 2017.

Für unsere Clubabende suchen wir laufend Vortragende, die ihr Spezialgebiet einem interessierten Publikum vorstellen wollen.

Der kleine unendliche Urlaub

Gruppe Or-Om

bis Do. 31. 1. 2017
Täglich 10:00-18:00 **Quartier 21 MQ Wien**

Familie Kartern machte einen sehr kleinen Urlaub nach Karifulin und stellte ein Foto davon ins Netz. Dort steht es mit den Milliarden Urlaubsfotos, die bisher hochgeladen wurden.

Der Sohn Alfred meinte: *„Eine eher dürftige Performance!“*, begann das Bild zu permutieren und stellte mehrere Milliarden Ergebnisse auf FLICKR. Nach 2 Millionen Jahren war er mit seinem Projekt noch immer nicht am Ende. Er arbeitete nämlich auch EXTERNE Elemente in die Bilder ein. Jedem Bild gab er einen Namen: beginnend bei Karifulin, Farifulin, Sarifulin usw. Infolge der Vielzahl der Bilder musste er letztlich neuen Buchstaben, Laute und Erweiterungen der bestehenden Alphabete erfinden zum Beispiel

ƃŋğB#Ωee→

Mutter Kartern sagte eines Tages zu Alfred: *„Dein ausgreifender Versuch, ein Urlaubsfoto als Pixelfolge ins Unendliche fortzusetzen hat bestimmte Grenzen. Denn ein Sandkorn in Deinem ersten Bild, offenbart sich dem Blick des Allsehers als ein Universum aus Myriaden Atomsonnenreichen – als Kleinbild des Kosmos, in dem der Geist des Ganzen so gegenwärtig und wirksam ist wie in den Galaxien. Vielleicht solltest Du Dich einmal mit dem Verhältnis dieser Teil-Unendlichkeiten zur Absoluten Unendlichkeit beschäftigen.“*

Urlaubsbilder auf FLICKR
https://www.flickr.com/groups/kleinurlaub/

Theorie unter
http://or-om.org/urlaub.pdf

Website
http://or-om.org/

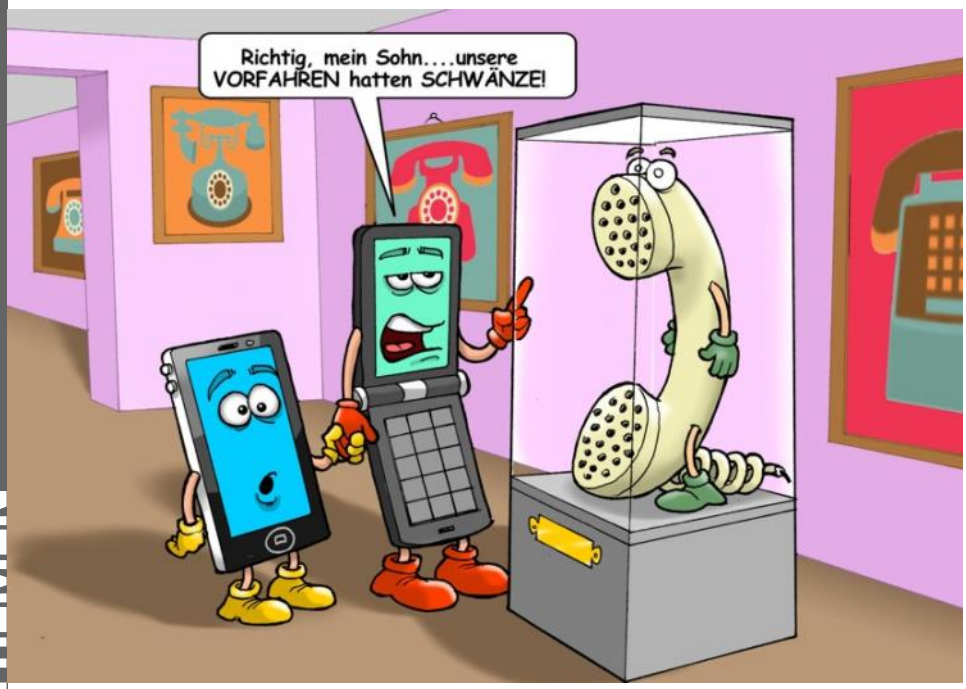
Projekte:
http://or-om.org/projectswebsite.pdf

Mail
or-om@chello.at

WIKI
https://marjorie-wiki.de/wiki/Gruppe_Or-Om

Quartier21 MQ Wien
http://www.quartier21.at/institutionen/

Evolution



Veranstaltungen von ClubComputer und Digital Society bis Ende 2017

	Feb	Mär	Apr	Mai	Jun	Jul	Aug	Sep	Okt	Nov	Dez
Meating	07.	07.	04.	02.		04.	01.	05.	03.	07.	05.
Digitalk	15.	15.	12.	17.				13.	11.	15.	
Meating	23.	23.	20.	18.				21.	19.	23.	
cccamp					24.						

Veranstaltungen bis März 2017

Di	**7.Feb Digitale Landkarten**
Mi	**15.Feb Digitalk**
Do	**23.Feb WordPress**
Di	**7.Mär Cookies**

Autoren

Berger Christian 2

Karikaturist und Comiczeichner für Kärntner Zeitungen

Firma Karicartoons

karicartoons@aon.at
http://www.karikaturen.guru/

Fiala Franz Dipl.-Ing. 1948 1, 2

Präsident von ClubComputer, Leitung der Redaktion und des Verlags der PCNEWS, Lehrer für Nachrichtentechnik und Elektronik .i.R.

Werdegang Arsenal-Research, TGM Elektronik

Absolvent TU-Wien, Nachrichtentechnik

franz.fiala@clubcomputer.at
http://www.fiala.cc/

Wöhrl Manfred, Prof. Dr. Mag. 30

Gründer und Geschäftsführer der R.I.C.S EDV-GmbH, Gerichtlich beeideter Sachverständiger, Vorstand bei Digital Society

manfred.woehrl@digisociety.at
http://www.rics.at/

Zahler Christian Mag. 1968 4,5

Gewerbetreibender, Autor von ADIM-Skripten, Erwachsenenbildung, MCSE, Lehrer für Technische Mechanik, Fertigungstechnik und Informatik am Francisco-Josephinum Wieselburg

Firma HBLFA Francisco-Josephinum; WIFI

office@zahler.at
http://www.zahler.at/

Inserenten

techbold 32

Dresdner Straße 89 1200 Wien
+43 1 34 34 333
office@techbold.at
http://www.techbold.at

Produkte Reparatur, Aufrüstung, Softwareinstallation, Datenrettung. Installation und Wartung von IT-Anlagen.

Kalender-Tipp

Du kannst Dir unseren dynamischen Kalender in der Google- oder Microsoft-Kalender-Anwendung abonnieren und danach erscheinen die Termine immer aktuell auf Deinem Desktop und—wenn gekoppelt—auch auf Deinem Handy und Du musst keine Termine mehr eintragen—auch keine Änderungen—sie erscheinen automatisch. Diese Adresse brauchst Du dazu:
http://buero.clubcomputer.at/calendar.aspx

Weitere Hinweise

http://buero.clubcomputer.at?svc=cccalendar

Weitere Themenvorschläge 2017

- Cookies
- OneNote *(Norbert Palecek)*
- HUAWEI Mate 9
- Office
- Workshop: Word
- Workshop: Datenbanken
- Bitcoin
- Protokolle
- Fernwartung (TeamViewer und Remote Desktop)
- USV, Unterbrechungsfreie Stromversorgungen *(Gerhard Muttenthaler)*

Impressum

Impressum, Offenlegung

Richtung Auf Anwendungen im Unterricht bezogene Informationen über Personal Computer Systeme. Berichte über Veranstaltungen des Herausgebers.

Erscheint 4 mal pro Jahr: Mär, Jun, Sep, Nov

Herausgeber **ClubComputer**
01-6009933-11 FAX: -12
office@clubcomputer.at
https://clubcomputer.at/
ZVR: 085514499
IBAN: AT74 1400 0177 1081 2896

Siccardsburggasse 4/1/22 1100 Wien

Gasthaus Kulturschmankerl,
Simmeringer Hauptstraße 152, 1110 Wien

HTL, 1030 Wien, Rennweg 89b oder

Digital Society
01-314 22 33
info@DigiSociety.at
https://digisociety.at/
ZVR: 547238411
IBAN: AT45 3266 7000 0001 9315

Lautensackgasse 10 1140 Wien und

Graben 17/10 1010 Wien

Druck **Ultra Print**
Pluhová 49, SK-82103 Bratislava
http://www.ultraprint.eu/

Versand 16Z040679 M

Akteure

Hosting **Werner Illsinger**
01-6009933-220 FAX: -9220
werner.illsinger@clubcomputer.at
http://illsinger.at/
http://illsinger.at/blog/

PCNEWS **Franz Fiala**
01-6009933-210 FAX: -9210
franz.fiala@clubcomputer.at
http://franz.fiala.cc/
http://franz.fiala.cc/blogpcnews/

Marketing **Ferdinand De Cassan**
01-6009933-230 FAX: -9230
ferdinand.de.cassan@clubcomputer.at
http://spielefest.at/

CC|Akademie **Georg Tsamis**
01-6009933-250 FAX: -9250
georg.tsamis@clubcomputer.at

ClubMobile **Paul Belcl**
01-6009933-288 FAX: -9288
paul.belcl@clubcomputer.at
http://www.belcl.at/
http://blog.belcl.at/

ClubDigitalHome **Christian Haberl**
01-6009933-240 FAX: -9240
christian.haberl@clubcomputer.at
http://blog.this.at/

WebDesign **Herbert Dobsak**
01-2637275 FAX: 01-2691341
dobsak@ccc.or.at
http://www.dobsak.at/

Digitalfotografie **Andreas Kunar**
andreas.kunar@clubcomputer.at
http://www.fotocommunity.de/pc/account/myprofile/16403

Linux **Günter Hartl**
ClubComputer-Portal: ‚Guenter.Hartl'

Services

http://buero.clubcomputer.at?svc=xx|yyy

Um Details zu unseren Services zu erfahren, gib statt `xx|yy` den Wert aus der linken Spalte ein (senkrechter Strich optional):

Club	
cc|calendar	Kalender
cc|clubcomputer	ClubComputer
cc|buchhaltung	Buchhaltung
cc|buero	Büroanwendung
cc|fax	Faxdienst
cc|hotline	Hotline
cc|impressum	Impressum ClubComputer
cc|konto	Konten
cc|newsletter	Newsletter
cc|support	Support
pc|pcnews	PCNEWS
at|cccat	cc|communications
at|impressum	Impressum ccc.at
at|domain	Domänenverwaltung
Mitglied	
cc|card	Mitgliedskarte
cc|login	Einloggen
cc|mitmachen	Mitglied werden
cc|webfree	Webpaket für Mitglieder
cc|welcome	Willkommen bei ClubComputer
Wir	
cc|camp	Jahresveranstaltung
cc|heuriger	Sommerheuriger
cc|meating	Clubabend
cc|weihnacht	Weihnachtsfeier
Print	
cc|folder	Folder ClubComputer
pc|news	Clubzeitung
cc|visit	Visitenkarte ClubComputer
Web-Master	
at|mail	Webmail
at|panel	WebsitePanel
at|drive	Cloudspeicher
cc|forum	Diskussionsforum
at|ftp	Ftp-Zugang
cc|see	Medienarchiv für Mitglieder
at|press	Gehostetes WordPress
at|wordpress	Wordpress
at|php	PHP-Konfiguration
at|server	Server-Explorer
at|sfm	Server File Manager
Web-4All	
pc|123	Ergänzende Programme
cc|allapps	Alle Anwendungen
cc|archiv	Dokumentenarchiv
cc|exweb	ExpressionWeb
cc|materialien	Materialien
cc|medien	Medienarchiv
pc|pdf	Alle PCNEWS-
cc|wapps	Web-Applikationen
cc|wissen	Wissensdatenbank
Web-Ext	
at|status	Status
at|facebook	Facebook ccc.at
cc|facebook	Facebook ClubComputer
cc|twitter	Twitter ClubComputer
cc|youtube	Youtube ClubComputer
ds|youtube	YouTube Digital Society
pc|scribd	PCNEWS online lesen
Partner	
cc|ADIM	Skriptenverlag
at|ht13r	HTL-Wien3, Rennweg

Netzwerktechnik

Christian Zahler

1 Netzwerk-Grundlagen

Christian Zahler

1.1 Größenordnung von Netzwerken

Ein PC-Netzwerk besteht aus miteinander verbundenen PCs. Die Verbindung kann dabei über Kabel erfolgen oder auch kabellos über Funk.

Grundsätzlich unterscheidet man:

- **LAN** *(local area network):* lokale, meist firmeninterne Netzwerke, die sich innerhalb eines Gebäudekomplexes befinden. Typischerweise gehört die Verkabelung und die Netzwerkinfrastruktur dem LAN-Betreiber.
- **WAN** *(wide area network):* Netzwerke, die „weit" entfernte Bereiche verbinden, etwa verschiedene Firmenniederlassungen. Auch das Internet entsteht durch die Vernetzung von kleinen lokalen Netzwerken durch WAN-Verbindungen.

Der Begriff **MAN** = *Metropolitan Area Network* ist eigentlich öffentlichen Netzen vorbehalten; in letzter Zeit verwenden aber auch Anwender mit vielen vernetzten Betriebsstellen (Banken) diesen Ausdruck.

Netzwerke wie das Internet (die aus vielen, weltweit miteinander verbundenen Netzwerken bestehen), werden manchmal auch als **GAN** = *Global Area Network* bezeichnet.

1.2 Vermittlungstechniken

Netzwerke können auf Grund ihrer verwendeten Nachrichtenvermittlungstechnik in folgende Kategorien unterteilt werden:

1. **Leitungsvermittlung** *(Circuit Switching, Line Switching,* Durchschaltvermittlung) Leitungsvermittlung wird in „klassischen" Telekommunikationsnetzen (Telefonnetz, ISDN) verwendet. Eigenschaften:

- Aufbau eines durchgehenden, nichtspeichernden Übertragungskanals („Leitung") zwischen den Endsystemen.
- Übertragungsverzögerungen sind auf physikalisch bedingte signaltechnische Laufzeiten beschränkt.
- Bitfolgen werden reihenfolgegetreu übertragen, damit wird die Absendereihenfolge beim Empfänger beibehalten *(wire-like feature).*
- Vermittlung in den Zwischensystemen erfordert keine zusätzlichen Kontrollinformationen zur Adressierung.

Bei diesem Verfahren steht immer eine dedizierte Leitung mit garantierter Datenrate zur Verfügung

2. **Nachrichtenvermittlung** *(Message Switching)*

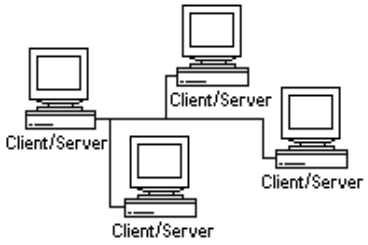
Bei der Nachrichtenvermittlung muss kein fester Pfad zwischen zwei Stationen eingerichtet werden. Vielmehr wird eine Zieladresse an die Nachricht angehängt, wenn eine Station senden will. Die Nachricht wird dann in einem Stück von Knoten zu Knoten durch das Netzwerk transportiert. Jeder Knoten empfängt die gesamte Nachricht, speichert sie zwischen und sendet sie zum nächsten Knoten.

- Einheiten der Vermittlung entsprechen anwendungsorientierten Gesichtspunkten und werden oft als „Nachricht" bezeichnet.
- Eine Nachricht wird typischerweise in mehreren Dateneinheiten vermittelt (Segmentierung und Reassemblierung).
- Im Gegensatz zur Paketvermittlung werden Nachrichten in den Zwischensystemen wieder zusammengesetzt (reassembliert). Daraus folgt, dass alle Dateneinheiten, die zur selben Nachricht gehören, an dasselbe nächste Zwischensystem werden müssen.
- Die Nachrichten selbst müssen nicht alle dem gleichen Weg folgen.
- Die Ende-zu-Ende-Verzögerung ist im Vergleich zur Paketvermittlung deutlich höher.
- Die Bandbreite wird bei dieser Technologie besser genutzt als bei der Leitungsvermittlung.
- Typisch ist das „*Store-and-Forward*"-Prinzip: Nachrichten werden bei jedem Vermittlungsknoten zwischengespeichert. Dadurch können Prioritäten festgelegt werden; ein Nachteil ist aber, dass für die Zwischenspeicherung oft große Massenspeicher nötig sind.

3. **Paketvermittlung** *(Packet Switching)*

Typische paketvermittelnde Netze sind TCP/IP-Netze (dazu gehört auch das Internet) oder *Frame Relay*-Netze.

- Die Vermittlung erfolgt auf Grund von Vermittlungsinformation in den Dateneinheiten (Paketen), etwa anhand der Zieladresse (in Datagrammen) oder anhand einer lokalen Kennung bei virtuellen Verbindungen
- Zwischensysteme verfügen über Speicher, damit Dateneinheiten auf das Freiwerden einer gewünschten Teilstrecke warten können. Auf Grund begrenzter Speicherkapazität können Dateneinheiten verloren gehen.
- Wartende Pakete werden gemäß der eingesetzten Verfahren weitergeleitet; es kann daher zu Reihenfolgevertauschungen kommen.
- Es besteht im Allgemeinen keine feste Zeitbeziehungen zwischen den einzelnen zu vermittelnden Dateneinheiten.
- Geschwindigkeitsanpassung zwischen unterschiedlich leistungsfähigen Endgeräten ist möglich.



1.3 Peer-to-Peer-Netze und Client-Server-Architekturen

Man unterscheidet zwei „Philosophien":

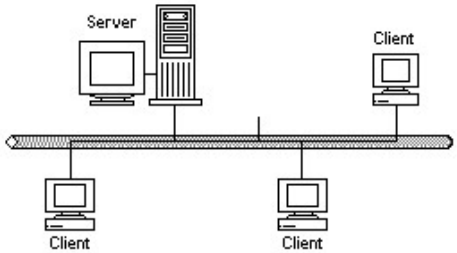
- **Peer-to-Peer-Netzwerke**: Bei einem solchen Netz können prinzipiell alle in das Netz eingebauten PCs ihre Ressourcen anderen PCs bzw. Anwendern zur Verfügung stellen.
  Peer-to-Peer-Netze brauchen keinen eigenen Server-Rechner, da jeder PC Server-Funktionen übernehmen kann. Alle Windows-Betriebssysteme sind in der Lage, sogenannte „Arbeitsgruppen" zu bilden.
- **Client/Server-Architekturen**: Hier gibt es eine Trennung der Ein-/Ausgabefunktion von der eigentlichen Verarbeitung. Auf der Workstation laufen Programme, die nur für die Ein-und Ausgabe zuständig sind *(Frontend-Software),* während – unbemerkt vom Anwender – das entsprechende *Backend*-Programm auf dem Server seine Aufgaben erfüllt (z.B. Speicherung, Suche von Daten). Das grundlegendste Backend-Programm ist das Netzwerk-Betriebssystem.

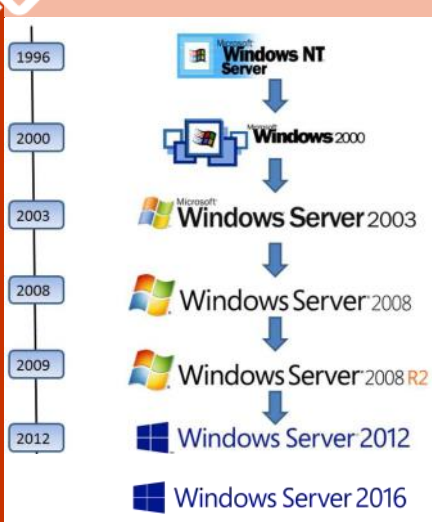
Die meisten Netzwerke arbeiten so, dass der Server dabei seine Fähigkeiten den anderen Rechnern (Workstations) zur Verfügung stellt. Einen Server, der ausschließlich das Netzwerk und die Datenübertragungen im Netzwerk verwaltet und kontrolliert, bezeichnet man als **Dedicated Server**. Ist der Server selbst gleichzeitig als Workstation verwendet, so spricht man von einem **Non-Dedicated Server**.

1.4 Server-Betriebssysteme

Für einen Client/Server-Netzwerkbetrieb benötigt man für den Server eigene Betriebssysteme. Netzwerk-Betriebssysteme müssen Multiprocessing unterstützen.

Typische Netzwerk-Betriebssysteme:





- **Microsoft Windows-Serverbetriebssysteme**

Typisch für die Microsoft-Serverproduktlinie ist die Möglichkeit, auch Anwendersoftware einsetzen zu können. Damit sind verbesserte Möglichkeiten der Protokollierung und Auswertung gegeben. Die aus den Microsoft Client-Betriebssystemen bekannte Oberfläche ermöglicht rasches Einarbeiten und die Konzentration auf die eigentlichen Systembetreuungsaufgaben.

Versionen:

1996 Windows NT

2000 Windows 2000

2003 Windows Server 2003

2008 Windows Server 2008

2009 Windows Server 2008 R2

2012 Windows Server 2012

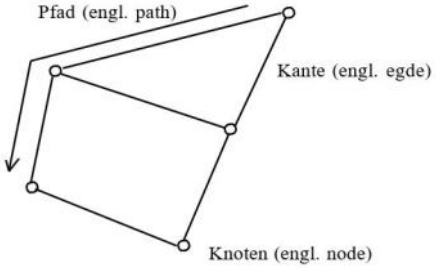
2016 Windows Server 2016

- **Unix** (in verschiedenen Dialekten: SCO-Unix (SCO = Santa Cruz Operation), Xenix, Sinix, AIX, ULTRIX, Irix, Linux, ...) Auf den Unix-Dialekt **Linux** soll gesondert verwiesen werden, da es – im Vergleich zu den anderen Dialekten – sehr preisgünstig ist. Linux bietet (mit kleinen Einschränkungen) die volle Unix-Funktionalität!

1.5 Netzwerk-Topologien

Die Struktur eines Netzwerks bezeichnet man als **Topologie**. Wie wichtig die Struktur eines Netzwerks ist, merkt man bei einem Leitungsausfall: ein gutes Netzwerk findet bei einem Leitungsausfall selbstständig einen neuen Pfad zum Empfänger.

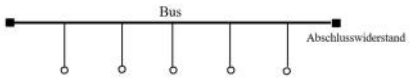
Ein allgemeines Netzwerk kann man sich etwa so vorstellen:



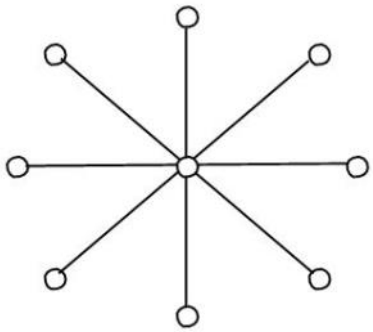
Dabei sind die Rechner selbst die Knoten, die Verbindungskabel stellen die Kanten dar.

Die wichtigsten Netzwerk-Topologien

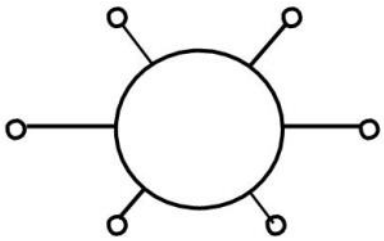
- **Bus-Topologie**: Bei einem Bussystem sind alle Rechner hintereinander geschaltet und über Abzweige (T-Stücke) an das Netzwerkkabel angeschlossen. Problem: Eine Verbindungsunterbrechung betrifft den ganzen Bus!



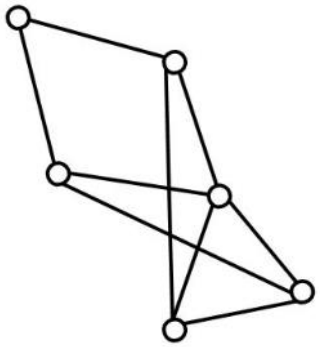
- **Stern-Topologie**: An einen zentralen Sternverteiler sind alle Server und Workstations angeschlossen. Durch den hohen Kabelbedarf teuer; die Sicherheit ist hier aber optimal.



- **Ring-Topologie**



- **Maschen-Topologie**: Vorherrschende Netzstruktur in großflächigen Netzen (z. B. öffentliche Telekommunikationsnetze).



- **Zelluläre Topologie**: Diese Topologie ist bei drahtloser Übertragung häufig anzutreffen, etwa in Mobilfunk-Netzwerken. Rund um einen Sender befindet sich eine "Zelle"; die Geräte innerhalb der Zelle kommunizieren über den Sender, der als Verteiler arbeitet. Die Sender wiederum sind miteinander maschenartig verknüpft.

Physikalische und logische Topologie

Interessant ist, dass sich die "sichtbare" Topologie (also die physische Verkabelungsstruktur) vom tatsächlichen Datenfluss unterscheiden kann. Deshalb verwendet man für die hardwaremäßige Realisierung den Begriff **"physikalische Topologie"**, während man für den tatsächlichen Datenfluss den Begriff **"logische Topologie"** verwendet.

Beispiel siehe Tabelle unten:

Netzwerktechnologie	logische Topologie	physikalische Topologie
Ethernet (IEEE 802.3)	Bus	Bus (veraltet) Stern
Token Ring (IEEE 802.5)	Ring	Ring (veraltet) Stern
Token Bus	Ring	Bus

2 Datenübertragung in Netzwerken

Bei der Datenübertragung in einem Netzwerk laufen viele Vorgänge ab, von denen der Anwender nichts merkt. So werden meistens nicht ganze Dateien übertragen, sondern in vielen Fällen sogenannte **Pakete**.

Damit ein Paket auch beim Empfänger ankommt, müssen eine Reihe von Informationen mit diesem Paket mitgeschickt werden.

Da die Datenübertragung in jedem Netzwerk sehr komplex ist, teilt man das Problem in Teilprobleme auf. Man unterscheidet sogenannte „Schichten", die bestimmte Aufgaben erfüllen; im Internet könnte man folgende Schichten unterscheiden:

- Application (Anwendung): Benutzerebene (Surfen über WWW, FTP, ...)
- Transportschicht: Transport der Meldungen (verlässlich, ...)
- Netzwerkschicht: Adressierung, Verwaltung
- Network Interface: Daten auf das Medium (Kabel) bringen bzw. vom Medium (abholen)
- Hardware: Lichtwellenleiter, Kupferkabel

Jede Schicht (Teilfunktion) wird durch ein sogenanntes **Protokoll** realisiert; in der Praxis gibt es spezielle Treiber, die die Aufgaben von Protokollen übernehmen (in Windows gibt es etwa die TCP/IP-Treiber).

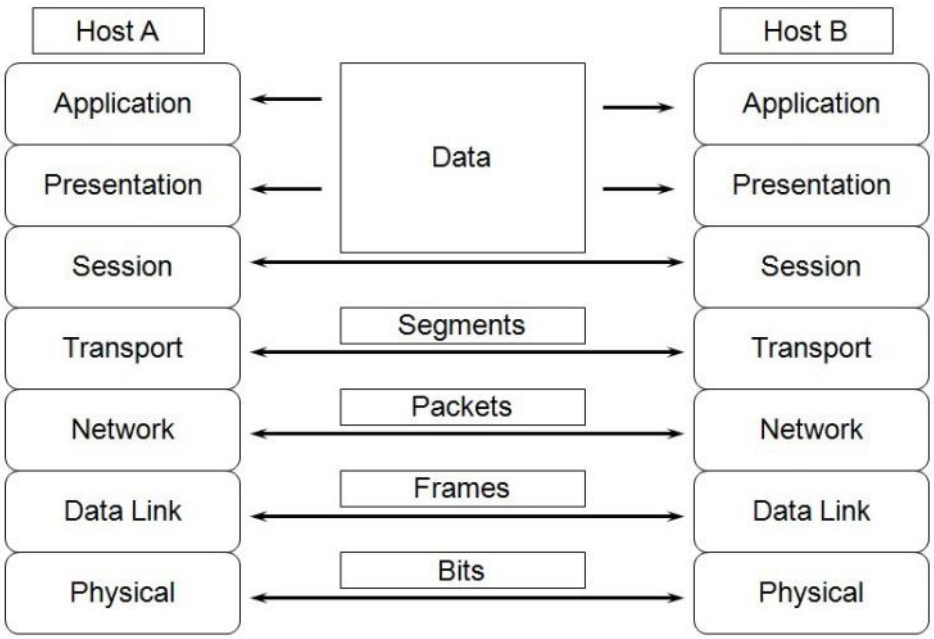
2.1 Das OSI-Referenzmodell

Wie schon mehrfach erwähnt, dominierten zu Beginn der Netzwerkgeschichte die proprietären (herstellerspezifischen) Netzwerke. Es gab mehrere Versuche zur Standardisierung der Netzwerkkonzeption; der vielleicht wichtigste Ansatz ist das OSI-Referenzmodell *(Open Systems Interconnection)*, das ab 1977 von der ISO *(International Standard Organization)* entwickelt wurde.

Dieses Modell ist allgemein akzeptiert und bildet die Referenz für viele Hersteller; allerdings müssen heute vielfach Übergangslösungen und Ergänzungen entwickelt werden, da das Modell in verschiedenen Fällen noch nicht ganz fertig, mangelhaft oder gar lückenhaft (Datenschutz, Netzwerkmanagement) ist. Zudem ist zu bemerken, dass das OSI-Modell für PC-Netze im Allgemeinen zu umfassend ist; nichtsdestoweniger realisieren alle heute eingesetzten Produkte bestimmte Untermengen der durch das OSI-Referenzmodell festgelegten Funktionen. Der Sinn eines generellen Modells zur Beschreibung der Netzwerkarchitektur ist die Beschreibung des Weges von Daten zwischen zwei An-

	OSI-Referenzmodell	Synonyme	Beschreibung	Beispiel LAN
7	***Application Layer*** (Anwendungsschicht)	Anwendungsschicht	Anwendungsunterstützende Dienste, Netzwerkverwaltung	Betriebssystem (Windows, Linux, etc.) und dessen Netzwerk-Dienste.
6	***Presentation Layer*** (Datendarstellungsschicht)	Präsentationsschicht	Umsetzung von Daten in Standardformate, Interpretation dieser gemeinsamen Formate	
5	***Session Layer*** (Kommunikationssteuerungsschicht)	Sitzungsschicht	Prozess-zu-Prozess-Verbindung	Netzwerk-Protokolle und Zusatz-Software (NetBEUI, IPX/SPX, TCP/IP etc.)
4	***Transport Layer*** (Transportschicht)	Transportschicht	Logische Ende-zu-Ende-Verbindungen	
3	***Network Layer*** (Vermittlungsschicht)	Netzwerkschicht	Wegbestimmung im Netz (Datenflusskontrolle)	
2	***Data Link Layer*** (Sicherungsschicht)	Verbindungsschicht	Logische Verbindungen mit Datenpaketen, Elementare Fehlerkorrektur	Netzwerkkarten-Treiber, Netzwerkkarte und Verkabelung
1	***Physical Layer*** (Bitübertragungsschicht)	Physikalische Schicht	Nachrichtentechnische Hilfsmittel zur Bitübertragung	

OSI-Referenzmodell Quelle: Basierend auf einer Grafik von Cisco Systems, Inc.



wendungen (letztlich tauschen nämlich Anwendungen immer Daten aus), um die Kommunikation in heterogenen Umgebungen zu vereinfachen. Damit dieses Modell möglichst breit verwendet werden kann, muss es einen gewissen Abstraktionsgrad besitzen. Es geht schließlich auch darum, durch einen modularen Aufbau das Netz genügend detailliert und produktübergreifend zu beschreiben. Das OSI-Modell bedient sich dazu einer Struktur, welche die Kommunikation im Netz in sieben aufgabenbezogene Schichten aufteilt. Jede Schicht übernimmt eine gewisse Anzahl von Funktionen und kann Dienstleistungen für die übergeordnete Schicht erbringen: (siehe Tabelle, vorige Seite oben)

Bei der Kommunikation zweier Computer über ein Netzwerk werden die Informationen grundsätzlich ebenenweise ausgetauscht. So kommuniziert zum Beispiel die Transportebene eines Computers mit der Transportebene des anderen Computers. Für die Transportschicht des ersten Computers ist es ohne Bedeutung, wie die eigentliche Kommunikation in den unteren Ebenen des ersten Computers, dann über die physikalischen Medien und schließlich durch die unteren Ebenen des zweiten Computers abläuft: (siehe Bild, vorige Seite unten)

Die untersten vier Schichten werden auch als "datenflussorientierte Schichten" bezeichnet, die oberen drei Schichten stellen die "Anwendungsschichten" dar.

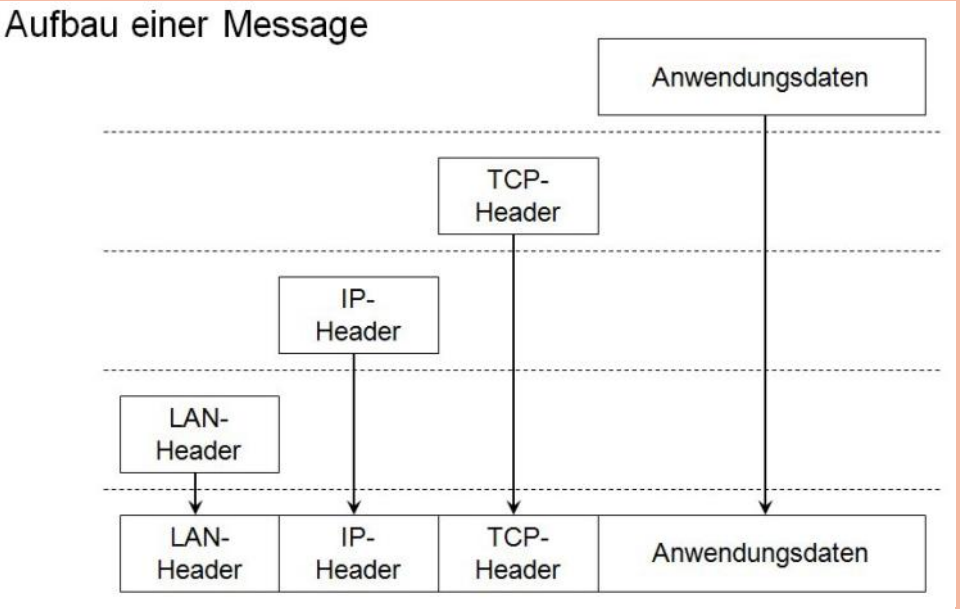
Die Vorteile des OSI-Referenzmodelles sind die leichte Analyse, der (relativ) systematische Entwurf und die Vermeidung von Doppelfunktionalität, die unabhängige Bearbeitung der Komponenten (Modularisierung), die leichtere Austauschbarkeit (Connectivity!) sowie die vereinfachte Fehlerbestimmung. So gesehen widerspiegelt das OSI-Referenzmodell die Modularisierungsphilosophie, wie man sie in vielen Bereichen der Ingenieurwissenschaften findet. Das OSI-Referenzmodell ist allerdings die Idealvorstellung eines Netzwerbetriebs, und es gibt nur wenige Systeme, die sich genau an das Modell halten. Das Modell wird jedoch häufig für Diskussionen und den Vergleich von Netzwerken herangezogen und ist – wie schon gesagt – bei der Fehlerlokalisierung von großem Nutzen.

Die englischen Namen der einzelnen Schichten lassen sich durch zwei „Eselsbrücken“ leichter merken:

„Please Do Not Throw Salami Pizza Away“ und in umgekehrter Reihenfolge

„All People Seem To Need Data Protocols“

Jede Schicht fügt spezielle Adress-und Protokollinformationen (sogenannte *„Header“)* zu den eigentlichen Daten hinzu. Dadurch wird das Datenpaket immer größer. Beim Empfänger durchläuft das Datenpaket die Protokolle in umgekehrter Reihenfolge,



wobei die Daten dabei sozusagen „ausgepackt“ werden.

Im Folgenden sollen die einzelnen Schichten nun noch etwas genauer gesprochen werden:

Physical layer (Physikalische Schicht, Bitübertragungsschicht)

Die Bitübertragungsschicht (engl. physical layer) ist die unterste Schicht. Diese Schicht stellt mechanische, elektrische und weitere funktionale Hilfsmittel zur Verfügung, um physikalische Verbindungen zu aktivieren bzw. deaktivieren, sie aufrechtzuerhalten und Bits darüber zu übertragen. Das können zum Beispiel elektrische Signale, optische Signale (Lichtleiter, Laser), elektromagnetische Wellen (drahtlose Netze) oder Schall sein. Die für sie verwendeten Verfahren bezeichnet man als übertragungstechnische Verfahren. Geräte und Netzkomponenten, die der Bitübertragungsschicht zugeordnet werden, sind zum Beispiel die Antenne und der Verstärker, Stecker und Buchse für das Netzkabel, der Repeater, der Hub, der Transceiver, das T-Stück und der Endwiderstand (Terminator).

Auf der Bitübertragungsschicht wird die digitale Bitübertragung auf einer leitungsgebundenen oder leitungslosen Übertragungsstrecke bewerkstelligt. Die gemeinsame Nutzung eines Übertragungsmediums kann auf dieser Schicht durch statisches Multiplexen oder dynamisches Multiplexen erfolgen. Dies erfordert neben den Spezifikationen bestimmter Übertragungsmedien (zum Beispiel Kupferkabel, Lichtwellenleiter, Stromnetz) und der Definition von Steckverbindungen noch weitere Elemente. Darüber hinaus muss auf dieser Ebene gelöst werden, auf welche Art und Weise überhaupt ein einzelnes Bit übertragen werden soll.

Damit ist Folgendes gemeint: In Rechnernetzen wird heute Information zumeist in Form von Bitfolgen übertragen. Selbstverständlich sind der physikalischen Übertragungsart selbst, zum Beispiel Spannungspulse in einem Kupferkabel im Falle elektrischer Übertragung, oder Frequenzen und Amplituden elektromagnetischer Wellen im Falle von Funkübertragung, die Werte 0 und 1 unbekannt. Für jedes Medium muss daher eine Codierung dieser Werte gefunden werden, beispielsweise ein Spannungsimpuls von bestimmter Höhe oder eine Funkwelle mit bestimmter Frequenz, jeweils bezogen auf eine bestimmte Dauer. Für ein spezifisches Netz müssen diese Aspekte präzise definiert werden. Dies geschieht mit Hilfe der Spezifikation der Bitübertragungsschicht eines Netzes.

Funktionen

- Übertragungsmedium
- Übertragungsgeräte
- Netzwerk-Architektur
- Datensignale

Typische Festlegungen der Bitübertragungsschicht:

- Wie viel Volt entsprechen einer logischen 1 bzw. 0?
- Wie viele Millisekunden dauert ein Bit?
- Soll eine gleichzeitige Übertragung in beide Richtungen erfolgen oder nicht (Duplexbetrieb)?
- Wie kommt die erste Verbindung zu Stande und wie wird eine Verbindung getrennt?
- Wie ist der Stecker für den Netzwerkanschluss mechanisch aufgebaut?

Typische Normen und Protokolle:

- Steckernormen (RJ11, RJ45), Kabelnormen (RG58)
- Schnittstellennormen (RS232 für die serielle Schnittstelle)

Data Link layer (Sicherungsschicht)

Die Sicherungsschicht erstellt auf der Basis der Rohdaten aus der physikalischen Ebene die verschiedenen zu übertragenen Pakete. Die Sicherungsebene ist zuständig für die fehlerfreie Übertragung der Pakete:

nach dem Senden eines Paketes wartet die Sicherungsebene auf eine Empfangsbestätigung der Zieladresse. Wird ein Paket nach einer bestimmten Zeit nicht bestätigt, wo wird es erneut gesendet.

Funktionen:

- Medienzugriff
- Physikalische Adressierung
- Paketbildung
- Flusskontrolle
- Fehlerprüfung

Die OSI-Schicht 2 legt also die zu verwendende Netzwerktechnologie fest; Beispiele dafür sind:

- IEEE 802.3 (Ethernet)
- IEEE 802.5 (Token Ring)
- IEEE 802.11 (WLAN)

In der Sicherungsschicht werden Daten in spezielle „Pakete“, sogenannte Frames (deutsch: Rahmen) verpackt. Darunter versteht man voneinander abgrenzbare Bitfolgen. Es werden besondere Bitfolgen als Rahmengrenzen verwendet, die innerhalb des Rahmens nicht auftreten dürfen.

Die OSI-Schicht 2 wird oft unterteilt in zwei Teilschichten:

2a-Schicht, MAC (Media Access Control)

In dieser Teilschicht wird der Zugriff auf das Übertragungsmedium in sogenannten Broadcastnetzen geregelt, in denen alle Stationen denselben Übertragungskanal benutzen (Beispiele: Ethernet, Token Ring). Die MAC-Schicht grenzt an die physikalische Schicht.

Die hardwaremäßige Netzwerkkarten-Identifikation erfolgt in Form einer 48 bit-Adresse, der sogenannten *Media Access Control-Nummer* (MAC-Adresse). Diese Adressen werden in hexadezimaler Schreibweise angegeben.

Die ersten 24 Bits (Bits 47 bis 24) beschreiben eine von der IEEE vergebene Herstellerkennung (auch OUI – *Organizationally Unique Identifier* genannt), die weitgehend in einer Datenbank einsehbar sind. Die verbleibenden 24 Bit (Bits 23 bis 0) werden vom jeweiligen Hersteller für jede Schnittstelle individuell festgelegt.

Beispiel:

00-F0-23 –	AF-98-27
Herstellernummer	Kartennummer

Herstellercodes von MAC-Adressen (Auswahl):

```
00-50-8b-xx-xx-xx   Compaq
00-07-E9-xx-xx-xx   Intel
00-60-2F-xx-xx-xx   Cisco
00-15-F2-xx-xx-xx   ASUS
```

Die MAC-Adresse, bei der alle 48 Bits auf 1 gesetzt sind (`ff-ff-ff-ff-ff-ff`), wird als Broadcast-Adresse verwendet, die an alle Geräte in einem LAN gesendet wird. Broadcast-Frames werden ohne besondere Maßnahmen nicht in ein anderes LAN übertragen.

2b-Schicht, LLC (Logical Link Control)

Logical Link Control (LLC) ist die Bezeichnung für ein Netzwerkprotokoll der Telekommunikation, das als IEEE 802.2 standardisiert wurde. Es ist ein Protokoll, dessen Hauptzweck in der Datensicherung auf der Verbindungsebene liegt, und gehört daher zur Schicht 2 des OSI-Modells. LLC ist eine *Protocol Data Unit* (PDU) der OSI-Schicht 2 und grenzt an OSI-Schicht 3. Sie verteilt eingehende Daten, indem sie diese an die entsprechenden Instanz-Protokolle der OSI-Schicht 3 weiterleitet. Daten, welche die OSI-Schicht 3 zur Übermittlung sendet, werden von LLC an den MAC-Layer der OSI-Schicht 2 weitergegeben.

Das Protokoll LLC fügt einem gegebenen IP -Paket zwei jeweils 8 Bit große Kennzeichen namens DSAP *(Destination Service Access Point:* Einsprungadresse des Empfängers) und SSAP *(Source Service Access Point:* Einsprungadresse des Absenders) hinzu. Außerdem existiert ein 8 oder 16 Bit großes Feld (Control) mit Steuerinformationen für Hilfsfunktionen wie beispielsweise Datenflusssteuerung.

Network layer (Vermittlungsschicht)

Die Vermittlungsebene bearbeitet die zirkulierenden Nachrichten und setzt logische Adressen und Namen in physikalische Adressen um Sie legt auch den Weg vom sendenden Computer über das Netzwerk zum Zielcomputer fest. Zudem kümmert sie sich um die Optimierung des Nachrichtenverkehrs (zum Beispiel durch Umschalten oder Festlegen der Leistungswege und der Steuerung der Belastung durch Datenpakete in komplexeren Netzwerken).

Funktionen

- Internetworking
- Routing
- Netzwerkkontrolle

Typische Protokolle auf der Vermittlungsschicht:

- Internet Protocol (IP)
- Internet Packet Exchange (IPX)

Transportlayer(Transportschicht)

Die Transportschicht stellt die zuverlässige Auslieferung der Nachrichten sicher und erkennt sowie behebt allfällige Fehler. Sie ordnet bei Bedarf auch die Nachrichten in Paketen neu, indem sie lange Nachrichten zur Datenübertragung in kleinere Pakete aufteilt. Am Ende des Weges stellt sie die kleinen Pakete wieder zur ursprünglichen Nachricht zusammen. Die empfangene Transportebene sendet auch eine Empfangsbestätigung.

Funktionen

- Adressierung
- Transportkontrolle
- Paketbildung

Typische Protokolle auf der Transportschicht

- *Transmission Control Protocol* (TCP)
- *User Datagram Protocol* (UDP)
- *Sequenced Packet Exchange* (SPX)

Session layer (Sitzungsschicht)

Diese Schicht ermöglicht zwei Anwendungen auf verschiedenen Computern, eine gemeinsame Sitzung aufzubauen, damit zu arbeiten und sie zu beenden. Sie übernimmt ebenfalls die Dialogsteuerung zwischen den beiden Computern einer Sitzung und regelt, welcher der beiden wann und wie lange Daten überträgt.

Funktionen:

- Erstellung einer Verbindung
- Datenübertragung
- Freigabe von Verbindungen
- Dialogsteuerung

Typische Protokolle der Sitzungsschicht:

- Authentifizierungsprotokolle wie Kerberos, NTLM, CHAP, EAP usw.

Presentationlayer(Darstellungsschicht)

Die Darstellungsschicht setzt die Daten der Anwendungsebene in ein Zwischenformat um. Diese Schicht ist auch für Sicherheitsfragen zuständig. Durch sie werden Dienste zur Verschlüsselung von Daten bereitgestellt und gegebenenfalls Daten komprimiert.

Funktionen

- Übersetzung
- Verschlüsselung
- Kompression

Typische Protokolle der Darstellungsschicht:

- Verschlüsselungsprotokolle wie SSL

Application Layer (Anwendungsschicht)

Dank der Anwendungsschicht können die Benutzeranwendungen auf die vom Netzwerk zur Verfügung gestellten Dienste zugreifen.

Funktion

- Benutzerschnittstelle

Typische Protokolle der Anwendungsschicht

- *Dynamic Host Configuration Protocol* (DHCP)
- *Domain Name System* (DNS)
- *Hypertext Transfer Protocol* (HTTP)
- *File Transfer Protocol* (FTP)
- *Simple Network Management Protocol* (SNMP)
- *Simple Mail Transfer Protocol* (SMTP)
- *Post Office Protocol* (POP)

2.2 Das TCP/IP-4 Schichten-Modell (DoD -Modell)

Dieses Modell stellt eine Vereinfachung des OSI-Modells dar, da es bewusst auf die Netzwerkprotokollsuite TCP/IP zugeschnitten wurde. Das Modell wurde ursprünglich vom US-amerikanischen ***Department of Defense*** entwickelt.

Grafik: Gegenüberstellung des OSI 7 Schicht- und des TCP/IP-Netzwerkmodells

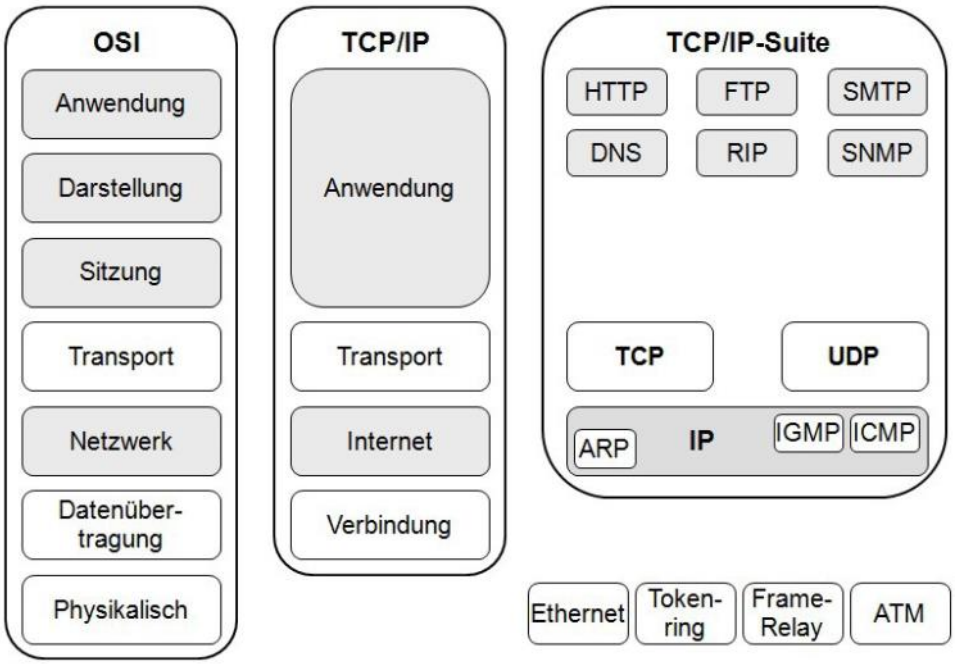
Die obersten drei Schichten sind zur **Anwendungsschicht** zusammengefasst; die hardwarenahen unteren beiden Schichten bilden die **Verbindungsschicht**.

Beispiele für Protokolle der Anwendungsschicht:

- **HTTP** = *Hypertext Transfer Protocol:* Surfen im WWW
- **FTP** = *File Transfer Protocol:* Upload und Download von Dateien
- **SMTP** = *Simple Mail Transfer Protocol:* Protokoll zum Senden von Mails (funktioniert nur, wenn Online!)
- **POP3** = *Post Office Protocol*, version 3: Protokoll zum Abholen von Mails (mit User- und Passwortabfrage)
- **NNTP** = *Network News Transfer Protocol*: Protokoll zum Arbeiten mit Newsgroups
- **Telnet**: Sitzung auf einem Remote Server (Terminal-Modus)
- **DNS**: Auflösung von Namen in IP-Adressen und umgekehrt

2.3 Aktive Netzwerkkomponenten im Überblick

Siehe Tabelle rechts.



Komponente	OSI	Bedeutung
Repeater	1	Repeater (dt. „Verstärker“) dienen innerhalb eines lokalen Netzes zur Signalverstärkung. so kann die Ausdehnung eines Netzes erhöht werden; allerdings müssen dabei die beiden Netze das gleiche Protokoll verwenden. **Repeater-Regel (5-4-3-Regel):** Es dürfen nicht mehr als fünf (5) Kabelsegmente verbunden werden. Dafür werden vier (4) Repeater eingesetzt. An nur drei (3) Segmente, dürfen Endstati-
Hub	1	Sternverteiler, wirkt wie Multiport-Repeater
Bridge	2	Eine Bridge kann zwei gleichartige Netzwerke mit unterschiedlichen (oder gleichen) Topologien miteinander verbinden, unter der Voraussetzung, dass beide Netze das gleiche Protokoll und die gleiche logische Adressierung verwenden. So kann z.B. ein TCP/IP-Netzwerk mit einer Ethernet-Topologie mit einem TCP/IP -Netzwerk auf Token-Ring-Basis verbunden werden. Bridges können ebenfalls verwendet werden, wenn es darum geht, größere Distanzen zwischen LANs zu überbrücken; in diesem Fall
Switch	2	Ein Switch (engl. Schalter; auch Weiche) ist eine Netzwerk-Komponente zur Verbindung mehrerer Computer bzw. Netz-Segmente in einem lokalen Netz (LAN).
Router	3	Ein Router verbindet normalerweise Netzwerke, welche eine unterschiedliche logische Adressierung, aber einheitliche Protokolle verwenden. Router werden häufig im WAN-Zusammenhang eingesetzt. Allerdings gibt es heute auch andere Einsatzmöglichkeiten für Router – z.B. für die Anbindung eines LANs ans Internet, wobei der (ISDN-/ADSL-)Router automatisch
Layer-3-Switch	3	Kombigeräte mit Switching- und Routing-Funktionalität
Gateway	7	Ein Gateway verbindet zwei unterschiedliche Netzwerke mit zwei separaten Protokollen miteinander (Achtung: in der Terminologie von TCP/IP bezeichnet das Gateway einen Router). Ein spezieller Kommunikationsserver übernimmt die Aufgabe, die ungleichen Protokolle und Datentransfermethoden miteinander zu verbinden. Gateways sind ebenfalls ein probates Mittel, LANs

2.4 Hub

Hubs (engl. = Nabe, Radnabe) agieren als Multiportrepeater. Sie stellen eine veraltete Technologie dar und wurden früher als Sternverteiler für Netzwerke mit Stern-Topologie verwendet.

Hubs arbeiten auf der Bitübertragungsschicht (Schicht 1) des OSI-Modells. Sie haben reine Verteilfunktion. Alle Stationen die an einem Hub angeschlossen sind, teilen sich die gesamte Bandbreite die durch den Hub zu Verfügung steht (z. B. 10 MBit/s oder 100 MBit/s). Die Verbindung von Computer zum Hub verfügt nur kurzzeitig über diese Bandbreite.

Ein Hub nimmt ein Datenpaket an und sendet es an alle anderen Ports. Dadurch sind alle Ports belegt. Diese Technik ist nicht besonders effektiv; daher werden in modernen Netzwerkinfrastrukturen Hubs nicht mehr eingesetzt und durch Switches ersetzt.

Sternverteiler (Hub), an den etwa 6-12 Clients, der Server und der Netzwerkdrucker angeschlossen werden können (Foto: C2000)

2.5 Switch

Ein Switch (engl. Schalter) ordnet durch MAC-Adressen (Schicht 2) eintreffende Pakete den korrekten Ports zu. Hersteller: zum Beispiel HP, 3 Com, Bay Networks, Cisco

Eigenschaften

- bei Kabelbruch nur ein PC betroffen hohe Uptime
- einfache Steigerung der Leistung von 100 Mbit/s 1000 Mbit/s
- dicke Kabelstränge in der Nähe des Sternverteilers

Ein Switch arbeitet auf der Sicherungsschicht (Schicht 2) des OSI-Modells und arbeitet ähnlich wie eine Bridge. Daher haben sich bei den Herstellern auch solche Begriffe durchgesetzt, wie z. B. Bridging Switch oder Switching Bridge. Ein Switch schaltet direkte Verbindungen zwischen den angeschlossenen Geräten. Auf dem gesamten Kommunikationsweg steht die gesamte Bandbreite des Netzwerkes zur Verfügung.

Arbeitsweise

Einfache Switches arbeiten auf der Schicht 2 (Sicherungsschicht) des OSI-Modells. Der Switch verarbeitet die 48 Bit langen MAC-Adressen (z. B. 08:00:20:ae:fd:7e) und legt dazu eine SAT *(Source-Address-Table)* an, in der neben der MAC-Adresse auch der physikalische Port, an dem diese empfangen wurde, gespeichert wird. Im Unterschied zum Hub werden Netzwerkpakete jetzt nur noch an den Port weitergeleitet, der für die entsprechende Zieladresse in der SAT gelistet ist. Ist eine Zieladresse allerdings noch unbekannt (Lernphase), leitet der Switch das betreffende Paket an alle aktiven Ports.

Switches unterscheidet man hinsichtlich ihrer Leistungsfähigkeit mit folgenden Eigenschaften:

- Anzahl der speicherbaren MAC-Adressen (Speicher)
- Verfahren, wann ein empfangenes Datenpaket weitervermittelt wird (Switching-Verfahren)
- Latenz (Verzögerungszeit) der vermittelten Datenpakete

Ein Switch ist im Prinzip nichts anderes als ein intelligenter Hub, der sich merkt, über welchen Port welche Station erreichbar ist. Auf diese Weise erzeugt jeder Switch-Port eine eigene *Collision Domain*.

Teure Switches arbeiten auf der Schicht 3, der Vermittlungsschicht, des OSI-Schichtenmodells (Layer-3-Switch oder Schicht-3-Switch). Sie sind in der Lage die Datenpakete anhand der IP-Adresse an die Ziel-Ports weiterzuleiten. Im Gegensatz zu normalen Switches lassen sich so, auch ohne Router, logische Abgrenzungen erreichen.

2.5.1 Switching-Technologien

1. Cut-Through

Der Switch leitet das Datenpaket sofort weiter, wenn er die Adresse des Ziels erhalten hat.

Vorteil: Die Latenz, die Verzögerungszeit, zwischen Empfangen und Weiterleiten ist äußerst gering.

Nachteil: Fehlerhafte Datenpakete werden nicht erkannt und trotzdem an den Empfänger weitergeleitet.

2. Store-and-Forward

Der Switch nimmt das gesamte Datenpaket in Empfang und speichert es in einen Puffer. Dort wird dann das Paket mit verschiedenen Filtern geprüft und bearbeitet. Erst danach wird das Paket an den Ziel-Port weitergeleitet.

Vorteil: Fehlerhafte Datenpakete können so im Voraus aussortiert werden.

Nachteil: Die Speicherung und Prüfung der Datenpakete verursacht eine Verzögerung von mehreren Millisekunden (ms), abhängig von der Größe des Datenpaketes.

3. Kombination aus Cut-Through und Store-and-Forward

Viele Switches arbeiten mit beiden Verfahren. Solange nur wenige Kollisionen auftreten wird Cut- Through verwendet. Häufen sich die Fehler schaltet der Switch auf Store-and-Forward um.

4. Fragment-Free

Der Switch empfängt die ersten 64 Byte des Daten-Paketes. Ist dieser Teil fehlerlos werden die Daten weitergeleitet.

Netgear GS105 ProSafe;
Switch mit 5 Ports, 10/100/1000 Mbit/s

Linksys SR2024;
Switch mit 24 Ports, 10/100/1000 Mbit/s

Vorteil: Die meisten Fehler und Kollisionen treten während den ersten 64 Byte auf. Nachteil: Dieses Verfahren wird trotz seiner effektiven Arbeitsweise selten genutzt.

2.5.2 Switch-MAC-Tabellenverwaltung

Switches haben den Vorteil, im Gegensatz zu Hubs, dass sie Datenpakete nur an den Port weiterleiten, an dem die Station mit der Ziel-Adresse angeschlossen ist. Als Adresse dient die MAC-Adresse, also die Hardware- Adresse einer Netzwerkkarte. Diese Adresse speichert der Switch in einer internen Tabelle. Empfängt ein Switch ein Datenpaket, so sucht er in seinem Speicher unter der Zieladresse (MAC) nach dem Port und schickt dann das Datenpaket nur an diesen Port. Die MAC-Adresse lernt ein Switch mit der Zeit kennen. Die Anzahl der Adressen, die ein Switch aufnehmen kann, hängt ab von seinem Speicherplatz.

Ein Qualitätsmerkmal eines Switches ist es, wie viele Adressen er insgesamt und pro Port speichern kann. An einem Switch, der nur eine Handvoll Computer verbindet, spielt es keine Rolle wie viele Adressen er verwalten kann. Wenn der Switch aber in einem großen Netzwerk steht und an seinen Ports noch andere Switches und Hubs angeschlossen sind, dann muss er evt. mehrere tausend MAC-Adressen speichern und den Ports zuordnen können. Je größer ein Netzwerk ist, desto wichtiger ist es, von vornherein darauf zu achten, dass die Switches genügend Kapazität bei der Verwaltung von MAC-Adressen haben.

2.5.3 Layer3-Switches

Der Ausdruck Layer-3-Switch ist etwas irreführend, denn es handelt sich um Multifunktionsgeräte, die eine Kombination aus Router und Switch darstellen.

2.6 Kollisions- und Broadcastdomänen

Eine Kollisionsdomäne ist ein Netzwerksegment in einem CSMA/CD-Netz (etwa Ethernet). Alle Stationen, die physisch miteinander verbunden sind, befinden sich in der gemeinsamen Kollisionsdomäne. Repeater und Hubs trennen Kollisionsdomänen nicht.

Bridges trennen Kollisionsdomänen, da sie auf OSI-Schicht 2 arbeiten. In einem geswitchten Netz besteht die Kollisionsdomäne nur aus zwei Stationen, dem Client und dem Switchport.

Eine **Broadcast-Domäne** ist ein logischer Verbund von Computern in einem lokalen Netzwerk, der sich dadurch auszeichnet, dass ein Broadcast alle Domänenteilnehmer erreicht.

Ein lokales Netzwerk auf der zweiten Schicht des OSI-Modells (Sicherungsschicht) besteht durch seine Hubs, Switches und/oder Bridges aus einer Broadcast -Domäne. Erst durch die Unterteilung in VLANs oder durch den Einsatz von Routern, die auf Schicht 3 arbeiten, wird die Broadcast-Domäne aufgeteilt.

Eine Broadcast-Domäne besteht aus einer oder mehreren Kollisionsdomänen.

2.7 VLANs (Virtual LANs)

Durch die Switching-Technik (OSI-Ebene 2) können sehr große LANs aufgebaut werden, ohne starke Bandbreiteneinbußen zu verursachen. Switches können sehr viele angeschlossene Stationen gleichzeitig verwalten (begrenzt durch die Größe ihrer MAC address table). Vorteil eines großen geswitchten Netzes ist die einfache Erreichbarkeit aller Stationen, die Einsparung von Routern und deren Verwaltung und eine geringe Latenz der Datenpakete.

Aus folgenden Gründen will man ein solches Netz oft wieder unterteilen:

- Die Broadcast-Last wird sehr hoch.
- Man möchte die Netze kompakt und überschaubar halten, z.B. nach Abteilungen getrennt, aber ohne VLANs kann jede Station jede andere direkt ansprechen (Sicherheitsproblem)

Eine Lösung dieser Probleme sind VLANs. Mit Hilfe von VLANs können auf einem Switch oder über mehrere Switches hinweg virtuell getrennte Netze betrieben werden. Diese Technik eignet sich auch für die standortübergreifende Vernetzung (z.B. per ATM) mehrerer VLANs über einen Switch bzw. Router.

Schon aus Ressourcengründern lässt sich ein Netz nicht überall über getrennte Switches aufbauen. Physisch getrennt verkabelte Netze sind aber auch unflexibel und Änderungen nur mit hohem Aufwand möglich. VLAN stellt unabhängig von der physischen Struktur eine logische Struktur des Netzes zur Verfügung.

Technologien

- **Port-based VLANs**: Hier wird ein managebarer Switch in mehrere logische Switches segmentiert. Ein Port gehört dann immer nur zu einem VLAN, um die so segmentierten Netze bei Bedarf zu verbinden kommt z.B. ein Router zum Einsatz; meist kann ein Layer-3-Switch auch diese Aufgabe erfüllen-
- **Tagged VLANs:** Hier tragen die Netzwerkpakete eine Markierung, welche die Zugehörigkeit zu einem VLAN anzeigt.

Funktionsweise nach IEEE 802.1Q: Jedem VLAN wird eine eindeutige Nummer zugeordnet. Man nennt diese Nummer VLAN ID. Ein Gerät, das zum VLAN mit der ID=1 gehört, kann mit jedem anderen Gerät im gleichen VLAN kommunizieren, nicht jedoch mit einem Gerät in einem anderen VLAN wie z.B. ID=2, 3, ...

Um zwischen den VLANs zu unterscheiden, wird nach IEEE 802.1Q das Ethernet-Frame um 4 Byte (= 32 Bit) erweitert. Davon sind 12 Bit zur Aufnahme der VLAN ID vorgesehen, so dass insgesamt 4096 - 2 = 4094 VLANs möglich sind (die VLAN-IDs "0" und "4095" sind reserviert und nicht zulässig).

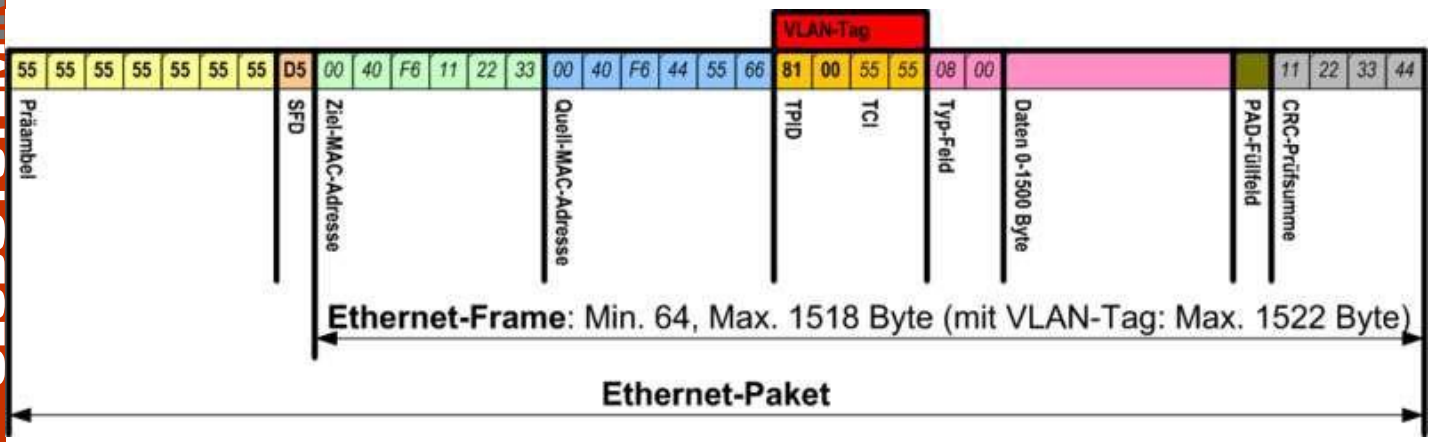
TPID *(Tag Protocol Identifier):* Fester Wert 0x8100. Bedeutung: Frame trägt die 802.1Q/802.1p-Tag- Information.

Priorität *(user_priority)* – Benutzer-Prioritätsinformationen.

CFI *(Canonical Format Indicator):*

- Wert 0: das Format der MAC-Adressen ist kanonisch (LSB zuerst)
- Wert 1: Format ist nicht-kanonisch. Benutzung im Token Ring/Source-Routed-FDDI-Media- Zugang, um die bit order der Adressinformationen des verkapselten Frames zu kennzeichnen.

VID *(VLAN Identifier):* VLAN-Nummer, zu dem der Rahmen gehört.



3 Kabelgebundene Signalübertragung

Heute werden für die Datenübertragung in Computernetzen meist **Kupferkabel** oder **Glasfaserkabel** verwendet. Die Daten selbst werden in Form von **elektrischen Signalen** übertragen. Von einem Signal spricht man, wenn man einer messbaren physikalischen Größe (etwa der elektrischen Spannung) eine Information zuordnet.

Vereinfacht gesagt, handelt es sich bei diesen Signalen um **Wechselspannungsimpulse**.

3.1 Analoge und digitale Signale

Als **Analogsignal** wird ein Signal bezeichnet, wenn seine Stärke (Amplitude) kontinuierlich jeden Wert zwischen einem Minimum und einem Maximum annehmen kann. Dieses trifft auf nahezu alle realen Prozesse oder Zustände zu. Theoretisch ist es möglich, beliebig kleine Signaländerungen zu registrieren.

Üblicherweise versteht man unter Analogsignal ein elektrisches Signal, meistens die elektrische Spannung, seltener Frequenz, Stromstärke oder Ladung. Man kennt aber auch analoge Signale auch aus mechanischen, pneumatischen, hydraulischen und anderen Systemen.

Der Hauptnachteil analoger Signale sind zufällige Variationen, die zwangsläufig auftreten, da kein System störungsfrei ist, und die im Gegensatz zu digitalen Signalen nicht mit Hilfe von Prüfbits korrigiert werden können. Hierbei gilt: je häufiger ein Signal kopiert wird oder je länger der Signalweg, desto stärker wird das Signal vom Rauschen dominiert. Diese Signalverluste und Signalverzerrungen sind unumkehrbar, da eine Verstärkung des Signals zusätzliches **Rauschen** addiert.

Ein **Digitalsignal** (von lat. *digitus* = Finger; mit Fingern wird gezählt!) überträgt eine Information, zum Beispiel eine elektrische Wechselspannung, in Form einer Zahlenkolonne, die die Information mathematisch beschreibt, im Gegensatz zum Analogsignal, das eine physikalische Größe entweder direkt überträgt oder durch eine andere physikalische Größe abbildet.

Zur Umwandlung in ein Digitalsignal muss das analoge Ausgangssignal zunächst zeitlich **quantisiert** werden, das heißt in feste Zeit-Intervalle zerlegt. Beispiel: bei der Aufnahme einer Audio-CD wird jeder Kanal (links/rechts) des Ausgangssignals 44.100-mal pro Sekunde abgetastet. Diese Frequenz von 44,1 kHz bezeichnet man als **Samplingfrequenz** oder **Abtastrate**. Details des Ausgangssignals, die feiner sind als dieses Zeitraster, können nicht erfasst werden.

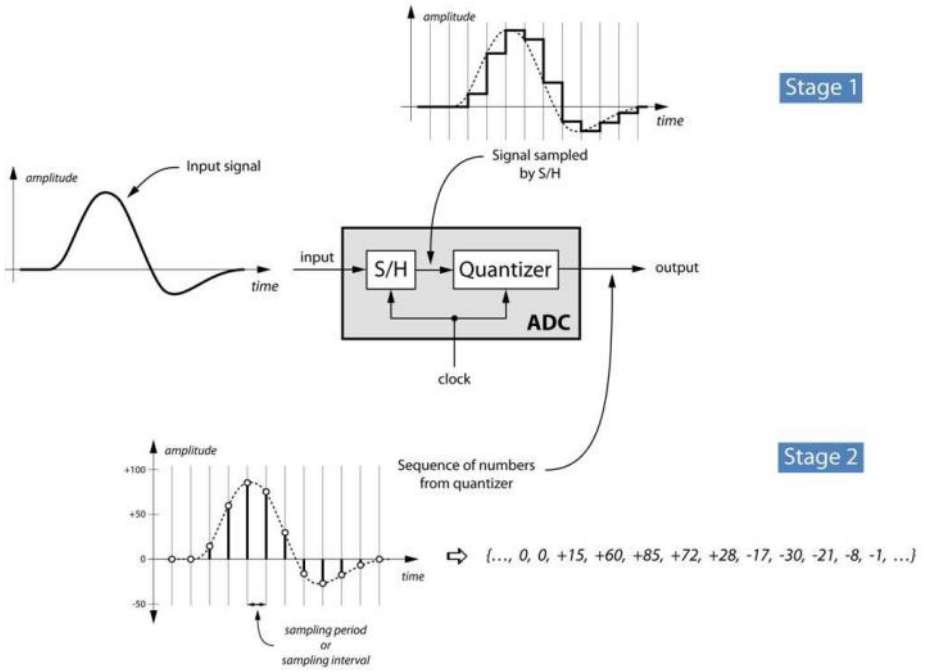


Abbildung: Digitalisierung eines Analogsignals (Quelle: www.nutaq.com)

3.2 Modulation

Für die Übertragung von Informationen mit entsprechender Geschwindigkeit wird die sogenannte **Modulation** verwendet. Das analoge oder digitale Nutzsignal verändert ein sinusförmiges Trägersignal. Geht man von einem analogen Nutzsignal aus, so spricht man von **analoger Modulation**, bei digitalen Nutzsignalen spricht man von **digitaler Modulation**.

Geräte, die Informationen auf eine Trägerfrequenz aufmodulieren und umgekehrt die aufmodulierten Informationen wieder von der Trägerfrequenz trennen können, werden als **Modems** bezeichnet (Modem = Modulator/Demodulator).

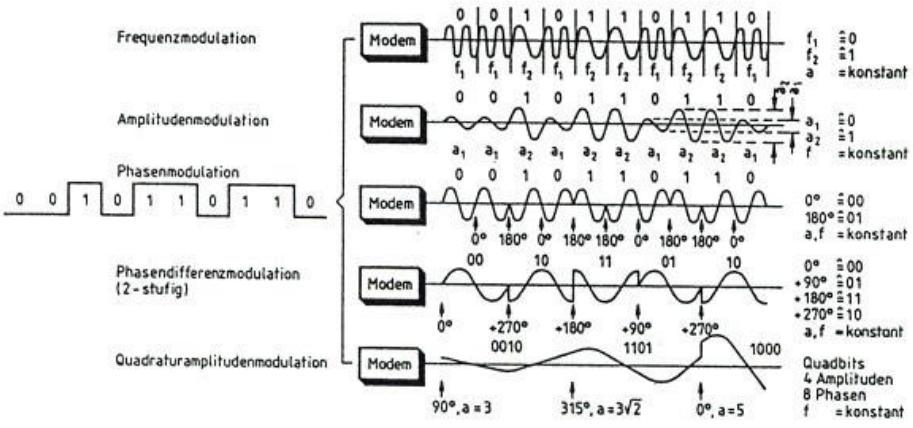
Übersicht

Man unterscheidet mehrere Arten der Modulation:

Bei der **Amplitudenmodulation** (bei digitalen Signalen: ASK = *Amplitude Shift Keying, Amplitudentastung*) wird die Amplitude (Signalspannung) des Signals verändert, das eine konstante Frequenz besitzt. Im einfachsten Fall erfolgt dies durch Ein- und Austasten des Trägers. Die Grundfrequenz des Trägers ist wesentlich höher, als die Anzahl der Austastvorgänge. Es ist das einfachste Verfahren, aber Unterbrechung und Nullbits sind voneinander nicht unterscheidbar.

Bei der **Frequenzmodulation** (bei digitalen Signalen: FSK = *Frequency Shift Keying*, Frequenzumtastung) wird die Frequenz (Tonhöhe) bei einem Signal bei konstanter Amplitude verändert. Den Wertigkeiten "1" und "0" werden zwei verschiedene Frequenzen zugeordnet. Zum Duplexbetrieb werden unterschiedliche Trägerfrequenzen für den Hinweg (Originate) und Rückweg (Answer) verwendet. Eine Unterbrechung (Ausfall des Trägers) ist erkennbar.

Bei der **Phasenmodulation** (bei digitalen Signalen: PSK = *Phase Shift Keying*, Phasen-



umtastung) hat das Signal eine konstante Frequenz. Es werden hier Phasensprünge in die Sinusschwingung "eingebaut". Stellen Sie sich eine Sinusschwingung vor. Ein Phasensprung führt dann zu einer bestimmten Amplitude, die vom Phasenwinkel abhängt, d. h. die Sinuswelle wird in ihrem Schwingungsanfang um den entsprechenden Phasenwinkel verändert. Mit PSK sind hohe Übertragungsraten erreichbar, aber es wenden auch hohe Anforderungen an die Hardware gestellt.

Die **Quadraturamplitudenmodulation** (QAM) kombiniert Frequenz- und Amplitudenmodulation. Sie wird beispielsweise bei DSL-Übertragungen (siehe Internet-Breitbandverbindungen) oder digitaler terrestrischer Fernsehübertragung (DVB-T, DVB-T2) verwendet.

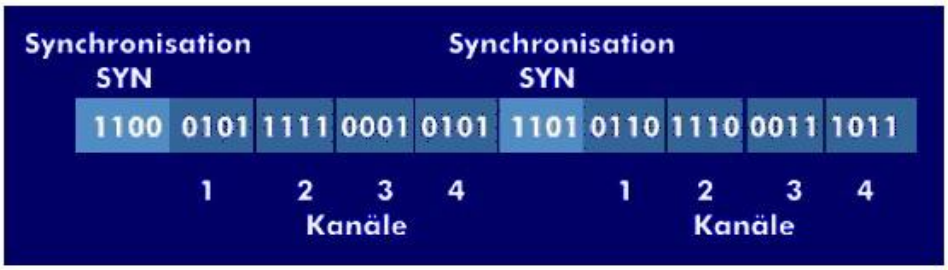
3.3 Multiplexing

Mit Hilfe von Modulation ist es möglich, mehrere Signale „gleichzeitig" auf einer physikalischen Leitung zu übertragen, ohne dass diese Signale einander gegenseitig beeinflussen. Diesen Vorgang bezeichnet man als **Multiplexing**.

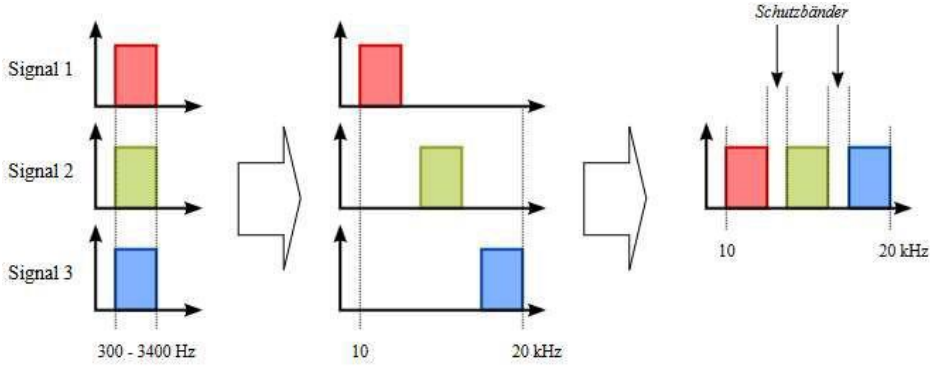
Auf diese Weise können über ein einziges Telefonkabel mehrere Gespräche und auch Daten übertragen werden; auch verschiedene Radiosender oder TV-Sender werden auf ähnliche Weise gleichzeitig übertragen.

- **Raummultiplexverfahren**: Hier verlaufen mehrere Kabeladern parallel; jede Ader wird exklusiv für ein anderes Signal genutzt.
- **Zeit-Multiplexing** (TDM = *time division multiplexing):* Die Daten verschiedener Sender werden in bestimmten „Zeitschlitzen" auf einem Träger übertragen. Man unterscheidet synchrones und asynchrones Zeit-Multiplexing. Beim Synchronverfahren wird ein Übertragungsrahmen verwendet, der aus einem Synchronisationszeichen und einer bestimmten Anzahl von jeweils gleich langen Zeitschlitzen (Kanälen) besteht.
- **Frequenz-Multiplexing** (FDM = *frequency division multiplexing):* Ein verfügbarer Frequenzbereich wird in mehrere Bänder aufgeteilt; über jedes Signal wird dann auf eine eigene Trägerfrequenz aufmoduliert.
- **Codemultiplexverfahren**: Dieses Verfahren wird in der Funktechnik und in Datenbussen eingesetzt.

Verschiedene Signalfolgen werden über eine Leitung oder eine Funkfrequenz übertragen und im Empfänger beziehungsweise mehreren Empfängern anhand ihrer unterschiedlichen Codierung erkannt und zugeordnet. Das Verfahren ähnelt dem Zeitmultiplexverfahren, jedoch ist keine Koordinierung der Zeitfenster erforderlich.



Zeitmultiplex



Frequenzmultiplex (Quelle: Wikipedia)

3.4 Datenübertragungsrate

Die Datenübertragungsrate (umgangssprachlich: Übertragungsgeschwindigkeit) bezeichnet die digitale Datenmenge, die pro Sekunde über einen Übertragungskanal fließen kann.

Die maximal mögliche Datenübertragungsrate, die fehlerfrei über einen Kanal übertragen werden kann, wird als Kanalkapazität bezeichnet. Zusammen mit der Latenzzeit (Antwortverzögerung) ist sie ein Maß für die Leistungsfähigkeit eines Kanals.

Die Datenübertragungsrate wird in **Bit pro Sekunde** bzw. einem Vielfachen davon angegeben.

Anmerkung: Manchmal findet man auch Angaben zur Schrittgeschwindigkeit, die in der Einheit **Baud** (benannt nach Émile Baudot, französischer Erfinder des 5-Bit-Baudot-Codes, der in der Frühzeit der Telekommunikation für Telegrafenanlagen verwendet wurde) angegeben wird. 1 Baud bezeichnet die Schrittgeschwin- Servbus, fdigkeit 1

Symbol pro Sekunde, wobei aber in einem Symbol mehrere bit Nutzdaten enthalten sein können. Überträgt man nun 2 Bit pro Takt (etwa durch die Zuordnung: **00** = 0 Volt, **01** = 5 Volt, **10** = 10 Volt, **11** = 15 Volt), so ist die Anzahl der Bit/Sekunde doppelt so hoch wie die Baud-Rate. 1000Base-T(Gigabit-Ethernet) hat eine Schrittgeschwindigkeit von 125 MBaud; pro Takt werden 2 Bit Nutzdaten übertragen; außerdem werden 4 Adernpaare gleichzeitig verwendet. Die Datenübertragungsrate beträgt daher

$$125 \cdot 10^6 \cdot 2 \cdot 4 \frac{bit}{s} = 10^9 \frac{bit}{s} = 1 \frac{Gbit}{s}$$

3.5 Störeinflüsse

Optimalerweise sollten die eingespeisten Signale unverändert beim Empfänger ankommen. Das ist jedoch nicht der Fall, da es **Störeinflüsse** gibt:

- **Störungen durch äußere elektromagnetische Felder**: Alle Leitungen und Geräte, durch die elektrischer Strom fließt, bauen ein Magnetfeld auf – dieses Phänomen wird als Elektromagnetismus bezeichnet. Verlaufen nun Netzwerkkabel durch sich ändernde magnetische Felder, so kommt es im Netzwerkkabel zur Entstehung von Induktionsspannungen, die das Signal verändern.
- **Störungen durch den Widerstand des Kabels selbst**

Diese Störeinflüsse bewirken Verluste.

3.5.1 Dämpfung (engl. attenuation, ATT)

Das Ausmaß des Signalverlusts wird als **Dämpfung** bezeichnet. Meist wird die Dämpfung als **Pegelgröße** in der physikalischen Einheit **Dezibel** (dB) angegeben, das bedeutet, dass man das Verhältnis Ausgangsgröße zu Eingangsgröße noch dekadisch logarithmiert (vereinfacht gesagt: Man nimmt von einer Zehnerpotenz nur den Exponenten; beispielsweise gilt: $lg10^4 = 4$).

Leistungsdämpfung

$$A_p = 10 \cdot \lg \frac{P_{Sender}}{P_{Empfänger}}$$

P_{Sender}...Leistung, die vom Sender ausgesandt wird, in Watt (W)

$P_{Empfänger}$... Leistung, die beim Empfänger ankommt, in Watt (W)

Spannungsdämpfung

$$A_u = 20 \cdot \lg \frac{U_{Sender}}{U_{Empfänger}}$$

U_{Sender}...Spannung, die vom Sender ausgesandt wird, in Volt (V)

$U_{Empfänger}$... Spannung, die beim Empfänger ankommt, in Volt (V)

Beispielwerte:

- Eine Dämpfung von 6 dB entspricht einem Signalverlust von 50%.
- Eine Dämpfung von 20 dB entspricht einem Signalverlust von 90%.

Die Dämpfung ist grundsätzlich abhängig von:

- Länge des Kabels
- Frequenz des übertragenen Signals

Bei Netzwerkkabeln wird die Dämpfung oft auf die Leitungslänge bezogen. Je geringer die Dämpfung, desto größer die maximal mögliche Leitungslänge.

Um eine korrekte Dämpfungsmessung durchzuführen, muss daher die Leitungslänge gemessen werden. Die Messung der Leitungslänge kann über eine Laufzeitmessung durchgeführt werden. Man sendet ein Signal in das Kabel, welches am Kabelende reflektiert wird, und misst die Zeitspanne, die vergeht, bis das reflektierte Signal empfangen wird.

$$c = \frac{2 \cdot l}{t} \Rightarrow c. \frac{t}{2}$$

Dabei bedeutet:

c...Signalausbreitungsgeschwindigkeit, auch **NVP** *(nominal velocity of propagation);* diese wird in % der Lichtgeschwindigkeit ($c_{Licht} = 3 \cdot 10^8$ m/s) angegeben und ist aus dem Datenblatt des Kabelherstellers ersichtlich. Übliche Werte sind 0,65 – 0,80 (also 65 % bis 80 % der Lichtgeschwindigkeit).

t/2...halbe Laufzeit (das Signal muss ja hin und her laufen)

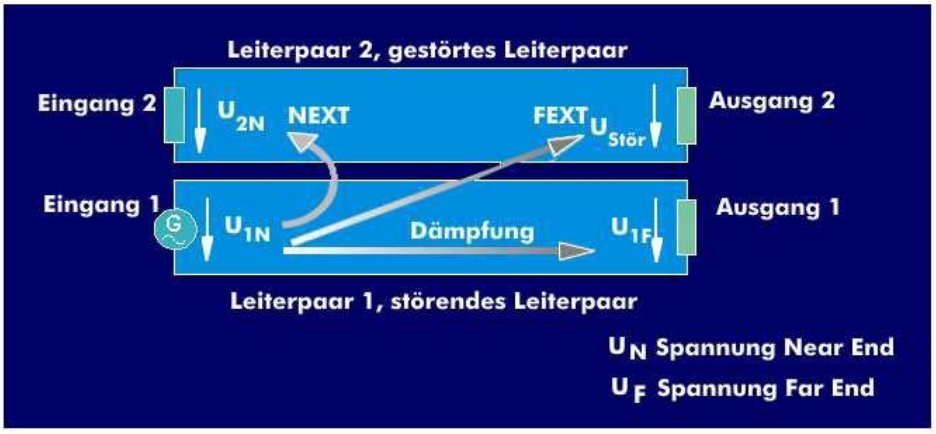
l...Kabellänge

Natürlich ist eine geringe Dämpfung gewünscht. Cat.5 nach ISO 11801 schreibt eine maximale Dämpfung von 24 dB vor.

3.5.2 Nebensprechen (Crosstalk)

Das Nebensprechen entsteht durch induktive Beeinflussung zweier parallel laufender Leitungen.

- **NEXT** *(Near End Cross-Talk)* = Nah-Nebensprechen: Hierbei wird, im Gegensatz zu NEXT, das Übersprechen von einem Aderpaar auf die anderen am fernen Ende gemessen. Anders als NEXT kann FEXT richtungsabhängig sein, darum gibt es für jedes Ende der gemessenen Verbindung 12 Messwerte (Paarkombinationen), insgesamt also 24.



Nah– und Fernübersprechen (Quelle: www.itwissen.info)

- **FEXT** *(Far End Cross-Talk)* = Fern-Nebensprechen: Hierbei wird, im Gegensatz zu NEXT, das Übersprechen von einem Aderpaar auf die anderen am fernen Ende gemessen. Anders als NEXT kann FEXT richtungsabhängig sein, darum gibt es für jedes Ende der gemessenen Verbindung 12 Messwerte (Paarkombinationen), insgesamt also 24.
- **ELFEXT** *(Equal Level Far End Cross-Talk):* Da für den Signalempfang natürlich der Störabstand entscheidend ist und das Signal am anderen Ende gedämpft ankommt, bezieht man den gemessenen FEXT-Wert nicht auf das Sendesignal in seiner Originalstärke, sondern auf den Empfangspegel. ELFEXT ist also ein errechneter Wert, der aus der Subtraktion der Dämpfung vom gemessenen FEXT entsteht und in dB angegeben wird.
- **AXT** *(Alien Crosstalk):* Darunter versteht man die Störung des übertragenen Signals durch äußere Felder. Alien Crosstalk tritt vor allem zwischen direkt benachbarten Datenkabeln sowie in Steckverbindern auf macht sich als elektromagnetisches Rauschen bemerkbar. Eine Reduzierung des Alien Crosstalk ist nur über mechanische Maßnahmen möglich. Dabei spielt die Bündelung und die parallele Verlegung von Datenkabeln eine Rolle, die vermieden werden sollten. Auch durch den Kabelaufbau, den Abstand der Datenkabel zueinander und die Schirmung kann das Fremdnebensprechen reduziert werden. Je nachdem, ob sich das Fremdnebensprechen auf das nahe oder ferne Kabelende bezieht, spricht man von Alien-NEXT und von Alien-FEXT. Die Grenzwerte dieser beiden Parameter sind in den Verkabelungsstandards festgelegt.

Bei Gigabit-Ethernet-Übertragungen über Kupferleitungen (1000Base-T) wird auf allen vier Aderpaaren gleichzeitig in beide Richtungen gesendet und empfangen. Das auf jedem einzelnen Paar empfangene Signal kann also von den Signalen gestört werden, die gleichzeitig auf drei anderen Paaren übertragen werden. Das heißt, die Störungen, die von den drei anderen Paaren im Kabel verursacht werden, addieren sich. Daher spielen bei Gigabit-Ethernet auch die sogenannten **Powersum-Werte** eine Rolle. Der Unterschied zwischen den Einzelwerten und den Powersum-Werten beträgt stets 3 dB.

- **PS-NEXT** *(Powersum Near End Cross Talk* - Summe Nahnebensprechdämpfungen)
- **PS-FEXT** *(Powersum Far End Cross Talk)*
- **PS-ELFEXT** *(Powersum Equal Level Far End Cross Talk)*

3.5.3 Übersprechdämpfung

ACR *(Attenuation to Crosstalk Ratio,* auch: Übersprechdämpfung): Diese Größe gibt das Verhältnis der Kabeldämpfung insgesamt zum Nahnebensprechanteil an.

$$ACR = NEXT - Kabeldämpfung$$

Der ACR-Wert drückt die Qualität eines Kabels aus. Je höher der Wert, umso höher ist die Qualität des Kabels (bezogen auf die Frequenz).

Der ACR-Wert ist frequenzabhängig: der NEXT-Wert wird mit steigender Frequenz kleiner, die Kabeldämpfung wird mit steigender Frequenz größer. Der ACR-Wert sinkt also mit steigender Frequenz. Ist der ACR-Wert kleiner als 3, so ist keine Datenübertragung mehr möglich.

Beispiel: Ein UTP-Kabel hat eine Kabeldämpfung von 19 dB und einen NEXT-Wert von 82 dB. Der ACR-Wert dieses Kabels beträgt daher

$$ACR = 82\ dB — 19\ dB = 63\ dB$$

Ein anderes UTP-Kabel mit einem ACR von 50 dB wäre von schlechterer Qualität.

PS-ACR *(Powersum Attenuation to Crosstalk Ratio* - Summe Signal-Störabstand): Differenz aus Dämpfung und PS-NEXT eines Paares.

3.5.4 Impedanz

Jeder Leiter weist einen bestimmten **elektrischen Widerstand** auf, den in Ohm Ω gemessen wird. Dieser elektrische Widerstand setzt sich in Wechselstromkreisen aus drei Teilen zusammen:

OHMscher Widerstand R (auch: Gleichstromwiderstand): Dieser Widerstand entsteht durch die Behinderung der Elektronen durch das Metallgitter des Kabels. Er ist verantwortlich dafür, dass sich das Kabel erwärmt, wenn Strom durchfließt. Er ist abhängig vom Kabelmaterial, vom Kabelquerschnitt und der Kabellänge

$$R = \rho . \frac{l}{A}$$

Der Gleichstromwiderstand bei Datenkabeln liegt – abhängig von Leiterquerschnitt und Kupferqualität bei etwa $50 - 100\ \Omega/\mathrm{km}$.

Induktiver Widerstand XL: Dieser Widerstand entsteht durch den ständigen Auf- und Abbau magnetischer Felder und ist abhängig von der Geometrie des Drahtes (eine Spule, also ein gewickelter Draht, mit vielen Windungen hat einen größeren induktiven Widerstand als ein gerades Drahtstück) und der Frequenz der Wechselspannung. Es gilt:

$$X_L = \omega \cdot L = 2 \cdot \pi \cdot f \cdot L$$

L ... Induktivität in Henry

f ... Frequenz in Hertz

Der Induktivitätsbelag von Kabeln wird in der Einheit H/km (Henry pro Kilometer) angegeben. Bei Datenkabeln liegt der Induktivitätsbelag im Millihenry-Bereich ($1\,\mathrm{mH} = 10^{-3}$ H).

Kapazitiver Widerstand *Xc*: Dieser Widerstand entsteht durch den Auf- und Abbau elektrischer Felder, vor allem an den Kabelenden. Es gilt:

$$X_C = \frac{1}{\omega \cdot C} = \frac{1}{2 \cdot \pi \cdot f \cdot LC}$$

C... Kapazität in Farad

f ... Frequenz in Hertz

Der Kapazitätsbelag von Kabeln wird in der Einheit F/km (Farad pro Kilometer) angegeben. Bei Datenkabeln liegt der Kapazitätsbelag im Nanofarad-Bereich ($1\ \mathrm{nF} = 10^{-9}$ F)).

Der Gesamtwiderstand (auch: Wellenwiderstand) wird als Impedanz Z bezeichnet. Sie lässt sich leider nicht als Summe berechnen, sondern mit der relativ komplizierten Formel

$$Z = \sqrt{R^2 + (X_L - X_c)^2} = \sqrt{R^2 + (\omega L - \frac{1}{\omega C})^2}$$

Auch die Impedanz wird in Ohm angegeben. Die Impedanz von Datenkabeln beträgt in der Regel 100 Ω ± 15 % bei 100 MHz.

Ein Netzwerkkabel wirkt als sogenanntes Tiefpassfilter, es lässt tiefe Frequenzen durch und unterdrückt höhere Frequenzen.

RL (Return Loss – Rückflussdämpfung) und **SRL (Structural Return Loss)**: Impedanzschwankungen entlang der Verbindung führen zu Signalreflexionen, die einerseits das zum anderen Ende gelangende Signal schwächen (Anteile, die reflektiert werden, dringen nicht bis zur anderen Seite durch), andererseits aber auch vom anderen Ende ankommende, entsprechend gedämpfte Signale stören könnten.

Die Rückflussdämpfung wird von beiden Seiten aus gemessen und in dB angegeben. Je größer der Zahlenwert, umso besser. Hinweis: RL-Werte unter 3 dB werden nur informativ angegeben.

Der Unterschied bei der Messung von RL und SRL ist, dass bei SRL das andere Ende mit einem 100 Ohm Widerstand abgeschlossen wird.

3.5.5 Skew Delay

Darunter versteht man den Unterschied zwischen den Signallaufzeiten in den einzelnen Adernpaaren eines Twisted Pair-Kupferkabels. Der Laufzeitunterschied resultiert aus der unterschiedlichen Verdrillung der einzelnen Kabelpaare. Der Wert wird in Nanosekunden (1 ns = 10^{-9} s) pro 100 m Kabelstrecke angegeben und liegt bei Cat 5e-Kabeln unter 50 ns/100 m; bei Cat 6/7-Kabeln liegt der Wert unter 20 ns/100 m.

Übertriebene Darstellung der unterschiedlichen Verdrillungen der Kabelpaare eines Twisted Pair-Kupferkabels (Quelle: www.siemon.com)

3.5.6 Rauschen

Bedingt durch die Wärmebewegung der Elektronen entsteht in jedem elektrischen Leiter ein Störstrom, der zufallsbehaftet ist. Macht man diese Stromschwankungen durch Verstärkung über einen Lautsprecher hörbar, so erklingt ein typisches Geräusch, das dem Phänomen den Namen gab.

Wärmerauschen ist von der Art her näherungsweise ein „weißes Rauschen", d.h. es werden alle möglichen Frequenzen gleich stark abgegeben.

Für die Signalübertragung bedeutet das, dass jedes Nutzsignal mit einem Rausch-Störsignal überlagert wird.

Die maximale Kanalkapazität, die erreicht werden kann, wenn man weißes Rauschen als Störfaktor berücksichtigt, lässt sich mit dem SHANNON-HARTLEY-Gesetz berechnen:

$$C = (f_{\max} - f_{\min}).\lg_2(1 + SNR) = (f_{\max} - f_{\min}).\frac{\ln(1 + SNR)}{\ln 2}$$

Dabei bedeutet:

f_{max}-f_{min}...Bandbreite in Hz

SNR...Signal-Rausch-Verhältnis (auch: Störabstand); gibt an, in welchem Verhältnis das Nutzsignal zum weißen Rauschen steht. Je geringer diese Zahl, umso schlechter hebt sich das Signal vom Hintergrundrauschen an; bei digitaler Übertragung steigt die Fehlerrate. Für einen Menschen ist in einem verrauschten Signal mindestens eine SNR von 6 dB nötig, um Sprache erkennen zu können.

Rechenbeispiel für VDSL2: VDSL2 benutzt 4096 Kanäle mit einer Bandbreite von jeweils 4,3125 kHz, die gesamte Bandbreite beträgt daher 17664 kHz. Wir nehmen an, dass wir eine gute SNR von 20 dB auf unserer Leitung erreichen können (muss gemessen werden).

$$C = 17664kHz \cdot \frac{\ln(1+30)}{\ln 2} = 77590\frac{kbit}{s}$$

Wir können also mit knapp 80 Mbit/s rechnen.

3.5.7 Grenzwerte für Datenkabel

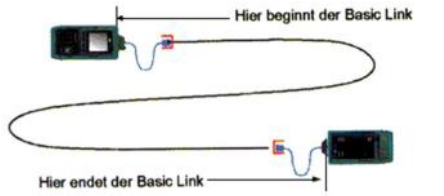
Die in der Folge angegebenen minimal erforderlichen Grenzwerte beziehen sich auf die Norm EN 50173-1; sie sind stets für die in der ersten Zeile angegebene Frequenz zu betrachten. Heute erhältliche Datenkabel haben

meist wesentlich bessere Werte, die in den entsprechenden Datenblättern des Herstellers angegeben sind und durch konkrete Kabelmessungen überprüft werden müssen.

3.5.8 Messen von Netzwerkverkabelungen und Netzwerkdosen

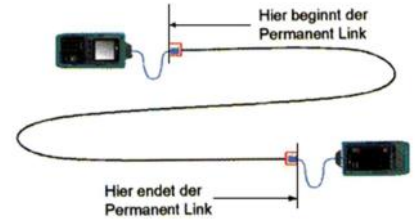
Für die Überprüfung der Funktionstüchtigkeit von Netzwerkverkabelungen gibt es Messgeräte, die mehrere Tests durchführen und dabei die besprochenen Kenngrößen wie Impedanz, Dämpfung, Nebensprechverhalten etc. messen.

- **Basic Link-Messung:** Die Basic-Link-Messung schließt die Einflüsse der Messkabel mit ein. Diese Art der Messung führt zu fehlerhaften Ergebnissen und wird daher heute nicht mehr verwendet.



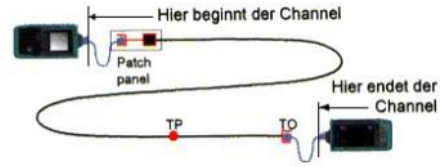
Grafik: www.netzmafia.de

- **Permanent Link-Messung:** Hier darf der Einfluss der Messkabel nicht in die Messwerte eingehen. Damit belegt der Installateur seinem Auftraggeber die Funktion genau der Strecke, die er installiert hat, üblicherweise das fest verlegte Kabel inklusive der Dosen an beiden Enden.



Grafik: www.netzmafia.de

- **Channel Link-Messung:** Bei dieser Messung wird der gesamte Übertragungsweg, über den die Netzkommunikation läuft, erfasst, also auch die Patchkabel. Nicht in den Messwerten niederschlagen dürfen sich nach der normgemäßen Channel-Definition die Anteile der letzten Steckverbinder, mit denen die Patchkabel an die Messgeräte angeschlossen werden.



Grafik: www.netzmafia.de

	Cat 5e	Cat 6	Cat 7
Frequenz	100 MHz	250 MHz	600 MHz
Dämpfung (ATT)	24 dB	35,9 dB	54,6 dB
Impedanz bei 100 MHz	100 Ω ± 15 %	100 Ω ± 15 %	100 Ω ± 15 %
NEXT	30,1 dB	33,1 dB	51,2 dB
PS-NEXT	27,1 dB	30,2 dB	48,2 dB
ELFEXT	17,4 dB	15,3 dB	31,3 dB
PS-ELFEXT	14,4 dB	12,3 dB	28,3 dB
Return Loss	10 dB	8 dB	8 dB
ACR	6,1 dB	-2,8 dB	-3,4 dB

Grafik: www.flukenetworks.com

Beispiele für Netzwerktester

Bild: links Fluke DXS-5000 CableAnalyzer zur Zertifizierung von Kupferkabeln; rechts Fluke Certifiber Pro zur Messung der Dämpfung in Glasfaserkabeln (Foto: Fluke)

IDEAL Networks SignalTEK II FO, Kabeltester für Kupfer- und Glasfaserkabel (Foto: www.conrad.at)

Prüfprotokoll Netzwerkkabel (CAT5) – bestandener Test

Kabelkennung: 06-16B
ELEKTRO XXXXXXXXXX GMBH
ORT: 3100 ST.PöLTEN
BEDIENER: ZAHLER
Standard-Version: 2.51
Software-Version: 2.5
NVP: 69,9% FEHLERANOMALIESCHWELLE: 15%
TEST DER KABELSCHIRMUNG: Aktivieren

Testzusammenfassung: PASS
RESERVE: 7,7 dB (NEXT @ Remote 45-78)
Datum/Uhrzeit: 10.02.2000 18:05:12
Test-Standard: TIA Cat 5 Basic Link
Kabeltyp: ScTP 100 Ohm Cat 5
FLUKE DSP-4000 Serien-Nr.: 7420098 LIA011
FLUKE DSP-4000SR Serien-Nr.: 7420098 LIA011

Wire Map PASS Ergebn. RJ45-STIFT: 1 2 3 4 5 6 7 8 S
| | | | | | | | |
RJ45-STIFT: 1 2 3 4 5 6 7 8 S

	Länge		Laufzeit		Laufzeit Differenz		Widerstand		Impedanz			Dämpfung		
Paar	(m)	Grnz.	ns	Grnz.	ns	Grnz.	Ohm	Grnz.	Ohm	Grnz.	Anom. (m)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)
12	52,2	94,0	249		0	50			113	80-120		10,0	100,0	21,6
36	52,8	94,0	252		3	50			112	80-120		10,3	100,0	21,6
45	52,8	94,0	252		3	50			111	80-120		10,7	100,0	21,6
78	53,4	94,0	255		6	50			106	80-120		10,9	100,0	21,6

	Ergebnisse der Haupteinheit						Ergebnisse der Remote-Einheit					
	geringster Abstand			Min. Wert			geringster Abstand			Min. Wert		
Paar	Ergebn. (dB)	Freq. MHz	Grnz. (dB)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)
NEXT												
12-36	41,0	61,8	32,8	40,6	70,8	31,8	42,7	59,2	33,0	39,9	97,8	29,5
12-45	51,9	25,2	39,1	48,2	67,0	32,2	48,5	44,2	35,1	47,3	72,4	31,7
12-78	47,7	59,8	33,0	47,2	72,2	31,7	47,1	60,0	32,9	45,5	96,2	29,6
36-45	38,9	95,4	29,7	38,9	95,4	29,7	44,5	42,0	35,5	39,2	99,6	29,3
36-78	60,3	7,8	47,3	44,4	93,4	29,8	60,0	7,7	47,4	46,1	94,4	29,7
45-78	54,7	10,0	45,6	43,5	89,8	30,1	51,6	12,7	43,9	41,8	85,0	30,5

Prüfprotokoll Netzwerkkabel (CAT5) – nicht bestandener Test

Kabelkennung: 06-19A
ELEKTRO XXXXXXXXXX GMBH
ORT: 3100 ST.PöLTEN
BEDIENER: ZAHLER
Standard-Version: 2.51
Software-Version: 2.5
NVP: 69,9% FEHLERANOMALIESCHWELLE: 15%
TEST DER KABELSCHIRMUNG: Aktivieren

Testzusammenfassung: FAIL
RESERVE: 9,8 dB (NEXT 12-36)
Datum/Uhrzeit: 10.02.2000 18:41:45
Test-Standard: TIA Cat 5 Basic Link
Kabeltyp: ScTP 100 Ohm Cat 5
FLUKE DSP-4000 Serien-Nr.: 7420098 LIA011
FLUKE DSP-4000SR Serien-Nr.: 7420098 LIA011

Wire Map PASS Ergebn. RJ45-STIFT: 1 2 3 4 5 6 7 8 S
| | | | | | | | |
RJ45-STIFT: 1 2 3 4 5 6 7 8 S

	Länge		Laufzeit		Laufzeit Differenz		Widerstand		Impedanz			Dämpfung		
Paar	(m)	Grnz.	ns	Grnz.	ns	Grnz.	Ohm	Grnz.	Ohm	Grnz.	Anom. (m)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)
12	50,9	94,0	243		0	50			112	80-120		6,2 F	2,3	3,0
36	51,8	94,0	247		4	50			110	80-120		6,2 F	2,3	3,0
45	51,1	94,0	244		1	50			110	80-120		6,3 F	2,4	3,1
78	52,2	94,0	249		6	50			108	80-120		6,3 F	2,3	3,0

	Ergebnisse der Haupteinheit						Ergebnisse der Remote-Einheit					
	geringster Abstand			Min. Wert			geringster Abstand			Min. Wert		
Paar	Ergebn. (dB)	Freq. MHz	Grnz. (dB)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)	Ergebn. (dB)	Freq. MHz	Grnz. (dB)
NEXT												
12-36	43,7	52,8	33,9	39,9	94,2	29,8	47,4	32,8	37,2	45,8	93,6	29,8
12-45	51,2	57,8	33,2	49,4	91,2	30,0	51,6	59,8	33,0	49,4	95,8	29,6
12-78	52,9	52,6	33,9	50,4	78,2	31,0	54,6	38,0	36,2	50,5	90,4	30,1
36-45	41,1	99,8	29,3	41,1	99,8	29,3	49,2	34,6	36,8	42,1	96,0	29,6
36-78	45,1	54,4	33,7	44,2	96,8	29,5	53,1	20,6	40,5	49,1	83,6	30,6
45-78	52,6	21,2	40,3	44,5	73,2	31,6	46,7	55,4	33,6	44,9	82,6	30,7

4 Netzwerk-Hardware und Verkabelung

Wir beginnen mit der „technischen“ Seite der Datenübertragung in einem Netzwerk, die im OSI-Modell die Schichten 1 und 2 umfasst.

Mit der Normung der verschiedenen Netzwerktechnologien auf den OSI-Schichten 1 und 2 beschäftigt sich die **Arbeitsgruppe 802** des *Institute for Electric and Electronic Engineers* (IEEE). Die entsprechenden Normungsvorschläge werden daher als 802.x-Normen bezeichnet.

Aus obiger Abbildung ist ersichtlich, welche Technologien der Schichten 1 und 2 aktuell sind: am bedeutendsten ist sicher **Ethernet**, die bei PC-Netzwerken standardmäßig verwendete Technologie.

4.1 Ethernet

Ende 1972 implementierte Dr. Robert Metcalfe mit seinen Kollegen am Xerox Palo Alto Research Center ein Netzwerk, um einige Xerox-Alto-Rechner zu vernetzen – einen zu dieser Zeit revolutionären Vorläufer der Personal Computer. Zunächst als **Alto Aloha Network** bezeichnet, setzte dieses Netzwerk bereits das CSMA/CD-Protokoll des späteren Ethernet ein. Die Übertragungsfrequenz lag jedoch zunächst nur bei 2,94 MHz, dem Systemtakt der Alto-Stations. Erst 1976 nannte Metcalfe das Netzwerk Ethernet.

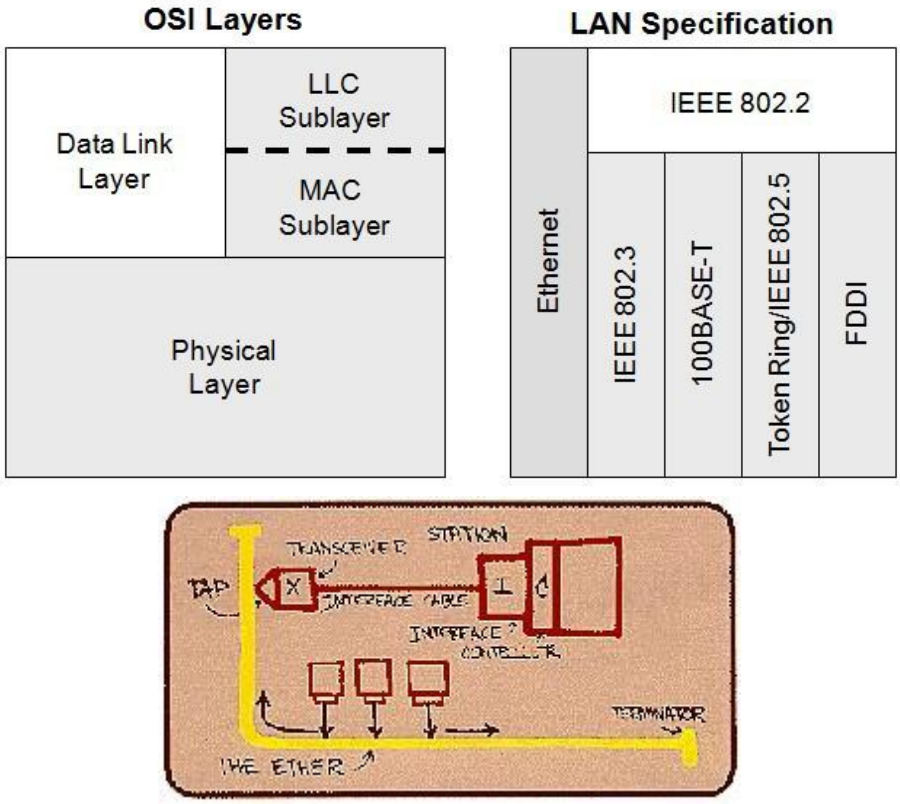
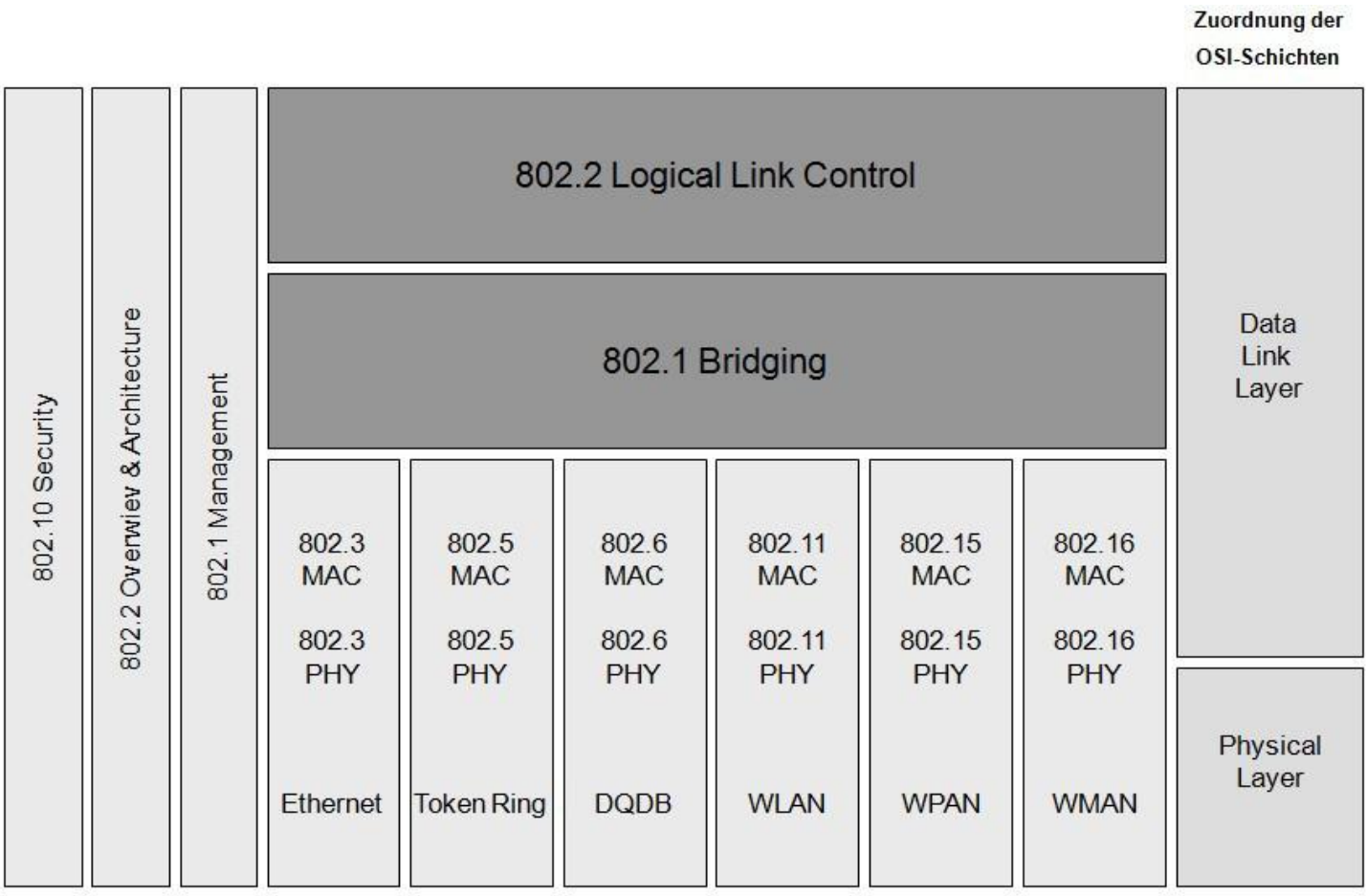


Abbildung: Schemazeichnung von Dr. Robert Metcalfe (Quelle: www.tecchannel.de)



4.1.1 Medienzugriffsverfahren von Ethernet – CSMA/CD

Ethernet verwendet das **CSMA/CD-Verfahren** = *Carrier Sense Multiple Access/ Collision Detection*.

- *Carrier Sense:* Vor dem Senden wird überprüft, ob das Medium (Buskabel) frei ist.
- *Multiple Access:* Mehrere Stationen dürfen gleichzeitig auf den Kanal (das Kabel) zugreifen.
- *Collision Detection:* Kollisionserkennung

EtherNet arbeitet mit dem CSMA/CD-Zugriffsverfahren *(carrier sense multiple access with collision detection* = Kollisionserkennung). Das bedeutet für den sendewilligen Rechner „erst hören" *(carrier sense)*, dann „auf das Medium zugreifen und senden" (multiple access) und Konflikte (gleichzeitiges Senden mehrerer Stationen) „erkennen" *(with collision detection)* und korrigieren. Alle Rechner sind hier an ein einziges Kabel gebunden (Bustopologie). Wollen nun zwei Rechner gleichzeitig Daten abschicken, so kommt es zu einer Kollision; ein Jam-Signal wird an alle beteiligten Stationen übermittelt. Alle an der Kollision beteiligten Geräte stoppen sofort ihre Bemühungen und warten eine zufällig bestimmte Zeit, ehe sie einen neuen Übertragungsversuch starten.

Das CSMA/CD-Verfahren ist ein **"nicht deterministisches Medienzugriffsverfahren"** (übersetzt heißt dies in etwa: "nicht zielorientiert", da Kollisionen bei diesem Verfahren ja weder vorhergesehen noch vermieden werden können).

4.1.2 MAC-Adresse

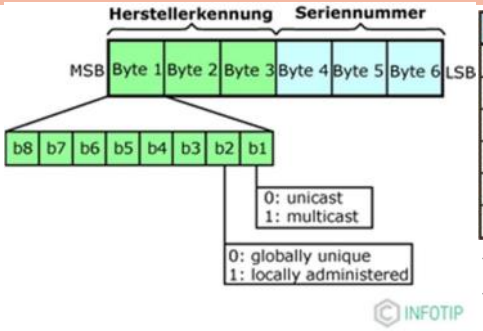
Alle Netzwerktypen und -topologien benutzen Hardware-Adressen, um die Datenpakete zu adressieren. Jede Netzwerkkarte besitzt eine einzigartige und eindeutige Hardware-Adresse, die früher fest auf der Karte eingebrannt war, die **Media Access Control-Adresse** oder kurz **MAC-Adresse**. In Ethernet-Netzwerken ist diese Adresse meist eine 48 bit-Binärzahl, die als 6 hexadezimal angegebenen Bytes angeschrieben wird.

Anmerkung: Das gilt natürlich auch für WLAN-Karten. Heute befindet sich die MAC-Adresse auf einem

EEPROM-Chip, der mit speziellen Mitteln umprogrammierbar ist. Diese Möglichkeit ist auch eine Schwachstelle, die für betrügerische Aktivität oder das Eindringen in Netzwerke genutzt werden kann.

Eine Ethernet-MAC-Adresse besteht aus zwei Teilen:

- Die ersten 3 Byte stellen einen Herstellercode dar (OUI, *organizationally unique identifier)*, wobei manche Hersteller über mehrere Codes verfügen.
- Die letzten 3 Byte stellen eine Seriennummer dar, die vom Hersteller während der Produktion als laufende Nummer vergeben wird.



OUI	Hersteller
00-03-93-xx-xx-xx	Apple Computer
00-60-2F-xx-xx-xx	Cisco
00-0B-3B-xx-xx-xx	devolo
00-0F-66-xx-xx-xx	Linksys
00-09-82 -xx-xx-xx	Loewe Opta GmbH
00-1C-EE-xx-xx-xx	Sharp

Grafiken: www.infotip.de

```
C:\> ipconfig /all
[…]
Ethernet-Adapter Ethernet: Verbindungsspezifisches DNS-Suffix:
Beschreibung. . . . . . . . . . . : Realtek PCIe GBE Family Controller
Physische Adresse . . . . . . . . : D4-3D-7E-4B-7A-1A
```

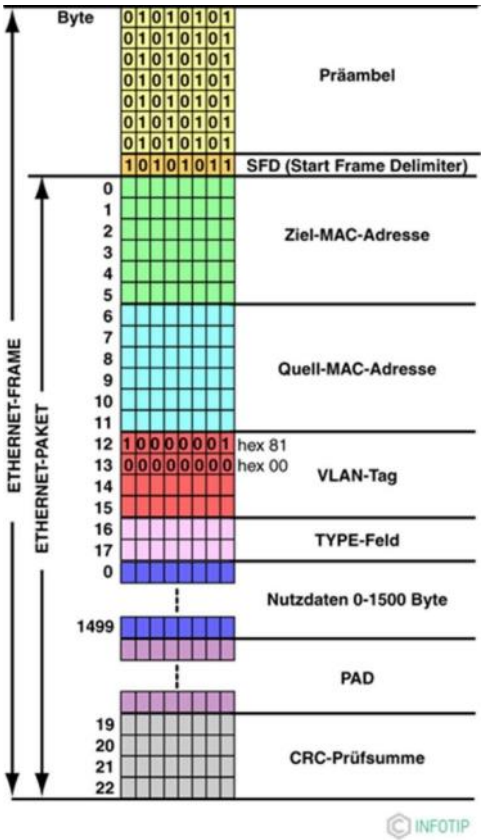
Feststellen der MAC-Adresse Ihrer Netzwerkkarte: Verwenden Sie in der Command Shell den Befehl `ipconfig /all`. Bei den Netzwerkadaptern suchen Sie die Zeile „Physische Adresse".

4.1.3 Ethernet-Frames

Netzwerksniffer analysieren Pakete ab der OSI-Schicht 2. Pakete auf OSI-Schicht 2 werden auch als **Frames (Rahmen)** bezeichnet. Je nach verwendeter Netzwerktechnologie sind Frames unterschiedlich aufgebaut.

Aufbau eines Ethernet II-Frames (Bild unten, Grafik: www.infotip.de):

- **Präambel (8 Byte):** besteht aus einem 7 Byte langem Synchronisationsteil (binär 1010101010 1010101010 1010101010 1010101010 1010101010 1010101010 1010101010) und einem 1 Byte langem *„Start Frame Delimiter"* (binär 10101011)



- **Ziel-MAC-Adresse (6 Byte):** Die Adresse des Netzwerkadapters, an den der Rahmen gesendet werden soll. Diese Adresse kann auch eine Gruppe von Netzwerkadaptern bezeichnen.
- **Quell-MAC-Adresse (6 Byte):** Die Adresse des Netzwerkadapters, von dem der Rahmen stammt.
- **VLAN-Tag (optional; 4 Byte):** Ein VLAN-Tag ist nur in Tagged-MAC-Frames enthalten. Die ersten beiden Bytes in diesem Feld enthalten ein fixes Kennzeichen (0x8100) als Markierung. In den nächsten zwei Bytes stehen die VLAN-Priority (3 Bit) und die VLAN-ID (12 Bit).
- **Typ (2 Byte, auch ETYPE, nur bei Ethernet_II-Frames):** Jede OSI-Schicht muss eine Information darüber bereitstellen, welches Protokoll in der darüberliegenden OSI-Schicht weiterarbeiten soll. In einem LAN-Header der OSI-Schicht 2 muss daher angegeben werden, welches OSI Schicht 3-Protokoll „übernehmen" und weitermachen soll.

```
ETYPE  Protokoll
0x0800 Internet Protocol, Version 4 (IPv4)
0x0806 Address Resolution Protocol (ARP)
0x8035 Reverse Address Resolution Protocol
(RARP)
0x809B AppleTalk (EtherTalk)
0x80F3 Appletalk Address Resolution Proto-
col (AARP)
0x8100 VLAN Tag (VLAN)
0x8137 Novell IPX (alt)
0x8138 Novell
0x86DD Internet Protocol, Version 6 (IPv6)
```

- **Nutzdaten:** Die gesendeten Informationen (oder ein Teil davon). Die erlaubte Gesamtlänge von Ethernet-Frames (MTU, maximum transfer unit) liegt zwischen 64 Byte und 1518 Byte; daraus ergibt sich auch die maximal mögliche Menge an übertragbaren Nutzdaten mit 1500 Byte.
- **PAD:** Ethernet-Frames, die kürzer als 64 Byte sind, werden hier auf die minimale Framegröße mit Füllbytes aufgefüllt.
- **CRC-Prüfsumme:** 32-Bit-Prüfsumme des ganzen Frames von der Ziel-MAC-

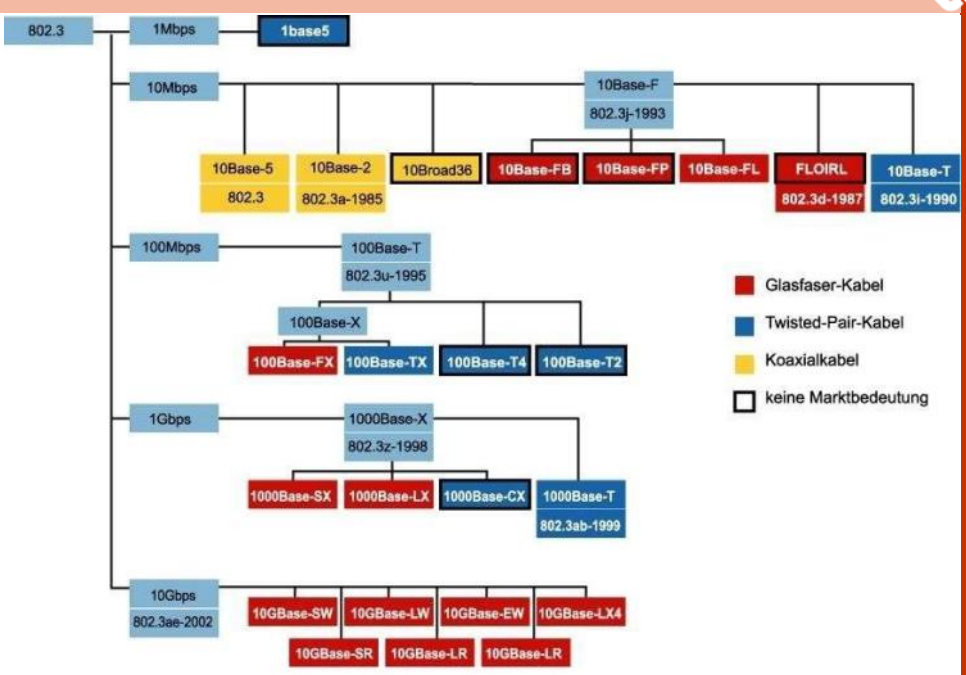
Adresse bis einschließlich dem PAD-Feld.

4.1.4 Ethernet-Verkabelungstopologien und -Normen

Logische Topologie aller Ethernet-Netzwerke: Bus-Topologie Physikalische Topologien:

- Bus-Topologie (veraltet)
- Stern-Topologie

Übersicht über Normen und Verkabelungstopologien im Ethernet-Bereich (Quelle: tecChannel.de):



© tecChannel.de

Die jeweiligen Übertragungsgeschwindigkeiten und Normen haben sich immer weiter verbessert. Der Ethernet-Standard wird auch heute noch weiterentwickelt:

- IEEE 802.3ba (2010): beschäftigt sich mit 40 Gbit/s und 100 Gbit/s-Ethernet; eine Reihe weiterer Standards beschäftigt sich mit den verwendbaren Kabeltypen
- IEEE 802.3bs (erwartet für 2017): beschäftigt sich mit 400 Gbit/s-Ethernet

4.1.5 Koaxial-Kupferkabel

Koaxialkabel werden grundsätzlich für Bus-Topologien eingesetzt. Sie wurden für 10 Mbps-Ethernet-Netzwerke (10Base-2, 10Base-5) verwendet; man findet sie heute nur noch in Altsystemen.

Die verwendeten Koaxialkabel bestanden aus einem Kupferkern, der durch eine Isolierschicht vom geflochtenen Außenleiter (ebenfalls aus Kupfer) getrennt war.

Koaxialkabel sind heute noch als Antennenkabel (für Fernsehempfang) in Verwendung. **(Bild unten links)**

4.1.6 Twisted Pair-Kupferkabel

Darunter versteht man Kupferkabel mit meist vier gekreuzten, verdrillten bzw. verseilten Adernpaaren. Die Verdrillung trägt dazu bei, um Störungen durch induktive Kopplungen benachbarter Leitungen zu verringern. Auch Abschirmungen verringern die Störeinflüsse durch äußere elektromagnetische Felder.

Die erreichbare Datenübertragungsrate hängt mit der Leitungslänge, der Abschirmung und der Steckerbauform zusammen. Alle Daten im technischen Datenblatt beziehen sich grundsätzlich auf eine maximale Kabellänge von **100 m.** **(Bild unten rechts)**

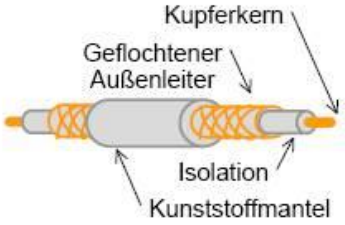
Für die verschiedenen Übertragungsgeschwindigkeiten werden die Bezeichnungen Cat1-Cat8 verwendet. **(Tabelle nächste Seite oben)**

Bezeichnung	Standard	Mbit/s	Kabeltyp	Max. Segmentlänge
10Base2 (1983)	IEEE 802.3 Clause 10	10	Koaxialkabel	185 m
10Base5 (1985)	IEEE 802.3 Clause 8	10	Koaxialkabel	185 m
10Base-T (1990)	IEEE 802.3 Clause 14	10	Twisted Pair-Kabel Cat 3	100 m
100Base-TX (1995)	IEEE 802.3 Clause 25	100	Twisted Pair-Kabel Cat 3/5; verwendet nur Adernpaare 2 und 3	100 m
100Base-FX (1995)	IEEE 802.3 Clause 26	100	Multimode-Glasfaserkabel	2000 m
1000Base-T (1999)	IEEE 802.3 Clause 26	1000	Twisted Pair-Kabel Cat 5e/6; verwendet alle 4 Adernpaare	100 m
1000Base-SX (1998)	IEEE 802.3 Clause 38	1000	Multimode-Glasfaserkabel; Wellenlänge 850 nm	200 m – 550 m
1000Base-LX (1998)	IEEE 802.3 Clause 38	1000	Singlemode-Glasfaserkabel; Wel-	5 km
10GBase-T (2006)	IEEE 802.3an	10000	Twisted Pair-Kabel Cat 6a/7; verwendet alle 4 Adernpaare	100 m
10GBase-LR (2002)	IEEE 802.3ae	10000	Singlemode-Glasfaserkabel; Wel-	10 km

Kabelschirmung

Da die alten Bezeichnungen nicht einheitlich und damit oft verwirrend oder sogar widersprüchlich sind, wurde mit der Norm ISO/IEC-11801 (2002) ein neues Bezeichnungsschema der Form XX/YZZ eingeführt.

Dabei steht XX für den Gesamtschirm, Y für die Adernpaarschirmung und ZZ gibt an, ob es sich um jeweils zwei Adern (TP =



Twisted Pair) oder vier Adern (QP = Quad Pair) handelt.

Gesamtschirmung

U/ ungeschirmt (engl. *unshielded*)

F/ Folienschirm (engl. *foiled*)

S/ Geflechtschirm (engl. *screened*)

SF/ Geflecht- und Folienschirm

Adernpaarschirmung

UTP ungeschirmt (engl. *Unshielded Twisted Pair)*

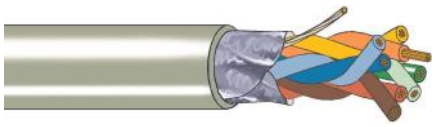
FTP Folienschirm (engl. *Foiled Twisted Pair)*

STP Geflechtschirm (engl. *Screened Twisted Pair*)

Damit ergeben sich folgende Schirmungstypen:

- **U/UTP:** Kabel ungeschirmt, Paare ungeschirmt (max. Cat 5e, 100 MHz)

- **F/UTP**: Kabel mit einem Folien-Gesamtschirm, Paare ungeschirmt (max. Cat 5e, 100 MHz)



- **SF/UTP**: Kabel mit einem Doppelschirm (Geflecht+Folie), Paare ungeschirmt (max. Cat 5e, 300 MHz)

- **FF/UTP**: Kabel mit einem Doppelschirm (Folie+Folie), Paare ungeschirmt
- **U/FTP**: Paare einzeln geschirmt (PiMf = Paare in Metallfolie), kein Gesamtschirm
- **F/FTP**: Paare einzeln geschirmt (PiMf = Paare in Metallfolie), Folien-Gesamtschirm
- **S/FTP**: Paare einzeln geschirmt (PiMf = Paare in Metallfolie), Geflecht-Gesamtschirm (max. Cat 6A/7, 750 MHz bzw. 1000 MHz)

Kabelquerschnitte – Patchkabel und Verlegekabel

Im Normalfall werden für die sogenannten Patchkabel (werden in Patch-Verteilern benutzt) Kabel mit Adernstärken von 26AWG bis 24AWG benutzt (AWG = American Wire Gauge). Sie sind deshalb flexibler als sogenannte Verlegekabel, die zwischen 22AWG und 26AWG gefertigt werden. Außerdem haben Patchkabel meist auch eine flexiblere Isolation.

Für Drahtquerschnitte wird wird im Computerbau üblicherweise statt Quadrat-Millimeter (mm²) das amerikanische Maß "AWG" benutzt.

AWG ist der US-Standard für den Durchmesser eines Leiters. Je höher die AWG-Nummer ist, desto dünner ist der Draht. Dieses Maß stammt von dem Fakt ab, daß die Original-Messung die Anzahl der Durchläufe durch die Draht-Ziehmaschine repräsentiert. Deshalb ist ein 24er-Draht dünner als ein 18er-Draht, da er noch 6mal durch die Maschine gezogen wurde.

26AWG: Durchmesser 0,40 mm; Querschnitt 0,13 mm²

24AWG: Durchmesser 0,51 mm; Querschnitt 0,20 mm²

22AWG: Durchmesser 0,64 mm; Querschnitt 0,32 mm²

Trotz der geringeren Dicke der Patchkabel (und damit etwas einfacheren Verarbeitbarkeit) sollte man für lange Strecken unbedingt Verlegekabel benutzen, da diese eine geringere Dämpfung haben. Mit Patchkabeln lässt sich unter Umständen nicht die gesamte mögliche Strecke überbrücken!

Kategorie	Klasse laut ISO/IEC	Frequenzbereich	Twisted Pair-Kabeltyp	Anwendung/Dienst
Cat1	Klasse A	0,4 MHz	UTP-1	Veraltet; Telefonie, Modem, DFÜ
Cat2	Klasse B	4 MHz	UTP-2	Veraltet; ISDN, IBM-Verkabelung Typ 3
Cat3	Klasse C	16 MHz	UTP-3	10BaseT- und 100BaseTX-Ethernet; heute vor allem als Telefonkabel eingesetzt
Cat4	–	20 MHz	UTP-4	Veraltet; Token Ring
Cat5	Klasse D	100 MHz	U/UTP	Fast Ethernet
Cat5e	Klasse D	100 MHz	F/UTP SF/UTP (bis 300 Mhz)	Baugleich mit Cat5, aber verbesserte Prüfnormen
Cat6	Klasse E	250 MHz	S/FTP	155-MBit-ATM, 622-MBit-ATM
Cat6e	Klasse EA	500 MHz	S/FTP	Fast Ethernet, Gigabit Ethernet, 10Gigabit-Ethernet
Cat7	Klasse F	600 MHz	S/FTP	ATM, Gigabit Ethernet, 10Gigabit-Ethernet
Cat7A	Klasse FA	1000 MHz	S/FTP	über 10GBase-T
Cat8	Klasse G	1600 – 2000 MHz	S/FTP	In Planung (2016/17); vier einzeln abgeschirmte symmetrische Adernpaare innerhalb eines gemeinsa-

Steckernormen und Verdrahtung

Stecker für Cat 5e-Verkabelung

Die Steckverbindungen sind als vollbestückte achtpolige Modularstecker **(8P8C)** ausgeführt, die umgangssprachlich **„RJ-45“** genannt werden, obwohl es sich meist um RJ-48 oder RJ-49 8P8C handelt (RJ =“registered jack“, deutsch "genormte Buchse").

Beim Ziehen von Verlegekabeln durch Kabelkanäle sind Kabelschuhe oft hinderlich. Die Kabel werden daher zunächst ohne Kabelschuhe gezogen, da für den Anschluss an Patchfelder ohnehin keine Kabelschuhe notwendig sind.

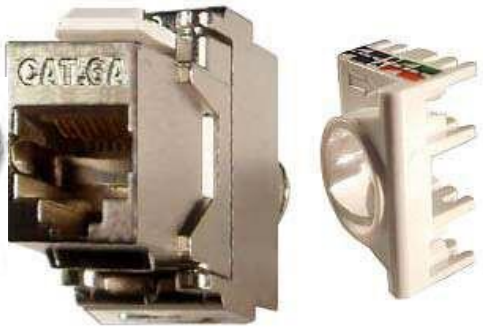
Im Einzelfall kann es vorkommen, einen RJ-45-Stecker an ein Twisted-Pair-Kabel anbringen zu müssen. Mit Hilfe einer **Crimpzange** (Bild nächste Seite) werden die Adern des Kabels und Steckers, bzw. einer Aderendhülse formschlüssig verbunden.

Eine wesentliche Erleichterung bei der Montage von Buchsen sind die Keystone-Module.

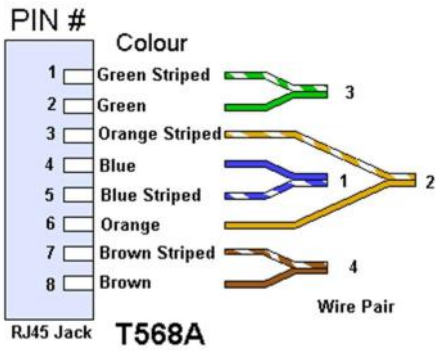
Darunter versteht man Buchsenmodule, die auf Verlegekabel montiert und an-

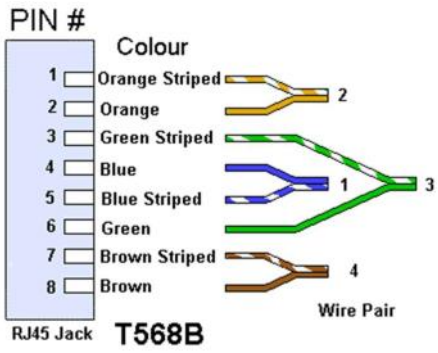
RJ-45 Stecker

Crimp-Zange



Keystone Modul für Cat 6A-Verkabelung





schließend in Patchpanels eingeclipst werden. Die Einbaumaße solcher Module sind standardisiert (nicht jedoch die Blechstärken).

Stecker für Cat 7/7A-Verkabelunge

- **GG-45** (GigaGate, entwickelt von Nexans): Dies geschieht mit Kippschaltern innerhalb des Steckers. Die Buchse ist RJ-45-kompatibel, sodass in neue GG-45-Buchen auch herkömmliche RJ-45- Stecker passen. Umgekehrt ist das jedoch nicht möglich! Der GG-45-Stecker verfügt über 12 Kontakte, von denen aber immer nur 8 verwendet werden. Die am Rand befindlichen Kontakte werden bei Cat 7-Betrieb verwendet, die mittleren Kontakte bei Cat-5e-Betrieb. Die „Nase" an der Front des GG-45-Steckers führt die Umschaltung in den Cat 7-Betrieb durch.

Bei den RJ-45- bzw. GG-45-Modularsteckern unterscheidet man drei verschiedene Verdrahtungstypen:

- TIA/EIA 568A
- TIA/EIA 568B (am häufigsten verwendet)
- USOC

EIA/TIA-568A und EIA/TIA-568B sind Standards für die Kontaktierung von achtpoligen "RJ-45"-Steckern und Buchsen. Sie wurden definiert durch die drei Organisationen Electronic Industries Alliance (EIA), *Telecommunications Industry Association* (TIA) und *International Telecommunications Union* (ITU). Beide Standards werden bei Computernetzen (LAN) im Ethernet (10Base-T, 100Base-TX und 1000Base-T) verwendet sowie bei vielen digitalen Telefonsystemen, wobei EIA/TIA-568B häufiger verwendet wird. Zusätzlich unterscheidet man „Straight" und „Crossover"-Kabel.

„Straight"-Kabel haben üblicherweise die T568B-Belegung an beiden Kabelenden. „Straight"-Kabel werden verwendet:

- zum Verbinden von PCs zum Hub bzw. Switch
- zum Verbinden einer Netzwerkdose zum Patch-Panel (Verteilerfeld)
- zum Verbinden eines Anschlusses am Patch-Panel zum Hub bzw. Switch

„Crossover"-Kabel haben üblicherweise an einem Ende die T568A-Beschaltung, am anderen Kabelende die T568B-Beschaltung. "Crossover"-Kabel werden verwendet:

- zum direkten Verbinden zweier PC-Netzwerkkarten
- zum direkten Verbinden zweier Hubs oder Switches

4.1.7 Lichtwellenleiter (LWL)

Lichtwellenleiter werden umgangssprachlich auch als Glasfaserkabel bezeichnet, obwohl das Leitermaterial heute auch aus Kunststoff bestehen kann. Die Informationen werden in Form von Lichtimpulsen weitergeleitet.

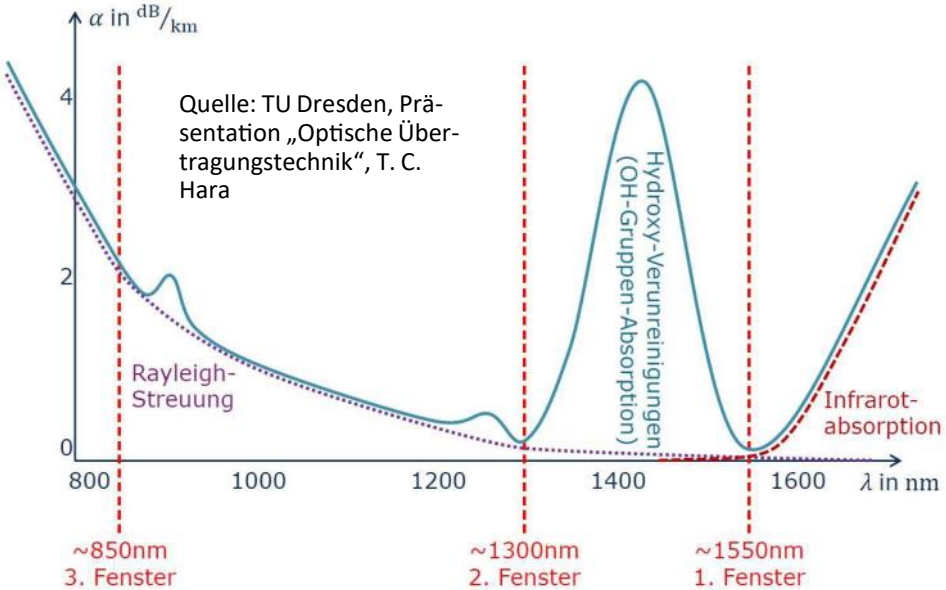
Aus technischen Gründen beschränkt man sich beim verwendeten Licht auf „nahes Infrarot", darunter versteht man den Wellenlängenbereich zwischen 800 nm und 1700 nm. Der Grund dafür ist, dass diese Wellenlängen einfach erzeugt werden können (mit LEDs oder kostengünstigen Lasern).

Hauptvorteil der Lichtwellenleiter sind die geringe Dämpfung und damit die Möglichkeit einer schnellen Datenübertragung über weite Strecken.

Material	Dämpfung
Fensterglas	50.000 dB/km
Optisches Glas	3.000 dB/km
Industrieller Lichtwellenleiter	3 dB/km

Die Dämpfung ist jedoch frequenzabhängig. Auf der folgenden Grafik ist der Dämpfungskoeffizient gegen die Lichtwellenlänge λ für hochreines Quarzglas aufgetragen.

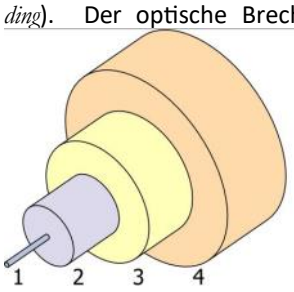
$$\alpha = \frac{10}{l_{Kabel}} \cdot \lg \frac{P_{Licht\ eingespeist}}{P_{Licht\ messbar}}$$



Quelle: TU Dresden, Präsentation „Optische Übertragungstechnik", T. C. Hara

Die Wellenlänge hängt über die Vakuum-Lichtgeschwindigkeit mit der Frequenz zusammen ($f=c/\lambda$). Man erkennt drei Wellenlängen, bei denen die Dämpfung minimal ist: 850 nm, 1310 nm und 1550 nm. Für diese drei Wellenlängen treten die geringsten Verluste auf, weshalb ausschließlich diese Wellenlängen für die Lichtwellenleitertechnik eingesetzt werden.

Lichtwellenleiter (Grafik: Wikipedia) bestehen aus einem Kern (1 – engl. *core*) und einem umgebenden Mantel (2 – engl. *cladding*). Der optische Brechungsindex des Mantels ist etwas geringer als der des Kerns. Mantel und Kern können aus Siliciumdioxid (Quarzglas) bestehen;



dabei wird der höhere Brechungsindex des Kerns durch Dotieren mit Germanium oder Phosphor erreicht. Bei Ethernet-Netzwerkkabeln vom Typ OM und OS hat der Mantel meist einen Durchmesser von 125 µm. Der Mantel ist von einer Schutzbeschichtung (3 – engl. coating) und einer äußeren Schutzhülle (4 – engl. jacket) umgeben.

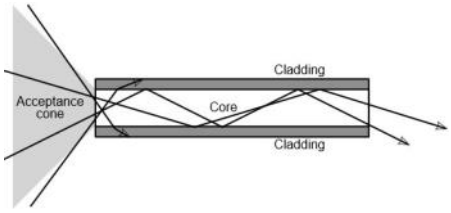
Das einfallende Licht wird durch Totalreflexion an der Grenze zwischen Kern und Mantel stets im Kabel geführt.

Als Lichtquelle werden LEDs oder Laser verwendet.

Verwendete Wellenlängen:

- 850 nm
- 1310 nm (O-Band)
- 1550 nm (C-Band)

In einer Ader werden meist 24 Glasfasern geführt.



Das Licht hat in der Glasfaser eine geringere Ausbreitungsgeschwindigkeit als im Vakuum. Die Lichtgeschwindigkeit im Vakuum beträgt

$$c_{Licht} = 3 \cdot 10^8 \frac{m}{s} = 300\,000 \frac{km}{s}$$

, die Ausbreitungsgeschwindigkeit in einer Glasfaser ist vom Brechungsindex abhängig.

Beispiel: Quarzglas mit $\approx 1{,}45$

$$c_{Quarzglas} = \frac{c_{Licht}}{n} = \frac{3 \cdot 10^8 \, m}{1{,}45 \, s} \approx 2{,}07 \cdot 10^8 \frac{m}{s} = 207\,000 \frac{km}{s}$$

Nach den Leitungseigenschaften unterscheidet man:

Kabelbezeichnung	Kabeltyp Kerndurchmesser	Farbe Schutzhülle	100Base-SX 850 nm	100Base-FX 1310 nm	1000Base-SX 850 nm	1000Base-LX 1310 nm	10GBase-SR 850 nm	10GBase-LR 1310 nm
OM1	Multimode 62,5 µm	orange	300 m	2000 m	300 m	500 m	30 m	220 m
OM2	Multimode 50 µm	orange	300 m	2000 m	500 m	500 m	80 m	220 m
OM3	Multimode 50 µm	aqua	300 m	2000 m	1000 m	500 m	300 m	220 m
OM4	Multimode 50 µm	aqua	–	2000 m	1000 m	500 m	500 m	220 m
OS1/OS2	Monomode 9 µm	gelb	–	10000 m	–	10000 m	–	10000 m

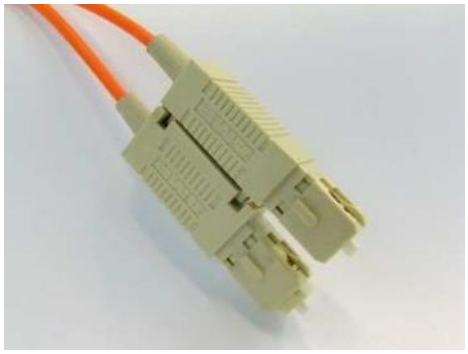
- **Multimodefasern**: Kerndurchmesser 50 – 1500 µm; es breiten sich gleichzeitig mehrere Lichtwellen aus.
  - **Stufenindexfaser**: Der Brechungsindex zwischen Kern und Mantelglas ändert sich schlagartig. Diese Variante hat die meisten Verluste; solche Kabel werden zum Beispiel als Patchkabel im Netzwerkschrank verwendet.
  - **Gradientenfaser**: Der Brechungsindex ändert sich nach außen hin kontinuierlich. Die Signalverluste sind geringer als bei der Stufenindexfaser; solche Kabel werden zum Beispiel für Verbindungen von Gebäuden oder Stockwerken benutzt.
- **Monomodefasern**: sehr geringer Kerndurchmesser (3 – 9 µm); dadurch kann sich nur ein Modus ausbreiten. Singlemodefasern erfordern den Einsatz sehr teurer Laser, was zu hohen Kosten führt. Solche Kabel werden für Langstreckenübertragungen verwendet.

Um welches Kabel es sich handelt, erkennt man an der Farbe der äußeren Schutzhülle. Die maximale Übertragungsreichweite hängt von der Datenrate und der genutzten Wellenlänge ab.

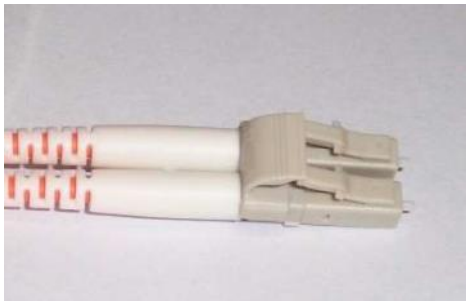
Steckertypen

Im Bereich der optischen Leiter gibt es eine Vielzahl von Steckertypen. Die beiden häufigsten Steckertypen im LAN-Bereich sind:

SC-Stecker (engl. *subscriber connector):* seit 2002 Standard für LAN-Verkabelungen. Dieser Stecker eignet sich für Multimode- und Monomodekabel. Als Verschlussmechanismus wird eine Push-Pull-Technik verwendet, das bedeutet, der Stecker verriegelt sich automatisch beim Einstecken und entriegelt sich beim Abziehen. SC-Stecker eignen sich für die Anbindung einer einzigen Glasfaser.
(Bildquelle: de.wikipedia.org)



LC-Stecker (engl. *lucent connector):* kleinerer Formfaktor als der SC- Stecker, neuer Standard für LAN-Verkabelungen. Der LC-Stecker verwendet einen Spannbügelverschluss. LC-Stecker eignen sich für die Anbindung einer einzigen Glasfaser.(Bildquelle: de.wikipedia.org)



Spleißen

Während das „Verlängern" von Kupferkabeln bzw. das „Reparieren" gebrochener Kupferkabel vergleichsweise wenig Aufwand erfordert, gestaltet sich dieser Vorgang bei Lichtwellenleitern aufwändig.

Unter dem Begriff Spleißen versteht man ein thermisches Verschweißen zweier Glasfasern. Eine Spleißverbindung stellt eine bruchfeste, dauerhafte, selbstheilende Verbindung dar und muss mit einer Spleißmaschine durchgeführt werden. Die Kabelenden müssen absolut plan und sauber sein, sie werden dann exakt zusammengeführt und unter Druck erhitzt. Nach dem Verschweißen wird drucklos abgekühlt.

Tipp: Eine Spleißmaschine ist sehr teuer; es rentiert sich nicht, selbst spleißen zu wollen. Verwenden Sie daher besser fertige, vorkonfektionierte Glasfaserkabel!

Vorteile von Lichtwellenleitern

- Glasfaserkabel haben eine wesentlich höhere Übertragungskapazität als Kupferkabel.
- Lichtwellenleiter haben eine geringe Dämpfung und ermöglichen die Übertragung über große Distanzen.
- Lichtwellenleiter sind unempfindlich gegenüber elektromagnetischen Störungen wie Übersprechen.
- Sie haben einen geringen Kabelquerschnitt und daher auch ein geringes Längengewicht.
- Kabelstränge lassen sich einfach bündeln.

Nachteile von Lichtwellenleitern

- Glasfaserkabel und passende Netzwerkkomponenten sind wesentlich teurer als Kupferkabel.
- Lichtwellenleiter lassen sich schwer „stückeln“ bzw. verlängern. Präzise und aufwändige Spleißtechnik ist notwendig.
- Schwierige Signalverstärkung
- Lichtwellenleiter sind mechanisch empfindlich.
- Beim Verlegen müssen höhere Krümmungsradien eingehalten werden, das Knicken von LWL ist verboten. Faustformel für LWL: minimaler Krümmungsradius = 10facher Außendurchmesser des LWL-Kabels (Beispiel: LWL mit 5 mm Außendurchmesser hat einen minimalen Biegeradius von 5 cm)
- Signalumwandlung zwischen Kupfer- und Lichtwellensegmenten erforderlich

4.2 Industrial Ethernet, PROFINET

Auch in der industriellen Fertigung müssen einzelne Geräte und automatisierungstechnische Komponenten miteinander vernetzt werden. Industrial Ethernet ermöglicht es, in das vorhandene LAN auch Geräte einzubeziehen, die für die Steuerung und Überwachung von Produktionsprozessen verwendet werden. Die im industriellen Umfeld verwendeten aktiven Netzwerkkomponenten sind an die industriellen Umgebungsbedingungen angepasst (erhöhte Schutzart, Säurefestigkeit etc.).

Der offene Industrial Ethernet- Standard für Automatisierung ist PROFINET *(Process Field Network)*. Er nutzt herkömmliche Verkabelungssysteme und TCP/IP, ist echtzeitfähig und ermöglicht die Integration von Feldbussystemen. Abbildung: Wikipedia

OSI-Schicht		Englisch	PROFINET		
7a	Anwendung	Application	IO-Dienste & -Protokolle	CBA-Dienste & -Protokolle	
7b			RPC	DCOM & RPC	
6	Darstellung	Presentation	leer	--	--
5	Sitzung	Session			leer
4	Transport	Transport	UDP	TCP	
3	Netzwerk	Network	IP, ARP, SNMP, DHCP		
2	Sicherung	Data Link	CSMA/CD, VLAN, DCP, MRP, MRRT, LLDP		
1	Bitübertragung	Physical	100BASE-TX, 100BASE-FX		

Auf den OSI-Schichten 1 und 2 verwendet man 100BASE-TX und 100BASE-FX Verkabelungstechnik. Das PROFINET-Protokoll kann mit jedem Ethernet-Analysewerkzeug (also etwa Wireshark) gelesen werden. In der Abbildung oben (Foto: Autor) ist ein Detail einer Siemens-SPS Simatic S7-1200 dargestellt.

Deutlich sieht man die PROFINET-Schnittstelle und ein an den RJ45-Steckplatz angeschlossenes Cat 5-Netzwerkkabel.

Die Verwendung des Ethernet-Standards erkennt man auch an der dargestellten MAC-Adresse.

Norm	Jahr	Frequenzbereich	Datenrate	realistische Datenrate
IEEE 802.11	1997	2,4 GHz	2 Mbit/s	
IEEE 802.11a / h	1999, 2003	5,150 – 5,725 GHz	54 Mbit/s	20 – 22 Mbit/s
IEEE 802.11b / g	1999, 2003	2,400 – 2,4835 GHz	11 Mbit/s	5 – 6 Mbit/s
IEEE 802.11n	2009	2,400 – 2,4835 GHz und	150 Mbit/s	100 – 120 Mbit/s
IEEE 802.11ac	2013	5,150 – 5,725 GHz	433 Mbit/s	100 – 120 Mbit/s

4.3 Wireless LAN (WLAN)

WLANs *(Wireless Local Area Networks)* sind Netze, die zur Datenübertragung Funktechnologie verwenden. Funkwellen sind elektromagnetische Wellen mit einer definierten Frequenz.

Gleichbedeutend wird auch der Begriff Wi-Fi verwendet, wobei damit eigentlich ein Firmenkonsortium (die Wi-Fi Alliance, www.wi-fi.org) gemeint ist, welches WLAN-Geräte zertifiziert.

Die Bedeutung von Wireless LAN-Infrastrukturen hat in den vergangenen Jahren stetig zugenommen.

Medienzugriff: **CSMA/CA** *(Carrier Sense Multiple Access / Collision Avoidance)*. Anders als bei Ethernet ist bei Funksignalen eine Kollisionserkennung nicht möglich. Daher wird vor dem Sendevorgang überprüft, ob der Sendekanal frei ist. Anders gesagt: Ein Sendevorgang wird nicht aufgenommen, solange eine Sendung läuft. Jeder Sender darf nur eine begrenzte Zeit senden. Ein typischer CSMA/CA-Sendevorgang würde daher beispielhaft wie folgt ablaufen (vereinfachte Darstellung):

1. Zuerst wird das Medium abgehört („horcht“, *„Carrier Sense“*).

2. Ist das Medium für die Dauer einer bestimmten Zeitspanne *(„Interpacket Gap“*, etwa 50 µs) frei, wird eine zufällige Wartezeit ausgewürfelt und nach Ablauf dieser gesendet.

3. Ist das Medium belegt, wird die voraussichtliche Belegungszeit gespeichert und nach Ablauf dieser Zeitspanne ein neuer Sendevorgang gestartet.

4. Nach vollständigem Empfang des Paketes wartet der Empfänger eine kurze Zeitspanne (etwa 10 µs), bevor das Bestätigungssignal (ACK für engl. *acknowledge*) gesendet wird.

4.3.1 WLAN-Standards

Es sind zwei Frequenzbereiche für WLAN üblich:

- **ISM-Frequenzbereich**: 2,400 – 2,485 GHz (lizenzfrei verwendbar; *industrial / medical / scientific purposes)*. Nachteil dieses Bereichs ist die Störanfälligkeit (etwa durch Mikrowellen-Geräte) und die kleine Frequenz-Bandbreite, wodurch nur geringe Datenübertragungsraten erreicht werden können.
- Frequenzbereich 5,150 – 5,725 GHz

Die meisten WLAN-Infrastrukturen basieren auf der Norm **IEEE 802.11**. Seit der Einführung dieser Norm gibt es eine ganze Reihe von Dokumenten, die den technischen Fortschritt der WLAN-Technologien dokumentieren.

Die Norm IEEE 802.11h erweitert die Sendeleistung gegenüber IEEE 802.11a auf 1000 mW.

4.3.2 Betriebsarten von WLANs

WLANs können in zwei verschiedenen Modi betrieben werden:

- **Ad hoc-Modus:** Funk-Lan-Karten senden direkt (Peer-to-Peer Netzwerk); sehr geringe Reichweite
- **Infrastruktur-Modus:** Dafür wird ein „Access Point“ benötigt (dieses Gerät ist mit einer Bridge, kombiniert mit einem Signalverstärker, vergleichbar: es stellt einen Übergang zwischen unterschiedlichen Medien dar)

In Firmeninfrastrukturen wird meist ein Infrastruktur-WLAN-Betrieb aufgebaut, der auf dem Einsatz von WLAN-Access Points basiert.

Der Infrastruktur-Modus ähnelt im Aufbau dem Mobilfunknetz: Ein drahtloser Router oder ein Access Point übernimmt die Koordination aller anderen Netzknoten (Clients). Dieser sendet in einstellbaren Intervallen (üblicherweise zehnmal pro Sekunde) kleine Datenpakete, sogenannte

„Beacons“ (engl. „Leuchtfeuer“), an alle Stationen im Empfangsbereich. Die Beacons enthalten u. a. folgende Informationen:

- Netzwerkname *(„Service Set Identifier“,* SSID)
- Liste unterstützter Übertragungsraten
- Art der Verschlüsselung

Dieses „Leuchtfeuer“ erleichtert den Verbindungsaufbau ganz erheblich, da die Clients lediglich den Netzwerknamen und optional einige Parameter für die Verschlüsselung kennen müssen. Gleichzeitig ermöglicht der ständige Versand der Beacon-Pakete die Überwachung der Empfangsqualität – auch dann, wenn keine Nutzdaten gesendet oder empfangen werden. Beacons werden immer mit der niedrigsten Übertragungsrate (1 MBit/s) gesendet, der erfolgreiche Empfang des „Leuchtfeuers“ garantiert also noch keine stabile Verbindung mit dem Netzwerk. Bild: Cisco Aironet AIR-AP1600 mit angeschraubten Antennen; Foto: Cisco

4.3.3 WLAN-Sicherheitsstandards

WLANs sind ohne zusätzliche Maßnahmen eine Sicherheits-Schwachstelle des gesamten Unternehmens. Deshalb haben sich im Laufe der Jahre eine ganze Reihe von Sicherheitsstandards entwickelt.

Man unterscheidet grundsätzlich drei Sicherheitsfunktionen, die voneinander unabhängig implementiert sein können:

- **Authentifizierung**: Computerauthentifizierung, Benutzerauthentifizierung
- **Verschlüsselung**: Die Daten zwischen Client und WLAN-Access Point werden verschlüsselt übertragen.
- **Datenintegrität**: Überprüfung, ob die Daten während der Übertragung nicht verändert wurden

Bei allen Sicherheitsstandards ist darauf zu achten, welche dieser drei Sicherheitsfunktionen implementiert wurden.

Der grundlegende Unterschied zwischen den "Personal" und "Enterprise"-Varianten von WPA und WPA2 ist die Art der Authentifizierung. Bei den "Personal"-Varianten wird ein *Pre-Shared Key* (PSK) verwendet, während bei den "Enterprise"-Varianten ein Authentifizierungsserver nötig ist.

4.3.4 IEEE 802.1X-Authentifizierung

EAP ist ein allgemeines, von der *Internet Engineering Task Force* (IETF) entwickeltes Authentifizierungsprotokoll, das verschiedene Authentifzierungsverfahren unterstützt. Mit EAP wird der eigentliche Authentifizierungsmechanimus nicht während der Herstellung der PPP-Verbindung gewählt, sondern erst nachher, in der Authentifizierungsphase. In dieser Phase handeln die Teilnehmer den sogenannten **EAP-Typ** aus.

	Verschlüsselung	Authentifizierung	Datenintegrität
WEP	RC4	Open System, Pre-Shared-Key	Keine
WPA-Personal	TKIP (RC4-basierend)	Pre-Shared Key	Michael
WPA-Enterprise	TKIP (RC4-basierend)	EAP, RADIUS (IEEE 802.1X)	Michael
WPA2-Personal	CCMP (AES-basierend)	Pre-Shared Key	AES-CBC-MAC
WPA2-Enterprise	CCMP (AES-basierend)	EAP, RADIUS (IEEE 802.1X)	AES-CBC-MAC

Von Microsoft unterstützte EAP-Typen	
EAP-MSCHAPv2 (Extensible Authentication Protocol – MSCHAPv2)	Computerauthentifizierung mit Zertifikat; Benutzerauthentifizierung mit Benutzername/Kennwort
EAP-TLS (EAP – Transport Layer Security)	RFC 5216. TLS ist ein Nachfolgestandard von SSL; zertifikatsbasierte Authentifizierung von Computern und Benutzern erforderlich (Smartcards)
EAP-IKEv2 (EAP – Internet Key Exchange v2)	RFC 5106. Authentifizierung mit Zertifikat.
PEAP/EAP-TLS	So wie EAP-TLS, allerdings mit verschlüssentem Kanal während des Verbindungsaufbaus
PEAP/EAP-MSCHAPv2	So wie EAP-MSCHAPv2, allerdings mit verschlüssentem Kanal während des Verbindungsaufbaus

Microsoft unterstützt folgende EAP-Typen:

Weitere EAP-Typen sind:

- **EAP-TTLS** *(Tunneled Transport Layer Security)*
- **LEAP** *(Lightweight Extensible Authentication Protocol, Cisco):* kann durch einfache Wörterbuch-Attacken geknackt werden.
- EAP-FAST *(Cisco, Flexible Authentication via Secure Tunneling):* Sowohl der Client als auch der Server generieren vor der Kommunikation einen Schlüssel

EAP ermöglicht zwar eine flexible Authentifizierung, jedoch wird die gesamte EAP-Konversation unverschlüsselt übertragen.

PEAP ist ein spezieller EAP-Typ, der zunächst für einen sicheren Kanal mit verschlüsselter Übertragung sorgt, dessen Unversehrtheit mit TLS gesichert wird. Anschließend findet eine neue EAP-Verhandlung mit einem anderen EAP-Typ statt. Vorteil der Verwendung von PEAP ist, dass bei WLAN-Authentifizierungen sogar kennwortbasierende Verfahren (PEAP-MSCHAPv2) genutzt werden können, die normalerweise anfällig für Wörterbuch-Angriffe sind.

4.4 PAN – Personal Area Networks („Bluetooth“)

Darunter versteht man einen Funk-LAN-Standard für Netze geringer Bandbreite mit kurzer Reichweite (< 10 m), genormt als IEEE 802.15.1.

1998 wurde von den Firmen IBM, Toshiba, Intel, Ericsson und Nokia die „Bluetooth Special Interest Group“ ins Leben gerufen, die sich seither mit der Weiterentwicklung und Anwendung dieses Standards beschäftigt. Der Name stammt von einem nordischen König mit dem Spitznamen „Blauzahn“.

Geräte, die Bluetooth unterstützen, werden mit dem Bluetooth-Logo gekennzeichnet (siehe Bild rechts).

Aktueller Standard: Bluetooth 4.2 (Dez. 2014)

Als Frequenzbereich wird der ISM-Bereich benützt (2,402 GHz bis 2,480 GHz). Eine spezielle Eigenschaft, das *„Frequency Hopping Spread Spectrum“* (FHSS) gewährleistet die Sicherheit der Datenübertragung: alle 625 µs wird die Trägerfrequenz geändert.

Mit Bluetooth ist eine Datenübertragungsrate von 64 kbit/s bei synchroner Sprachübertragung und 732,2 kbit/s Download/57,6 kbit/s Upload bei asynchronen Datenübertragungen erreichbar. Ab Bluetooth 2.0 + EDR *(Enhanced Data Rate)* sind Datenübertragungsraten bis ca. 2,1 Mbit/s möglich.

Die Geräte identifizieren einander automatisch, indem sie ihre 48 Bit-MAC-Adressen austauschen.

Anwendungsgebiete:

- Peripheriegeräte (Maus, Drucker, ...)
- Freisprechanlagen in PKWs
- PDA: Damit wird die automatische Synchronisation mit dem PC – wenn dieser Bluetooth unterstützt – verbessert.

4.5 PROFIBUS

PROFIBUS *(Process Field Bus)* ist ein Standard für die Feldbus-Kommunikation in der Automatisierungstechnik. In der Fertigungstechnik hat sich PROFIBUS DP (Dezentrale Peripherie) durchgesetzt. PROFIBUS PA (Prozess-Automation) wird zur Kommunikation zwischen Mess- und Prozessgeräten, Aktoren und Prozessleitsystem bzw. SPS/DCS in der Prozess- und Verfahrenstechnik eingesetzt.

PROFIBUS PA (Prozess-Automation) wird zur Kommunikation zwischen Mess- und Prozessgeräten, Aktoren und Prozessleitsystem bzw. SPS/DCS in der Prozess- und Verfahrenstechnik eingesetzt.

Verkabelung (OSI-Schicht 1)

- Verdrillte Kupfer-Zweidrahtleitung in einer Bus-Topologie. Als Anschluss wird ein 9-poliger D-Sub-Stecker verwendet.
- Lichtwellenleiter in Stern-, Bus- oder Ring-Topologie.

Medienzugriff (OSI-Schicht 2): Kombination aus Token-Passing-Verfahren (Token-Ring-Logik) mit Master-Slave. Die SPS bzw. Prozessleitsysteme sind dabei die Master, die einzelnen Sensoren und Aktoren die Slaves.

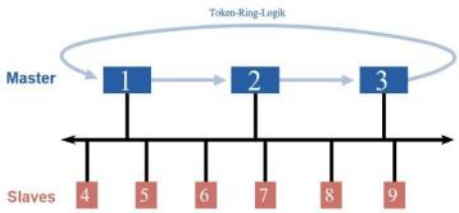
4.6 CAN-Bus

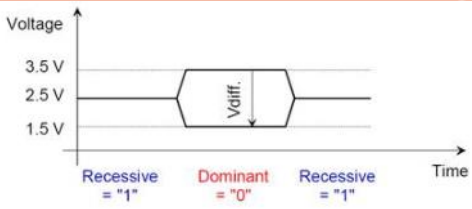
Der **CAN-Bus** *(Controller Area Network)* ist ein serielles Bussystem und gehört zu den Feldbussen. Er wird in der Kraftfahrzeugtechnik verwendet.

Um die Kabelbäume in Fahrzeugen (bis zu 2 km) zu reduzieren und dadurch Gewicht zu sparen, wurde der CAN-Bus 1983 von Bosch für die Vernetzung von Steuergeräten in Automobilen entwickelt und 1987

OSI-Schicht	Englisch	PROFIBUS			
7 Anwendung	Application	DP-V0	DP-V1	DP-V2	Management
6 Darstellung	Presentation	--			
5 Sitzung	Session				
4 Transport	Transport				
3 Netzwerk	Network				
2 Verbindung	Data Link	FDL			
1 Medium	Physical	EIA-485	Optisch	MBP	

zusammen mit Intel vorgestellt. CAN ist





als ISO 11898 international standardisiert und definiert die Layer 1 (physikalische Schicht) und 2 (Datensicherungsschicht) im ISO/OSI-Referenzmodell.

Zusammen mit der OSI-Schicht 7 ergeben sich dann verwendbare Systeme.

Eigenschaften des CAN-Bussystems

- Serielle Kommunikation
  - Vereinfachung in der Verdrahtung
  - Bessere Informationsaufteilung
- Multimasterfähigkeit
  - Jeder einzelne Knoten kann Kommunikation einleiten
  - Unabhängig senden und empfangen

Adressierung

- CAN adressiert nicht die Teilnehmer, sondern die Nachrichten, die übermittelt werden (Identifier)

Physische Eckdaten

- Maximale Kabellänge: 40 m
- Maximale Entfernung eines Teilnehmers zum Bus: 1,0 m
- Minimaler Abstand zwischen zwei Knoten: 0,1 m
- Maximal 30 Knoten

Aufbau eines Frames

Ein CAN-Frame kann bis zu **134 Bit** lang sein. Allgemein bestehen Netzwerkpakete immer aus einem Header (Kopfteil) und den Nutzdaten selbst (Workload). Ein CAN -Frame besteht aus:

- Identifier (CAN 2.0a: 11 bit » 2^{11} = 2048 Nachrichten; CAN 2.0b: 29 bit » 2^{29} = 2537 Mio. Nachrichten)
- Daten (Bild unten)

Signalpegel am CAN-Bus

Übertragungsgeschwindigkeit und Performance:

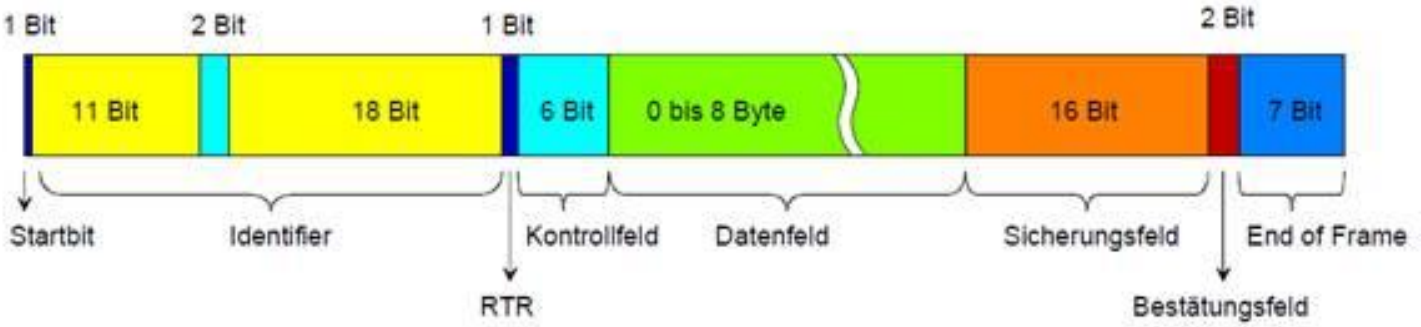
Taktrate: 250 kbit/s (Vergleich: ADSL 500 kbit/s, 100 oder 1000 Mbit/s LAN)

- 100 Botschaften/s (Wiederholrate 10 ms) =5%
  - Drehmoment/ Geschwindigkeitssignale am Motor
  - Hubwerkssteuerung
- 10 Botschaften/s (100 ms repetition) =0.5%
  - Gaspedal
  - GPS
  - Prozessdaten
- 1 Botschaft/s (1s repetition) =0.05%
  - Display updates
  - System Status

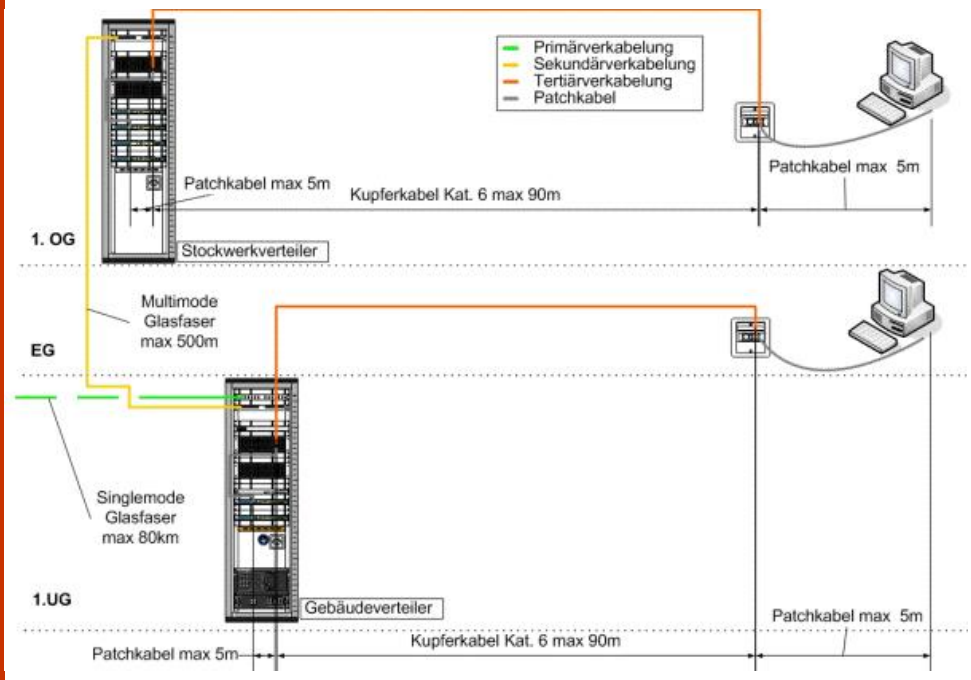
Im landtechnischen Bereich ist der CAN-Bus Basis für ISOBUS-Anwendungen. Dabei geht es um die standardisierte Übertragung von Daten zwischen Traktor und Arbeitsgerät (Düngestreuer, Pflug etc.). Hauptvorteil ist, dass Geräte verschiedener Hersteller miteinander kombiniert werden können.

4.7 FDDI (Fiber Distributed Data Interface)

Eine moderne Variante stellen die so genannten FDDI-Ringe dar *(Fiber Distributed Data Interface)*. Das Übertragungsmedium ist ein **Glasfaserkabel**, mit dem sich Übertragungsraten von 100 MBit/s erreichen lassen. Das derzeit modernste FDDI-LAN bedient sich eines Doppelringes, wobei beide Ringe im Gegensinn durchlaufen werden. Für den Stationszugriff wird auch hier ein Token-Signal verwendet.



5 Strukturierte Gebäudeverkabelung



Unter strukturierter Gebäudeverkabelung versteht man einen einheitlichen Aufbauplan für Verkabelungen für unterschiedliche Dienste (Sprache oder Daten). Als physische Topologie werden Stern-Netzwerke aufgebaut.

Normen

- **EN 50173-1**: Europäische Norm „Anwendungsneutrale Kommunikationskabelanlagen“
- **ISO/IEC 11801** (1995): Internationale Norm *„Generic cabling for customer premises“*
- **TIA/EIA 568**: nordamerikanische Norm *„Commercial building telecommunications cabling standard“*

Man unterscheidet drei Bereiche:

- **Primärbereich** (auch: Campusbereich): Verbindung der Gebäude eines Standortes untereinander
- **Sekundärbereich** (auch: Steigbereich): Verbindung der einzelnen Stockwerte eines Gebäudes
- **Tertiärbereich** (auch: Horizontalbereich): Verbindung der Wanddosen mit dem Etagenverteiler und In allen drei Bereichen der Inhouse-Verkabelung (oft auch Ebenen genannt) können sowohl Verkabelungen mit symmetrischen Kupferkabeln (Twisted Pair) und -komponenten als auch mit Lichtwellenleiterkabeln und komponenten verwendet werden. Im Primärbereich werden ausschließlich LWL-Kabel und -Komponenten verwendet.

Anwendungsneutrale Gebäudeverkabelung (Quelle: http://www.bve.be.ch)

Verteilerschränke

An strategisch günstigen Positionen im Gebäude werden **Verteilerschränke** positioniert. Üblicherweise wird ein **Gebäude-Hauptverteiler** vorgesehen; dieser wird dann mit Lichtwellenleitern mit **Etagen-** bzw. **Stockwerksverteilern** verbunden.

In den Verteilerschränken sind **Montagerahmen (Profilschienen)** im Abstand von 19“ (482,6 mm) verbaut (sogenanntes **19 Zoll-Rack**). Die Außenmaße von Netzwerkschränken sind 600 x 600 mm bzw. 800 x 800 mm. Schränke mit größerer Tiefe (1000 mm) können zusätzlich auch Server-Geräte enthalten.

Die Geräte, die sich montieren lassen, müssen ein ganzzahliges Vielfaches einer **Höheneinheit** (HE) aufweisen, die mit 1,75 Zoll festgelegt sind (4,45 cm).

Größere Schränke haben eine Standardhöhe von 2 m (42 nutzbare Höheneinheiten), kleinere Schränke mit Bauhöhen von 1,2 m können auch an der Wand montiert werden.

Netzwerkschrank 800 x 800 mm mit 19“Rack

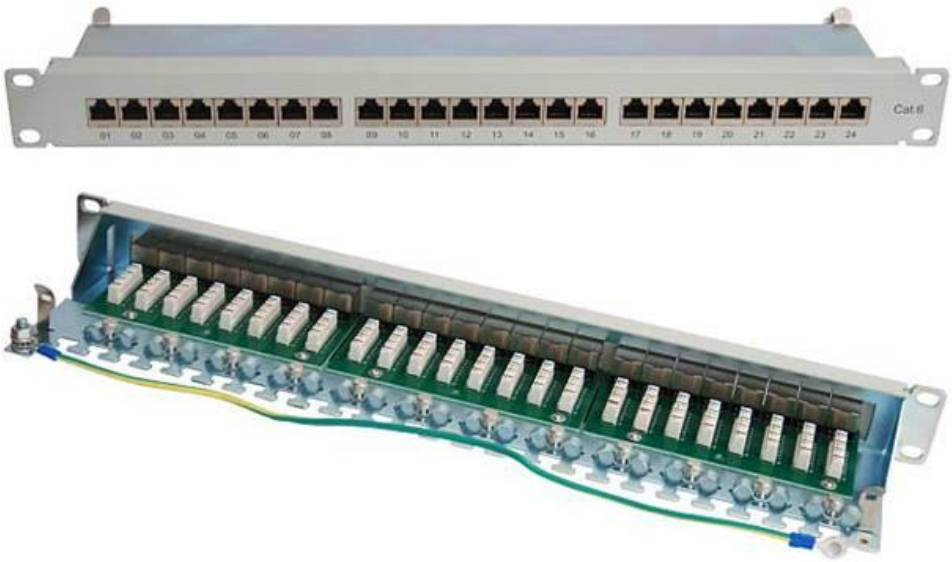
Bekannte Hersteller von Verteilerschränken:

- Rittal (www.rittal.de)
- Schrack (www.schrack.at)

Für die entsprechende Kühlung sind **Einschublüfter** erhältlich. Die Schranktemperatur sollte 25°C nicht übersteigen.

Selbstverständlich muss das Rack mit einem Fundamenterder bzw. der Potenzialausgleichsschiene verbunden werden. Um größtmögliche Flexibilität zu erreichen, werden zunächst **Patchpanels** (Rangierfelder) mit einer Höheneinheit montiert. Diese gibt es für die 19“-Montagerahmen, aber bei Bedarf auch für kleinere Schränke (etwa 10“).

An die Patchpanels werden die **Verlegekabel** angeschlossen, welche die Netzwerk-Doppeldosen in den einzelnen Räumen



LSA-Anlegewerkzeug

des Gebäudes mit dem Verteilerschrank verbinden. Wenn Sie über eine Telefonanlage verfügen, so benötigen Sie ein weiteres Patchfeld für die Verbindung der einzelnen Klappen (Nebenstellen) der Telefonanlage.

Zum Anschließen der Verlegekabel ans Patchfeld verwendet man eine spezielle Verbindungstechnik, die als **Schneidklemmtechnik** (oder **LSA-Technik** = löt-, schraub- und abisolierfreie Technik) bezeichnet wird.

Mit einem speziellen Auflegewerkzeug werden die Adern eines Kabels mitsamt der Isolierung in eine Schneidklemme gepresst. Dabei wird durch das Werkzeug das überschüssige Adernende gekürzt; durch die scharfen Kontakte in der Schneidklemme wird die Adernisolierung durchtrennt und eine gasdichte elektrische Verbindung hergestellt.

Rückseite eines Patchpanels mit Verlegekabeln; achten Sie auf eine Zugentlastung (ist mit speziellen Kabelschellen realisierbar).

Wichtig: Vergessen Sie nicht, die Anschlüsse am Patchpanel und auf der Netzwerk-Doppeldose in den Räumen übereinstimmend zu **beschriften**!

Abbildungen: Zu den Anschlüssen 31 und 32 am Patchpanel gehören die Anschlüsse 31 und 32 an der Netzwerk-Doppeldose!

Anschließend werden die Switches montiert. Es gibt Switches in 19"-Rackbauweise, andere Geräte sind Standgeräte, die auf zusätzlich erhältliche Geräteböden gestellt werden können.

In der folgenden Abbildung sehen Sie, wie die Switch-Ports mit Hilfe kurzer Patchkabel mit den entsprechenden Anschlüssen am Patchpanel verbunden werden.

Tipp: Wenn Sie auch Beschaltungen für Telefondosen benötigen, so verwenden

Sie Patchkabel mit unterschiedlicher Farbe!

Selbstverständlich gibt es auch Patchpanels und Switches mit Anschlüssen für Glasfaserkabel.

Für die Flexibilisierung der verwendeten Kabeltypen sind auch „Medienübersetzer" (sogenannte **Transceiver**) von Lichtwellenleiter auf Twisted Pair-Kupferkabel erhältlich.

Für solche streichholzschachtelgroßen Übersetzer im GigabitEthernet-Bereich ist auch der Begriff GBIC *(Gigabit Interface Converter)* üblich. Es gibt heute bereits GBICs in noch kleinerer Bauform, die als SFPs *(Small Form-Factor Pluggable)* bezeichnet werden.

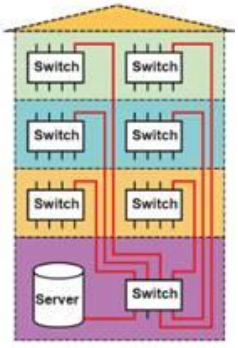
Kaskadieren mehrerer Switches: Entscheidend für die Leistungsfähigkeit der Netzwerkverkabelung ist die Berücksichtigung der benötigten Bandbreite.

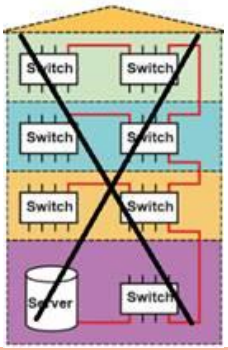
Bild unten links: Switches sind sternförmig verbunden: Alle Stockwerks-Switches sind direkt mit dem ZentralSwitch verbunden.

Empfehlung: Verwenden Sie einen leistungsfähigen Zentral-Switch und binden Sie den Server mit Glasfaserkabel an!

Bild unten rechts: SO NICHT!

Die Stockwerks-Switches sind busartig miteinander verbunden. Der (geringe) Vorteil einer kürzeren Verkabelungsstrecke hat den gewaltigen Nachteil, dass die Bandbreite umso geringer wird, je weiter ein PC vom Server entfernt ist.

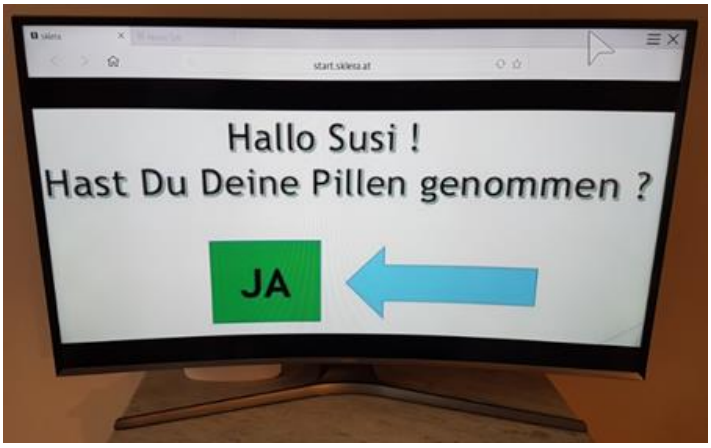




Smart TV und AAL

Manfred Wöhrl

Ambient Assisted Living (**AAL**, auf Deutsch **Altersgerechte Assistenzsysteme für ein selbstbestimmtes Leben**, umgebungsunterstütztes Leben, selbstbestimmtes Leben durch innovative Technik oder Assistenzsysteme fürs Alter). Manchmal liest man auch **Active and Assisted Living**.



Dieser Artikel beschäftigt sich mit den Möglichkeiten des Einsatzes neuer Fernsehgeräte mit eingebauter „Intelligenz“, d.h. TVs, die eigentlich bereits vollständige Computer sind, von denen Zig-Tausende in den österreichischen Haushalten installiert sind und nur ein Teil im Internet angebunden ist.

Durch Einsatz dieser Geräte im Bereich von AAL können Services speziell für ältere Leute äußerst kostengünstig und effizient angeboten werden, wobei klarerweise auch andere Assistenzsysteme zusätzlich verwendet werden können und sollen. Im speziellen könnten diese zusätzlichen Unterstützungssysteme mit dem Smart-TV kommunizieren und diesen im einfachsten Fall auch als Kommunikationsschnittstelle zu betreuenden Stellen verwenden.

In den letzten Jahren hat sich das Fernsehgerät der ersten Stunde zu einem universellen Computer entwickelt. Die Einsatz-Palette reicht dabei von einfacher, gezielter Informationsverteilung bis zu vollständigen Dialogsystemen inklusive Videokonferenz im betreuten Wohnen aber auch in Seniorenheimen für die Kommunikation mit Bekannten und Verwandten. Im Vordergrund steht dabei vor allem die Lesbarkeit angezeigte Information auf größeren Bildschirmen, leistbar geworden durch den Preisverfall bei Smart-TVs in den letzten Jahren. Gerade im Seniorenbereich spielt die Größe eines Bildschirms eine wesentliche Rolle, da durch meistens eine im fortgeschrittenen Alter zunehmende Sehschwäche auftritt. Hier wird es oft schwierig, mit Standard-Apps zu operieren, auch wenn ihn Zukunft die Sprachkommunikation auf dieser Ebene zunehmen wird. Mobile Devices - wie bereits vielfach im Einsatz - können durchaus als Bedienelement für den großen TV-Schirm dienen und diesen vor allem als Anzeigeanzeigegerät verwenden. Die bereits vielfach eingesetzte Kopplung von Handy und Tablett mit dem Smart TV zum Spiegeln der Anzeige ist oft betagten Benutzern von der Bedienung her nicht einfach und stabil genug und daher kaum zumutbar.

Dieser Artikel soll neue Wege für die Kommunikation im höheren Alter aufzeigen, die es ermöglichen sollen, einer möglichen Vereinsamung entgegenzuwirken und den Kontakt zu Verwandten und Bekannten auch bei reduzierter Mobilität weiterhin zu gewährleisten. Zusätzlich bieten die intelligenten Bildschirme als neuartige Dialogsysteme neben der üblichen Funktion als Fernsehgeräte eine Reihe operativer Ergänzungen für Betreuer bzw. Verwandte.

Eine wesentliche Voraussetzung für den multifunktionellen und gleichzeitig einfach benutzbaren Einsatz des TV Gerätes ist der Wechsel der bisher mitgelieferten Fernbedienung ein!

Lösungsansatz

- Einsatz spezieller Fernbedienung mit wenigen Tasten; diese müssen erhoben und somit spürbar sein, eventuell mit kleinem eingebauten Touchpad. (Bilder rechts unten; Quelle: Amazon)
- Verwenden eines kleinen Tablet-Computers zur Verwendung als Fernbedienung und universelles bedienen Gerät für andere AAL-Dienste. Hier ist besonders auf die einfache Benutzbarkeit zu achten!
- Generell Wechsel auf sprachgesteuerte Devices von Fernbedienungen mit eingebauten Mikrofon bis zur Sprachüberwachung der gesamten räumlichen Umgebung, die automatisch Hilferufe erkennt und Aktionen einleitet.

Leitsysteme

Unter dem Schlagwort „Digital-Signage“ kann auf einfache Art und Weise über Internet zeitgesteuert und zielgerichtet Information auf eine beliebige Zahl von Bildschirmen übertragen werden. Speziell durch den Einsatz großer Bildschirme ist diese Technik auch bei eventueller Sehschwäche der Zielgruppe bei zusätzlicher akustischer Signalisierung sinnvoll einsetzbar. Besonders in Seniorenheimen können damit bei entsprechender Positionierung in den Etagen und bei Aufzügen Orientierungshilfen gegeben werden. In einem speziellen Modell könnte über Bluetooth- oder RFID-Technik auch ein persönliches Leitsystem etabliert werden d.h. der Bildschirm erkennt Personen in seinem Umfeld und kann damit zielgerichtet diese mit Hinweisen versorgen. Diese Personalisierung könnte nach dem heutigen Stand der Technik auch über Bildanalyse einer Webcam erfolgen.

Planungshilfen

Durch die Dialogfähigkeit intelligenter TV-Bildschirme kann von der Menüauswahl im Reha-Zentrum bis zum Reservierungssystem bzw. Buchungssystem von Leistungen eines Hauses die Anwendung variieren.

Erinnerungssysteme

In Ergänzung zum Planungssystem können Erinnerungen für die Einnahme von Medikamenten (inklusive Bestätigung auf einer Taste der Fernbedienung) - auch mit Unterbrechung des augenblicklich laufenden TV-Programms - inklusive akustischen Signal übertragen werden. Bei Einsatz im Seniorenheim oder Reha-Zentrum kann auch automatisch und zeitgerecht auf medizinische Termine hingewiesen werden.

Informationssysteme

Ein einfaches Auskunftssystem in unterschiedlichen Ausprägungen, gesteuert mit einigen wenigen Tasten kann sinnvolle Informationen über das Haus bzw. im be-

treuten Wohnen über geplante Termine, eventuell Busfahrpläne usw. bereitstellen, ohne „verwirrenden“ Informationsflut seitens Internet, Google und Co.

Dialogsysteme

Durch eine Reihe von nationalen und internationalen Initiativen steigt die verfügbare Bandbreite im Internet und damit auch die Möglichkeit, kostengünstig und in entsprechender Qualität einfache Videokonferenzsysteme umzusetzen. In einfachster Form kann ein Dialog zwischen zwei Personen unter Einsatz einer Webcam und eines intelligenten TV-Gerätes in ansprechender Form gestaltet werden. Auch hier steht die Usability absolut im Vordergrund, die Verwendung muss mit wenigen Aktionen, angepasst an die altersbedingten sensorischen Einschränkungen der Benutzer möglich sein.

Überwachungssysteme

Als vollwertige Computer bieten moderne Smart-TVs auch die Möglichkeit des Anschlusses von Sensoren bzw. über Schnittstellen die Verbindung zu medizinischen Unterstützungstechniken. Damit könnte der Smart-TV eine zentrale Rolle bei zukünftigen AAL-Implementierungen darstellen.

Der wesentliche Vorteil des Einsatzes des Smart-TVs als Element in der Seniorenbetreuung liegt vor allem in der großen Verbreitung, der Einfachheit des Systems, entsprechend lange Garantiezeit, einfache Installation und Fernwartung. Für die praktische Umsetzung sind Systemintegratoren gefragt, die neben der Lieferung des Smart-TV und eventuell der Bereitstellung eines WLAN Zuganges auch dessen Integration ins Netz durchführen, die bei entsprechender Kenntnis in wenigen Minuten erledigt ist. Gefragt ist eine Kooperation mit einem Handynetzbetreiber bzw. mit TV-Geräteanbietern. Das Know-how für Entwicklungen für Lösungen bzw. Anwendungen im Bereich Smart-TV ist vorhanden bzw. sind bereits Anwendungen, zumindest rudimentär am Markt vorhanden. Eine abgestimmte Koordination von bereits unterschiedlichen Aktivitäten im AAL und entsprechende Zusammenführung von Stakeholder könnte kurz bzw. mittelfristig zu leistbaren und akzeptablen Produkten - auch mit nicht unbeträchtlichen Exportchancen - führen.

Wie nebenstehende Tabelle zeigt, gibt es für Senioren eine Vielzahl von Einsatzmöglichkeiten in nahezu allen Bereichen:

Die Technik

Durch den Einsatz neuester Techniken und Methoden können kostengünstige Lösungen umgesetzt werden. Dazu zählen vor allem

- Datenablage und Infrastruktur: Die Cloud
- Device-Unabhängigkeit: HTML-5 und moderne Entwicklungswerkzeuge
- Benutzerakzeptanz: Usability nach dem Stand der Technik, speziell für ältere Benutzer
- Offene Systemumgebung: einfache Schnittstellen - Realisierung zu anderen Assistenzsystemen (IoT... Internet of Things)

In Zukunft wird das unterlagerte Betriebssystem in einem TV-Gerät zunehmend der „Master“ sein, d.h. der Benutzer muss nicht umständlich aus seiner TV-Umgebung ins Internet wechseln und dort seine Webseite aufrufen, sondern das intelligente TV startet prinzipiell unter Rechnerkontrolle und die Anzeige von Fernsehkanälen ist nur mehr eine Anwendung, ebenso wie Videoconferencing oder andere Aufgaben, wie Erinnerungs- oder Leitsysteme bzw. Informationsabfragen. Letztere kann damit viel einfacher gestaltet werden, ältere Benutzer „verirren“ sich nicht mehr so leicht wie bisher im World Wide Web. Damit entsteht auch eine neue Art der Informationsverteilung und ein neuer Markt für zielgerichtet für Senioren entwickelte Anwendungen, transparent und einfach in der Handhabung, jenseits des sich derzeit entwickelnden Apps-Wildwuchses.

Zusammenfassend ist festzustellen, dass in den nächsten Jahren zunehmend Digital-Natives, die von Kindheit an mit dem Umgang digitaler Systeme vertraut sind - altersbedingt - als Zielgruppe für AAL in den Vordergrund treten werden, wodurch die Akzeptanz von digitalen Assistenzsystemen deutlich steigen wird. Die Scheu vor „Überwachung“ wird der Erkenntnis über den Nutzen im Notfall weichen. Zusätzlich kommen neue Techniken - speziell in der Kommunikation mit dem Benutzer, wobei im hohen Alter die Sprache als Eingabe und parallel dazu die Reaktion des „intelligenten“ technischen Umfeldes sowohl akustisch als auch in großer Darstellung am TV in den Vordergrund treten werden. Nach einer Statistik wird bis zum Jahr 2030 die Zahl der zu betreuenden älteren Mitbürger um 54 % steigen. Um diesen Zuwachs sowohl organisatorisch als auch finanziell meistern zu können, sind in Zukunft vor allem preisgünstige Assistenzsysteme notwendig. Daher müssen vorhandene Ressourcen, wie ein Fernsehgerät und dessen technische Möglichkeiten, mehrfach und optimal genutzt werden, bzw. in ein umfassendes Assistenzmodell eingebunden werden. Dabei bietet gerade die „Intelligenz“ des TV-Gerätes in seinem bereits offenen Ansatz (basierend auf Linux-Derivaten) Schnittstellenmöglichkeiten, die bei vielen anderen Assistenztechniken (wie zum Beispiel Schlüsselsystemen) auf der proprietären Welt noch deutlich fehlen! Unternehmen und auch öffentliche Stellen sind gefordert, gerade im Bereich von AAL umgehend Standards und Normen umzusetzen und wo sie fehlen, noch zu definieren. Speziell Fördermaßnahmen sollten dringend auf die Einhaltung solcher Standards und Normen beharren.

Der Autor

Prof. Mag. Dr. Manfred Wöhrl ist seit mehr als 30 Jahren im Bereich der IT mit den Spezialgebieten IT-Security und Innovative Technologien tätig, war lange Jahre Lektor an der Universität Wien, Lehrbeauftragter an der Donauuniversität, der Wirtschaftsuniversität Wien und der Fachhochschule Krems und Vortragender bei einer Reihe von Seminaren und Tagungen.

Derzeit ist er Geschäftsführer der R.I.C.S. EDV-GmbH, als Systemintegrator fokussiert auf praxisorientierte Lösungen für Kunden mit speziellen Anforderungen im Web-Umfeld.

Als Sachverständiger betreut er eine Reihe renommierter Unternehmen bei der Planung und Umsetzung zukunftsweisender Strategien in der IT. Dazu zählt auch das Thema Cloudtechnik, deren sichere Implementierung und sinnvoller Einsatz im Marketing, z.B. durch Verwendung von Digital-Signage der nächsten Generation.

Einsatzmatrix	Seniorenheim	Betreutes Wohnen	Privatbereich
Leitsysteme	x	-	-
Planungshilfen	x	x	-
Erinnerungssysteme	x	x	x
Informationssysteme	x	x	x
Dialogsysteme	x	x	x
Überwachungssysteme	x	x	x

techBold