TECHNISCHE UNIVERSITÄT WIEN

VIENNA UNIVERSITY OF TECHNOLOGY

IBK Institut für Breitbandkommunikation

Unterlagen zu den Vorlesungen

DATENKOMMUNIKATION

und

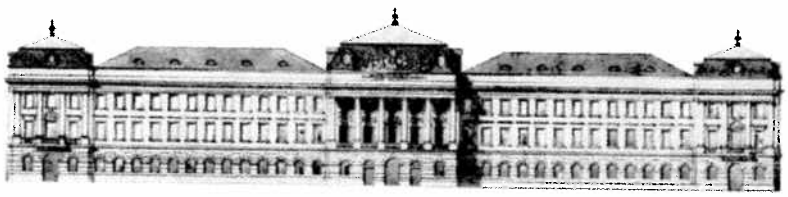
KOMMUNIKATIONSPROTOKOLLE

Teil 1

o. Univ. Prof. Dr. Harmen R. van As

Technische Universität Wien, Institut für Breitbandkommunikation

A-1040 Wien, Favoritenstr. 9-11/388



Datenkommunikation Teil 1

Vorlesung Datenkommunikation

Version: Feb.

Teil 1.0: Einleitung

- Übersicht über die Vorlesung, Ziele, Fragestellungen
- Akteure in der Telekommunikation
- Netzausdehnungen, Netzebene-Architektur, Akronyme
- OSI-Referenzmodell
- Standardisierung

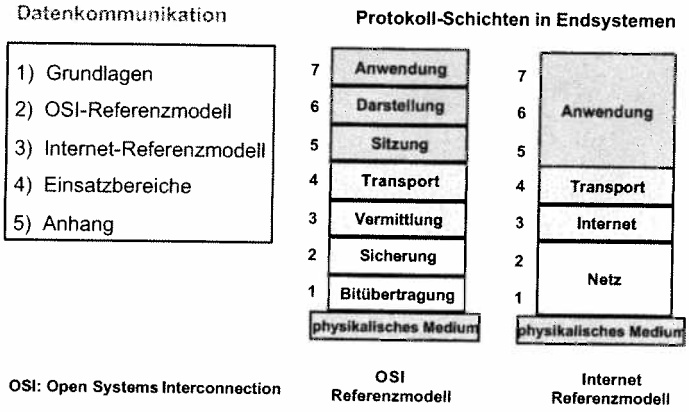


Bild: Übersicht der Vorlesung

Teil 1: Grundlagen

0) Einleitung
1) Überblick
2) Anwendungsgebiete und Anforderungen
3) Adressierung und Netzstrukturen
4) Kommunikationsverfahren
5) Übertragung
6) Vermittlung
7) Schichtenmodelle und Protokolle

Bild: Übersicht über Teil 1 der Vorlesung

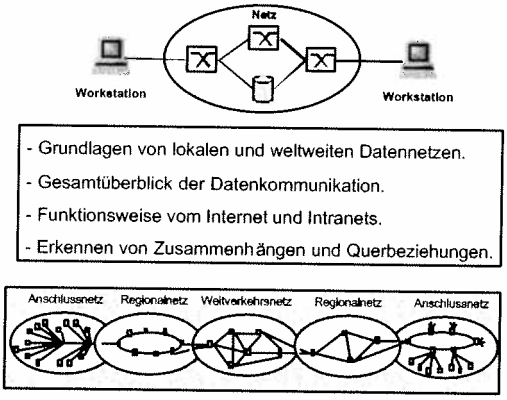


Bild: Ziele der Vorlesung

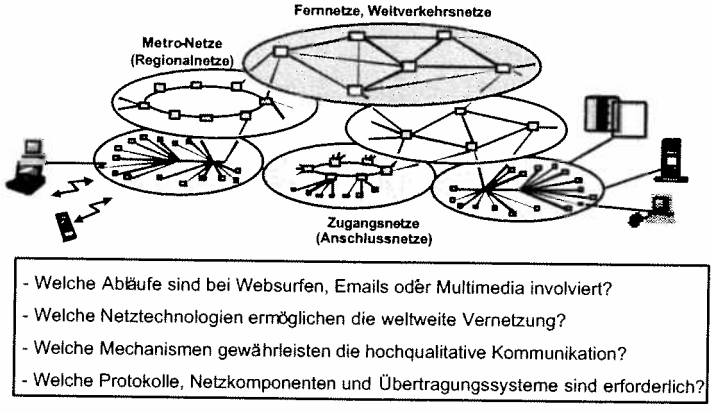


Bild: Zentrale Fragen in der Vorlesung

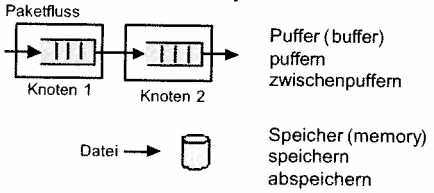
Bitraten

bit/s		
kbit/s	kilo	10^3
Mbit/s	mega	10^6
Gbit/s	giga	10^9
Tbit/s	tera	10^{12}
Pbit/s	peta	10^{15}

Speicher Puffer

KB	Kilobyte	
MB	Megabyte	**k = 1000**
GB	Gigabyte	**K = 1024**
TB	Terabyte	
PB	Petabyte	

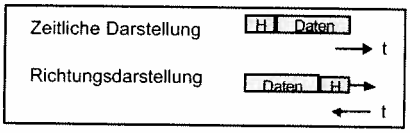
1 Byte = 1 Oktett = 8 Bit



englisch	deutsch
Network	Netz Netzknoten Netzhierarchie Netzschnittstelle Netzmanagement
Circuit	Netzwerk Schaltungsnetzwerk
Air interface	Funkschnittstelle

In meinen Vorlesungen und Prüfungen:

NIE: Netzwerk
NIE: Luftschnittstelle



Echte Profis in der Telekommunikation kennen die Unterschiede:

Netz – Netzwerk
Funkschnittstelle – Luftschnittstelle
Puffer – Speicher
K und k

Bild: Bezeichnungen

1.1 Überblick

Datenkommunikation im weltweiten Netz von verteilen Systemen erlaubt durch den hohen Vermaschungsgrad der Netze, die Netzressourcen flexibel auszunutzen, den Netzlast über mehrere Wege auszugleichen, und bei einem Kabelbruch oder einem Knotenausfall die Redundanz der Netzressourcen auszunutzen. Internet-Kommunikation ist distanzunabhängig. Bei jeder Webabfrage kann, teilweise fast verzögerungslos, ein anderes Kontinent angesprochen sein. Die Vorlesung soll einen Einblick hinter den Kulissen ermöglichen und Fragen, wie sie im Bild aufgelistet sind, beantworten.

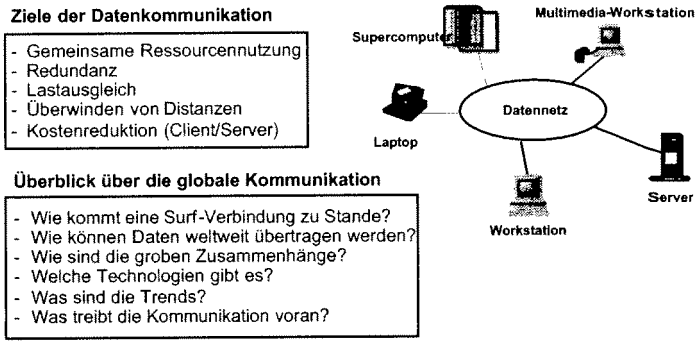


Bild: Abschnitt 1.1. – Überblick

1.2 Anwendungsgebiete und Anforderungen

Die schnelle Entwicklung der Technologien der Datenkommunikation werden vorangetrieben durch attraktive Dienste, die von Geschäftsbereichen und privaten Haushalten intensiv genutzt werden und so für die Akteure der Telkommunikation finanziell stimulierend wirken. Wichtige Anwendungsgebiete sind heute der Informationszugriff sowie die visuelle Kommunikation. Wesentliche Anwendungen sind im Bild aufgelistet. Jede Anwendung stellt seine speziellen Anforderungen an die Netztechnologien. Die härteste Anforderung kommt von der interaktiven Echtzeit-Kommunikation zwischen Menschen, wo der Verzögerungszeit durch das Netz enge Grenzen gesetzt werden müssen, um eine natürliche Konversation zu erlauben. Der Idealwert von 80 ms wird in Paketvermittelten Netzen bei weitem nicht erreicht.

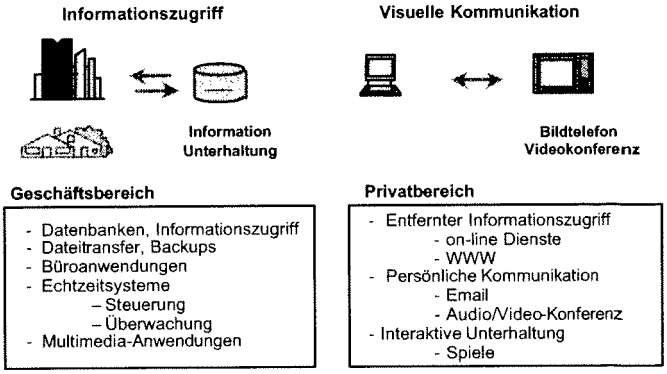


Bild: Abschnitt 1.2. - Anwendungsgebiete und Anforderungen

1.3 Netzstrukturen

Hauptaufgabe von Netzen ist die Vernetzung von Endsystemen. Dabei können wir zwischen der physikalischen Netzinfrastruktur und der logischen Vernetzung auf dieser Infrastruktur unterscheiden. In lokalen Netzen sowie in Industrienetzen findet man Stern-, Bus- und Ringstrukturen, aber auch vermehrt Vermaschung. Verkabelte Zugangsnetze sind hauptsächlich stern- oder ringförmig. Dagegen sind Fernsehkabelnetze nur baumförmig. In Regionalnetzen werden gerne Ringe eingesetzt und im Fernnetz findet man vermaschte Ringstrukturen. Eine globale Netzinfrastruktur ist hierarchisch aufgebaut.

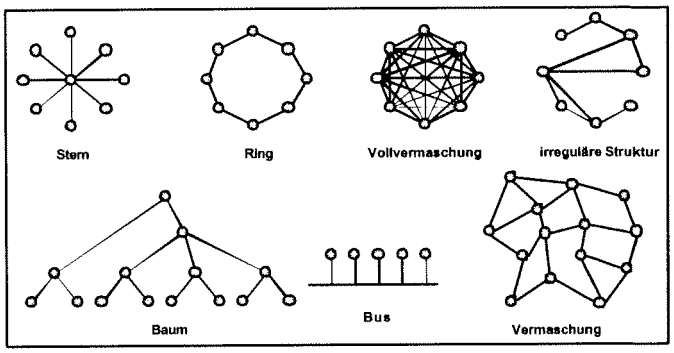


Bild: Abschnitt 1.3. - Netzstrukturen und Netztopologien

1.4 Nummerierung und Adressierung

Bei der globalen Vernetzung spielt auch die Adressierung ein zentrale Rolle. Hier gibt es eine Reihe von Adressier- und Nummerierungssysteme, die alle zusammen wirken müssen.

PSTN	Public Switched Telephone Network
ISDN	Integrated Services Digital Network
NSAP	Network Service Access Point
ATM	Asynchronous Transfer Mode
Email	Electronic Mail
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IEEE MAC	IEEE Medium Access Control
Identifier	interne Netzadressierung
SAP	Service Access Point (Protokoll-Pfade)

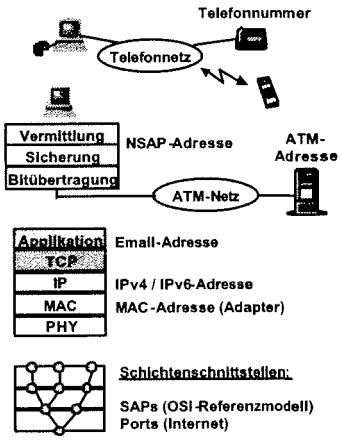


Bild: Abschnitt 1.4. – Nummerierung und Adressierung

1.5 Kommunikationsverfahren

Zur Aufteilung der Aufgaben in einer Kommunikationsverbindung wird ein Modell benötigt. Je nach Verbindungsart werden nicht alle Funktionsteile vorhanden sein. In einem Rechner werden zum Beispiel alle Daten bereits in digitaler Form erzeugt. Hauptkomponenten in der Senderichtung sind die Quellencodierung zur Digitalisierung und Datenreduktion, die Kanalcodierung zur gezielten Datenzusatz, die Leitungs- oder Basisbandcodierung zur Übertragungsanpassung und die Modulation im Falle einer Übertragung auf einem Frequenz- oder Wellenlängenträger.

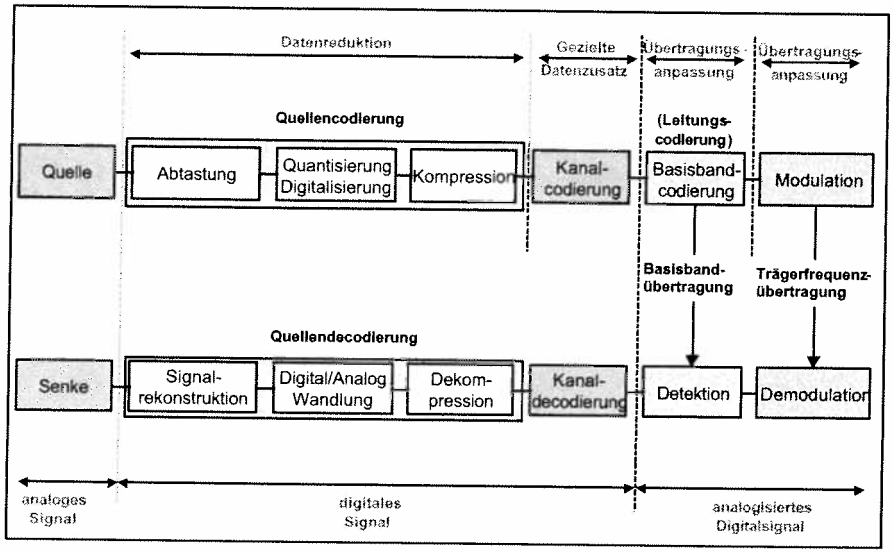


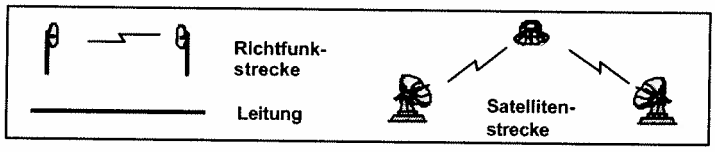
Bild: Abschnitt 1.5. – Kommunikationsverfahren

Ferner kann unterschieden werden zwischen einem rein-analogen Signal in analogen Endeinrichtungen, einem Digitalsignal in der Systemhardware und einem analogisierten Digitalsignal auf der Übertragungsstrecke.

1.6 Übertragung

Hauptthemen bei der Übertragung sind die Beschreibung der diversen Übertragungsmedien, die Angabe der Übertragungsarten, die Vorstellung der Multiplex- und Duplexverfahren auf Leitungen und im Funk sowie die Taktrückgewinnung am Empfänger.

- **Multplexverfahren** dienen dazu, das betrachtete Übertragungsmedium (Kupferleitung, Koaxialkabel, Glasfaser oder Funkraum) mehrfach auszunutzen.
- **Duplexverfahren** sind Übertragungsverfahren, bei dem Daten gleichzeitig in beiden Richtungen übertragen werden (Raum, Frequenz, Wellenlänge, Zeit, Code).



- **Übertragungsmedien:** Kupferkabel, Koaxialkabel und Glasfaser
  Richtfunkstrecke und Satellitenstrecke
- **Übertragungsbetrieb:** parallel, seriell, simplex, duplex
- **Übertragungsmultiplex:** Raum, Frequenz, Wellenlänge, Zeit, Code, Paket
- **Synchronisation:** Bit, Byte, Übertragungsrahmen

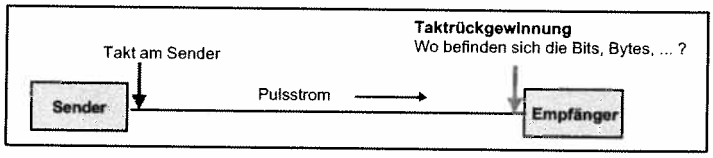


Bild: Abschnitt 1.6. – Übertragung

1.7 Vermittlung

Bei der Vermittlung geht es in erster Linie um die Gegenüberstellung von Leitungs- und Paketvermittlung und die dazu benötigten synchronen und asynchronen Koppelnetze. Dabei betrachtet man die Raum-, Zeit, und Wellenlängenvermittlung sowie deren Kombinationen. Ferner wird die allgemeine Struktur von Vermittlungsstellen und Router vorgestellt.

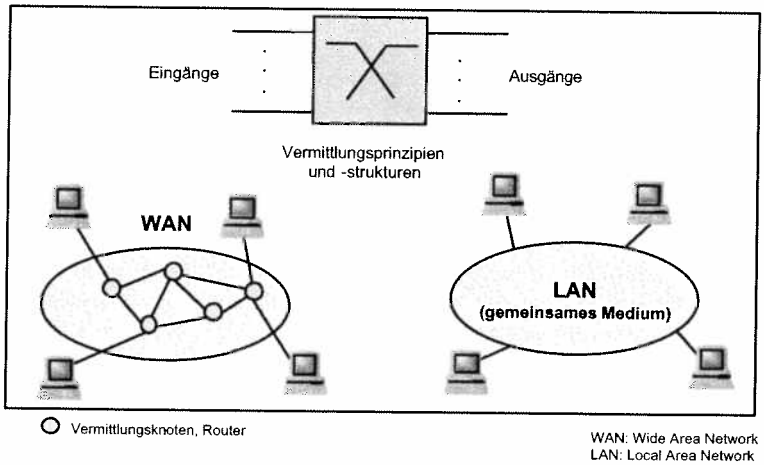


Bild: Abschnitt 1.7. - Vermittlung

1.8: Schichtenmodelle und Protokolle

Neben dem siebenschichtigen OSI-Referenzmodell muss man weitere Referenzmodelle (Protokollstapel, protocol stack) betrachten. So hat das Internet-Modell nur vier Schichten, das LAN-Modell eine weitere Unterteilung der beiden ersten Schichten und so gibt es ein paar Referenzmodelle mehr. Wesentlich ist aber das Schichtungskonzept. Ferner sind in modernen Protokolldefinitionen Referenzmodellerweiterungen zu betrachten. Dabei sind erstens zwei Zusatzprotokollstapel eingeführt und betrachtet so Signalisierung (Kontrolle), Benutzer und Netzmanagement. Zweitens verwendet man den Begriff Stratum, wo die Bitübertragungsschicht ersetzt wird durch die Protokollstruktur der verwendeten Technologie, z.B. Internetprotokoll – ATM – SDH – Optik bewirkt einen dreimaligen Ersatz.

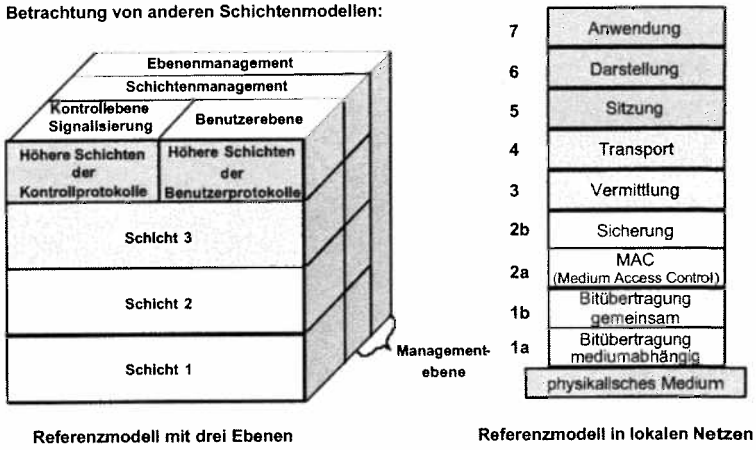


Bild: Abschnitt 1.8. - Schichtenmodelle und Protokolle

Die **Akteure** im Netz-Lebenszyklus sind Personen oder Institutionen, die in einer oder in mehreren Phasen beteiligt sind. Die verschiedenen Akteure haben unterschiedliche Aufgaben und müssen unterschiedliche Qualifikationen besitzen.

Der **Anwender** (user) eines Rechnernetzes ist die wirkliche Ursache für die Realisierung und den Betrieb solcher Netze. Somit kommt den Bedürfnissen des Anwenders die höchste Priorität zu. Technische Eigenschaften und Besonderheiten sind nur von Bedeutung, wenn sie zum Anwendernutzen beitragen.

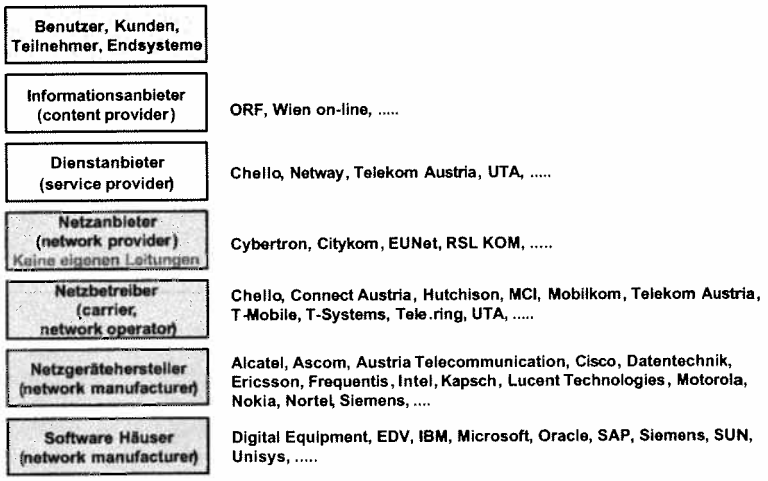


Bild: Akteure in Telekommunikation

Ein **Netzplaner** ist für die Planung eines neuen oder die Migration eines bestehenden Netzes zuständig. Der Netzinstallateur führt primär Installationen durch, muss aber zur Inbetriebnahme und Fehlersuche manchmal den Netztechniker oder Netzingenieur zuziehen.

Ein **Provider** ist allgemein ein Lieferant bzw. Dienstanbieter. Bei Netzen wird zwischen Network Provider (Netzanbieter) und Service Provider (Dienstanbieter) unterschieden. Ein Netzanbieter stellt Netzdienste (auch als Transportdienste bezeichnet) zur Verfügung, deren Eigenschaften höchstens bis zur OSI-Schicht 3 vorgegeben sind. Im Gegensatz dazu werden Kommunikationsdienste (auch als Telematikdienste bezeichnet) vom Provider bis zur OSI-Schicht 7 spezifiziert. Das Endgerät muss sich an die jeweiligen Vorgaben des Providers halten.

Content Provider stellen (Informations-)Inhalte zu Verfügung. Dazu bereiten sie Informationen so auf, dass die Darstellung dem World Wide Web angemessen ist. Im Tätigkeitsgebiet des Content Providers gibt es eine Anzahl verschiedenartiger Akteure:

- **WebDesigner** setzen Papierdokumente in ansprechende elektronische Dokumente um.
- **Autoren bzw. Dozenten** bereiten Lehrinhalte für Teleteaching und Telelearning auf.
- **Web Master** aktualisieren Webseiten (Einfügen neuer Inhalte und Fehlerbeseitigung).
- **Post Master** betreiben Mail Server.
- **Informationsmanager** erstellen und betreiben Kataloge und Suchmaschinen.
- **Portalbetreiber** bieten Webseiten mit einem breiten Informations-, Dienstleistungs- und Warenangebot aus einem bestimmten Themenbereich an.

Ein **Service Provider** bietet Dienste an, die bis zur Schicht 7 des OSI-Modells oder darüber hinaus reichen.

- Ein **ISP (Internet Service Provider)** betreibt ein Netz, das mit dem Internet verbunden ist. Die Größe des Netzes kann von lokal bis global reichen. Die Zugangspunkte des Netzes werden als PoP (Point of Presence) bezeichnet, sie sollen möglichst nah beim Nutzern ein, damit zwischen Nutzer und PoP eine Zugangsleitung mit Ortstarif ausreichend ist. Der ISP betreibt im Allgemeinen verschiedene Server (DNS-Server, E-Mail Server, WWW-Server, ...). ISPs sind mit mehreren anderen ISPs verbunden, um den Datenverkehr ohne lange Umwege weiterleiten zu können. Verbindungen zu zentralen Austauschpunkten sind ebenfalls vorteilhaft. Viele ISPs bieten weitere Leistungen an.
- **Content Hosting** ist eine Dienstleistung eines Providers, der seinem Kunden Server zur Verfügung stellt, auf denen der Kunde seine Inhalte anbieten kann. Er erspart dem Kunden den Betrieb eines eigenen Servers und eine Standleitung vom Server zum ISP.
- **Server Housing** bedeutet dass der Server im Besitz des Kunden ist, aber physisch befindet sich der Server jedoch beim Provider, der auch für dessen Betrieb verantwortlich ist.

Ein **Netzanbieter** (Reseller, Wiederverkäufer) ist ein Provider, der Netzdienste anbietet, ohne selbst ein Netzbetreiber zu sein. Dazu kauft er bei einem Netzbetreiber Übertragungskapazität in großen Mengen ein und verkauft sie an seine Kunden weiter.

Netzbetreiber (carrier) betreiben Netze, die sie der Allgemeinheit zur Nutzung anbieten. Damit handelt es sich um öffentliche Netze. Private Netze (corporate networks) werden von Firmen oder Institutionen nur für die eigene Nutzung betrieben. Corporate Networks sind jedoch (außerhalb des LAN-Bereichs) auf Leitungen angewiesen, die von öffentlichen Netzbetreibern gemietet werden. Aus der Sicht des Netzmanagements ist die Firma/Institution aber als Netzbetreiber zu verstehen. Ein Corporate Network kann auch auf dem Wege des Outsourcing durch einen Dienstanbieter für eine auftraggebende Firma realisiert und betrieben werden.

Access Provider ermöglichen den Zugang zu einem Netz, das dann als Backbone- oder Kernnetz zu verstehen ist. Der Access Provider selbst stellt also ein Zugangsnetz zur Verfügung. Dieses kann dem Access Provider selber oder einem anderen Netzbetreiber gehören.

Ferner gibt es **Gerätehersteller** und **Software-Häuser**, die die entsprechenden Produkten entwickeln, herstellen und verkaufen.

Beide nachfolgende Bilder zeigen die Standorte der Festnetzbetreiber und Internet Service Provider.

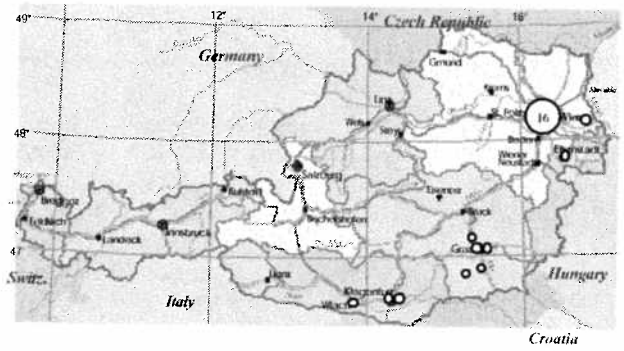


Bild: Festnetzbetreiber in Österreich

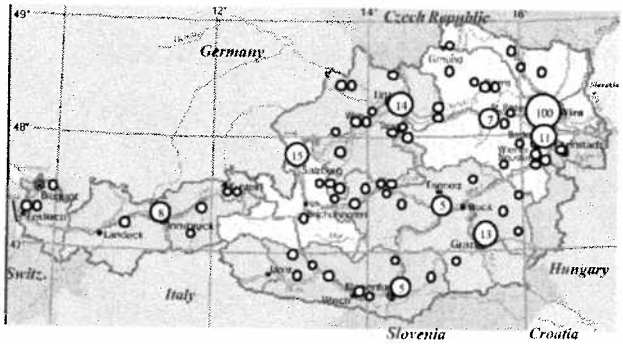


Bild: Internet Service Provider in Österreich

Internet-Verkehr zwischen ISPs wird über Internet Exchange Knoten ausgetauscht. Die Standorte in Europa sind im nachfolgenden Bild dargestellt.

In Österreich wird diese Funktion vom Rechenzentrum der Universität Wien übernommen. Hier werden alle österreichischen ISPs unter sich und mit dem Ausland verbunden. VIX (Vienna Internet eXchange) verbindet auch das ACONET (Academic Computer Network) mit anderen akademischen Netzen und dem weltweitem Internet. Zur Überwachung und Abrechnung werden die Datenvolumen in den diversen Richtungen gemessen und gespeichert.

Das paneuropäische Netz Géant bildet die europäische akademische Netzinfrastruktur. Über die nationalen akademischen Netze sowie interkontinentale Verbindungen mit den akademischen Infrastrukturen dort, sind alle Universitäten und Forschungseinrichtungen weltweit mit gute Durchsatzraten erreichbar.

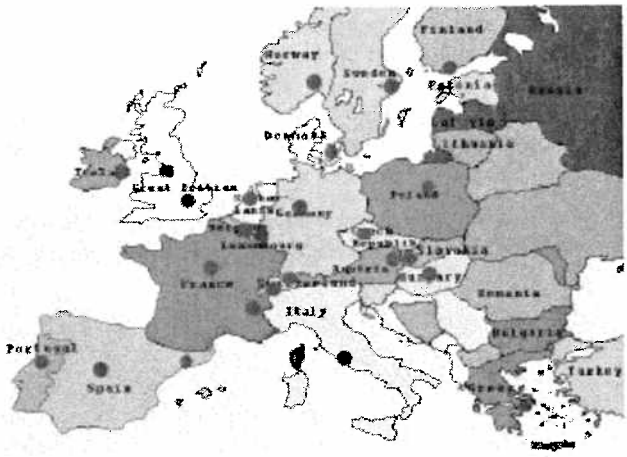


Bild: Internet Exchange Knoten in Europa

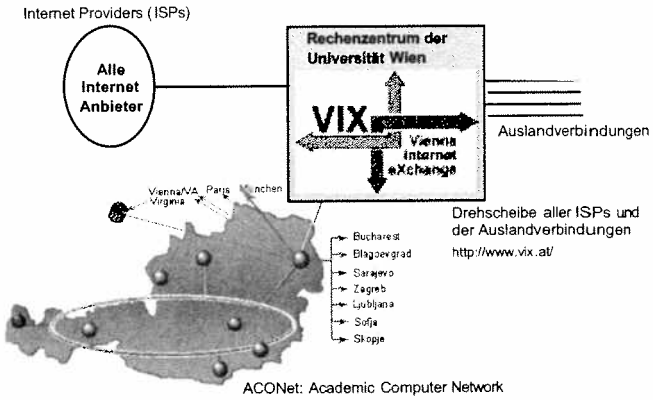


Bild: Internet Exchange Knoten in Österreich

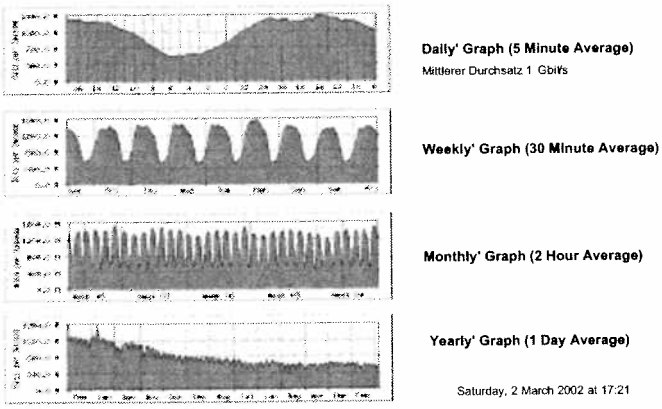


Bild: Verkehrsmessungen im VIX

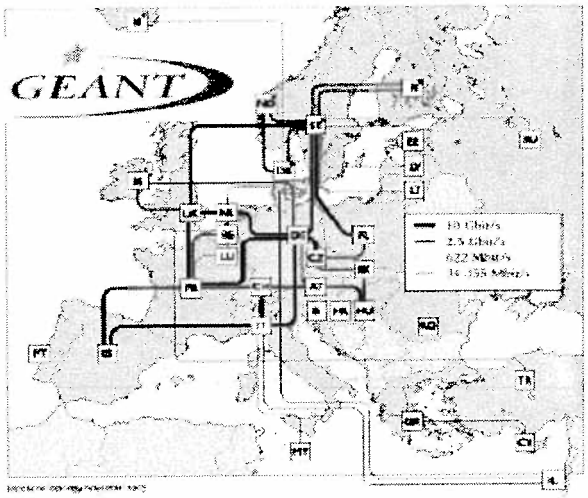


Bild: Research and Educational Network (GEANT)

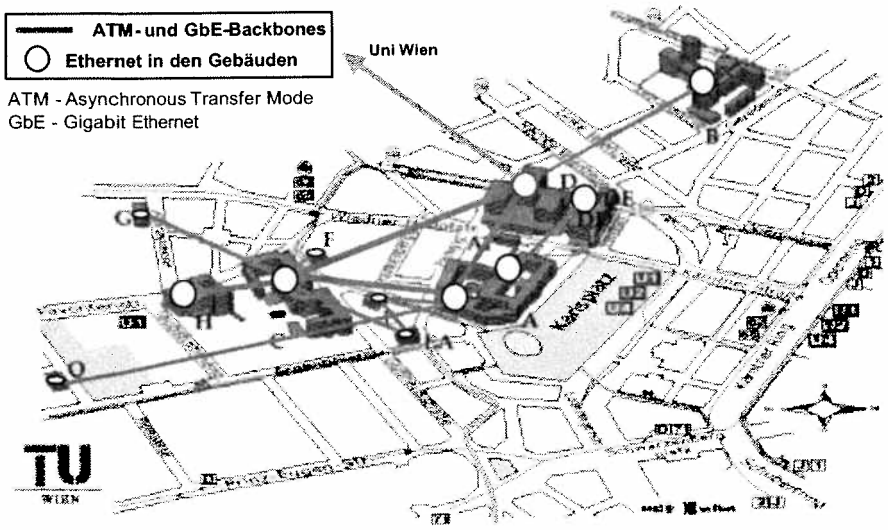


Bild: Backbone-Netz der TU

Das Backbone-Netz der TU-Wien basiert auf ein ATM-Netz, worüber sowohl Telefonie als auch Datenkommunikation abgewickelt wird sowie auf Gigabit-Ethernet (GbE) für reine Daten. In den Gebäuden sind die Institutsnetze und die Netze anderer Abteilungen der TU über eine strukturierte Verkabelung am Backbone angeschlossen. Diese Netze basieren auf der Ethernet Technologie mit 10/100 Mbit/s Rechneranschlüssen und bis zu 1 Gbit/s Verbindungen zwischen Hubs, Switches und Routern.

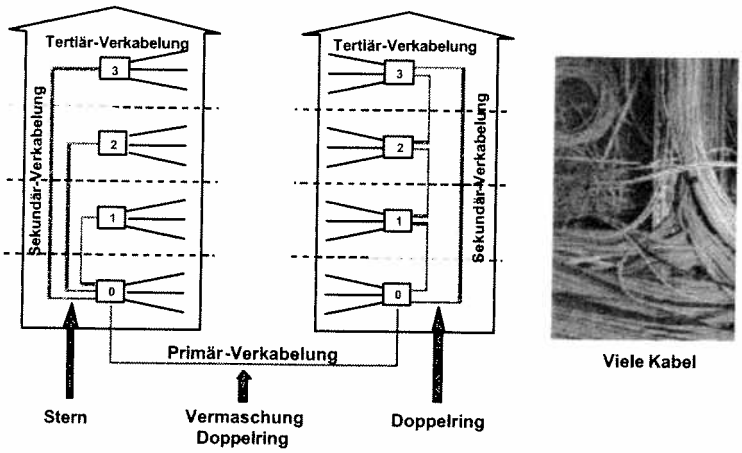


Bild: Strukturierte Gebäudeverkabelung

In heutigen Ethernet-basierten Netzen findet man Ethernet mit 10 und Fast-Ethernet mit 100 Mbit/s zwischen Endsystemen und Hubs und Switches. Die Switches werden wiederum mit Fast-Ethernet oder Gigabit-Ethernet (GbE) mit einer Bitrate von 1 Gbit/s verbunden. Auch 10 Gigabit-Ethernet (10GbE) mit einer Bitrate von 10 Gbit/s wird bereits eingesetzt. All diese Systeme haben ihre eigene Verkabelungsanforderungen. Eine strukturierte Verkabelung mit einer Primär-Verkabelung zwischen Gebäuden und Standorten, eine Sekundär-Verkabelung zwischen den Etagen und eine Tertiär-Verkabelung pro Stockwerk versucht man den Kommunikationsinfrastruktur möglichst flexible und zukunftssicher zu gestalten. Zur Auswahl stehen eine Vielzahl von abgeschirmten und nicht-abgeschirmten elektrischen Kabeltypen sowie verschiedenen Glasfaser- und Lasertypen.

Rechnerdistanz	Ausdehnung	Beispiel
1 cm	Chip	Chip-Rechnernetz
10 cm	Rechnerplatine	Platine-Rechnernetz
1 m	System	Mikroprozessornetz
5 m	Direkte Umgebung	Pikonetz: **PAN** (Personal Area Network)
10 m	Raum	Massenspeichernetz: **SAN** (Storage Area Network)
100 m	Gebäude	Lokales Netz: **LAN, WLAN** (Wireless Local Area Network)
1 km	Campus	
10 km	Stadt	Regionalnetz: **MAN** (Metropolitan Area Network)
100 km	Land	Weitverkehrsnetz: **WAN** (Wide Area Network)
1000 km	Kontinent	Globales Netz: **GAN** (Global Area Network)
10.000 km	Welt	

Bild: Ausdehnung von Kommunikationsnetzen

Einteilung nach geographischer Netzausdehnung:

- Verbindungsnetz zwischen Modulen auf einem Chip (Ausdehnung unter 1 cm).
- Verbindungsnetz zwischen Mikrorechnern oder Chips auf einer Platine (Ausdehnung in Bereich von 10-30 cm).
- Verbindungsnetz in einem Multi-Rechnersystem innerhalb eines gleichen Systems (Ausdehnung ein paar Meter).

- **PAN** (Personal Area Network) oder Piconetz: Die Ausdehnung beträgt wenige Meter und entspricht der Arbeitsumgebung einer Person an ihrem Arbeitsplatz. Die primäre Anwendung ist die Kommunikation zwischen Bestandteilen eines Rechnerarbeitsplatzes (Rechner, Laptop, Maus, Scanner, Drucker, Speicher, Netzanschluss).

- **SAN** (Storage Area Network- bzw. System oder Server Area Network): Die Ausdehnung beschränkt sich auf einen Raum (Rechenzentrum). Es wird zur Vernetzung der Komponenten eines großen Rechnersystems eingesetzt. Insbesondere werden Massenspeicher untereinander und mit anderen Netzen (LAN, WAN) vernetzt. Beispiele für SANs sind die Hochgeschwindigkeitsverbindungssysteme FCS (Fiber Channel System) und HIPPI (High Performance Parallel Interface).
- **LAN** (Local Area Network): Die Ausdehnung liegt zwischen 10 m und einigen km. Hauptzweck ist die Kommunikation innerhalb von Arbeitsgruppen und Abteilungen.
- **MAN** (Metropolitan Area Network): Die Ausdehnung liegt im Bereich einer Großstadt (bis ca. 100 km). Anwendungen sind die Vernetzung sehr leistungsfähiger Rechner oder Netzknoten im Regionalbereich
- **WAN** (Wide Area Network): Die Ausdehnung ist größer als bei MANs, dabei sind potenziell sehr viele Teilnehmer angeschlossen.
- **GAN** (Global Area Network): Das Netz besitzt eine weltweite Ausdehnung und bietet potenziell universelle Erreichbarkeit.

Netze jeglicher Ausdehnung sind kontinuierlich Änderungen und Erweiterungen unterworfen.
Die Phasen des Netz-Lebenszyklus sind:

- **Planungsphase:** ist von grundlegender Bedeutung für den Nutzen, der aus Netzanwendungen entsteht. Die spätere Beseitigung von Planungsmängeln und -fehlern ist aufwändig und langwierig.
- **Realisierungsphase:** ist auf Basis einer guten Planung eher unproblematisch.

- **Nutzungsphase:** ist die wichtigste und längste Phase des Netz-Lebenszyklus. Für sie ist ein angemessenes, gut funktionierendes **Netz- bzw. Systemmanagement** unerlässlich.
- **Migrationsphase:** mit der Zeit ändern sich die Anforderungen an ein Netz, so dass sogar ein gut geplantes Netz hin und wieder an die aktuelle Situation angepasst werden muss. Dies geschieht in der Migrationsphase. Die erforderlichen Verfahren und Maßnahmen sind weitgehend dieselben wie in der Planungsphase.

Die Architektur der Kommunikationsnetze lässt sich grob nach zwei Gesichtspunkten einteilen: geographisch in Anschlussnetze, Regionalnetze und Weitverkehrsnetze sowie funktionell als geschichtetes Modell in die zwei Hauptbereiche Transport und Netzintelligenz. Der Mobil- und Satellitenkommunikation kommt in allen geographischen Netzteilen eine bedeutende Rolle zu und die geschichtete Netzstruktur im Transportnetz ist weiter unterteilt.

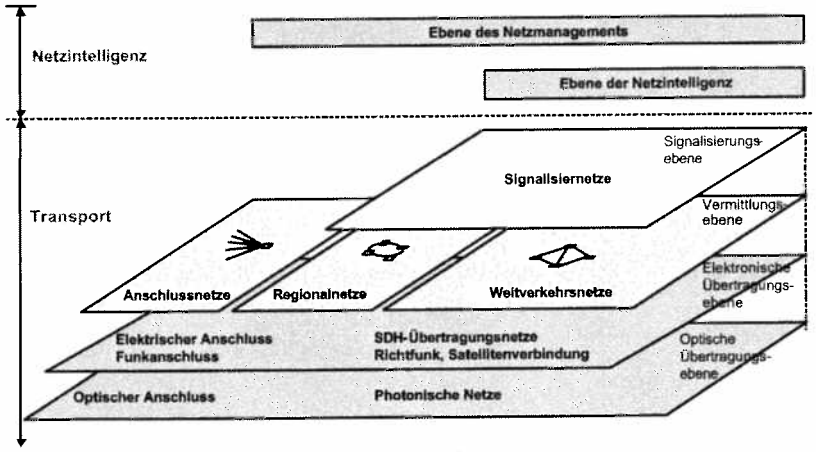


Bild: Ebene-Architektur von Kommunikationsnetzen

Ähnlich wie im OSI-Referenzmodell für die Protokollschichtung (layering) wird die Netzarchitektur in Ebenen (planes) eingeteilt. Im Mittelpunkt steht die Vermittlungsebene. Hier sind die Netzkomponenten aller Vermittlungstechnologien zu finden. Es gibt drei hierarchische Netzbereiche: die Anschlussnetze (Zugangsnetze, access networks), die Regionalnetze (metropolitan area networks, MANs) und die Weitverkehrsnetze (Fernnetze, wide area networks, WANs). Zwischen allen Netzkomponenten muss übertragen werden. Alle Übertragungseinrichtungen und -medien kann man entweder in einen elektrischen oder einen optischen Übertragungsebene einteilen.

Im Netzanschlussbereich wird über elektrische Leiter, Funk oder Glasfaser übertragen. Im Weitverkehrsnetz ist die Übertragung, mit Ausnahme von Richtfunk- und Satellitenstrecken, nur optisch über Glasfaser. Allerdings braucht jede optische Übertragung auch elektronische Endausrüstungen. Deshalb ist die elektrische Übertragungsebene immer mit dem optischen Übertragungsebene verknüpft. Wichtige elektrische Endausrüstungen speziell im Fernbereich sind die sogenannten SDH-Übertragungssysteme (SDH steht für Synchronous Digital Hierarchy). Sie bilden ein autonomes und flexibles Übertragungsnetz mit schneller Rekonfigurierbarkeit bei Ausfall von Knoten und Glasfaserkabeln. Die standardisierten Übertragungsbitraten sind 155 Mbit/s, 622 Mbit/s, 2.5 Gbit/s, 10 Gbit/s und 40 Gbit/s. Netzknoten kommunizieren über ein ausfallsicheres, eigenständiges Netz. Dies ist das Signalisierungsnetz Nummer 7 (SS7, Signalling System Number 7). Über diese Signalisierungsebene laufen auch alle Kommunikationsabläufe zur Netzintelligenzebene sowie zur Netzmanagementebene.

Die Ebenen können allgemein in zwei Bereiche eingeteilt werden: Transport und Netzintelligenz. Der Transport besteht aus allen Aufgaben, die für Vermittlung und Ende-zu-Ende Verbindungen notwendig sind. Sie werden maßgebend durch die Vermittlungstechnologien und die Kommunikationsprotokollen in den Endsystemen geprägt.

Die **Netzintelligenz** wird durch den Begriff und Realisierung der sogenannten Intelligente Netze verkörpert. Intelligente Netzen bestehen aus einem virtuellen Netz von Service Control Points (SCP) mit Datenbanken. Die Kommunikation zwischen den Service Control Points zu den Vermittlungsknoten geschieht über das Signalisierungsnetz SS7, ein robustes, eigenständiges, paketvermittelndes Netz.

Die verteilte Netzintelligenz erlaubt es:
- durch ein hierarchisches Zustandsdatenbanksystem die Netzressourcen optimal auszunutzen,
- neue Dienste flexibel und rasch einzuführen,
- kostenfreie oder kostenlimitierte Nummer (800er Bereich) und Marktorientierte Nummern (900er Bereich) zu betreiben,
- flächengreifende Dienste anzubieten, z. B. Erreichbarkeit aller Firmenstandorte unter der gleichen Vorwahlnummer,
- Mobilität in Mobilnetzen durchzuführen.

Das **Netzmanagement** erlaubt es, alle Netzeinrichtungen, bis zu jedem Kleinkomponenten, zentral zu überwachen und steuern. Die Bereiche OAMP (Operation, Administration, Maintenance and Provisioning) bilden die Basis für
- den optimalen Netzbetrieb,
- die Verwaltung der System- und Teilnehmereinrichtungen sowie die Verwaltung der Kundendienste,
- den effektiven Netzunterhalt,
- das Einrichten von speziellen Netzkonfiguration und Diensten wie zum Beispiel für Firmennetze.

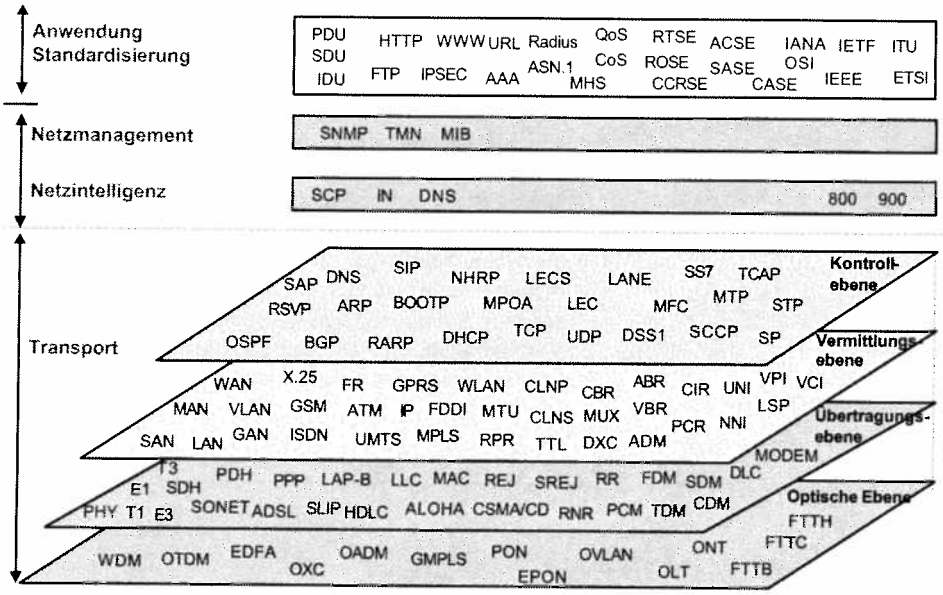


Bild: Zahlreiche Akronyme

Abkürzungen, Akronyme

In der Datenkommunikation gibt es zahllose Abkürzungen, die in Spezifikationen, Fachliteratur und -gesprächen, Produktbeschreibungen und sogar in der Werbung verwendet werden. Und bei jeder standardisierten Technologie gibt es mehr davon! Diese Kurzbezeichnungen muss man deshalb mühelos einordnen können. Das Bild zeigt eine Reihe von Abkürzungen, die alle in der Vorlesung vorkommen, auf den verschiedenen Netzebenen abgebildet.

Das OSI-Referenzmodell

Die ISO (International Standardisation Organisation) hat ab 1977 das ISO/OSI-Modell der Kommunikation in offenen Systemen entwickelt. OSI steht für Open Systems Interconnection. Ziel war es, die komplexe Aufgabe der Kommunikation zwischen verschiedenartigen Endsystemen in weniger komplexe Teilaufgaben zu zerlegen, die den einzelnen Schichten des Modells zugeordnet sind. Insgesamt sind 7 Schichten vorhanden. Die unterste Schicht 1 repräsentiert die physikalische Netzanbindung, also die Übertragungstechnik. Die Schichten 2-6 befassen sich mit zunehmend allgemeineren Funktionen der Kommunikation. Schicht 7 ist die Anwendungsschicht als Schnittstelle zwischen Kommunikations- und Anwendungssystem. Die Schichten 1-4 werden zusammen als Transportsystem, die Schichten 5-7 als Anwendungssystem bezeichnet. Dies hat aber nichts mit der eigentlichen Anwendungssoftware (Anwenderprogramm bzw. Anwendungsprozess) zu tun, die im ISO/OSI-Modell nicht betrachtet wird.

Schichtenmodelle spielen in der Kommunikationstechnik und allgemein in der Informatik an verschiedenen Stellen eine wichtige Rolle.

Sie basieren auf den folgenden Überlegungen:

- **Teilung und Beherrschung der Aufgaben:** Ein komplexes System wird zerlegt, um es für Synthese und Analyse besser beherrschbar zu machen.
- **Unabhängigkeit der Schichten:** Eine Schicht nutzt nur die Schnittstellenspezifikation zur unmittelbar darunter liegenden Schicht. Das bedeutet, der innere Aufbau der Schichten ist unwichtig, solange ihr Verhalten an der Schnittstelle gleich bleibt. Damit kann eine Schicht ausgetauscht oder ihr innerer Aufbau (Hard- oder Software) verändert werden, ohne dass das Gesamtsystem beeinflusst wird. Somit können Schichten modular (baukastenartig) kombiniert werden.
- **Abschirmung tiefer liegender Schichten:** Eine Schicht sieht nur das Verhalten der unmittelbar darunter liegenden Schicht, nicht aber das der anderen Schichten. Damit wird die wahrgenommene Komplexität des Systems reduziert (Kapselung oder Geheimnisprinzip).
- **Standardisierung:** Die Definition einzelner Schichten erleichtert die Standardisierung. Eine Schicht kann wesentlich schneller und leichter standardisiert werden als ein komplexes Gesamtsystem.

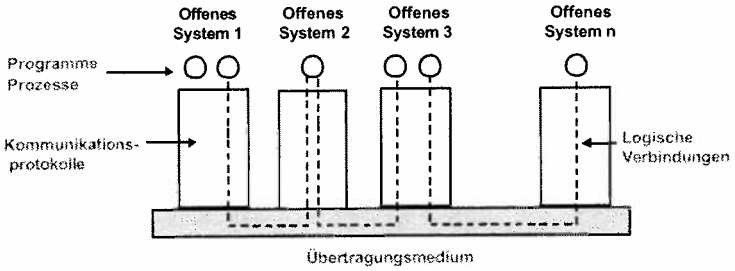


Bild: OSI: Open Systems Interconnection

Offene (Kommunikations-)Systeme bestehen aus (Hard- und Software-) Komponenten verschiedener Hersteller und sind bezüglich ihrer Anzahl und ihrer Ausdehnung nicht begrenzt. Die Offenheit wird durch eine Reihe von offenen, d.h. frei zugänglichen und nutzbaren Standards für den Informationsaustausch gewährleistet. Offene Teilsysteme können mit anderen offenen Teilsystemen, die dieselben Standards verwenden, problemlos kommunizieren. Anwenderprogramme oder Anwenderprozesse kommunizieren miteinander über logische Verbindungen, die alle das physikalische Übertragungsmedium, das Netz, benutzen.

Das Basisreferenzmodell ist ein allgemeines Architektur-Modell für die Kommunikation zwischen Systemen auf der Basis digital codierter Daten (einschließlich Text, Sprache und Bild). Das Referenzmodell definiert, welche Funktionen in welchem Zusammenhang in einer Kommunikation auftreten und stellt damit den Rahmen für die Erarbeitung von Normen auf, die nötig sind, um das Normungsziel - Offene Kommunikationssysteme (OSI: **O**pen **S**ystems **I**nterconnection) - zu erreichen.

Es beruht auf drei Konzepten:
- Strukturierung.
- Dienste.
- Protokolle.

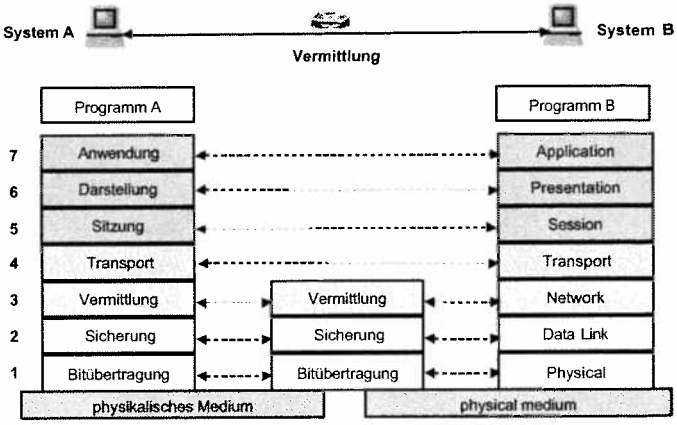


Bild: OSI-Referenzmodell

Die sieben Schichten des OSI-Modells haben grob die folgenden Aufgaben:

- **Schicht 1, Bitübertragungsschicht** (physikal layer) definiert die mechanische und elektrische Eigenschaften sowie die Funktionen und Abläufe der Bitübertragung.
- **Schicht 2, Sicherungsschicht** (data link layer) stellt sicher, dass auf einer Punkt-zu-Punkt-Übertragungsstrecke trotz gelegentlicher Störungen ein fehlerfreier Bitstrom übertragen wird.
- **Schicht 3, Vermittlungsschicht** (auch Netzschicht, network layer) bewirkt die **Adressierung** des Zielsystems und die Wegesuche durch mehrere **Transitsysteme** (Zwischensysteme) hindurch. Sie ermöglicht somit das **Internetworking** (Vernetzung von Netzen). Schichten 1-3 stellen zusammen eine Verbindung zwischen Endsystemen (Ende-zu-Ende) her.
- **Schicht 4, Transportschicht** (transport layer) stellt sicher, dass Folgen von Datenpaketen fehlerfrei, vollständig und in der richtigen Reihenfolge vom Sender zum Empfänger gelangen. Sie bildet Netzadressen auf logische Namen ab, um die richtige Anwenderprogramme auf beiden Seiten finden zu können.
- **Schicht 5, Sitzungsschicht** (auch Kommunikationssteuerungsschicht, session layer) ermöglicht die Auf- und Abbau von Kommunikationsbeziehungen (Sitzungen, sessions) sowie deren Wiederherstellung nach Störungen im Transportsystem.
- **Schicht 6, Darstellungsschicht** (presentation layer) vereinbart die verwendeten Datenformate bzw. Datencodierungen und Datenkomprimierungen sowie Umwandlungen zwischen verschiedenen Darstellungen.
- **Schicht 7, Anwendungsschicht** (application layer) stellt der Anwendungssoftware Kommunikationsdienste zur Verfügung. Aus Sicht des Anwenders ist dies die wichtigste Schicht. Sie ist am leichtesten durch Betrachtung der einzelnen Dienste zu verstehen.

Strukturierungskonzept
Das Referenzmodell beschreibt die Kommunikation zwischen Systemen, die über Übertragungsstrecken untereinander verbunden sind. Es unterscheidet drei Grundelemente:
- Verarbeitungsinstanzen,
- Systeme,
- Übertragungsstrecken.

Verarbeitungsinstanzen sind logische Einheiten, zwischen denen Kommunikation letztlich stattfindet. Der Begriff der Verarbeitungsinstanz stellt eine Abstraktion dar, hinter der real zum Beispiel ein menschlicher Benutzer an einer Benutzerstation stehen kann, oder auch ein Programm, das auf einem Rechner ausgeführt wird.

Systeme sind entweder Endsysteme, welche Verarbeitungsinstanzen enthalten, oder Transitsysteme, die Verbindungen zwischen Endsystemen herstellen, falls diese nicht direkt miteinander verbunden sind. Der Begriff des Systems stellt eine Abstraktion dar, hinter der real beispielweise ein oder mehrere Verarbeitungsrechner mit Software, Peripheriegeräten, Benutzerstationen, Übertragungsmitteln oder auch Vermittlungsknoten stehen können.

Übertragungsstrecken verbinden Systeme untereinander.

Das Prinzip der Schichtung (Layering)
Die Verarbeitungsinstanzen stützen sich in ihrer Kommunikation auf eine Hierarchie von Kommunikationsdiensten, die aus der funktionalen Zerlegung der in jeder Kommunikation auftretenden allgemeinen Komponenten hervorgeht. Ein in der Hierarchie höherer Kommunikationsdienst umfasst dabei alle in der Hierarchie niedrigeren Kommunikationsdienste.

Auf diese Weise entstehen Funktionsschichten. Sie erstrecken sich ebenso wie die Kommunikationsdienste über Systemgrenzen hinweg. Was eine derartige Funktionsschicht zu leisten hat, ist durch die sie unmittelbar eingrenzenden Kommunikationsdienste als Differenz zwischen dem jeweils höheren und niederen Kommunikationsdienst bestimmt. Die Kommunikationsdienstleistung, die in einer Schicht zu dem sie begrenzenden niederen Kommunikationsdienst addiert werden muss, um den sie begrenzenden höheren Kommunikationsdienst zu erfüllen, muss nun wieder in einem durch ein Schichtenprotokoll geregeltes Zusammenspiel zwischen Instanzen erbracht werden, die verschiedenen Systemen, aber derselben Schicht angehören. Auf diese Weise entsteht aus der Hierarchie von Kommunikationsdiensten eine Hierarchie von Instanzen und Protokollen. Die Bilder zeigen die diversen Betrachtungsweisen zur Einteilungsmöglichkeiten der Schichten.

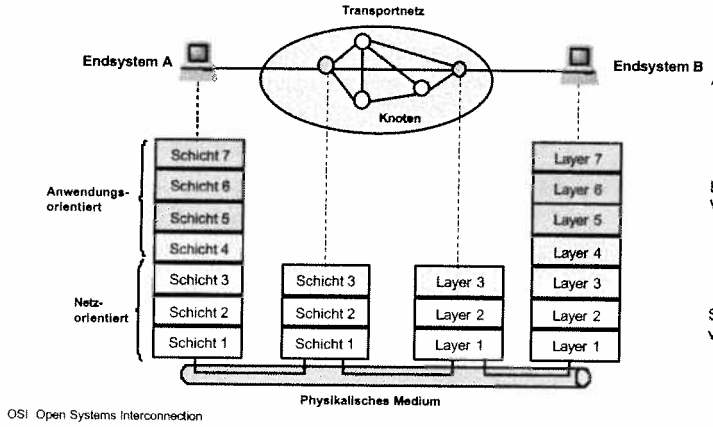


Bild: Netzweites OSI-Referenzmodell

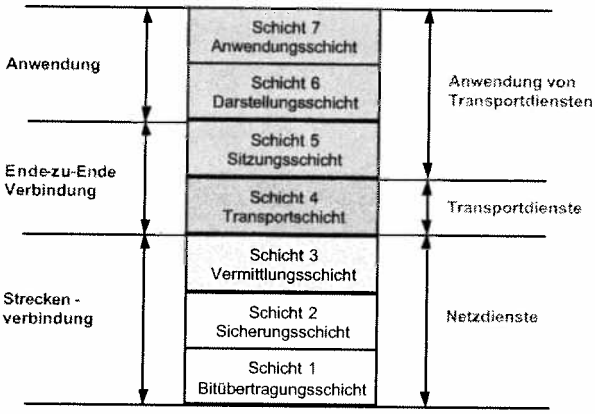


Bild: Schichten im OSI-Referenzmodell

Für den Protokollablauf zwischen gleichnamigen Schichten sind Zusatzinformationen notwendig. Dazu werden vor der Dateneinheit der jeweiligen Schicht Header-Information (H7, H6, H5, ...) mitübertragen. Die Daten eines Programms werden auf der Anwenderschicht mit Header H7 ergänzt. H7 mit Daten gelten nun als Daten (payload) für Schicht 6, die diese Daten mit seinem Header ergänzt, usw. Auf Schicht 2 gibt es zusätzlich ein Trailer (T2), der mindestens eine Prüfsumme (Frame Check Sequence, FCS oder Cyclic Redudancy Check, CRC) zur Überprüfung der Richtigkeit der Übertragung enthält.

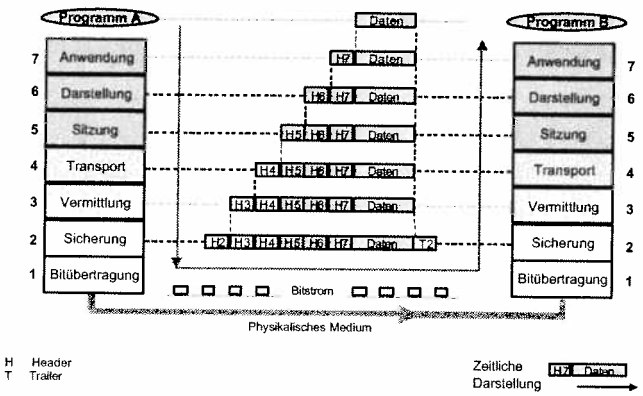
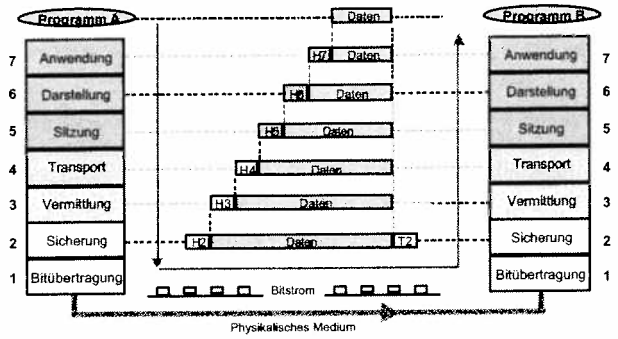
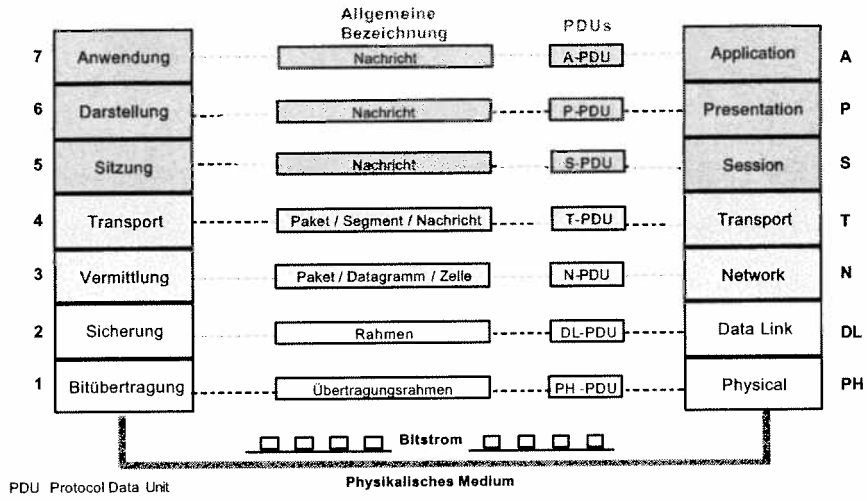


Bild: Daten und Zusatzinformation in Endsystemen A und B





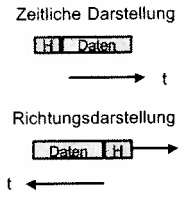


Bild: Darstellungsart

Bild: Übermittlungs- und Übertragungseinheiten

Je nach Protokollschicht werden die Dateneinheiten (Data Unit, DU) verschieden bezeichnet. Allgemein werden Protocol Data Units (PDU) zwischen gleichen Protokollschichten der beiden Endsystemen ausgetauscht, zum Beispiel T-PDU auf der Transport Schicht. Wie im Bild zu sehen ist, werden ferner folgende Bezeichnungen für die Dateneinheiten der Schichten verwendet:

- **Daten (data):** E-Mail, File, Bild, Audiostrom, Videostrom.
- **Nachricht (message):** Dateneinheit der Ende-zu-Ende Kommunikation.
- **Segment (segment):** Segmentierter Nachrichtenteil der Ende-zu-Ende Kommunikation.
- **Paket (packet):** Vermittelte Dateneinheit durch das Netz über einer logischen Verbindung.
- **Datagramm (datagram):** Vermittelte Dateneinheit ohne logische Verbindung.
- **Zelle (cell):** Vermittelte Dateneinheit mit fester Länge über einer logischen Verbindung.
- **Rahmen (frame):** Dateneinheit der Schicht-2.
- **Übertragungsrahmen (transmission frame)** Übertragungsstruktur auf Schicht 1.

Die Darstellung der Dateneinheiten ist entweder zeitlich oder richtungsorientiert. Bei der zeitlichen Darstellung kommt zuerst der Header und danach die Daten, weil dies der zeitlichen Reihenfolge der übertragenen Bits entspricht. Bei der Richtungsdarstellung möchte man den Flussrichtung der Dateneinheit im Vordergrund stellen. Die Zeitachse ist dann in umgekehrter Richtung.

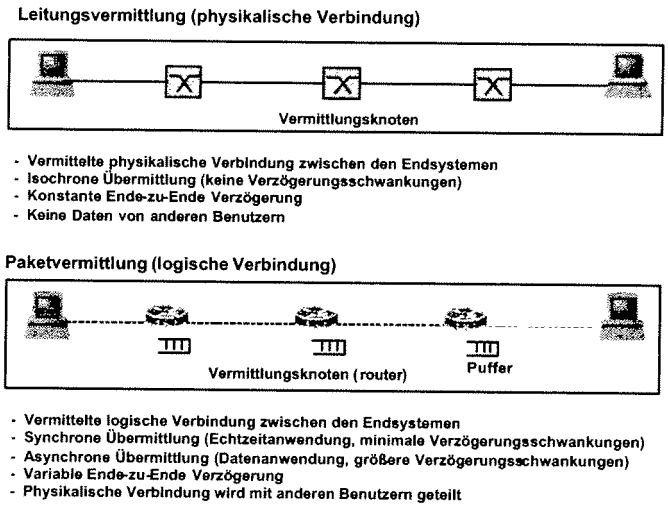


Bild: Physikalische und logische Verbindung

In der Vermittlungstechnik wird zwischen Leitungs- und Paketvermittlung unterschieden. Bei der Leitungsvermittlung (Durchschaltevermittlung) ist eine physikalische Verbindung zwischen den Endsystemen vorhanden. Dies bedeutet, dass alle gesendete Bits nach einer konstanten Verzögerung beim anderen Benutzer ankommen. Die Übermittlung ist deshalb isochron. Man spricht von Übermittlung (Übertragung plus Vermittlung), weil es sich hier um eine Zusammenschaltung von vermittelten Übertragungsabschnitten handelt. Bei Paketvermittlung hat man eine logische Verbindung zwischen beiden Endsystemen. Dies bedeutet an beiden Enden der Verbindung existieren Sofware Modulen (Instanzen, entities), die eine logische Verknüpfung bezüglich der Adressierung und des momentanen Zustandes des Datenaustausches herstellen.

Viele logische Verbindungen teilen sich die Netzressourcen (physikalische Leitungen sowie Puffer und Rechenleistung in den Netzknoten) und somit kommt es zu Stausituationen, die Verzögerungsschwankungen hervorrufen. Bei Echtzeitverbindungen (Telefonie, Videokonferenz) werden die Ende-zu-Ende Verzögerungsschwankungen durch geeignete Maßnahmen minimalisiert und begrenzt. Dies kann beispielsweise erreicht werden durch Prioritäten, Ressourcenreservierung und einen Puffer zur Ausgleich der Verzögerungsschwankungen im empfangenden Endsystem. Durch trotzdem verbleibende Verzögerungsschwankungen spricht man hier nicht von einer isochronen Übermittlung, sondern eine synchronen Übermittlung. Der Kommunikation bei allen anderen Anwendungen ist ein wesentlich größerer Verzögerungsschwankungsbereich unterworfen. Die Übermittlung wird als asynchron bezeichnet.

Funktionalitäten der sieben OSI-Schichten

Schicht 1: Bitübertragungsschicht (Ph: Physical)

Diese Schicht bewirkt eine ungesicherte Übertragung von Bits zwischen benachbarten Netzelementen (Netzknoten, Endgeräte, Rechner). Die einzelnen Aufgaben sind im Bild aufgeführt. Zu beachten ist, dass ein Übertragungsabschnitt zuerst physikalisch aktiviert werden muss, bevor die bitserielle Übertragung von Schicht-1 Datenblöcken stattfinden kann. Auf der Schicht 1 werden also die bitübertragungstechnischen Eigenschaften einer Übertragungsstrecke beschrieben, beispielsweise die Eigenschaften des Übertragungsmediums, das verwendete Übertragungsverfahren sowie Bauform und Belegung der Steckverbindungen zwischen Endgerät oder Arbeitsplatzrechner des Benutzers und dem Netz. Dies kann je nach Übertragungsverfahren ein Modern, ein ISDN-Adapter oder ein sonstiger Netzadapter sein. Die aktivierte physikalische Verbindung läuft über eine elektrische Leitung, eine Glasfaser oder eine Funkverbindung.

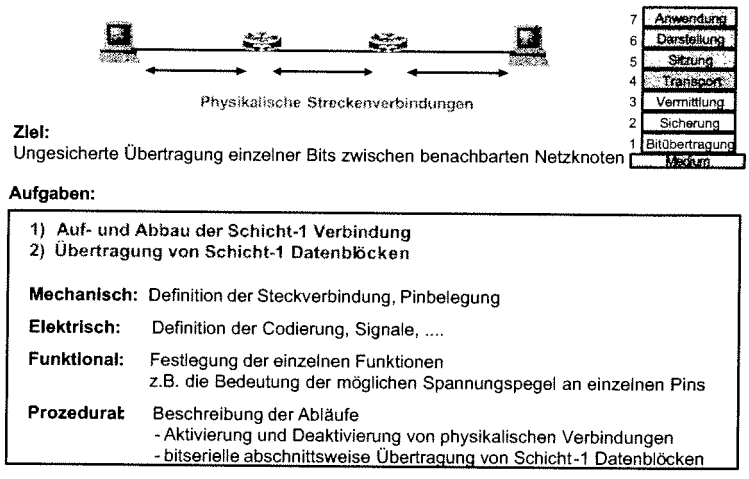
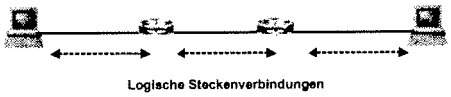


Bild: Schicht 1: Bitübertragungsschicht

Schicht 2: Sicherungsschicht
(DL: Data Link)

Die Sicherungsschicht macht die ungesicherten Übertragungen zu gesicherten Systemverbindungen. Dazu wird zuerst eine logische Schhicht-2 Verbindung zwischen den benachbarten Netzknoten aufgebaut. Allgemein gilt, dass abgesehen von Schicht 1, wo eine physikalische Verbindung bestehen muss, auf allen anderen Schichten jeweils logische Verbindungen aufzubauen sind. Die logischen Verbindungen der Schichten 2 und 3 sind abschnittsweise, also von Netzsystem zu Netzsystem. Die bgischen Verbindungen ab Schicht 4 hinauf sind Ende-zu-Ende. Allgemein sind die ersten zwei Aufgaben jeder Schicht, die Auf- und Abbau der logischen Verbindung und der Austausch von Datenblöcken. Zu beachten ist, dass je nach Schicht die Datenblöcke verschieden bezeichnet werden.



Ziel:
Gesicherte Übertragung der in einem Rahmen (frame) zusammengefassten Bits zwischen benachbarten Netzelementen

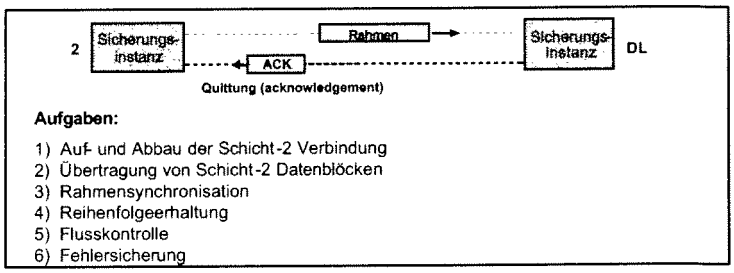


Bild: Schicht 2: Sicherungsschicht

Schicht 3: Vermittlungsschicht
(N: Network)

Durch Wegelenkung (Leitungsvermittlung) bzw. Routing (Paketvermittlung) verknüpft die Vermittlungsschicht gesicherte logische Punkt-zu-Punkt Verbindungen zu Endsystemverbindungen (von Endsystem zu Endsystem). Die Endsysteme werden dadurch direkt oder abschnittsweise über Transitsystemen miteinander verbunden. Zu den Aufgaben der Vermittlungsschicht gehören auch die Abwicklung der Paketflüsse durch Flusskontrolle sowie Überlastabwehr in Falle von Stausituationen. Eine Fehlersicherung kann fehlende Pakete (beispielsweise durch einen. Pufferüberlauf) oder eine Verletzung der Paketreihefolge auffangen. Zu dieser Schicht gehört auch die Signalisierung sowie die Nummerierung und Adressierung.

Ziel:
Vermittlung (routing) von Paketen durch das Netz

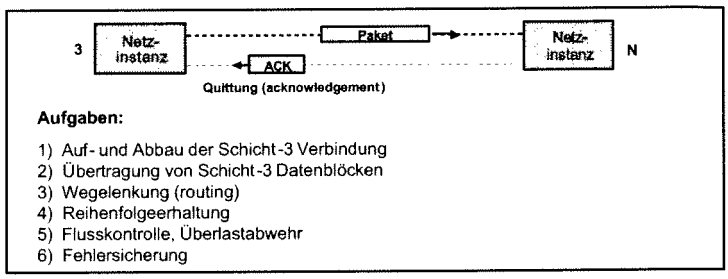
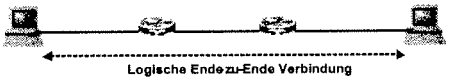


Bild: Schicht 3: Vermittlungsschicht

Schicht 4: Transportschicht
(T: Transport)

Die Transportschicht erweitert Endsystemverbindungen zu Verbindungen von Transportanwendungen. Unter einer Transportanwendung ist eine Zuordnung zwischen einer Anwendungsinstanz, einer Darstellungsinstanz und einer Sitzungsinstanz zu verstehen. Die Transportschichtverbindung ist, wie alle Schichtverbindungen darüber, eine logische Ende-zu-Ende Verbindung. Sie ermöglicht ähnliche Aufgaben wie sie auch die Schichten 2 und 3 abschnittsweise durchführen können, nämlich Reihenfolgeerhaltung, Flusskontrolle und Fehlersicherung.



Ziel:
Gesteuerte Übermittlung von Nachrichten zwischen Endsystemen

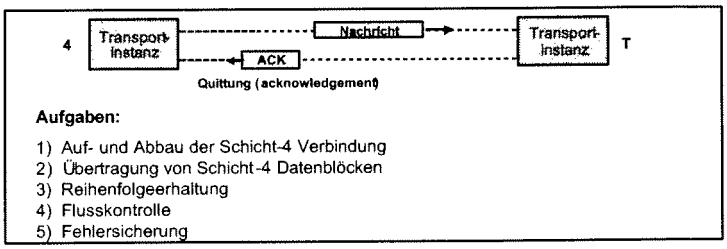
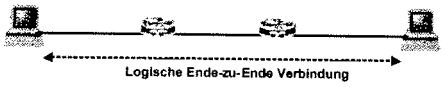


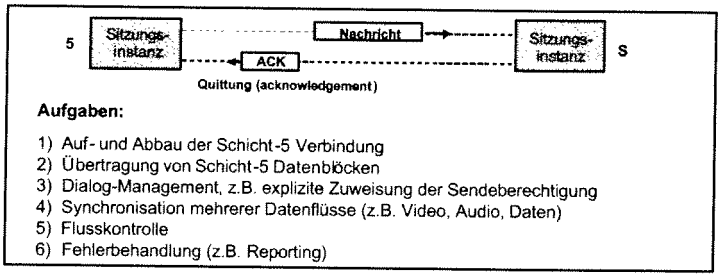
Bild: Schicht 4: Transportschicht

Schicht 5: Sitzungsschicht
(S: Session)

Die Kommunikationssteuerungsschicht oder Sitzungssicht stellt Protokollelemente zur Verfügung, die zur Eröffnung einer Kommunikationsbeziehung (Sitzung), ihrer geordneten Durchführung und Beendigung notwendig sind. Diese Protokollelemente dienen zur Dialogmanagement, zur Synchronisation mehrerer Datenflüsse und zur Feststellung von Übereinstimmungen zwischen den beiden Sitzungsinstanzen. Die Sitzungsschicht ist auf dieser Weise in der Lage, z. B. beim Wegfall der Transportverbindung einer Datenaustausch in der Mobilfunk, die Anwendung darüber zu informieren und die Transportverbindung wieder kontrolliert aufzusetzen.



Ziel:
Management von Ende-zu-Ende Verbindungen



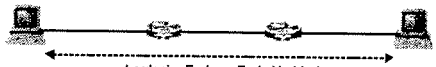
Aufgaben:

1) Auf- und Abbau der Schicht-5 Verbindung
2) Übertragung von Schicht-5 Datenblöcken
3) Dialog-Management, z.B. explizite Zuweisung der Sendeberechtigung
4) Synchronisation mehrerer Datenflüsse (z.B. Video, Audio, Daten)
5) Flusskontrolle
6) Fehlerbehandlung (z.B. Reporting)

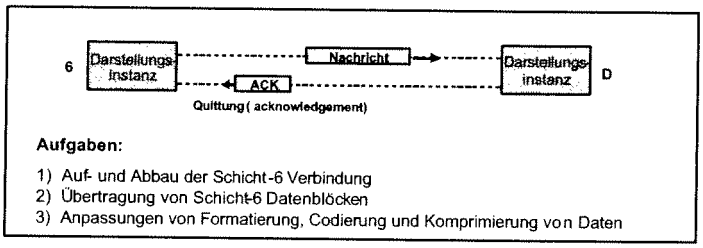
Bild: Schicht 5: Sitzungsschicht

Schicht 6: Darstellungsschicht
(P: Präsentation)

Die Darstellungsschicht stellt Protokollelemente zur Verfügung, die es die Darstellungsinstanzen ermöglichen, die Formatierungsanpassung sowie Codierung und Komprimierung eindeutig zu bestimmen, und legt im Darstellungsprotokoll die Regeln fest, wie die in der gemeinsamen Sprache die Darstellung der Information auszutauschen ist.



Ziel:
Darstellungsanpassungen von Ende-zu-Ende Verbindungen



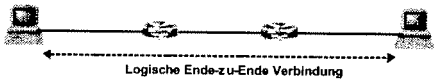
Aufgaben:

1) Auf- und Abbau der Schicht-6 Verbindung
2) Übertragung von Schicht-6 Datenblöcken
3) Anpassungen von Formatierung, Codierung und Komprimierung von Daten

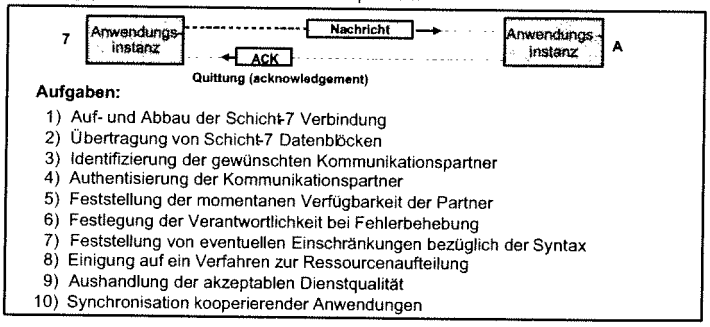
Bild: Schicht 6: Darstellungsschicht

Schicht 7: Anwendungsschicht
(A: Application, Anwendung)

In der Anwendungs- oder Verarbeitungsschicht als der höchsten Schicht des Referenzmodells manifestiert sich die Funktion der Informationsverarbeitung in einer Kommunikation. Die kommunizierenden Anwendungsinstanzen bilden die verteilten Anwendungen. Die Anwendungsprotokolle, die ihre Zusammenarbeit regeln, sind deshalb anwendungsspezifisch. Die Aufgaben sind grob wie folgt einzuteilen: 1) Identifizierung und Authentisierung der Partner, 2) Verfügbarkeitsüberprüfung, 3) Feststellung der Verantwortlichkeit für die Fehlerbehebung sowie die Feststellung einer Syntaxeinschränkung, 4) Aushandlung der Ressourcen und Dienstqualität, und 5) Synchronisation der Anwendungen.



Ziel:
Einigungsprozess zwischen Kommunikationspartnern



Aufgaben:

1) Auf- und Abbau der Schicht-7 Verbindung
2) Übertragung von Schicht-7 Datenblöcken
3) Identifizierung der gewünschten Kommunikationspartner
4) Authentisierung der Kommunikationspartner
5) Feststellung der momentanen Verfügbarkeit der Partner
6) Festlegung der Verantwortlichkeit bei Fehlerbehebung
7) Feststellung von eventuellen Einschränkungen bezüglich der Syntax
8) Einigung auf ein Verfahren zur Ressourcenaufteilung
9) Aushandlung der akzeptablen Dienstqualität
10) Synchronisation kooperierender Anwendungen

Bild: Schicht 7: Anwendungsschicht

Schicht 1

1) Auf- und Abbau der Schicht-1 Verbindung
2) Übertragung von Schicht-1 Datenblöcken

Schicht 2

1) Auf- und Abbau der Schicht-2 Verbindung
2) Übertragung von Schicht-2 Datenblöcken
3) Rahmensynchronisation
4) Reihenfolgeerhaltung
5) Flusskontrolle
6) Fehlersicherung

Schicht 3

1) Auf- und Abbau der Schicht-3 Verbindung
2) Übertragung von Schicht-3 Datenblöcken
3) Wegelenkung (routing)
4) Reihenfolgeerhaltung
5) Flusskontrolle, Überlastabwehr
6) Fehlersicherung

Schicht 4

1) Auf- und Abbau der Schicht-4 Verbindung
2) Übertragung von Schicht-4 Datenblöcken
3) Reihenfolgeerhaltung
4) Flusskontrolle
5) Fehlersicherung

Schicht 5

1) Auf- und Abbau der Schicht-5 Verbindung
2) Übertragung von Schicht-5 Datenblöcken
3) Dialog-Management
4) Synchronisation mehrerer Datenflüsse
5) Flusskontrolle
6) Fehlerbehandlung

Schicht 6

1) Auf- und Abbau der Schicht-6 Verbindung
2) Übertragung von Schicht-6 Datenblöcken
3) Anpassungen von Formatierung, Codierung und Komprimierung von Daten

Schicht 7

1) Auf- und Abbau der Schicht-7 Verbindung
2) Übertragung von Schicht-7 Datenblöcken
3) Identifizierung der gewünschten Kommunikationspartner
4) Authentisierung der Kommunikationspartner
5) Feststellung der momentanen Verfügbarkeit der Partner
6) Festlegung der Verantwortlichkeit bei Fehlerbehebung
7) Feststellung von eventuellen Einschränkungen bezüglich der Syntax
8) Einigung auf ein Verfahren zur Ressourcenaufteilung
9) Aushandlung der akzeptablen Dienstqualität
10) Synchronisation kooperierender Anwendungen

Bild: Aufgaben der sieben OSI-Schichten

Normen und Standards

Normen und Standards sind für die Kommunikation in ausgedehnten Netzen von zentraler Bedeutung. Einerseits müssen unterschiedliche Endgeräte mit dem Netz sowie untereinander problemlos kommunizieren können, andererseits sollen Netze verschiedener Betreiber ebenfalls ohne wesentliche Anpassungen miteinander verbunden werden können.

Normen werden von **staatlich anerkannten Gremien** entwickelt. Sie sollen einen breiten Konsens darstellen, weshalb ihre Erarbeitung sehr viel Zeit benötigt. Deshalb können Nonnen, gemessen an der raschen Entwicklung der Datennetze und des Internet, bei ihrer Verabschiedung schon veraltet sein oder nicht mehr den neuesten Stand der Technik repräsentieren.

Standards werden hingegen von Zusammenschlüssen **(Konsortien** etc.) aus Institutionen und Firmen entwickelt und publiziert. Damit ist die **Aktualität** meistens sichergestellt. Jedoch werden besonders wichtige Themenbereiche oft von mehreren, konkurrierenden Zusammenschlüssen bearbeitet, was dem potentiellen Anwender die Festlegung auf einen Standard erschwert.

Normen wie Standards leben davon, dass Hersteller grundsätzlich vergleichbarer Produkte sich an die Vorgaben halten. Dies wird als **Konformität** zur Norm/zum Standard bezeichnet. Die Konformität der Produkte soll zu deren **Interoperabilität** (die Fähigkeit zur problemlosen, uneingeschränkten Zusammenarbeit) führen. In der Praxis ergibt sich aus Konformität leider nicht immer die Interoperabilität. Kommunikationsprodukte sind häufig komplex, d. h. sie bestehen aus vielen Teilen (Hard- und Software-Blöcken), die in ihrem Zusammenwirken zu sehr unterschiedlichen Verhaltensweisen führen. Die Normen und Standards sind entsprechend umfangreich.

Dies führt zu zwei **Problemen,** die meistens für eine mangelnde Interoperabilität verantwortlich sind:

- Der Umfang der Norm/des Standards führt dazu, dass oft **nur ein Teil der Vorgaben** in einem Produkt **realisiert** wird. Wenn nun zwei Hersteller zwei verschiedene Untermengen (subsets) an Vorgaben realisieren, ist die Interoperabilität zumindest eingeschränkt.
- Der Umfang einer Norm/eines Standards führt zusammen mit den bekannten Problemen, einen Sachverhalt sprachlich eindeutig und vollständig zu formulieren, zu **Interpretationsspielräumen.** Falls verschiedene Entwickler zu verschiedenen Interpretationen kommen, ist die Interoperabilität ebenfalls gefährdet.

Normungsgremien sind globale, regionale (Europa, Nordamerika, Asien, ...) oder nationale Gremien. Für eine globale Kommunikation wie auch zur Verhinderung von Handelshemmnissen ist es sinnvoll, Normen Top-Down einzuführen. D. h., dass zuerst globale Normen publiziert werden, die dann unverändert als regionale und nationale Normen übernommen werden. Im Bereich der Kommunikationstechnik sind die folgenden Normungsgremien von besonderer Bedeutung:

ISO (International Standardization Organization): eine in 1946 gegründete Untereinrichtung der UNESCO. Sie ist für die globale Normung in vielen Gebieten zuständig.

- **International Organization for Standardization (ISO)**
  Dachverband der nationalen Standardisierungsbehörden (www.iso.ch)
- **International Telecommunication Union (ITU)**
  internationale Vereinigung der Telekommunikationsgesellschaften (www.itu.int)
  Bereiche
  - ITU-T (Telecommunication)
  - ITU-R (Radiocommunication)
- **European Telecommunication Standards Institute (ETSI)**
  europaweite Harmonisierung der nationalen telekommunikationsnormen (www.etsi.org)
- **Internet Society (www.isoc.org)**
  Dachorganisation verschiedener Internet Organisationen
  Bereiche
  - Internet Engineering Task Force (www.ietf.org)
  - Internet Architecture Board (www.iab.org)
  - Internet Research Task Force
  - World Wide Web Consortium (www.w3c.org)
  - Internet Assigned Numbers Authority (www.iana.org)
- **IEEE, Institute of Electrical and Electronics Engineers**
  weltweit größte Berufsvereinigung (www.ieee.org)

Bild: Internationale Standardisierungsorganisationen

Das einzige offizielle weltweite internationale Gremium, das sich mit technischen Aspekten der Telekommunikation beschäftigt, ist die International Telecommunication Union (ITU, Internationale Fernmeldeunion) mit Sitz in Genf. Sie wurde im Jahre 1865 in Paris gegründet und ist heute eine Unterorganisation der UNO mit derzeit 190 Mitgliedsländern. Hauptmitglieder sind die Regierungen dieser Mitgliedsländer, einzelne Organisationen aus den Bereichen Netzbetreiber, Industrie, Wissenschaft, sowie regionale und internationale Organisationen können ebenfalls Mitglied sein - derzeit sind es ca. 370 jedoch mit geringeren Rechten.

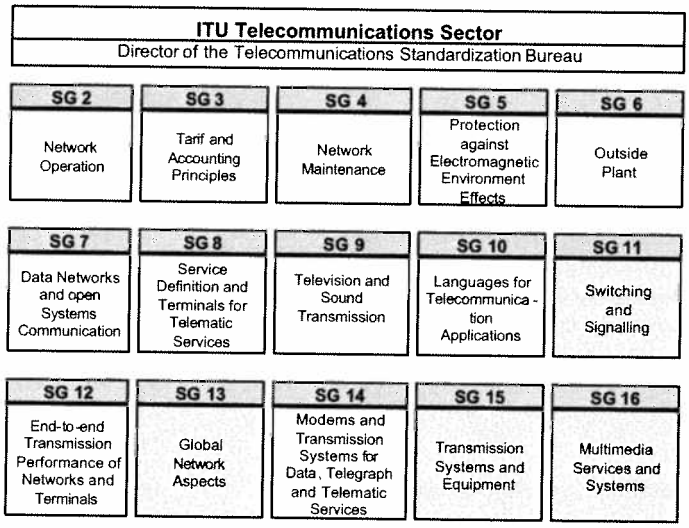


Bild: Organisation von ITU-T

ITU-T (International Telecommunications Union, Telecommunications Standardization Sector): Eine Unterorganisation der UN, die für die weltweite Standardisierung im Bereich öffentlicher Kommunikationsnetze zuständig ist. Bis 1992 trug die ITU-T den Namen **CCITT** (Comité Consultatif International Télégraphique et Téléphonique). Es gibt 16 viele Arbeitsgruppen (study groups), wobei die Resultate der SG 11, 13, 15 und 16 für die Themen der Vorlesung von besondere Interesse sind.

A	Organization of the work of ITU-T
B	Means of expression: definitions, symbols, classification
C	General telecommunication statistics
D	General tariff principles
E	Overall network operation, telephone service, service operation and human factors
F	Non-telephone telecommunication services
G	Transmission systems and media, digital systems and networks
H	Audiovisual and multimedia systems
I	Integrated services digital network
J	Transmission of television, sound programme and other multimedia signals
K	Protection against interference
L	Construction, installation and protection of cables and other elements of outside plant
M	TMN and network maintenance: intern. transmission systems, telephone circuits, telegraphy, fax
N	Maintenance: international sound programme and television transmission circuits
O	Specifications of measuring equipment
P	Telephone transmission quality, telephone installations, local line networks
Q	Switching and signalling
R	Telegraph transmission
S	Telegraph services terminal equipment
T	Terminals for telematic services
U	Telegraph switching
V	Data communication over the telephone network
X	Data networks and open system communication
Y	Global information infrastructure and internet protocol aspects
Z	Languages and general software aspects for telecommunication systems

Bild: ITU-T Empfehlungen (Recommendations)

Die ITU-T publiziert Empfehlungen (de-facto Normen), die eine Basis für die globale Telekommunikation bilden. Sie sind in Serien thematisch gegliedert. Speziell interessant für die Themen der Vorlesung sind die Empfehlungen E, G, H, I, K, M, Q, U und V.

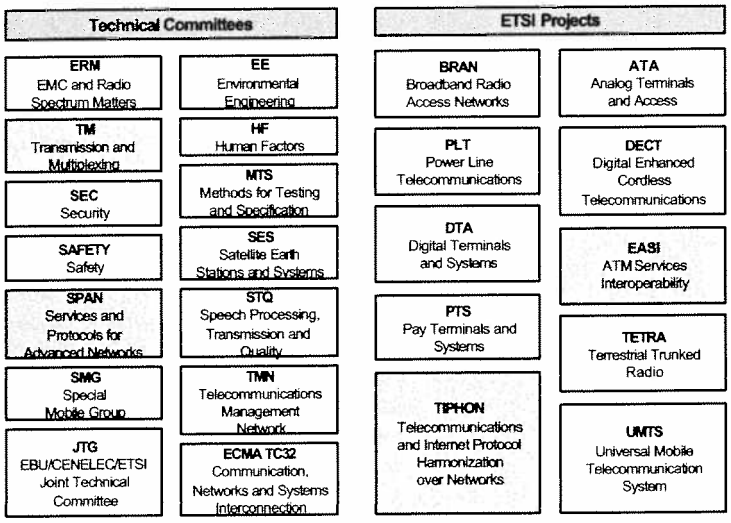


Bild: ETSI Technische Komitees und Projekte

ETSI (European Telecommunications Standards Institute):

Standardisierungsgremium, das auf Initiative der EU 1988 gegründet wurde. Dadurch wurde der Einfluss der nationalen Gremien geschwächt, die Position der Hersteller gestärkt und der Standardisierungsprozess beschleunigt. ETSI publiziert ETS (European Telecommunication Standard), die als nichtzwingende Empfehlungen gelten, sofern sie nicht von der EU oder nationalen Normungsgremien als Normen übernommen werden. I-ETS (Interim ETS) sind provisorische, also noch nicht ausgereifte Standards. ETR (European Technical Report) können Vorläufer von ETS sein. TBR (Technical Bases for Regulation) dokumentieren Untersuchungen, die sich mit technischen Aspekten der Deregulierung befassen.

Im Internet-Bereich ist die Standardisierung und die Vorgehensweise gänzlich verschieden zur bekannten Standardisierung in der Telekommunikation.

- **ISOC (Internet Society):** wurde 1992 als internationale Organisation zur Förderung des Internet gegründet. Sie ist organisatorisch dem IAB übergeordnet. Es ist aus einem Direktor und 18 Board Members zusammensetzt
- **IETF (Internet Engineering Task Force):** Diese Organisation bearbeitet kurz- und mittelfristige technische Probleme des Internet. Sie besteht aus acht Bereichen (areas) mit jeweils einigen Arbeitsgruppen.
- **IRTF (Internet Research Task Force):** koordiniert Forschungsaktivitäten zum Internet. Sie ist jedoch weit weniger bedeutsam als die IETF, in der de facto die meisten Forschungsaufgaben bearbeitet werden.
- **IAB (Internet Architecture Board):** steuert die Arbeiten von IETF und IRTF. Es besteht aus einem 20-Köpfiges Gremium, das für die generelle Architektur des Internet verantwortlich ist und 1989 aus dem Internet Activities Board hervorging.
- **ICANN (Internet Corporation for Assigned Names and Numbers):** vergibt Adressen und legt die Bedeutung von Konstanten fest, die in Protokollen vorkommen (Beispiel: Portnummern). **IANA (Internet Assigned Numbers Authority)** war bis 1998 für diese Aufgaben zuständig.

Die Organisationen **ARIN, RIPE** and **APNIC** vergeben Adressen auf geographischer Basis.

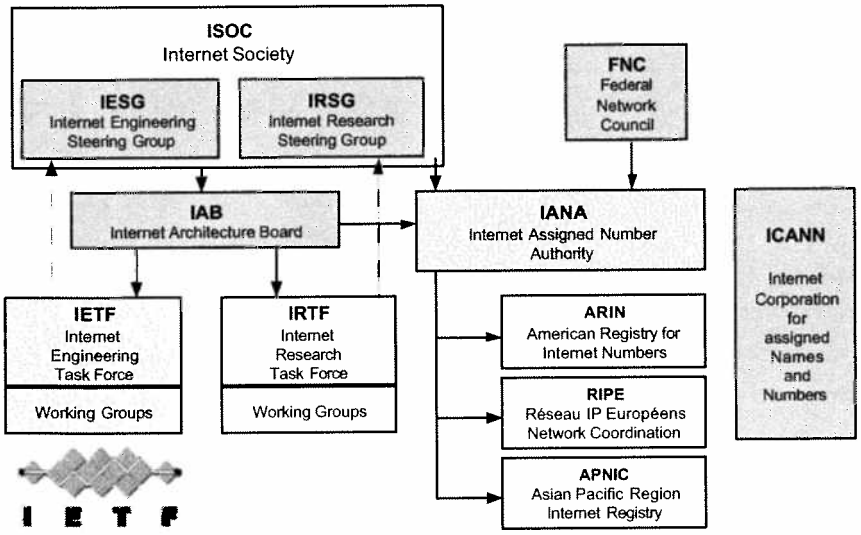


Bild: Organisation der Internet-Standardisierung

Außerhalb dieser Organisation aber in enger Kooperation ist das WWW Consortium (W3C), das sich um Aspekte des World Wide Web kümmert.

Die technische Sacharbeit wird in der Internet Engineering Task Force (IETF) geleistet. Sie wurde 1986 als Forum für die technische Koordination unter den Beteiligten an den entsprechenden Forschungsprojekten gegründet. Innerhalb der IETF gibt es derzeit 127 Arbeitsgruppen. Die Areas werden jeweils von einem Area Director geleitet, diese sind Mitglieder der IESG. Es gibt acht Themenbereiche (Areas):

1	Applications Area	28 Arbeitsgruppen	Weiterentwicklung bestehender Protokolle für Dienste wie ftp, World Wide Web (http), Verzeichnisdienste usw. sowie Definition von neuen Protokollen (Internet-Fax, Drucken übers Internet, ...).
2	General Area	1 Arbeitsgruppe	Organisation der Internet-Standards.
3	Internet Area	15 Arbeitsgruppen	Neue Möglichkeiten des Transports von IP.
4	Operations and Management Area	23 Arbeitsgruppen	Weiterentwicklung des Management-Protokolls (SNMP), Spezifikation der unterschiedlichen Management Information Bases (MIB).
5	Routing Area	17 Arbeitsgruppen	Weiterentwicklung der Routing-Protokolle.
6	Security Area	15 Arbeitsgruppen	Verschlüsselung, Authentication, Datenschutz, Firewall.
7	Transport Area	24 Arbeitsgruppen	alle Arten des Transports von Information über IP, z. B. Audio und Video, Protokolle für Real-time Transport und für Qualitätserweiterung von IP sowie Multimedia-Aspekte und Gateways.
8	User Services Area	4 Arbeitsgruppen	nicht-technisch, Benutzung des Netzes, Hinweise und Regeln.

Die Mitglieder der Arbeitsgruppen erarbeiten Dokumente und kommunizieren meist per E-Mail miteinander. Zusätzlich werden jährlich drei Treffen mit Gegenwärtig ca. 2000 Teilnehmern veranstaltet Entscheidungen basieren auf den Prinzipien "rough consensus" (die Interessierten müssen sich einig sein, es findet kein formaler Abstimmungsprozess statt) und "running code" (eine Implementierung als lauffähige Software bzw. als Gerät ist notwendig).

Die IETF produziert zwei Typen von Dokumenten:

- Internet Drafts sind Arbeitspapiere, die über einen Zeitraum von 6 Monaten gespeichert werden. Sie haben keinen offiziellen Status, führen aber bei genügend Interesse zu einer Diskussion und können dann RFCs werden. Internet Drafts werden sehr dynamisch erzeugt und auch wieder verworfen. Sie können in zwei Kategorien eingeteilt werden: solche, die einen offiziellen Status haben, also ein anerkanntes Arbeitsgebiet umfassen, und solche, die eine Einzelperson eingebracht hat, um ein neues Thema anzustoßen.

- Request for Comments (RFC) sind die offiziellen Dokumente, sie werden permanent gespeichert. RFCs können wiederum in die folgenden Kategorien eingeteilt werden:
- **Internet standard:** ein ausgereifter, gültiger Standard.
- **Draft standard:** ein überprüfter Entwurf mit zwei unabhängigen realisierten Implementierungen.
- **Proposed standard:** ein Vorschlag, der bereits überprüft wurde.
- **Experimental:** ein Konzept, das versuchsweise eingesetzt wird, aber nicht als Standard vorgeschlagen wird.
- **Historic:** ein veraltetes Konzept, das nicht mehr eingesetzt werden soll.

Jedes Protokoll wird mit einem Status versehen, der seine Anwendung bestimmt.

- **Required** verlangt eine Implementierung in allen Systemen, die TCP/IP benutzen,
- **Recommended** (der Einsatz wird emp fohlen),
- **Elective** (kann wahlweise eingesetzt werden),
- **Limited use** (nicht zur allgemeinen Anwendung),
- **Not recommended** (nicht einsetzen).

Die RFCs werden einfach laufend durchnummeriert. Alle Dokumente sind für jedermann frei zugänglich auf Web- und FTP-Servern gespeichert.

IEEE 802.x Standards seit 1980

802.1	**LAN/MAN Management**
802.1d	**Transparent / Source Routing, Transparent Bridging**
802.2	**Logical Link Control (LLC)**
802.3	**CSMA/CD (Ethernet)**
802.4	Token Bus
802.5	Token Ring
802.6	Distributed Queue Dual Bus (DQDB)
802.7	Broadband LANs
802.8	Multimode Fiber Optic Media
802.9	Integrated Services LAN (ISLAN)
802.10	Interoperable LAN/ MAN Security (SILS)
802.11	**Wireless LAN**
802.12	Demand Priority LAN (100VG-AnyLAN)
802.13	n/ a
802.14	Hybrid Fiber Coax (HFC) networks
802.15	**Wireless Personal Area Network (WPAN)**
802.16	**Broadband Wireless Access**
802.17	**Resilient Packet Ring (RPR)**
802.20	**Mobile Broadband Wireless Access (MBWA)**

Bild: IEEE 802.x Standards

IEEE
(Institute of Electrical and Electronics Engineers)
Ein weltweiter Ingenieursverband, der insbesondere bei der Standardisierung von LANs eine zentrale Rolle spielt.

In der Vorlesung behandelte Standards sind:
802.1d
802.2
802.3
802.4
802.5
802.11

Standards, die heute alle zwei Monate tagen sind:
802.3 802.16
802.11 802.17
802.15 802.20

Die rasche technische Entwicklung hat auch zu einer Vielzahl von Gruppierungen geführt (als **Konsortien, Allianzen, Foren** etc. bezeichnet), die eng umgrenzte Sachgebiete bearbeiten und zugehörige Standards publizieren und versuchen, diese durchzusetzen. Beispiele sind:

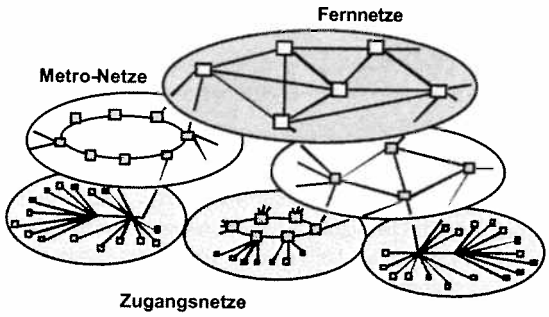
- Für ATM: ATM-Forum, http://www.atmforum.com/
- Für Frame Relay: Frame Relay Forum, http://www.frforum.com/
- Für xDSL: ADSL Forum, http://www.adsl.com/
- Für drahtlose LANs: Wireless LAN Alliance, hitp://www.wlana.com/
- Für Mobilfunknetze: Third Generation Partnership Project, http:// www.3gpp.org/

1.1 Grundlagen: Überblick

Version: Feb. 2004

Inhalt

- Schlüsseltechnologien
- Integration von Diensten
- Weltvernetzung
  (Kupfer-, Glasfaser-, Funk-, und Satellitenverbindungen)
- Durchschalte- und Paketvermittlung
- Struktur des Internet als Netz der Netze
- Heutiger Stand und Trends
- Zugangstechnologien
- Mobilität
- Netzintelligenz



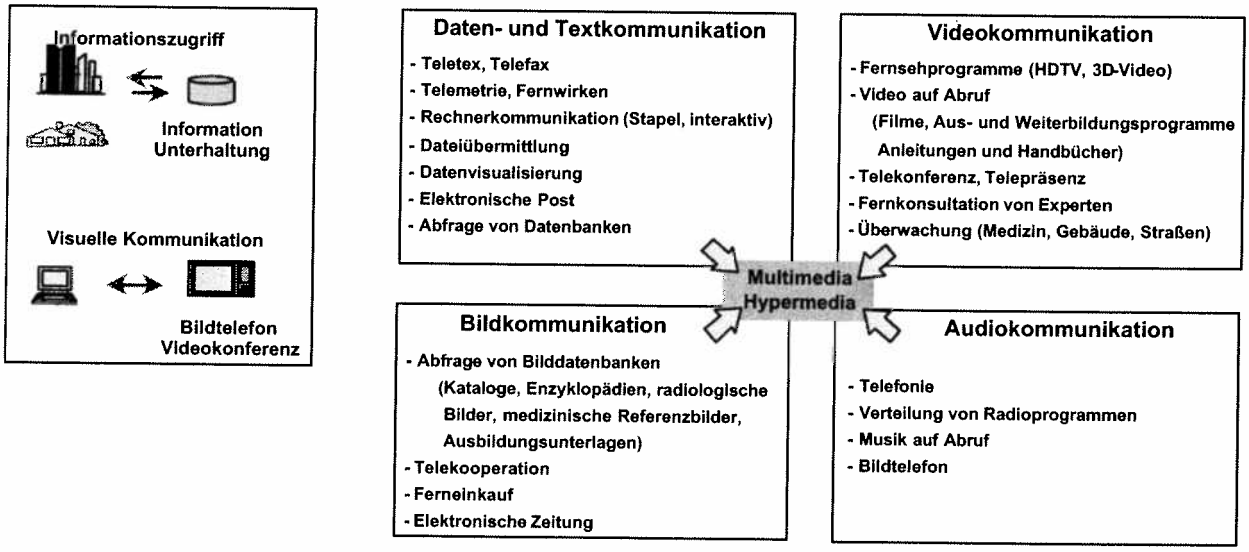
Schlüsseltechnologien künftiger Kommunikationsnetze

Die Telekommunikation ändert sich wahrscheinlich schneller als alle anderen Infrastrukturen oder Geschäftsbereiche. Der Markt rund um die Kommunikationsnetze ist stark im Wandel. Ausgelöst durch rasante technologische Entwicklungen einerseits sowie die Privatisierung und die Liberalisierung des Telekommunikationssektors andererseits, entsteht eine beträchtliche Vielfalt von Netztechnologien und Netzen, welche zu einer globalen Vernetzung zusammenwachsen müssen.

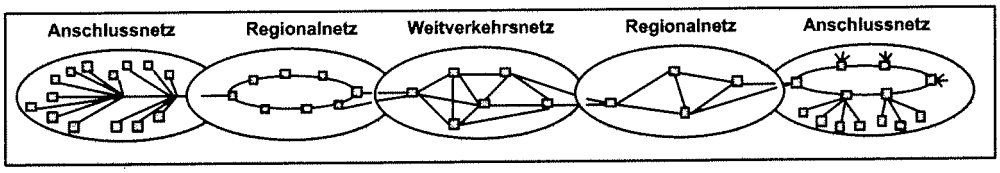
Der technologische Fortschritt im Telekommunikationssektor wird im wesentlichen durch drei Basistechnologien bestimmt:

- **Halbleitertechnologie:** Die Verarbeitungsleistung pro Siliziumfläche erhöht sich alle 3-4 Jahre um den Faktor 10.
- **Glasfasertechnik und Photonik:** Die maximale Übertragungsgeschwindigkeit einer Glasfaser nimmt alle 4-5 Jahre ebenfalls um den Faktor 10 zu. Dies eröffnet völlig neue Perspektiven bei der Architektur von Telekommunikationsnetzen. Die verfügbare steigende Rechenleistung führt dazu, dass die verschiedenen Formen von Intelligenz über das Netz verteilt und sogar in die Endgeräte der Teilnehmer verlagert werden. Zur Weiterentwicklung der verteilten Intelligenz tragen die sinkenden Übertragungskosten im Netz wesentlich bei.
- **Softwaretechnologie:** In verteilten Umgebungen sind objektorientierte Softwaremethoden unumgänglich. Netzmanagement heterogener Netze und verteilte Netzintelligenz basierend auf objektorientierten Methoden sind somit Hauptthemen der Zukunft.

Im nationalen Bereich ist die Telekommunikation der Schlüssel zur Steigerung wirtschaftlicher Effektivität und Effizienz. Als weltumspannende Infrastruktur wird sie zum zentralen Nervensystem einer globalisierten Wirtschaft. Somit sind höchste Maßstäbe für die Ausfallsicherheit der Netze und die Sicherheit der Informationsbehandlung gesetzt.



Mit der Verschmelzung der Telekommunikation, der Unterhaltung und der Informationstechnik hat die Multimedia-Zukunft begonnen. Die Multimedia-Kommunikation bringt eine Fülle von Möglichkeiten, um Arbeitsabläufe in allen Branchen der Wirtschaft effektiver zu gestalten und um dem Informationsaustausch im gesellschaftlichen Bereich zu neuen Dimensionen zu verhelfen. Der weitverbreitete Einsatz des Personal-Computers als Telekommunikationsendgerät ist vermutlich der bedeutendste Faktor für die Entwicklung von Multimedia-Diensten. Dabei spielen heute die On-Line Dienste und Informations-Surfen im Internet eine Vorreiterrolle.



Die Information-Highways ermöglichen auch eine Liberalisierung der Informationsmärkte, in denen man entscheiden kann, wie man sich die Information wünscht und aus welcher Quelle man die Information beziehen will. Man ist nicht mehr auf die herkömmlichen lokalen Informationsquellen, wie zum Beispiel die örtliche Bibliothek oder Tageszeitung, beschränkt. Die Errichtung von elektronischen Märkten unter Berücksichtigung höchster Sicherheitsvorkehrungen hat bereits begonnen. Die Integration von Sprach-, Daten- und Videoanwendungen erfordert hohe Übertragungsraten, eine flexible Zuteilung der Übertragungskapazitäten sowie Mechanismen zur Einhaltung einer gewünschten Kommunikationsqualität.

Die rasante Weiterentwicklung der Mobil- und Satellitenkommunikation erweitert den Anschlussbereich der Festnetze hin zu kompletter Flächendeckung. Somit wird eine globale, universelle und persönliche Mobilität ermöglicht: jeder persönlich zugeschnittene Dienst kann orts- und geräteunabhängig in Anspruch genommen werden. Qualität und Darstellung des gewählten Dienstes werden dabei automatisch an die Eigenschaften des benutzten Endgerätes angepasst. Jeder Teilnehmer hat damit einen universellen Kommunikationsdienst, der gleichermaßen zu Hause, im Büro, auf der Straße und im Urlaub benutzt werden kann.

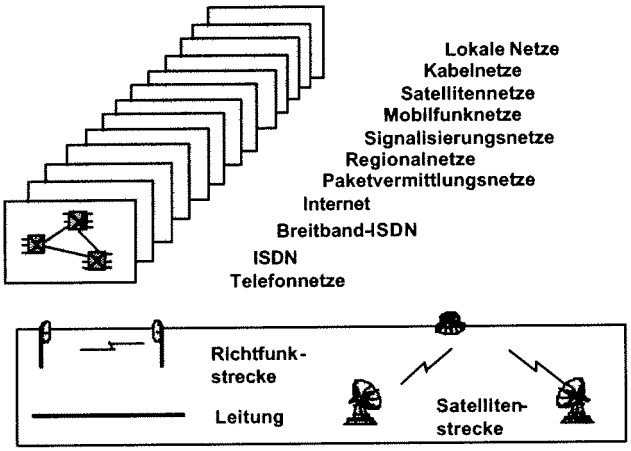


Bild: Eine Vielfalt von Netzen

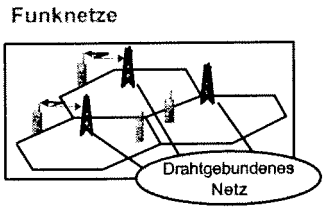
Transportnetze

Die Vernetzung zwischen den Anschlussregionen wird von Transportnetzen bewerkstelligt. Sie ermöglichen eine weltumspannende Kommunikation mit höchster Verfügbarkeit der Übertragungswege. Die in mehreren Ebenen strukturierten Netze bestehen aus dem

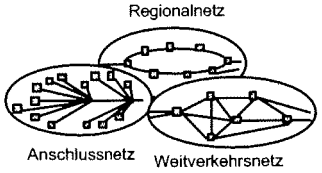
- Vermittlungsteil (Durchschalte- oder Paketvermittlung),
- Übertragungsteil (elektronische und photonische Ebene),
- Signalisierungsteil (Paketvermittlung).

Die Vielfalt der diversen Netztypen ist im Bild aufgelistet, wobei wiederum eine Reihe von Netztechnologien pro Netztyp existiert.

Alle Netzknoten der Transportnetze sind durch Glasfaser, Richtfunk-, oder Satellitenstrecken mit deren Endsystemen in der elektronischen Übertragungsebene verbunden. Die optischen Systemteile mit deren elektronischer Steuerung befinden sich in der photonischen Ebene.



Durchschaltevermittlung	
GSM	Global System for Mobile Communication
Paketvermittlung	
GPRS	General Packet Radio Service
UMTS	Universal Mobile Telecommunication System
WLAN	Wireless Local Area Network
VSAT	Very Small Aperature Terminal Network



Durchschaltevermittlung	
POTS	Plain Old Telephone System
ISDN	Integrated Services Digital Network
Paketvermittlung	
X.25	X.25 Packet Switching
FR	Frame Relay
ATM	Asynchronous Transfer Mode
IP	Internet Protocol
SS7	Signalling System Number 7
LAN	Local Area Network
CATV	Cable TV Network

Bild: Durchschalte- und Paketvermittlung

Netze können allgemein in Funk- und Festnetze eingeteilt werden. In beiden Netztypen findet man Netztechnologien, die entweder auf Durchschaltevermittlung oder Paketvermittlung basieren.

Die Vermittlungseinteilung ist im Bild zu sehen. Nur drei Netztechnologien, verwenden Durchschaltevermittlung. Nach allgemeiner Trend werden alle Dienste (Daten, Text, Sprache, Audio und Video) vermehrt über Paketvermittlungsnetzen abgewickelt.

Zu beachten ist auch, dass Funknetze aus einem Funknetzteil und einen Festnetzteil bestehen. GSM verwendet zum Beispiel ISDN im Festnetzteil. Bei UMTS wird die Internet-Technologie (IP-Netze) eingesetzt.

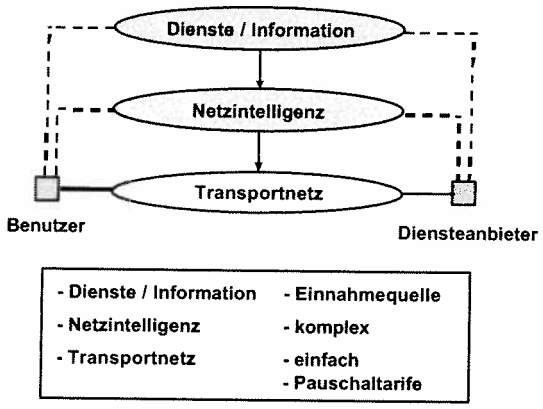


Bild: Allgemeiner Trend in Kommunikationsnetzen

Moderne Kommunikationsinfrastrukturen sind nicht mehr in erster Linie Einkommensquellen der Netzbetreiber, sondern vor allem als Schlüssel zur Erhaltung oder Steigerung des nationalen Wohlstandes zu betrachten. Es sind gleichzeitig viele Schlüsseltechnologien verschiedenster Netze zu betrachten. Sie alle erfüllen ihren eigenen Zweck, erfordern jedoch ein homogenes Zusammenspiel von vielen heterogenen Welten. Die damit verbundene Komplexität spiegelt sich vor allem im Bereich Netzsteuerung und Netzmanagement wider. Hier sind die höchsten Herausforderungen in der Realisierung künftiger Netze zu erwarten.

Als ein allgemeiner Trend können Kommunikationsnetze in drei Dienstebenen eingeteilt werden: Transport, Netzintelligenz und Telekommunikation- und Informationsdienste. Das Transportnetz macht die reine Übermittlung und Bittransport. Die Ebene ist deshalb möglicht einfach zu halten. Die ganze Kontrolle des Netzes ist getrennt und komplex. Bezüglich Einnahmenquellen gibt es eine deutliche Verschiebung vom Informationstransport zu Telekommunikation- und Informationsdienste.

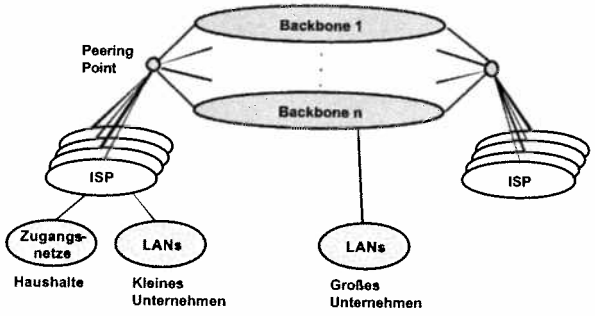


Bild: Allgemeiner Aufbau des Internet

Das Internet besteht aus einer Vielzahl von Netzen, die über Übergabeknoten mit einander verbunden sind. Haushalte und ein kleine Unternehmen sind über ISPs (Internet Service Providers) angeschlossen. Die Haushalte erreichen die ISPs über diversen Zugangsnetztechnologien, Unternehmen haben ihre LANs und sind entweder über einen oder mehrere ISPs angeschlossen oder haben einen direkten Anschluss an einem der Internet Backbones, die schlussendlich alle Netze miteinander verbinden.

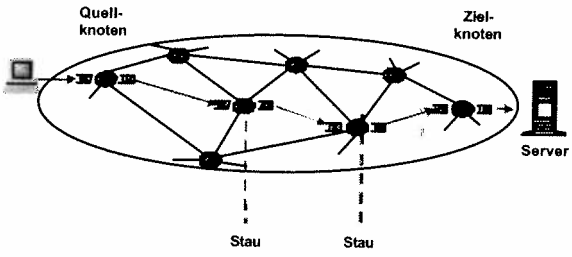


Bild: Internet-Kommunikation

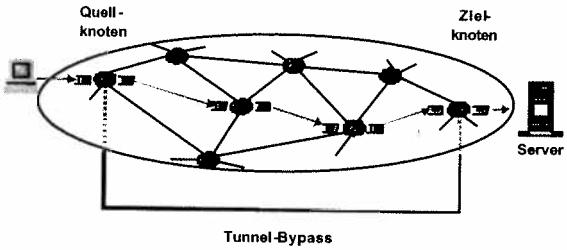


Bild: Bypass-Tunnel

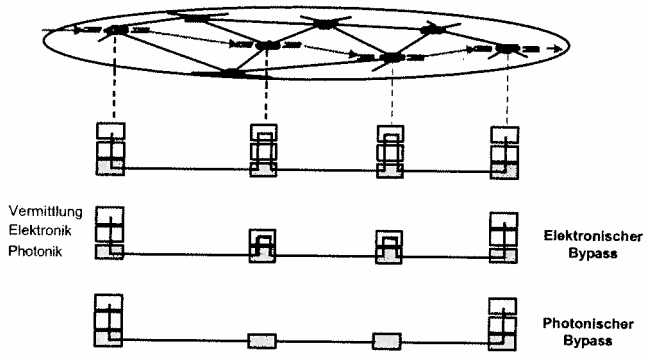
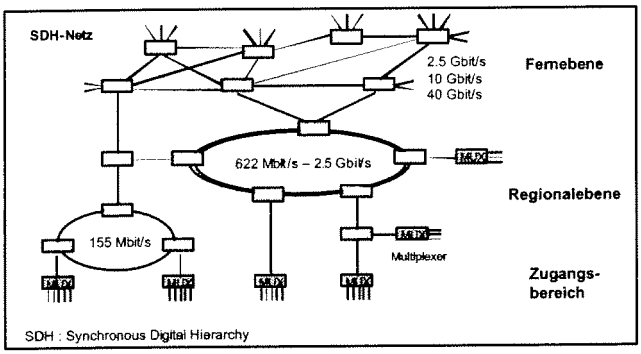


Bild: Bypass-Tunnel

Um in einem Internet-Netz Staus in Zwischenknoten umgehen zu können, werden sogenannte Bypass-Tunnels benutzt. Sie ermöglichen hochbitratige Punkt-zu-Punkt Verbindungen zwischen Routern, sodass Endziele über möglichst wenige Router erreichbar sind. Mit der sogenannten SDH-Übertragungstechnologie erhält man einen elektronischen Bypass. Hier wird die Vermittlungsschicht in den Zwischenknoten umfahren, aber in jedem Zwischenknoten finden optisch-elektronischen Umwandlungen statt. Somit wird in der elektronischen Ebene vermittelt. Bei einem optischen Bypass, bleibt die Dateninformation optisch bis zum Zielknoten. Die Vermittlung der Punkt-zu-Punkt Verbindungen in den Zwischenknoten geschieht in diesem Fall in der optischen Übertragungsebene.



SDH-Netz:
Autonomes Übertragungsnetz mit schneller Rekonfigurierung bei Knoten- und Leitungsausfällen
Übertragungsbitraten: 155 Mbit/s, 622 Mbit/s, 2.5 Gbit/s, 10 Gbit/s, 40 Gbit/s

Bild: Tunnel-Bypass durch Übertragungsnetze

SDH-Übertragungsnetze: In allen Industrie-Ländern hat eine Umstellung der Übertragungsnetze von der plesiochronen Hierarchie (PDH) zur synchronen digitalen Hierarchie (SDH) stattgefunden. Neben wesentlichen technischen und wirtschaftlichen Vorteilen sind es auch die Flexibilität in der Betriebsführung, die integrierte Netzmanagement-Funktion und die schnellen Schutzmechanismen zur Erhöhung der Netzverfügbarkeit, welche diese Umstellung vorangetrieben haben. Die PDH-Übertragungssysteme spielen in diesen Ländern nur noch eine Rolle als Zugangsleitungen zwischen Businesszentren zum Fernnetz.

Beachten Sie die im Bild erwähnten Eigenschaften und standardiserten Bitraten.

Ausfallsicherheit in SDH-Übertragungsnetzen: Die modernen, hochausgelasteten Digitalnetze erfordern aufgrund von möglichen Leitungsunterbrechungen sowie Knotenausfällen und Funktionsstörungen durch defekte Hardware- oder Software-Systemkomponenten sowohl vorsorgende Maßnahmen in deren Planung als auch Steuerungsverfahren im Betrieb. Die Netzausfallsicherheit ist die Fähigkeit des Netzes, beim Ausfall einer Netzkomponente den Verkehr wiederherzustellen, falls beispielsweise eine komplette Übertragungsleitung oder ein Vermittlungsknoten ausfällt. Zur Gewährleistung einer hohen Dienstqualität müssen in diesen Netzen für die betrachteten Fehlerfälle redundante Übertragungskapazitäten bereitgestellt werden, um betroffene Kommunikationsverbindungen über alternative Wege führen zu können. Diese sogenannten Ersatzkapazitäten werden bereits in der Dimensionierungsphase vorgesehen. Das Umlenken der betroffenen Kommunikationsverbindungen auf Ersatzwege erfolgt mittels Ersatzschalteverfahren, die sowohl die Auswahl des alternativen Weges als auch die Steuerung des Ersatzschaltevorganges beinhalten.

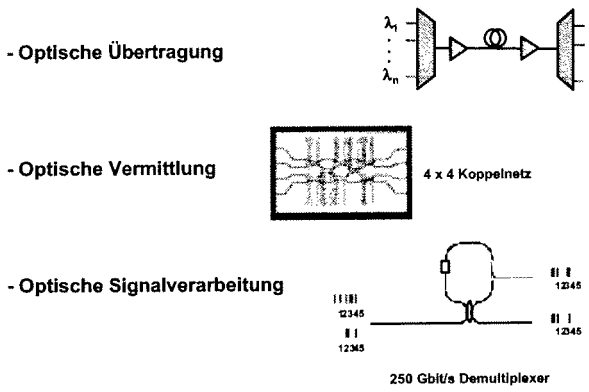


Bild: Photonische Netze

Photonische Netze: Leistungsstarke photonische Übertragungsnetze werden die heutigen Netztechnologien unterstützen, um den künftigen Verkehrsansturm der Multimedia-Zukunft bewältigen zu können. Sie werden das zentrale Nervensystem der Kommunikationsinfrastruktur bilden. Gleichzeitig werden sie auch die hohen Anforderungen an Flexibilität und Verfügbarkeit der Netze gewährleisten können. In photonischen Netzen werden die Informationssignale volloptisch übertragen, vermittelt und verarbeitet. Heute beschränkt man sich jedoch auf die Übertragung von mehreren Wellenlängenkanälen über einen Glasfaser: Die Vermittlungsknoten selbst sind elektronisch. Die optische Vermittlung ist zwar in Produkten vorhanden, aber der Betrieb solcher Knoten bereitet noch einige Probleme. Einfache optische Signalverarbeitung und auch optische Paketvermittlung ist im Labor möglich. Es bleibt aber noch ein langer Weg bis diese Technologien marktreif sind.

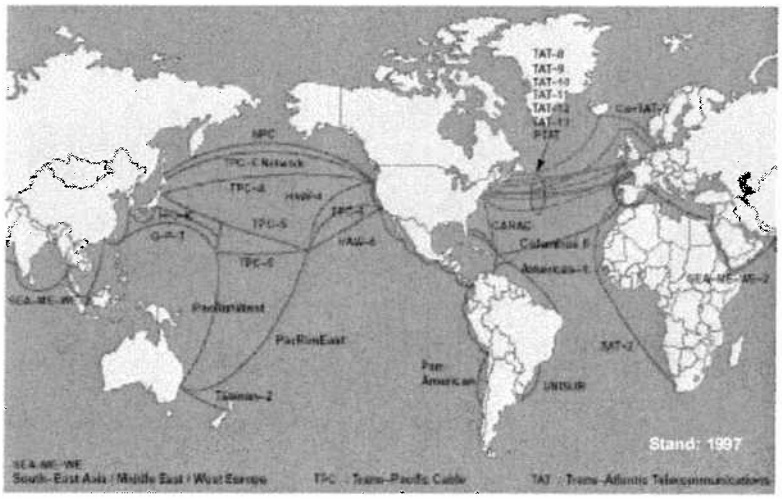


Bild: Interkontinentale Übertragungssysteme

Das Übertragungspotential einer einzigen, haardünnen Glasfaser liegt bei 30 Terahertz, tausend mal größer als die nutzbare Kapazität des Funkraumes. Die enorme Übertragungskapazität der Glasfaser kann nur mit Hilfe optischer Wellenlängen- oder Zeit-Multiplextechniken genutzt werden. Beim optischen Wellenlängenmultiplexen (WDM) überträgt man, ähnlich wie bei Radio- und Fernsehkanälen im Funkraum, viele optischen Signale mit unterschiedlichen Wellenlängen über eine Glasfaser. Optische Glasfaserverstärker ermöglichen heute eine rein optische Verstärkung. Langfristig ist es ein Ziel der photonischen Netze, möglichst viele Kommunikationsmetropolen direkt und rein optisch miteinander zu verbinden. Mit den optischen Tiefseekabelsystemen in den Atlantischen und Pazifischen Ozeanen hat die globale Vernetzung bereits eingesetzt.

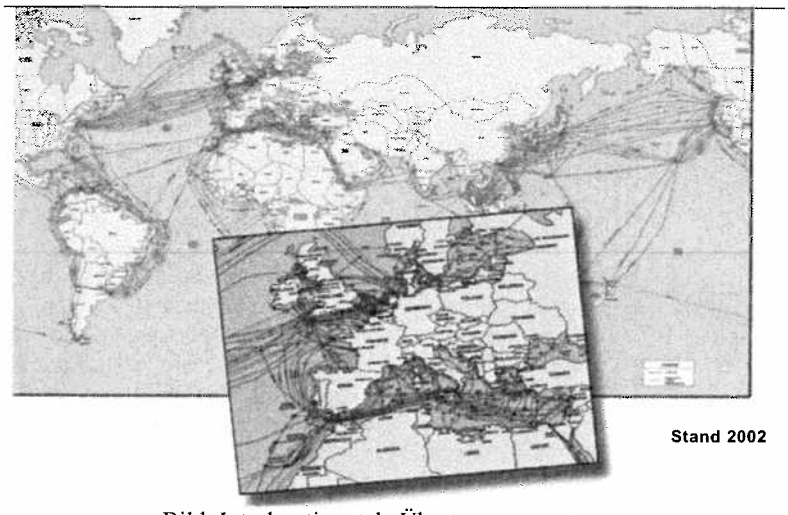


Bild: Interkontinentale Übertragungssysteme

Neben allgemeinen Merkmalen wie hoher Durchsatz von Nutzdaten, extrem niedrige Fehlerrate, hohe Zuverlässigkeit und Netzverfügbarkeit, sollen die drei folgenden Merkmale photonischer Netze speziell hervorgehoben werden: optische Transparenz, dynamische Netzkonfiguration und optis che Transitverbindungen.

Optische Transparenz bedeutet, dass die optische Ende-zu-Ende Verbindung unabhängig von der Signalform, Bitrate sowie Übermittlungsformat und -Protokoll ist. Die elektronischen Endgeräte bestimmen somit die Verbindungseigenschaften und nicht mehr das Netz selbst, wie das heute der Fall ist. Dabei können in den einzelnen Wellenlängenkanälen einer Glasfaser gleichzeitig Signale mit unterschiedlichen Eigenschaften übertragen werden.

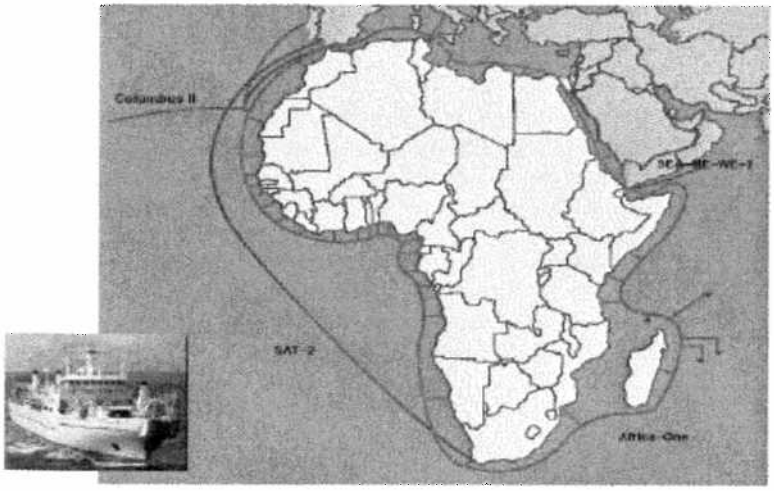


Bild: Photonisches Netz : AFRICA–ONE

Entsprechend der dynamischen Netzkonfiguration können auf den fest installierten Glasfasernetzen, je nach der momentanen Verkehrssituation, Wellenlängen- und/oder Zeitkanäle in wenigen Millisekunden geschaltet werden. Optische Transitverbindungen schließlich bedeuten, dass jeder Kommunikationsverkehrsstrom direkt vom Ursprungs- zum Zielknoten volloptisch durchgeschaltet wird.

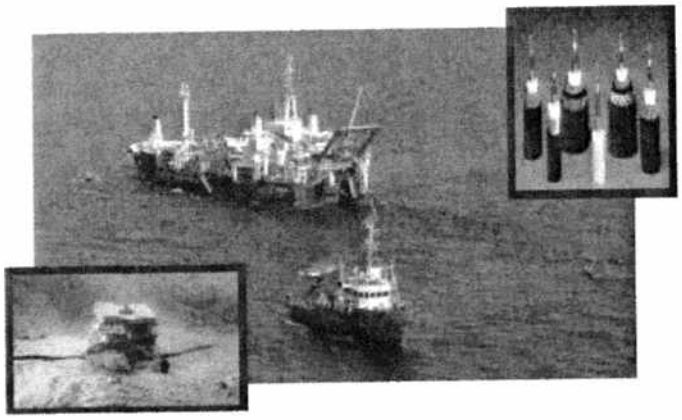


Bild: Tiefsee-Kabelverlegung

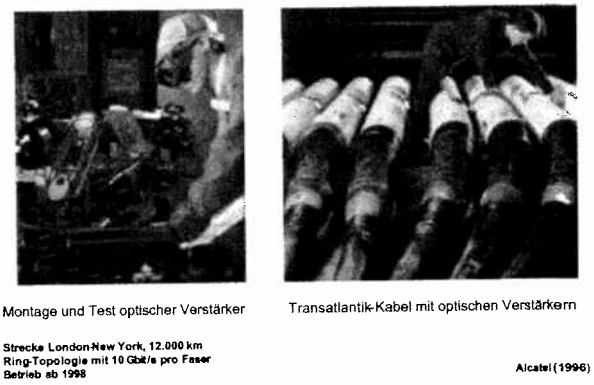


Bild: Optische Verstärker für Tiefsee-Kabel

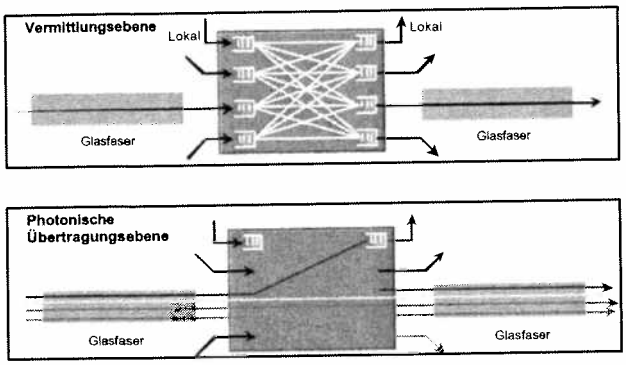
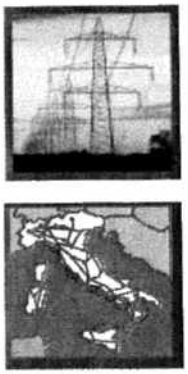


Bild: Staufreie Superhighways

Bei der traditionellen optischen Übertragung mit einem optischen Kanal müssen alle Pakete in der Vermittlungsschicht zu den richtigen Ausgängen vermittelt werden. In vielen Fällen gibt es Hauptverkehrsflüsse von bestimmten Eingängen zu bestimmten Ausgängen. Dies kann mit der WDM-Technologie, wo mehrere parallelen Wellenlängenkanäle existieren, ausgenutzt werden. In diesem Fall werden alle Pakete, die nicht im betrachteten Knoten terminieren, einen Transitwellenlängen zugeordnet, so dass ein optischer Bypass-Tunnel entsteht.



- Wasserwege, Seen und Meeresküsten
- Hochspannungsmasten
- Elektrizitätskabel
- Eisenbahntrassen
- Autobahnen
- Öl- und Gaspipelines
- Kanalisation
- Versorgungssysteme für Trinkwasser

Bild: Neue Möglichkeiten der Glasfaserverlegung

Neben den traditionellen Betreibern von nationalen und privaten Kommunikations- und Fernsehverteilnetzen gibt es heute viele neue Anbieter von Glasfasernetzen, wie die Energieversorgungsunternehmen, die Eisenbahngesellschaften und ganz allgemein auch die öffentliche Hand. Auf Grund der optischen Eigenschaften bieten die Glasfaserkabel auch neue Möglichkeiten für die Verlegung. Jede Verlegungsart braucht aber einen geeigneten Kabelmantel. Stichworte dazu sind: Wasserwege, Seen und Meeresküsten; Hochspannungsmasten; Elektrizitätskabel mit Glasfasern; Eisenbahnstrecken; Öl- und Gaspipelines; Kanalisation; Versorgungssysteme von Trinkwasser.

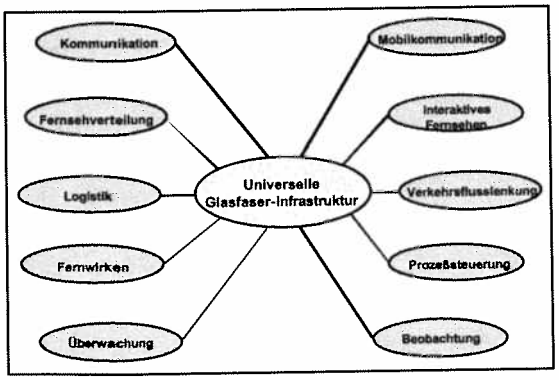


Bild: Glasfasernetze als universelle Infrastruktur

Somit ist es möglich, Fasernetze als eine leistungsfähige, universelle Kommunikationsinfrastruktur zu betreiben. Darin sind bestehende Netze auf einfache Art integrierbar und alle Kommunikationsdienste auf natürliche Weise vom Netz trennbar. Zusätzlich ist die gleiche optische Infrastruktur zum Beispiel mitverwendbar für terrestrische Basisnetze der Mobilkommunikation, für Überwachungs- und Steuerungsnetze der Verkehrsleitsysteme und Flugüberwachungssysteme sowie für analoge beziehungsweise digitale Fernsehverteilnetze.

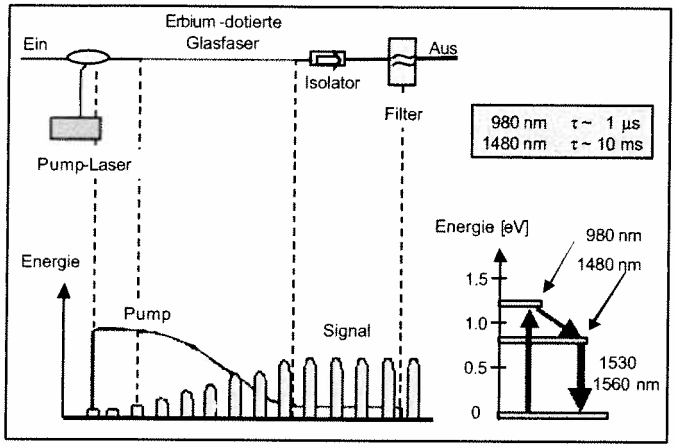


Bild: Erbium-dotierter Glasfaserverstärker

Optische Verstärker verwenden ein speziell dotiertes Glasfaserstück von etwa 50 m Länge, um die Amplituden sämtlicher optischen WDM-Kanäle im Glasfaser zu verstärken. Im 1500 nm optischen Fenster, wo die Dämpfung der Glasfaser am geringsten ist, wird Erbium verwendet. Der Verstärker wird kurz als EDFA (Erbium Doped Fiber Amplifier) bezeichnet. Die notwendige optische Energie kommt aus einem sogenannten Pumplaser, der entweder im optischen Bereich 980 nm oder 1480 nm arbeitet. Die im Spezialglasfaser gepumpte Energie kann statistisch etwa 10 ms auf dem Energieniveau 1480 nm erhalten bleiben, um dann diese Energie bei Anwesenheit von optischen Signalen im Bereich 1530-1560 nm abzugeben. Ein optischer Filter ist notwendig, um die Pumpwellenlänge nicht weiter propagieren zu lassen. Ein optischer Isolator vermeidet Reflektionen von optischen Energie in der Gegenrichtung.

Heutiger Stand und Trend

Der Trend in Kommunikationsnetzen mit speziellem Fokus auf der photonischen Infrastruktur lässt sich wie folgt charakterisieren. Bedeutende technologische Fortschritte, eine zunehmende Vielfalt an Kommunikationsdiensten, steigende Anforderungen an Flexibilität und Verfügbarkeit sowie ein schnell anwachsendes Verkehrsvolumen haben die Kommunikationsnetze durch verschiedene Entwicklungsstadien geführt. Mit den optischen Netzen zeichnet sich ein neues Kommunikationszeitalter am Horizont ab, in welchem der stetig wachsende Wunsch nach einer uneingeschränkten, komfortablen und vor allem preisgünstigen Telekommunikation in Erfüllung gehen könnte.

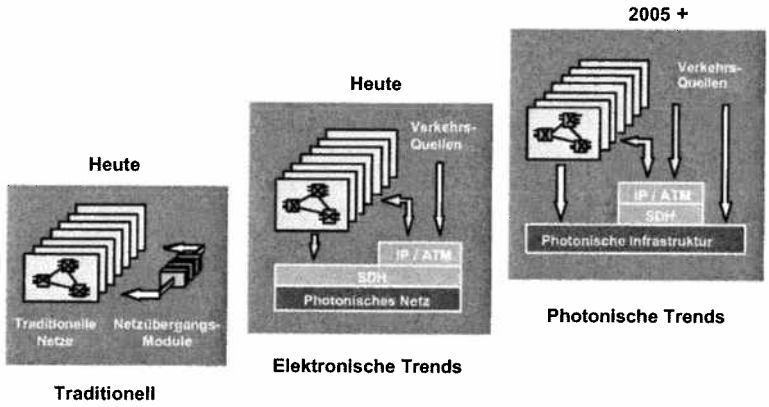


Bild: Technologie-Trends

- Paralleler Massentransport von Bitströmen
- Minimale Ende-zu-Ende Verzögerung
- Einfacher Betrieb
- Niedrige Betriebskosten
- Niedrige Grundtarife

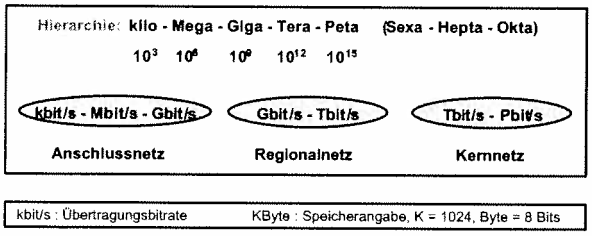


Bild: Trends mit photonischen Technologien

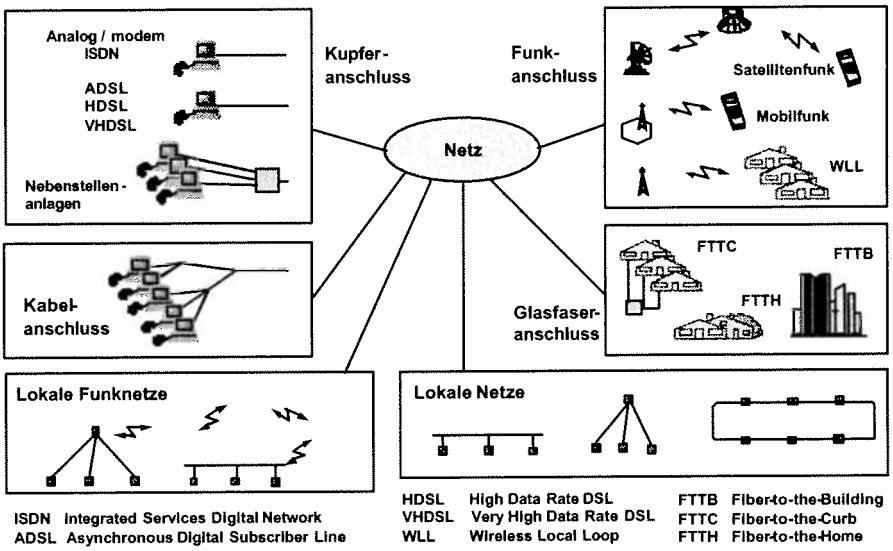


Bild: Netzanschluss

Zugangsnetze (access networks) verbinden den Teilnehmer mit dem eigentlichen Netz. Die Anforderungen an einen Zugang ergeben sich aus den genutzten Anwendungen. Dabei führt die Diensteintegration dazu, dass das Zugangsnetz ebenfalls für alle Dienste/Anwendungen ausgelegt werden muss. Unter einem FSN (Full Service Network) versteht man ein Zugangsnetz das alle zukünftig absehbaren Dienste (interaktive und Verteildienste, Breitband- und Schmalbanddienste) gleichermaßen erbringen kann und damit aus Sicht des Anwenders zukunftssicher sein soll. Nur in Sonderfällen (z. B. bei schmalbandiger, drahtloser Übertragung) wird der Kunde zu Kompromissen bereit sein. Derzeitige Zugangsnetze zu den privaten Haushalten mit deren heute noch stark begrenzten Übertragungskapazitäten sind ungeeignet, eine massive Anwendung von Multimedia-Kommunikation aufnehmen zu können.

Im Geschäftsbereich bieten die lokalen Netze intern hohe Bitraten an, jedoch die Kapazität zwischen den einzelnen Geschäftsstellen sowie zu den öffentlichen Netzen ist noch stark eingeschränkt. Die Zugangsnetze als Verbindung zwischen Teilnehmern und den Weitverkehrsnetzen werden heute neu überdacht. Die heutigen Netzzugänge konzentrieren den Telefonverkehr, um die Anzahl der nötigen Leitungen zu den Vermittlungsknoten zu reduzieren. Teilnehmern während längerer Zeit größere Übertragungskapazitäten zur Verfügung zu stellen, ist zweifellos eine Herausforderung für die Neu- und Umgestaltung der Zugangsnetze. Dabei geht es vor allem um die Reduzierung der Kosten für Betrieb und Unterhalt, die Vereinfachung des Netzmanagements sowie die Erschließung zusätzlicher Einnahmequellen durch neue Dienste. Das vordringlichste Ziel dabei ist die Anbindung an das Internet und On-Line Dienste unter Verwendung von Kupferadern, Koaxialkabel, Glasfasern oder Funk. Durch den Einsatz der Signalverarbeitung sind die Übertragungsraten auf den Kupferadern im Bereich von einigen Mbit/s gesteigert worden. Damit können Multimedia-Dienste ohne den sofortigen Netzausbau mit Glasfasern bis zu den privaten Haushalten angeboten werden. Die mehrheitlich verwendete oder geplante hybride Netzarchitektur besteht aus einem optischen hochbitratigen Übertragungssystem und symmetrischen Kupferdoppeladern bis zu den Teilnehmern.

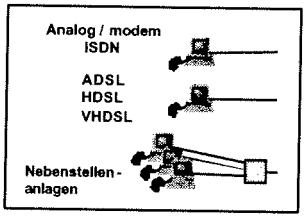
Zugangsnetze können ganz unterschiedlich realisiert werden:

- **Leitungsgebundene Anschlüsse** wie beim Telefonnetz und ISDN. Höhere Datenraten als 56 kbit/s (mit Modem) bzw. 128 kbit/s (bei ISDN mit Kanalbündelung) werden mit xDSL-Zugängen erreicht. Während symmetrische Kupferkabel für den größten Teil der existierenden Zugänge verwendet werden, wird die Glasfaser hier in Zukunft eine größere Verbreitung erhalten. Kabelnetze werden ebenfalls als Zugangsnetze eingesetzt, sofern ein geeigneter Rückkanal zur Verfügung steht. Zudem gab es eine kurze Phase große Entwicklungsanstrengungen, um die Stromversorgungsnetze als Zugänge für Rechnernetzen zu erweitern.
- **Leitungsungebundene (drahtlose) Anschlüsse** sind mit ungerichteter (schnurloses Telefon, Mobiltelefon) oder gerichteter (Richtfunk) Übertragung möglich. Satelliten werden hier ebenfalls eine zunehmende Bedeutung erhalten. Optische Funkzugänge sind zur Zeit auf sehr Zugangsverfahren kurze Distanzen beschränkt, es gibt aber Entwicklungen in Richtung auf breitere Anwendungsbereiche.

Insgesamt herrscht im Bereich der Zugangsnetze ein intensiver Wettbewerb, da der letzte Kilometer (last mile) vom Netzzugangspunkt zum Endkunden einen Engpass darstellt. Heute spricht man auch vermehrt vom ersten Kilometer (first mile).

Die Teilnehmeranschlussleitung steht einem Teilnehmer exklusiv zur Verfügung. Sie ist also ein dediziertes Medium im Gegensatz zu einem gemeinsamen LAN-Medium. Die Teilnehmeranschlussleitung wird auch als local loop bezeichnet und überbrückt den letzten Kilometer (last mile) von der Ortsvermittlungsstelle zum Teilnehmer. Sie kann auch drahtlos realisiert werden (WLL: Wireless Local Loop).

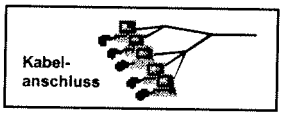
Das Zugangsnetz im Telefonnetz ist strukturiert in Hauptkabel, Kabelverzweiger, Verzweigungskabel, Endverzweiger und Endleitungen.



ISDN Integrated Services Digital Network
ADSL Asynchronous Digital Subscriber Line
HDSL High Data Rate DSL
VHDSL Very High Data Rate DSL

Teilnehmeranschlussleitung im Telefonnetz

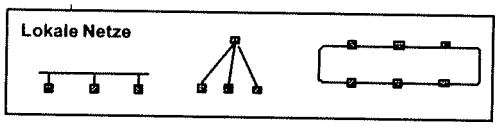
Die Teilnehmeranschlussleitung im Telefonnetz ist eine verdrillte Zweidrahtleitung (Doppelader, TP: Twisted Pair, UTP: Unshiehled TP) mit Kupferadern der Durchmesser 0,4; 0,6 oder 0,8 mm. Die Dämpfung dieser Leitung ist näherungsweise proportional zu ihrer Länge, proportional zur Wurzel der übertragenen Frequenz und umgekehrt proportional zum Aderndurchmesser. Damit sind Distanz und Bandbreite strikt begrenzt. Für größere Distanzen können Adern mit größerem Querschnitt eingesetzt werden. Im Telefonnetz ist eine Bandbreite von 3,4 kHz ausreichend, die erforderliche Länge beträgt einige wenige km. Die Adern werden mit a und b, die Teilnehmerschnittstelle selbst als a/b-Schnittstelle bezeichnet. Im Endgerät wird die Teilnehmeranschlussleitung durch die Teilnehmerschaltung abgeschlossen. Im herkömmlichen Telefonnetz werden deren Funktionen durch die Abkürzung BORSCHT (Battery Feed, Overvoltage Protection, Ringing, Signaling, Coding, Hybrid, Testing) zusammengefasst.



Zugang über Kabelnetze

Kabelnetze werden für Verteildienste (Rundfunk, Fernsehen) in großem Umfang eingesetzt. Die auf Koaxialkabel basierenden Kabelfemsehnetze eignen sich aufgrund ihrer Baumstruktur sehr gut für eine kostengünstige Verteilung von Fernseh- und Radioprogrammen an die angeschlossenen Teilnehmer.

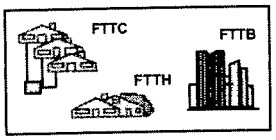
Für interaktive Anwendungen ist jedoch ein Rückkanal erforderlich. Dieser kann über das Telefonnetz realisiert werden, was jedoch für den Benutzer unangenehm ist. Deshalb wurden bereits viele Kabelnetze durch eigene Rückkanäle ergänzt. Als Übertragungsmedium wurden früher ausschließlich Koaxialkabel eingesetzt, heute werden zunehmend Teilstrecken mit Glasfasern (HFC: Hybrid Fiber Coax) eingefügt. Der Anwender benötigt ein Kabelmodem zum Zugriff auf den interessierender) Kanal. Diese Netze sind heute in vielen Ländern bereits gut ausgebaut und werden nun mit Glasfasersystemen ergänzt. Durch die Liberalisierung der nationalen Fernmeldegesetze eröffnen sich Möglichkeiten, diese Netze auch für die Telekommunikation sowie Video-Abrufdienste zu erschließen.



Lokale Netze: Traditionelle lokale Netze verwenden ein gemeinsames Übertragungsmedium. Sie entstanden, um den Datenaustausch mit stark schwankenden Datenmengen flexibel und wirtschaftlich zu ermöglichen.

Standardisierungsaktivitäten haben dem kommerziellen Einsatz dieser lokalen Netze zu einer großen Verbreitung verholfen, insbesondere Ethernet und früher auch Token Ring. Die Weichen sind nun neu gestellt. Die neuen Netzarchitekturen enthalten Switches. Diese Switch-Technologien haben im Vergleich zu traditionellen lokalen Netzen, in denen sich die Benutzer die gemeinsame Übertragungskapazität teilen müssen, erhebliche Vorteile: die Bandbreite kann individuell zugeteilt werden, und es sind unterschiedliche Übertragungsraten im selben Netz möglich, so dass äußerst flexibel und individuell auf Benutzerbedürfnisse reagiert werden kann. Daneben ergänzen drahtlose Netze und Hochgeschwindigkeitsverbindungsnetze zwischen Rechnern die Vielfalt standardisierter Netze für den lokalen Bereich.

Stadtnetze: In allen mittleren und größeren Städten findet man heute eine ähnliche Bedarfsstruktur im Kommunikationsbereich vor. Stadtverwaltungen und städtische Unternehmen wie kommunale Energieversorger und Verkehrsbetriebe sind über den gesamten Stadtbereich verteilt und haben einen vielfältigen Bedarf zur Kommunikation innerhalb ihrer Strukturen. Krankenhäuser, Schulen und Bibliotheken werden zunehmend vernetzt. Alle diese Benutzer benötigen ein großes Spektrum an verschiedenen Diensten. Hier bietet es sich an, ein diensteintegrierendes und unternehmensübergreifendes Übertragungsnetz zu betreiben. Grundgedanke ist dabei, alle Ressourcen von den Anwendern gemeinsam zu nutzen.



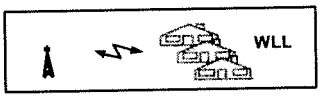
FTTB Fiber-to-the-Building
FTTC Fiber-to-the-Curb
FTTH Fiber-to-the-Home

Glasfaseranschluss
Für zukünftige Teilnehmeranschlussleitungen ist das Übertragungsmedium Glasfaser geeignet. Dieses Konzept wird als **FTTH** (Fiber-To-The-Home) bezeichnet, wenn die Glasfaser bis zum Teilnehmer führt. Die hohen Verlegungskosten werden jedoch nur eine langfristige Umstellung zulassen. Ein Kompromiss wird durch FTTC (Fiber-To-The-Curb) angestrebt. Hier führt die Glasfaser nur bis zum Straßenrand (Curb), für die letzten Meter werden vorhandene Kupferdoppeladern genutzt. **FTTB** (Fiber-To-The Building) ist ein ähnliches Konzept.

FITL (Fiber In The Loop) und **FTTx** (x steht als Platzhalter) sind Oberbegriffe für den Einsatz von Glasfasern im Teilnehmeranschlussbereich stehen. Zugangsnetze mit Glasfasern werden als PON (Passive Optical Network), also ohne Zwischenverstärker (Gegensatz: AON: Active Optical Network) ausgeführt. Auf Seite der Ortsvermittlungsstelle ist das Glasfaserzugangsnetz durch eine OLT (Optical Line Termination), auf Seite des Kunden durch eine ONU (Optical Network Unit) terminiert.

Drahtlose Anschlüsse

Leitungsgebundene Zugänge sind mit hohen Installationskosten verbunden und erlauben nur die Nutzung an einem festen Ort. Drahtlose Zugänge vermeiden Kosten für die Verlegung von Leitungen und können auch von mobilen Teilnehmern genutzt werden. Drahtlose Zugänge mit ungerichteter Ausbreitung können durch Mobilfunknetze realisiert werden. Wenn keine Mobilität erforderlich ist, können Richtfunknetze eingesetzt werden. Kommunikationssatelliten können in bestimmten Fällen für den Netzzugang sinnvoll sein. Zugangsnetze mit optischer Übertragung in der Atmosphäre sind ebenfalls vorstellbar.



WLL Wireless Local Loop

Richtfunkanschluss
Richtfunk ist die Übertragung elektromagnetischer Wellen mit scharf bündelnden Antennen (Richtantennen). Aus physikalischen Gründen ist dies nur bei hinreichend hohen Frequenzen möglich. Dafür erhält man eine Punkt-zu-Punkt-Verbindung, die im Raummultiplex mit anderen Verbindungen auf derselben Frequenz betrieben werden kann. Zugänge mit Richtfunk werden als WLL (Wireless Local Loop) bezeichnet.

LMDS (Local Multipoint Distribution Service): arbeitet im 26-GHz-Band mit Distanzen von 3-5 km. Mehrere breitbandige, bidirektionale Kommunikationsbeziehungen zwischen der Basisstation (hub) und den Teilnehmergeräten (radio termination) sind gleichzeitig möglich. In einem geografischen Sektor mit 15^0 Öffnungswinkel kann eine Gesamtdatenrate von 7 - 2 Mbit/s erreicht werden. LMDS ist insbesondere für Ballungsgebiete geeignet.

MMDS (Multichannel Multipoint Distribution System): Arbeitet in den Frequenzbereichen um 2,5 GHz und 3,5 GHz. Wegen den gegenüber LMDS niedrigeren Frequenzen ergeben sich größere Distanzen von bis zu 15 km. Da diese Frequenzbereiche auch von bestehenden Richtfunkstrecken benutzt werden, ist durch geeignete Planung eine Koexistenz mit diesen sicherzustellen.

MVDS (Multichannel Video Distribution Service): Ist ein Broadcast-System im Frequenzbereich von 40-45 GHz, das Distanzen von ca. 2-5 km überbrücken kann. Unidirektional werden Datenraten bis 40 Mbit/s erreicht.

Zugang mittels optischer Freiraumübertragung
Zugänge mittels optischer Übertragung sind prinzipiell durch ungerichtete oder gerichtete Ausbreitung in der Atmosphäre möglich. Die ungerichtete Ausbreitung ist zwangsläufig mit einer hohen Dämpfung verbunden, so dass sie nur über kurze Distanzen eingesetzt werden kann. Beispiele sind drahtlose, optische LANs. Für Zugangsnetze ist eine größere Distanz erforderlich, die eine gerichtete Ausbreitung verlangt.

Mobilität und mobile Netzanbindung

Zunehmend möchten Teilnehmer ihre Kommunikationsdienste unabhängig vom jeweiligen Standort nutzen und sich dabei überall der selben Prozeduren bedienen. Gleichzeitig wollen sie zu jeder Zeit und an jedem Ort auf kontrollierte Art und Weise für andere Teilnehmer erreichbar sein. Die Kontrolle der Erreichbarkeit ist erforderlich, um die Privatsphäre zu erhalten. Das entfernte Ziel ist die globale Mobilität mit einem persönlichen, endgerät- und ortsunabhängigen Netzzugang zu den Festnetzen, Mobilkommunikationsnetzen oder Satellitennetzen.

Mobilität im Festnetz: Teilnehmer werden Anrufe auf der Basis einer einzigen Nummer durchführen und entgegennehmen können, unabhängig von der Person und vom Netz, von jedem Endgerät, fest oder mobil, und über eine Vielzahl von Netzen: Festnetze, Mobilkommunikationsnetze, öffentliche, private, herkömmliche Netze oder Netze einer neuen Generation, unabhängig von der geographischen Position und nur mit der Begrenzung durch die Eigenschaften des Endgerätes und des Netzes, sowie mit den vom Dienstanbieter auferlegten Einschränkungen. Die Teilnehmer werden bei der Anmeldung an der Definition ihrer Dienste teilnehmen und können sie später durch Verwendung von Smart-Cards modifizieren. Das Ziel ist eine einzige Mobilitätsverwaltung für alle Arten von Anschlussnetzen

Mobilkommunikationsnetze: Die mobile Kommunikation gilt heute als der Telekommunikationsbereich mit der stärksten Expansion. Die Mobilkommunikation ist inzwischen eine bedeutende Alternative und Ergänzung zum Festanschluss – mit ihren modernen Vermittlungs- und Übertragungstechniken und immer kleineren, leistungsfähigeren und preisgünstigeren Geräten, die grenzüberschreitende Kommunikation über große Distanzen ermöglichen. Beschränkte sich die Mobilkommunikation bisher in erster Linie auf die Sprachdienste, so wird es in Zukunft verstärkt darum gehen, in weltweiten intelligenten Mobilkommunikationsnetzen höher bitratige Sprache und Dienste für Bilder und Daten anzubieten sowie die Kooperation von Mobilkommunikation- und Festnetzen zu optimieren.

Zukünftige Mobilkommunikationssysteme werden personalisierte Systeme sein (die der Teilnehmer jederzeit bei sich trägt) und eine Vielzahl von Kommunikationsdiensten für mobile oder fest angeschlossene Teilnehmer bieten. Die angebotenen Dienste werden idealerweise mindestens mit den an den Festanschlüssen bereitgestellten übereinstimmen, wobei die Dienstgüte vergleichbar mit der des Festanschlussnetzes ist. Darüber hinaus werden zusätzliche Dienste angeboten, bei denen die speziellen Eigenschaften der Mobilität, wie z.B. Flächendeckung und Verfügbarkeit, vom Netzbetreiber berücksichtigt werden. Diese Dienste werden beeinflusst durch wirtschaftliche Erwägungen, behördliche Regelungen, politische Faktoren und durch die Ausrichtung des Systems durch verschiedene Betreiber. Es ist wichtig, darauf hinzuweisen, dass nicht alle Dienste überall verfügbar sein werden.

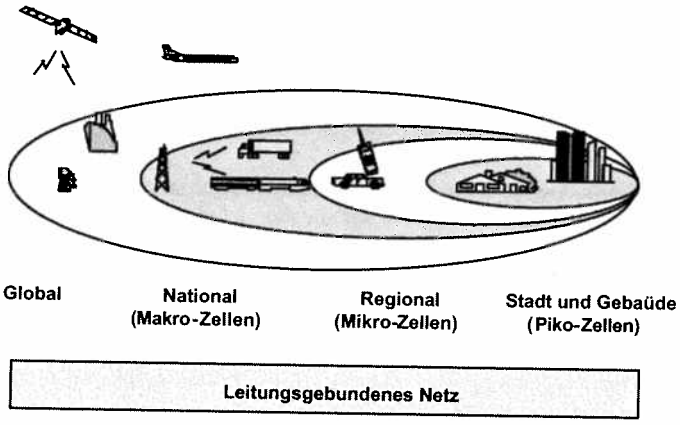


Bild: Mobilko mmunikation

Zugang über Mobilfunknetze

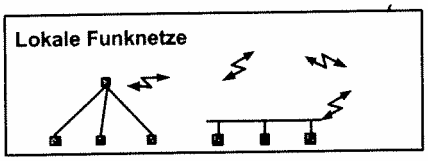
GSM (Global System for Mobile Coniniunications) ist das aktuelle, weitverbreitete Mobilfunksystem. Es wird als Mobilfunksystem der zweiten Generation betrachtet. GSM basiert auf Funkzellen, deren Ausdehnung in Abhängigkeit der Teilnehmerdichte variiert. Zur Vermeidung von häufigem handover (Wechsel der Funkzelle infolge der Mobilität des Teilnehmers) werden Overlay-Zellen verwendet. In Europa gibt es die Varianten GSM 900 (Frequenzband 880 MHz bis 960 MHz) und GSM 1800 (Frequenzband 1710 MHz bis 1880 MHz). Die Charakteristiken von GSM im Hinblick auf die digitale Übertragung sind durch Mehrwegeausbreitung, Funkstörungen und entsprechend hohe Fehlerraten gekennzeichnet. Dies macht den Einsatz einer automatischen Fehlerkorrektur und der Übertragungswiederholung ARQ erforderlich.

Die **Trägerdienste** (Bearer Services) in GSM bieten asynchrone und synchrone, leitungs- oder paketorientierte Datenübertragung mit Datenraten von 300 bit/s bis zu 9,6 kbit/s. Jeder Trägerdienst wird durch eine eigene Nummer angesprochen. **Telematikdienste** (Tele Services) in GSM sind u. a. Faxübertragung, Kurznachrichtendienste (SMS: Short Message Service) sowie der Zugang zu MHS-Systemen (Message Handling System). In GSM ist die Datenrate auf 9,6 kbit/s beschränkt. Höhere Datenraten werden durch Weiterentwicklungen möglich:

- **HSCSD** (High Speed Ciruit Switched Data): Datenrate bis 57,6 kbit/s durch Bündelung von zwei oder mehr Datenkanälen eines Trägers.
- **GPRS** (General Packet Radio Service): Paketübertragung (der Kanal -wird nur belegt, solange es tatsächlich etwas zu senden gibt) und Kanalbündelung werden kombiniert. Die maximale Datenrate beträgt 160 kbit/s, realistisch sind ca. 115 kbit/s.
- **EDGE** (Enhanced Data Rates for GSM Evolution):eineWeiterentwicklung von HSCSD und GPRS mit den Bezeichnungen ECSD (Enhanced CSD, für leitungsvermittelte Dienste) und EGPRS (Enhanced GPRS, für paketvermittelte Dienste). Als realistische Datenrate werden 110 kbit/s bei voller Mobilität und 220 kbit/s im stationären Betrieb angenommen.
- **UMTS** (Universal Mobile Teleconimunication Systeni) ist das Mobilfunksystem der dritten Generation. Als Zugriffs- bzw. Multiplex-Verfahren wird WCDMA (Wide Band CDMA, zu CDMA statt FDMA/TDMA bei GSM eingesetzt. Dadurch ergeben sich höhere Datenraten, die in Abhängigkeit von der Geschwindigkeit des mobilen Nutzers.

Datenrate	Geschwindigkeit des Nutzers
144 kbit/s	niedrig
384 kbit/s	hoch (bis 500 km/h)
2 Mbit/s	stationär (fest)

Datenraten in UMTS



Lokale Funknetze (WLAN, Wireless LAN): Der Funkzugang zum Netz mit 11 Mbit/s (IEEE 802.11b) oder 52 Mbit/s (IEEE 802.11a) pro Funkzelle bietet wichtige Zugangsmöglichkeiten für Heim, Businesszentren oder sogenannte Hot-Spots.

Erdnahe Satellitensysteme

Iridium	795 km	6 Orbits	Motorola	1998
Globalstar	1,389 km	6 Orbits	Loral-Qualcomm	1998
Odyssey	10,335 km	3 Orbits	TRW	2000

Bild: Nomadologie: Globale Erreichbarkeit

Satellitennetze: Bisher werden zu Kommunikationszwecken fast ausschließlich Satelliten in geostationären Umlaufbahnen in ca. 36.000 km Höhe verwendet. Sie sind vor allem für die Kommunikation mit langsam beweglichen Stationen wie auf Schiffen geeignet, weil die Empfangsantennen sehr groß sein müssen. Als neues Konzept für mobile Teilnehmer wird ein Satellitennetz mit niedrig fliegenden nichtgeostationären Satelliten bevorzugt, wobei hier zwischen LEO-Satelliten (low earth orbit, 500 km bis 1500 km Bahnhöhe) und MEO-Satelliten (medium earth orbit, 10.000 km bis 20.000 km Bahnhöhe) unterschieden wird. Um die globale Abdeckung der Erdoberfläche zu gewährleisten, ist bei Benutzung nichtgeostationärer Satelliten eine größere Anzahl Satelliten nötig. Diese bewegen sich nicht synchron mit der Erdrotation, wie es bei geostationären Satelliten der Fall ist.

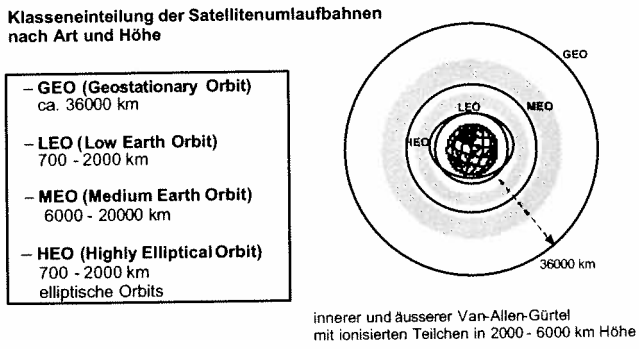


Bild: Klassifizierung von Satelliten

Satelliten in einer Erdumlaufbahn können als drahtlose Zugangswege zu Netzen eingesetzt werden. Geostationäre Satelliten werden bereits für den Internetzugang genutzt, wobei nur der Download (vom Server zum Client) über die Satellitenstrecke geführt werden kann. Der Rückkanal wird mit Hilfe des konventionellen Telefonnetzes realisiert.

Schmalbandige LEO-Satelliten sind als Konkurrenz zu Mobiltelefonnetzen zu sehen.

Breitband-LEO-Satelliten sollen Datenraten bis zu 155 Mbit/s (downstream) und 2 Mbit/s (upstream) zur Verfügung stellen. Satellitensysteme sind mit sehr hohen Investitionskosten verbunden, die deren Wirtschaftlichkeit in Frage stellen können. Die große Laufzeit auf geostationären Satellitenstrecken kann nachteilig sein. Dies ist insbesondere der fall für interaktive Anwendungen. Zudem stellen die Downstream-Kanäle shared media dar, die sich viele Nutzer teilen müssen.

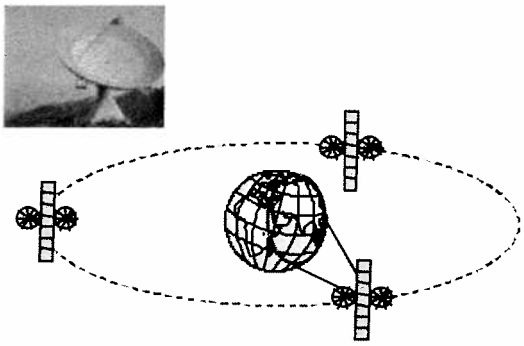
	Höhe	Umlaufzeit	Geschwindigkeit
LEO	700 km	1,5h	27 000 km/h
MEO	10 000 km	6 h	18 000 km/h
GEO	36 000 km	24 h	11 000 km/h

Tabelle 1: Orbitale Parameter

	Signallaufzeit (hin und zurück)	Größe der Endsysteme	Anzahl Satelliten
LEO	5 - 10 ms	klein	> 40
MEO	70 - 80 ms	mittelgroß	10 - 15
GEO	230 - 250 ms	groß	3 - 4

Tabelle 2: Wesentliche Merkmale des Satellitensysteme

Tabelle 1 enthält Umlaufhöhe, Umlaufzeit und Umlaufgeschwindigkeit für die drei Satellitenklassen LEO, MEO und GEO. Tabelle 2 enthält Roundtrip-Signallaufzeit, die Größe der Endsysteme sowie die benötigte Zahl von Satelliten für eine globale Funkversorgung.



Ausleuchtung der Erde mit 3 Satelliten möglich

Bild: Geostationäre Satelliten

- Orbit in 36.000 km Entfernung von Erdoberfläche in Äquatorebene
- Satellit synchron mit Erddrehung (Umlaufzeit: 1 Tag)
- feste Position der Antennen, kein Nachführen erforderlich
- Kurskorrektur der Satelliten erforderlich
- Funkversorgung relativ großer Gebiete, Frequenzen schlecht wiederbenutzbar
- große Antennen und hohe Sendeleistungen erforderlich
- große und schwere Benutzergeräte
- lange Signallaufzeit: ca. 275 ms, Übertragungsfehler
- meist Rundfunk- und Fernsehsatelliten
- typisch:
  - ca. 20 Transponder pro Satellit, Bandbreiten pro Transponder: ca. 50 MHz
- Anwendung:
  - Ausstrahlung von Fernsehprogrammen
  - Unterstützung der Kommunikation über Ozeanen, dünn besiedelten Gebieten, ...

Bild: Eigenschaften von geostationäre Satelliten

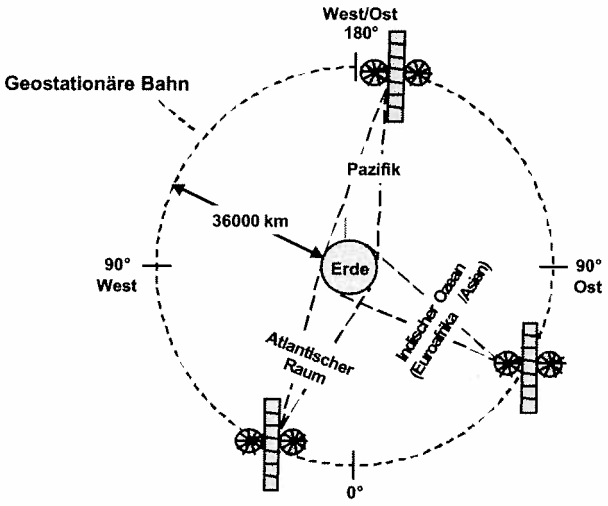


Bild: Geostationäre Satelliten im INTELSAT-Netz

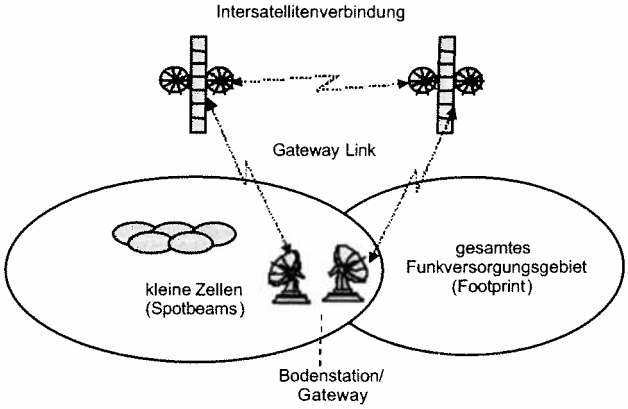


Bild: Satellitensystem

- Orbit in 500 - 2000 km Höhe
- Sichtbarkeitsdauer eines Satelliten 10 - 40 Minuten
- relative Geschwindigkeit: wenige km/s
- erfordert Gesprächsübergabe (Handover)
- viele Satelliten für globale Funkversorgung nötig
- Laufzeit mit terrestrischen Weitverkehrsverbindungen vergleichbar: ca. 5 - 10 ms
- kleinere Benutzergeräte
- kleinere Funkversorgungsgebiete
- bessere Frequenznutzung

Bild: Eigenschaften von LEO-Satellitensystemen

LEO Low Earth Orbit

- Orbit in 5000 - 12000 km Höhe
- **Vergleich mit LEO-Systemen:**
  - Geschwindigkeit des Satelliten langsamer
  - weniger Satelliten benötigt
  - Verbindungen meist ohne Handover möglich
  - längere Signallaufzeiten, ca. 70 - 80 ms
  - höhere Sendeleistung nötig

Bild: Eigenschaften von MEO-Satellitensystemen

Forderung: zeitkontinuierliche und globale Funkversorgungsfläche
Frage: Wie viele Satelliten sind notwendig ?

Gesichtspunkten:

Orbithöhe	GEO (Geostationary Orbit)	36.000 km
	MEO (Medium Earth Orbit)	10.000 km
	LEO (Low Earth Orbit)	700 - 2.000 km
minimale Neigungswinkel (ε_{min}) typisch:		GEO 5°
		LEO/MEO 10°
Mehrfach-Funkversorgung (mehrfach sichtbar)		Satelliten-Diversität mit Handover
Anzahl Satelliten:	GEO	3 - 4
	MEO	10 - 15
	LEO	> 40

Bild: Parameter für globale Funkversorgung

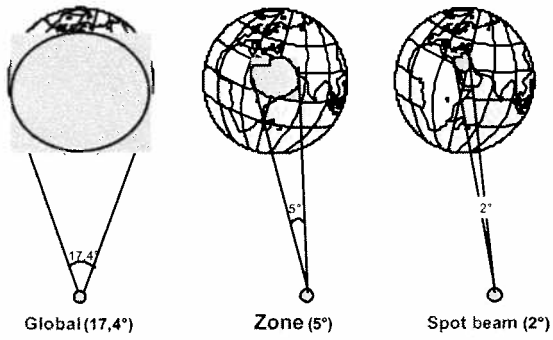
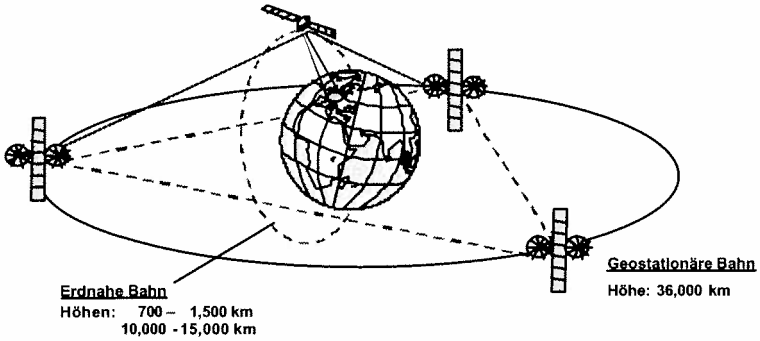


Bild: Größe der Funkversorgungsflächen von GEO-Satelliten



Iridium	**795 km**	**66 Satelliten**	**6 Orbits**	**Motorola**	**1998**
Globalstar	**1389 km**	**48 Satelliten**	**6 Orbits**	**Loral-Qualcomm**	**1998**
Odyssey	**10,335 km**	**12 Satelliten**	**3 Orbits**	**TRW**	**2000**

Bild: Kommunikationsnetze im Weltall

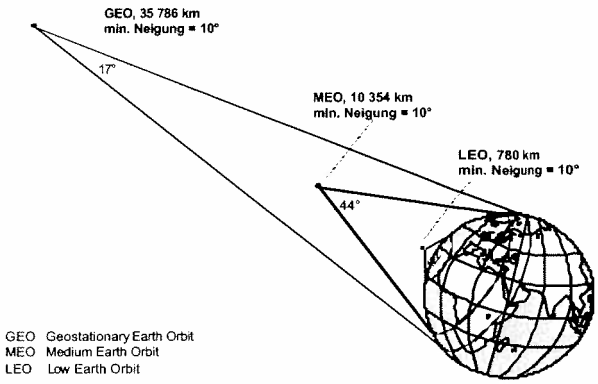


Bild: Funkversorgungsfläche

- Zwischen den Satelliten optische oder Funk- Links
- Funk-Links zur Erde

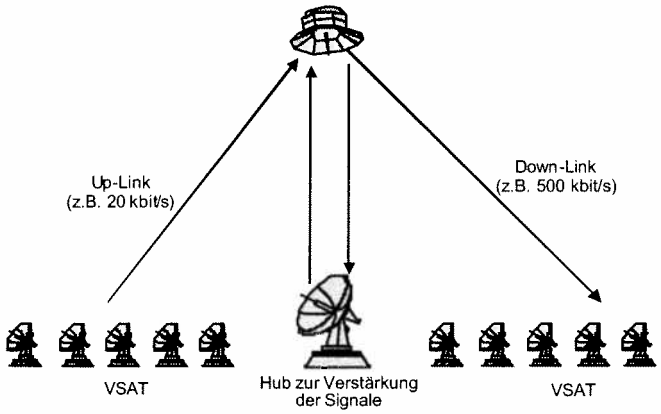


Bild: VSAT- Satellitensysteme

VSAT-Satellitensysteme

Sie bieten die Möglichkeit GEO-Satelliten mit kleinen Sende- und Empfangseinrichtungen zu erreichen. Dadurch können die sogenannten VSAT-Stationen (Very Small Aperture Terminal) zum Beispiel auf Fahrzeuge mit geführt werden

Netzintelligenz

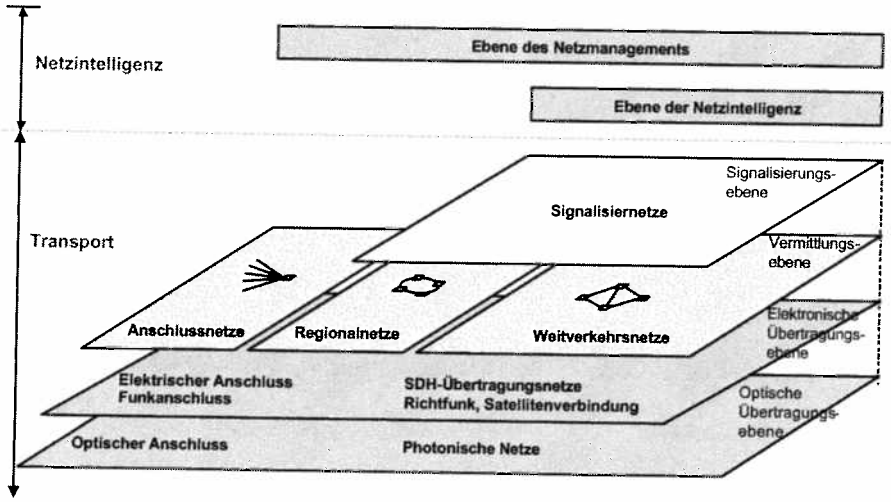


Bild: Ebene-Architektur von Kommunikationsnetzen

Netzkontrolle, Management und Sicherheit

Die größten Herausforderungen und höchsten Kosten der modernen Kommunikationsinfrastrukturen liegen in den Bereichen Steuerung, Management sowie Ausfall- und Informationssicherheit. Es ist daher notwendig, diesen Bereichen besondere Aufmerksamkeit zu widmen.

Signalisierungssystem Nr.7 (SS7): Für den Informationsaustausch zwischen den Netzknoten und als Infrastruktur für die verteilte Netzintelligenz bildet das Signalisierungssystem Nr.7 ein eigenständiges Paketvermittlungsnetz. Diese Signalisiernetze haben somit eine zentrale Bedeutung für die Signalisierungsabläufe in vielen der oben erwähnten Netze. Deshalb werden sehr viele Vorkehrungen getroffen, um eine extrem hohe Netzverfügbarkeit gewährleisten zu können.

Intelligente Netze: Die Vernetzung von informationsverarbeitenden Einheiten zur Unterstützung von Mehrwertdiensten oder zur Abwicklung der Mobilkommunikation bezeichnet man als intelligentes Netz (IN). Dieses Konzept bietet die Möglichkeit, neue sowie kundenspezifische Dienste schnell und flexibel einzuführen. Darüber hinaus bilden die intelligente Netze die Basis für personenbezogene Kommunikationsformen, welche für Benutzermobilität benötigt werden.

Netzmanagement: Zur Gewährleistung eines sicheren und effektiven Betriebs der Kommunikationsnetze oder LAN-Vernetzungen sind Netzmanagementsysteme erforderlich. Zu den Aufgaben gehören die Konfigurierung, Überwachung, Fehlererkennung und -behebung sowie die Verwaltung der Netze. Ein effektives Netzmanagement für heterogene Netze ist die Herausforderung der kommenden Jahre. Mit dem Netzmanagementkonzept TINA (Telecommunication Information Network Architecture) haben Netzbetreiber sowie Hersteller der Telekommunikations- und Computerindustrie eine neue Software-Architektur entworfen, welche Diensteanbieter bei der Implementierung und Nutzung von Multimedia-Diensten unterstützt. Das Konzept besteht im wesentlichen darin, das Übertragungsnetz von der Steuerungs- und Verwaltungsebene zu trennen und diese vollständig Software-orientiert und unabhängig vom zugrundeliegenden Übertragungsnetz zu machen. Es handelt sich um einen verteilten, objektorientierten Ansatz, der die Stärken der Telekommunikationsindustrie mit denen der Computerindustrie verbindet. Ziel ist es, einer Vielzahl von Diensteanbietern unabhängig voneinander eine schnelle und effiziente Einführung neuer Kommunikationsdienste zu erleichtern.

Netzsicherheit: Sicherheit hat aufgrund der zunehmenden Bedeutung der Informationsverarbeitung sowie ihrer weltweiten Vernetzung eine zentrale Stellung erlangt. Deshalb wird in erheblichem Umfang in die Sicherheit der Informationsverarbeitungssysteme investiert und es werden Möglichkeiten entwickelt, Kommunikationsdienste und deren Netzverbindungen individuell und von Ende-zu-Ende zu sichern. Wichtigste Funktionen der Netzsicherheit sind hierbei: Partner-Authentikation, Nachrichtenauthentizität und Integrität durch elektronische Unterschriften, Nachrichtenvertraulichkeit, Zugangssicherung sowie Sicherheitsmanagement. Eine Herausforderung bei der Implementierung von Sicherheitsfunktionen ist die große Vielfalt der Netze, Übertragungsprotokolle sowie der Endgeräte mit ihren Betriebssystemen und unterschiedlicher Anwendungssoftware. Daher kann es kaum einheitliche technische Lösungen für Authentikations-, Zugangssicherungs- und Vertraulichkeitsfunktionen geben. Dies ergibt sich insbesondere aus der Forderung, Sicherheitsfunktionen möglichst anwendungsnah zu realisieren. Allerdings ist es durchaus möglich, einzelne Sicherheitskomponenten zu modularisieren und für den Einsatz bei unterschiedlichen Anwendungen entsprechend zu konfigurieren. Hierzu gehören vor allem Komponenten des Schlüsselmanagements wie die Chipkarte für die Aufbewahrung und Verarbeitung persönlicher Schlüsselinformationen, sowie zentrale Dienstleistungsfunktionen für die Schlüsselverwaltung.

1.2 Grundlagen: Anwendungsgebiete und Anforderungen

Version: Feb. 2004

- Übersicht über Anwendungen
- Dienste und deren Anforderungen
- Interaktive Datenkommunikation, Datei-Transfer
- Echtzeit-Kommunikation
- Client-Server Modell

Kommunikationsnetze erlauben einen zeitweisen oder dauernden Datentransport zwischen (räumlich) entfernten Benutzern (Teilnehmern). Teilnehmer können sowohl Menschen als auch Maschinen sein, welche über Teilnehmerendeinrichtungen (Terminal Equipment, TE) an das Kommunikationsnetz angeschlossen sind.

Die Kommunikation besteht aus drei Phasen:

- Aufbau eines Übermittlungspfades (Verbindung) zwischen zwei oder mehreren miteinander Daten austauschenden TEs. Dazu werden dem Netzsteuerungstechnische Informationen (Rufnummer, Adresse) übergeben.
- Nachrichtenaustausch.
- Abbau der Verbindung.

Unter einem Kommunikationsdienst werden alle funktionellen Eigenschaften eines Kommunikationsnetzes verstanden, welche eine bestimmte Kommunikationsform zwischen TEs (Terminal Equipment) unterstützen, einschließlich aller funktionellen, qualitativen und rechtlichen Aspekte.

- **Funktionelle Aspekte** beziehen sich auf standardisierte Netzschnittstellen und Prozeduren.
- **Qualitative Aspekte** enthalten Aussagen über die Dienstgüte oder Dienstqualität (Blockierverhalten, Übertragungsfehler).
- **Rechtliche Aspekte** betreffen den Versorgungsanspruch, Einhaltung des Fernmeldegeheimnisses oder die Gebührenerhebung, welche in einer Telekommunikationsordnung niedergelegt sind.

Kommunikationsdienste werden weiter unterteilt hinsichtlich des Funktionsumfanges und der Abwicklungsform und sind durch zusätzliche Dienstmerkmale näher festgelegt.

Moderne Netze erlauben die Integration mehrerer oder sogar aller verschiedener Kommunikationsdienste. Diese Entwicklungen führten zur Einführung des **Diensteintegrierenden Digitalnetzes** (Integrated Services Digital Network, **ISDN**), zur Entwicklung der Zellenvermittlungstechnologie ATM (Asynchronous Transfer Mode) und heute zur Weiterentwicklung der Paketvermittlungs-technologie IP (Internet Protocol) zu einem diensteintegrierendes Paketvermittlungsnetz.

Diensteintegrierende Netze

ISDN: Leitungsvermittlung
ATM: Zellenvermittlung
IP: Paketvermittlung

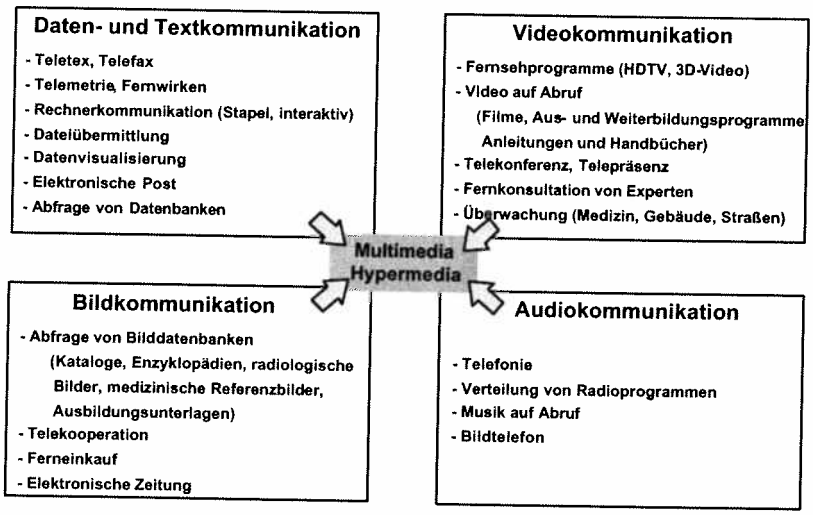


Bild: Diensteintegration

Multimedia-Kommunikation

Die Grundkommunikationsformen (Daten, Text, Bild, Video und Audio) können in einer Anwendung entweder einzeln auftreten oder in Kombination (Multimedia-Kommunikation). Man spricht von Hypermedia, wenn die auf dem Bildschirm erscheinende Information nicht nur von einer Quelle kommt, sondern durch Pointer-Anbindungen über das Internet aus Daten aus verschiedenen globalverteilten Quellen stammt. Einige Anwendungen sind im Bild aufgelistet.

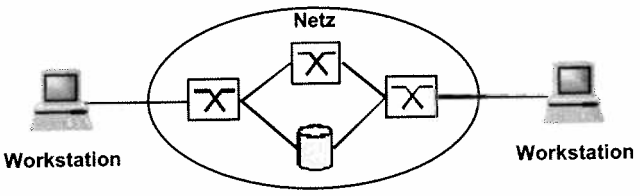


Bild: Multimedia-Kommunikation

Merkmale der Multimedia-Kommunikation:

- Daten-, Text-, Bild-, Video- und Audiokommunikation.
- Dynamische Aktivierung während einer Sitzung.
- Datenströme mit stark variierender Intensität.
- Unterschiedliche Dienstgüte-Anforderungen.
- Erzeugung, Manipulation, Speicherung und Zugriff.
- Echtzeitbedingungen (Information auf Anfrage).

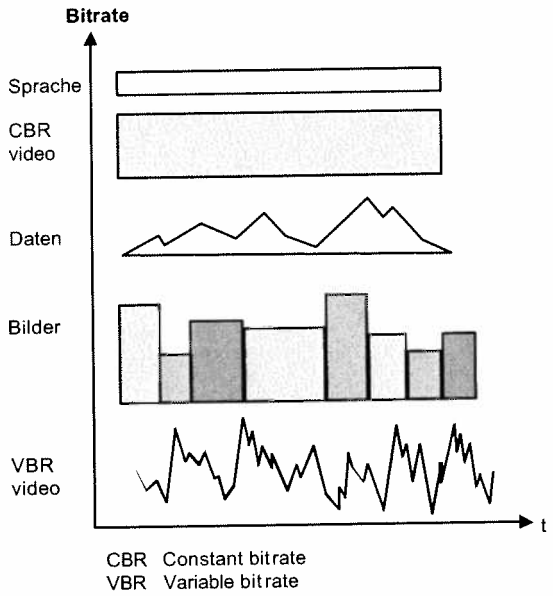


Bild: Eigenschaften von Verkehrsquellen

Die Anwendungen der Kommunikation lassen sich unterscheiden hinsichtlich der Form der Kommunikation:

- Datenkommunikation,
- Textkommunikation,
- Festbildkommunikation (Graphik)
- Bewegtbildkommunikation (Video),
- Sprach- und Audiokommunikation.

Jeder dieser Kommunikationsformen stellen eigene Ansprüche an das Netz. Hier spielen u.a. die folgenden Qualitätsanforderungen eine große Rolle:

- Durchsatz (Bitrate),
- Ende-zu-Ende Verzögerung,
- Verzögerungsschwankungen (Jitter),
- Fehlerrate (Bit-, Zellen- oder Paketfehlerrate),
- Verfügbarkeit (Netz- oder Dienstverfügbarkeit).

Das Bild illustriert den Verlauf der Bitrate verschiedener Verkehrsquellen: Sprache, Video mit konstanter Bitrate (CBR, Constant Bit Rate), Datentransfer und Transfer von Bildern und Video mit variabler Bitrate (VBR, Variable Bit Rate).

Typische Multimedia-Anwendungen sind:

- Zugriff auf MM-Dokumente (MM-Retrieval),
- Verteilte MM-Konferenz,
- Rechnerunterstütztes, kooperatives Arbeiten (Computer Supported Cooperative Work, CSCW),
- Rechner- und netzunterstütztes Unterweisen (Distance Learning).

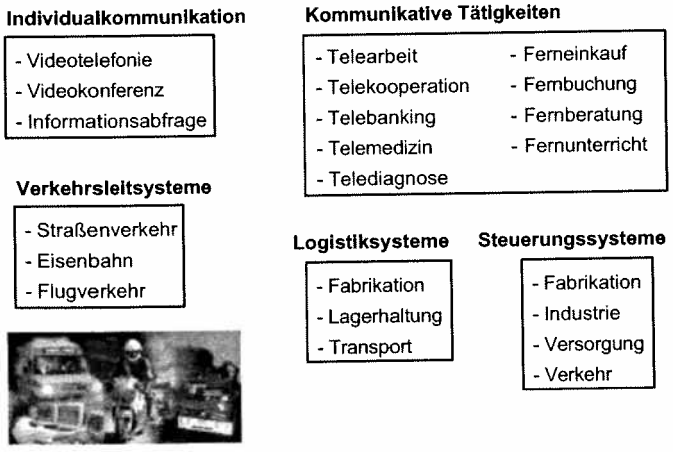


Bild: Kommunikationsanwendungen

Neben der Individualkommunikation und alle kommunikative Tätigkeiten mit der Präfix "Tele" oder "Fern" erstreckt sich der Bereich Telekommunikationsdienste auch hin zu vielen anderen Bereichen wie Verkehrsleitsysteme sowie Logistik- und Steuerungssysteme.

Einteilung der Kommunikationsdienste

Kommunikationsdienste lassen sich nach unterschiedlichen Merkmalen unterteilen:

- Funktionsumfang,
- Abwicklungsform.

a) Funktionsumfang

Der Funktionsumfang erstreckt sich auf die Punkte, zwischen denen die Kommunikation angewandt wird, und die funktionellen Eigenschaften des Dienstes. Es werden grundsätzlich zwei Dienstkategorien unterschieden:

- Übermittlungsdienste (Bearer Services),
- Teledienste (Tele Services).

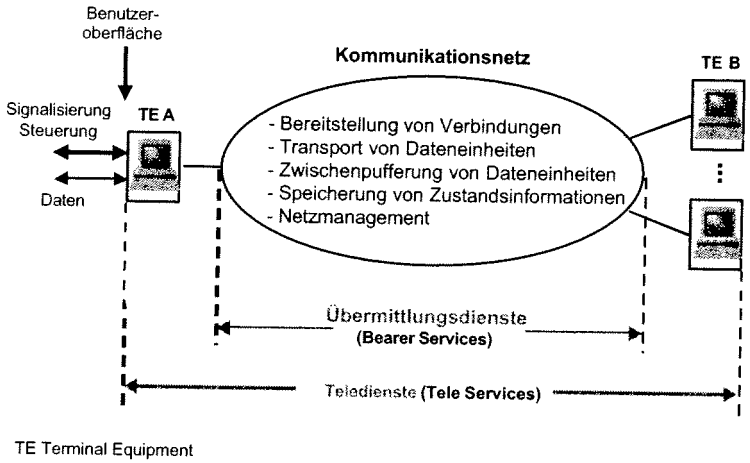


Bild: Wirkungsbereich von Diensten

Übermittlungsdienste (Bearer Services)
Code- und Anwendungs-unabhängige Datenübermittlung, d.h. Auf- und Abbau von Verbindungen über das Netz und Übertragung der Nutzinformation **ohne** Berücksichtigung der Kommunikationsfunktionen der TE. (Schichten 1-3 des ISO-Referenzmodelles)

Teledienste (Tele Services)
Benutzer-Benutzer-Kommunikation **mit** Einschluss der Kommuni-kationsfunktionen der TE, d.h. unter Einschluss der Steuerung des Dialogs innerhalb einer Verbindung, der Festlegung, der Codierung und der Formate (Schichten 4-7).

Interaktive Dienste (Interactive Services)

Dialogdienste (Conversational Services)
Bidirektionale (Dialog-)Kommunikation zwischen zwei TE ohne wesentliche Zwischenpufferung der Benutzerinformationen.

Beispiele: Telefon, Videotelefon, Datendialogkommunikation, und Filetransfer.

Speicherdienste (Messaging Services)
Benutzer-zu-Benutzer-Kommunikation mit Zwischenspeicherung von Benutzerinformation.

Beispiele: Elektronische Post, E-mail, Message Handling, Voice-mail und Video-mail.

Abrufdienste (Retrieval Services)
Abruf gespeicherter Informationen aus (öffentlichen) Datenbanken auf Anforderung durch individuelle Benutzer.

Beispiele: Abruf von HiFi-Audioprogrammen (audio retrieval), Abruf von Videoprogrammen (video retrieval), Abruf von gespeicherten Daten (data retrieval).

b) Abwicklungsform

Sie bestimmt, welche Eigenschaften der Kommunikationsdienst im Hinblick auf seine Nutzung aufweist.

Die folgende Einteilung folgt der Definition der ITU-Standardisierung:

- Interaktive Dienste (Interactive Services)
- Verteildienste (Distributive Services)

Verteildienste (Distributive Services)

Verteildienst ohne Rückkanal
Informationen werden von einer zentralen Stelle aus in kontinuierlich ablaufender Form angeboten und können von einer unbegrenzten Anzahl von Benutzern empfangen werden ohne Einflussnahme auf Beginn, Ende oder die Reihenfolge des Informationsangebotes.

Beispiele: Rundfunk und Fernsehen.

Verteildienst mit Rückkanal
Individueller Zugang zu zentral angebotenen Informationen mit der Möglichkeit, die Darstellung individuell zu gestalten, z. B. hinsichtlich Beginn, Unterbrechung, Wiederholung, Zeitlupe.

Beispiele: interaktives Fernsehen (Video-on-Demand), interaktiver Rundfunk, Televoting.

Anwendungen und Dienste

Aus der Sicht des Netzes stellen Anwendungen bestimmte Anforderungen, die zu erfüllen sind, damit der Anwender den erwarteten Nutzen erhält. Anwendungen im Zusammenhang mit Netzen sind Anwendungsprogramme, die (jedoch nicht notwendigerweise) von Personen genutzt werden. Die Anwendungsprogramme rufen die im Netz verfügbaren Dienste über ihr API (Application Programming Interface, Anwendungsprogrammierschnittstelle) auf. Der Dienst wird durch Kommunikationssoftware (Protokollstapel) realisiert, die (zumindest in den unteren Schichten) ein fester Bestandteil des Betriebssystems der zugrunde liegenden Plattform (Rechner) ist.

Anforderungen

Erreichbarkeit (connectivity)
Alle Mitarbeiter und Geschäftspartner (Kunden, Lieferanten) sollen erreicht werden können.

Verfügbarkeit/Zuverlässigkeit (availability / reliability)
Die Kommunikation soll jederzeit ohne Einschränkungen möglich sein.

Sicherheit (security)
Die Kommunikation soll vertraulich und fehlerfrei sein, die Echtheit der Kommunikationspartner und der Nachrichten soll gewährleistet sein.

Kosten: Die Gesamtkosten sollen möglichst niedrig sein.

Diese Anforderungen sind teilweise widersprüchlich. Demzufolge muss eine gute Lösung einen vernünftigen Kompromiss ergeben. Dabei sind verschiedenartige technische und organisatorische Lösungen zu berücksichtigen.

Bild: Anforderungen an die Geschäftskommunikation

Übertragungsmedium
Leitungsgebundene Übertragung (Kupfer oder Faserkabel) oder Funkübertragung (Funk oder optisch).

Zeitliche Verfügbarkeit
Zeitbegrenzt (Wählverbindung) oder permanent (Festverbindung).

Art der Nutzung
Exklusiv oder nichtexklusiv (gemeinsames Medium, shared Medium).

Die Netzverbindungen können nach verschiedenen Kriterien eingeordnet werden.

Private Netze
Sie sind im Besitz einer Firma/Institution und werden ausschließlich von dieser genutzt. Die Investitionskosten sind vom Besitzer voll zu tragen, dafür fallen keine nutzungsabhängigen Kosten an. Vorschriften zur Technik (Protokolle) müssen nicht streng beachtet werden. Sicherheitsprobleme spielen in der Regel keine wesentliche Rolle.

Öffentliche Netze
Ein Netzbetreiber finanziert und betreibt ein Netz (oder mehrere Netze), über das seine Kunden kommunizieren können und dafür feste und (oder) nutzungsabhängige Gebühren bezahlen. Standards stehen bei Netzbetreiber im Vordergrund und die Sicherheit ist von größerer Bedeutung.

VPN (Virtual Private Network)
Ein Netz, das sich wie ein privates Netz verhält, jedoch auf der Infrastruktur eines öffentlichen Netzes aufsetzt. Damit ist die Sicherheit ein zentrales Anliegen. Ein VPN beinhaltet jedoch auch einen eigenen Adressierungsplan sowie eigenes Management und Verrechnung (Accounting).

LAN (Local Area Network): Sie sind private Netze, die im wesentlichen ohne Vorschriften und Nutzungsgebühren von jedermann installiert und betrieben werden können. Trotzdem sind LAN weitgehend standardisiert, da nur so hinreichend große Märkte mit funktionierendem Wettbewerb und zueinander kompatiblen Produkten entstehen können. LANs sind geografisch auf das Grundstück eines Eigentümers beschränkt. (Ausnahme: drahtlose Verbindungen zwischen LAN-Inseln auf verschiedenen Grundstücken.)

- **Großflächige Netze (WAN, MAN):** Netze, die von Netzbetreibern (carrier) oder Netzanbietern betrieben werden.
- **Firmennetze (corporate networks):** Ein Unternehmen kann für sich selber ein WAN betreiben ohne darauf Dienste für andere zu erbringen. Dazu werden Leitungen von Netzbetreibern gemietet und zu einem scheinbar firmeneigenen Netz verbunden. Das Unternehmen ist selbst für den Betrieb und das Management dieses Netzes verantwortlich.
- **RAS (Remote Access Service):** ein Netz, das hauptsächlich auf Wählleitungen öffentlicher Netze aufsetzt. Die Funktion von RAS ist die eines Zugangsnetzes.
- **VPN (Virtual Private Network):** Ziel eines VPN ist der Ersatz teurer, exklusiver Übertragungswege durch gemeinsam genutzte Leitungen. Die Unterscheidung in Kern und Zugangsnetz ist hier weniger bedeutsam. Das Internet bietet eine attraktive Basis für die Realisierung von VPN.
- **Internet, Intranet, Extranet:** Das Internet ist ein öffentliches und offenes Netz. Ein Intranet ist ein Netz, das die gleiche Technik (Protokolle) benutzt wie das Internet, aber nur für eine geschlossene Benutzergruppe (z. B. die Mitarbeiter einer Firma) zur Verfügung steht. Ein Extranet ist ein Intranet, das zusätzlich ausgewählten Partnern (Kunden, Lieferanten) den

Zugang ermöglicht. Ein Intranet kann grundsätzlich ohne Zugang zum Internet existieren. In der Regel wird jedoch ein - unidirektionaler oder selektiver - Internetzugang gewünscht sein). Dadurch wird aber das Problem der Sicherheit des Intranet gegenüber dem Internet aufgeworfen. Die Realisierung eines Intranet auf der Struktur des Internet ist aus wirtschaftlichen Gründen vorteilhaft. Allerdings stellen sich bei dieser Variante schwerwiegende Sicherheitsprobleme. Ein Intranet kann auch dadurch abgegrenzt werden, dass es private IP-Adressen nutzt.

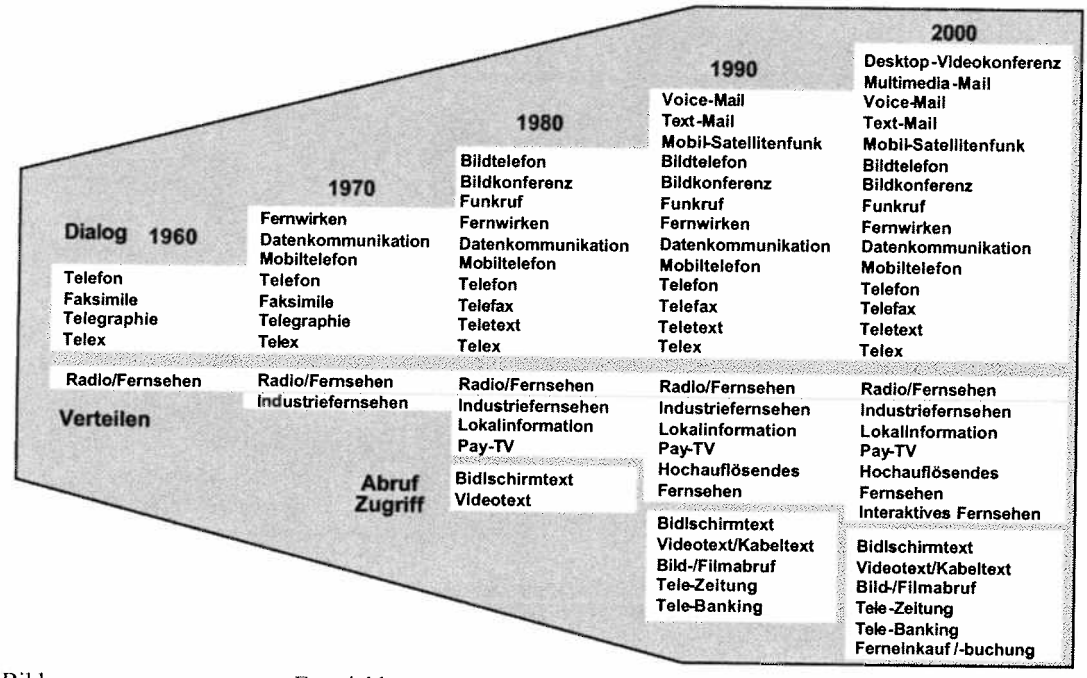


Bild: Entwicklung der Kommunikationsdienste

Dienstmerkmale

Moderne Kommunikationsdienste weisen sehr unterschiedliche Merkmale auf, welche aus der Informationsdarstellung, der Codierung, der Nutzung oder dem Benutzerverhalten resultieren:

- Bitrate (Bandbreite): konstant oder variabel,
- Betriebsverhalten: kontinuierlicher oder büschelartiger Betrieb,
- Konfiguration: Punkt-zu-Punkt, Punkt-zu-Mehrpunkt und Mehrpunkt (Konferenz),
- Verbindungshäufigkeit und Verbindungsdauer.

- **Diensteintegration**
  - Mehrere Dienste pro Netz
  - Video-, Sprach- und Datenübertragung
- **Leistungsfähigkeit**
  - Hohe Bitrate
- **Übermittlungsgüte**
  - Geringe Verzögerungen
  - Geringe Verzögerungsschwankungen (Jitter)
  - Geringe Fehlerraten
- **Vermittlungsgüte**
  - Verbindungsaufbaudauer
  - Blockierwahrscheinlichkeit
- **Erreichbarkeit**
  - Vernetzung
  - Verbindung von Teilnetzen
- **Verfügbarkeit**
- **Wirtschaftlichkeit**
- **Sicherheit und Privatsphäre**

Bild: Anwendungsanforderungen

Netzanforderungen

Zur Unterstützung der Kommunikation stellen Kommunikationsdienste unterschiedliche Anforderungen an das Kommunikationsnetz hinsichtlich

- Diensteintegration,
- Leistungsfähigkeit (Durchsatz, bzw. Bitrate),
- Übertragungsgüte (Bitfehlerrate, Informationsverzögerung),
- Vermittlungsgüte (Verbindungsaufbaudauer, Blockierwahrscheinlichkeit),
- Erreichbarkeit (Grad der Vernetzung),
- Verfügbarkeit (Ausfallsicherheit, Selbstheilbarkeit, automatische Rekonfigurierbarkeit),
- Wirtschaftlichkeit (Gebührenstruktur),
- Sicherheit und Privatsphäre.

- **Reihenfolgetreue:**
  Definiert die Akzeptanz von möglichen Reihenfolge-Vertauschungen

- **Segmentierte Datenzustellung:**
  Spezifiziert, ob der Empfang von segmentierten Dateneinheiten zulässig ist

- **Maximale Dateneinheitsgröße:**
  Wird für die Anwendungsschnittstelle definiert

- **Gruppenzustellung:**
  Spezifiziert den Anwendungswunsch nach Gruppenkommunikation und deren Semantik

- **Fehlertoleranz:**
  Erlaubt die Angabe von tolerierbarem Datenverlust, akzeptabler Datenreplikation und Datenverfälschung

- **Sicherheitsanforderungen:**
  Angaben über die Daten- und Zugriffs-Sicherheit sind möglich

Bild: Qualitative Dienstparameter

Für jeden Dienst sind dienstspezifische Vereinbarungen zu treffen.

Beispiele für qualitative Dienstparameter sind:

- Reihenfolgetreue,
- Segmentierungserlaubnis,
- Maximale Größe der Dateneinheiten,
- Individual- oder Gruppenkommunikation,
- Fehlertoleranz,
- Sicherheitsanforderungen.

- **Durchsatz:**
  Menge der zwischen Dienstbenutzern ausgetauschten Daten je Zeiteinheit
- **Burstiness:**
  Maximale zu mittlerer Bitrate innerhalb eines Bursts oder mittlere Burstlänge
- **Verzögerung:**
  Zeitspanne zwischen der Übernahme einer Dateneinheit und Auslieferung
- **Verzögerungsschwankung (Jitter):**
  Schwankung in der Verzögerung von Dateneinheiten
- **Antwortzeit:**
  Zeit, die zusätzlich zur zweifachen Verzögerung die Verarbeitungszeit des Empfängers einschließt
- **Datenverfälschung:**
  Anzahl der verfälschten Dateneinheiten
- **Datenverlust**
  Anzahl der verlorengegangenen Dateneinheiten
- **Netz- oder Dienstverfügbarkeit**
  Spezifiziert die maximale Zeit eines Unterbruches

Bild: Quantitative Dienstparameter

Für jeden Dienst sind auch quantitative Vereinbarungen über Kommunikationseigenschaften zu treffen.

Es gibt fünf Basisanforderungen:

- Durchsatz (Bitrate),
- Ende-zu-Ende Verzögerung,
- Verzögerungsschwankungen (Jitter),
- Fehlerrate (Bit-, Zellen- oder Paketfehlerrate),
- Verfügbarkeit (Netz- oder Dienstverfügbarkeit).

Bei der Burstiness handelt es sich um den zeitlichen Verlauf der Bitrate. Die Antwortzeit (Roundtrip delay) bestimmt die Wartezeit eines Benutzers auf die Rückantwort. Und Datenverfälschung ist einer der verschiedenen Gründe für Datenfehler.

Sprache	2,4 – 64 kbit/s
Audio Disk	1,5 – 6 Mbit/s
Audio MP3	128 kbit/s
Video	
unkomprimiert	100 Mbit/s
unkomprimiert hochauflösend	1 – 2 Gbit/s
komprimiert DVD	1,5 Mbit/s
komprimiert	5 Mbit/s
komprimiert hochauflösend	20 – 100 Mbit/s
Video	
1000 × 1000 Pixel à 24 Bits	24 Mbit/s
Röntgentomographie	5 Mbit/s

Bild: Durchsatzanforderungen

Abhängig von der Quelle werden unterschiedliche Durchsatzanforderungen an das Netz gestellt. Bei den aufgeführten Audio- und Videoquellen handelt es sich um konstante Bitraten. Die Verkehrsart wird als Streaming bezeichnet.

- Die Basisrate für Sprache ist 64 kbit/s. Mit verschiedenen Kompressionsverfahren, die alle standardisiert sind, entstehen die konstante Raten 32 kbit/s, 16 kbit/s, ..., bis zu 2.4 kbit/s. Ab 16 kbit/s nimmt die Qualität stark ab. Jede Kompression verursacht eine Verzögerung.
- Musik von einer CD erfordert mindestens eine Bitrate von 1,5 Mbit/s, bei MP3 reduziert sich die Rate auf 128 kbit/s.
- Die Video-Raten sind 100 Mbit/s und 1 Gbit/s (hochauflösend). Bei Off-line-Kompression auf einer DVD reduziert sich die Bitrate auf 1,5 Mbit/s. Für Echtzeit-Kompression sind die Werte von 5 Mbit/s und 20 Mbit/s (hochauflösend) erzielbar.

Sprache	analog digital	3 kHz	GSM Telefonie	13 kbit/s 64 kbit/s, 32 kbit/s, ... 2,4 kbit/s
Audio	analog digital	20 kHz	CD-Qualität MP3-komprimiert	1,5 bis 6 Mbit/s 128 kbit/s
Video	analog digital	5-6 MHz	Fernsehen in Studioqualität Digitalvideo (unkomprimiert) Digitalvideo (komprimiert) HDTV (unkomprimiert) HDTV (komprimiert)	50 -100 Mbit/s 100 - 500 Mbit/s 20 - 100 Mbit/s 2 Gbit/s 100 Mbit/s
Text	digital			50 kbit/s -10 Mbit/s
Daten	digital		Datentransfer Telekonferenzen	1 - 150 Mbit/s < 150 Mbit/s
Bilder	digital		Graphiken Fotos Hochauflösende Bilder	einige 100 kbit/s einige Mbit/s < 150 Mbit/s

Bild: Signal- und Datenquellen

Neben Signal- und Datenquellen mit einer konstanten Bitraten (Sprache, Audio, Video) sind auch Quellen mit Datenbursts (Text, Daten, Bilder) zu betrachten. Sie beanspruchen das Netz kurz, aber maximal bis zur vollen Anschlussrate. Bei Ethernet bis zu 10 Mbit/s, 100 Mbit/s, 1 Gbit/s. Im allgemeinen wird die momentane Rate von den Protokollen abhängig sein.

Sprach-, Audio und Videoquellen können auch eine variable Bitrate produzieren:

- **Sprache:** Pausenunterdrückung,
- **Audio:** hohe Bitrate bei schnell wechselnden Klängen.
- **Video:** hohe Bitrate bei schnell wechselnden Szenen.

Daten und Bilder

A4 Textseite	3 KByte
A4 gescannte Seite (niedrige Auflösung)	4 MByte
A4 gescannte Seite (hohe Auflösung)	8 MByte
Bild 1280 x 1024 x 16	2,5 MByte
Bild 1280 x 1024 x 24	4 MByte
Bild 4096 x 4096 x 16	34 MByte
Bild 4096 x 4096 x 24	50 MByte

Anzahl Bits für Farben oder Graustufen

Bildgröße in Pixels (Bildpunkten)

E-Mail

Text	1.5 KByte
HiFi-Audio	10 Mbyte / min
Kleinbildvideo	50 Mbyte / min
Graphik	1 Mbyte / Graphik
Foto	4 Mbyte / Foto

Bild: Datenmenge

Anwendung	Erforderliche Datenrate
Persönliche Kommunikation	0,3 - 9,6 kbit/s
E-Mail-Übertragung	2,4 - 9,6 kbit/s
Fernsteuerung	9,6 - 56 kbit/s
Digitale Sprachübertragung (Telefonqualität)	64 kbit/s
Datenbankabfrage	bis 1 Mbit/s
Audiosignale (hohe Qualität)	1 - 2 Mbit/s
Videosignale (komprimiert)	2-10 Mbit/s
Videosignale (z. B. für Telemedizin)	bis 50 Mbit/s
Dokumentverwaltung (Document Imaging)	10 - 100 Mbit/s
Bildkommunikation (Scientific Imaging)	bis 1 Gbit/s
Video (Bewegtbild)	1 - 2 Gbit/s

Bild: Erforderliche Datenraten

Datenraten

Je nach Anwendung sind Datenraten von weniger als 1 kbit/s bis zu über 1 Gbit/s erforderlich.

Übertragungssystem	Datenrate
Modem an Wählleitung	1,2 - 56 kbit/s
Dateiübertragung über serielle Schnittstelle	bis 115 kbit/s
Parallele Schnittstelle	300 kbit/s
WAN-Verbindung, ISDN, Fractional T1	64 kbit/s
WAN-Verbindung, T1, T3	1,5 Mbit/s, 45 Mbit/s
WAN-Verbindung, E1, E3	2 Mbit/s, 34 Mbit/s
Token Ring LAN	4, 16, 100 Mbit/s
Ethernet LAN	10, 100 Mbit/s, 1, 10 Gbit/s
HSSI (High-Speed Serial Interface)	52 Mbit/s
FDDI (Fiber Distributed Data Interface)	100 Mbit/s
FCS (Fibre Channel System)	1 Gbit/s
SDH (verfügbar)	155 Mbit/s -10 Gbit/s
SDH, SONET (verfügbar)	50 Mbit/s -10 Gbit/s
SDH, SONET (zukünftig)	40 Gbit/s

Bild: Datenraten von Übertragungssystemen

Durch Wahl eines geeigneten Übertragungssystems können diese Datenraten verfügbar gemacht werden. Die Schnittstelle zwischen Endgerät und Netz muss ebenfalls die geforderte Datenrate zulassen.

Übertragungsmedium	Bitfehlerwahrscheinlichkeit
Funkkanal	10^{-1} - 10^{-3}
Telefonleitung	10^{-5}
Digitales Datennetz	10^{-6} - 10^{-7}
Koaxialkabel im LAN	10^{-9}
Glasfaser (Lichtwellenleiter)	10^{-12}

Bild: Bitfehlerwahrscheinlichkeiten ohne Fehlerkorrektur

Fehlerraten

Die Bitfehlerwahrscheinlichkeit auf einem Übertragungsmedium ist von großer Bedeutung für die Dienstgüte. Wenn die Bitfehlerrate eines Mediums zu hoch ist, muss eine Fehlerkorrektur eingesetzt werden. Die von der Anwendung geforderte Restfehlerwahrscheinlichkeit bestimmt den dafür nötigen Aufwand. Beispielsweise wird für die Datenübertragung mittels GSM eine Restfehlerwahrscheinlichkeit kleiner als 10^{-7} verlangt, während die Fehlerwahrscheinlichkeit des Übertragungskanals mehrere Größenordnungen höher liegt.

Quality-of-Service (Dienstgüte, Dienstqualität)

Unter **Dienstgüte (QoS**: Quality-of-Service) versteht man das Verhalten eines Netzes, das bestimmte Arten von Verkehr bevorzugt gegenüber anderen Arten behandelt. Damit ist zunächst nichts über die verwendeten Mechanismen oder die Art und quantitative Festlegung der erreichbaren Güte gesagt.
Der Begriff COS (Class-of-Service) drückt aus, dass verschiedene Arten von Verkehr (Daten, Sprache, Video, ...) in Klassen eingeteilt werden, die vom Netz unterschiedlich behandelt werden. Die Anwendung der Begriffe QoS/COS im Zusammenhang mit Multimedia ist also naheliegend. Man unterscheidet drei Dienstgüteklassen:

- **Best-Effort-Dienste:** Dienste, die keine Garantien ermöglichen. Auf der Vermittlungsschicht des Internet erbringt IP einen Best-Effort Dienst.
- **Vorhersagbare Dienste** (auch historische Dienste): Die Grenzwerte der Dienstgüteparameter sind Schätzungen des vergangenen Verhaltens, die der Dienst auch zukünftig zu erfüllen anstrebt.
- **Garantierte Dienste:** Sie stellen QoS-Garantien zur Verfügung, die durch Dienstgüteparameter (Grenzwerte) entweder deterministisch oder im statistischen Mittel beschrieben werden. Beispiel für einen deterministischen Parameter ist die Laufzeit bzw. deren Schwankung. Ein statistischer Grenzwert könnte beispielsweise die Fehlerrate sein.

Anforderungen an die Dienstgüte:

Echtzeitanwendungen (Pakete müssen innerhalb festgelegter Zeitgrenzen zugestellt werden) versus Nicht-Echtzeitanwendungen. Die Sprachübertragung im Internet stellt Echtzeitanforderungen, da bei zu großen Verzögerungen der Pakete die Sprache unverständlich wird. FTP funktioniert hingegen auch bei großen und stark schwankenden Verzögerungen. Echtzeitanwendungen können als intolerant (Verluste, also auch die verspätete Ankunft von Paketen, können nicht hingenommen werden) und tolerant (gelegentliche Verluste können toleriert werden) klassifiziert werden. Die Sprachübertragung ist tolerant, da einzelne fehlende Abtastwerte des Sprachsignals durch Interpolation vorhandener Werte geschätzt werden können, ohne dass die Qualität des Sprachsignals stark leidet. Steuerungsdaten, beispielsweise für Roboter, müssen jedoch absolut fehlerfrei übertragen werden, da sonst nicht einschätzbare und potenziell gefährliche Folgen eintreten können.
Im einfachsten Fall sind Echtzeitanwendungen nichtadaptiv. Adaptive Anwendungen können sich an variierende Übertragungsparameter (in einem gewissen Umfang) anpassen und damit dem Anwender eine höhere subjektive Qualität bieten. Die Übertragung von Sprachsignalen kann verzögerungsadaptiv sein, wenn der Zeitpunkt des Auslesens des Empfangspuffers in Abhängigkeit der gemessenen, mittleren Verzögerung angepasst wird. Eine Bildübertragung kann ratenadaptiv sein, da Algorithmen für die Bildcodierung in der Regel einen Kompromiss zwischen Datenrate und Bildqualität zulassen.

- **Nicht-Echtzeitanwendungen** stellen keine konkreten Anforderungen an die Verzögerung und kommen mit Paketverlusten zurecht (in der Regel durch wiederholte Übertragung). Gleichwohl präferiert der Anwender kurze Verzögerung und geringe Verluste. Anwendungen in dieser Kategorie können interaktiv (WWW, FTP) oder asynchron (E-Mail) sein.

Zur qualitativen und quantitativen Erfassung der erbrachten Qualität oder Güte eines Dienstes werden unterschieden:
- **Dienstgüte, Dienstqualität** (Quality-of-Service, QoS),
  Gesamtheit der Qualitätsmerkmale eines Kommunikationsdienstes aus der Sicht des Benutzers dieses Dienstes
- **Netzgüte, Netzqualität** (Network Performance),
  Fähigkeiten des Kommunikationsnetzes, die Kommunikationsaufgaben zu erfüllen,
- **Verkehrsgüte, Verkehrsqualität** (Grade-of-Service, GoS).

Teil der Netzgeräte, der von der Bemessung der Netzbetriebsmittel und der Netzorganisation abhängt. Hierfür werden konkrete und messtechnisch erfassbare Metriken eingeführt wie
- Paketverlust-Wahrscheinlichkeit
- Paketfehlerrate, Zellfehlerrate
- Verbindungsaufbauverzugs-Dauer
- Transferdauer
- Transferdauerschwankung

Datenart	Durchsatz	max. Bitfehlerrate	Verzögerung	Jitter
Text Daten Echtzeitdaten	50 kbit/s einige 10 Mbit/s einige Mbit/s	$< 10^{-5}$ 0 0	1 – 10 s > 1 s 1 ms – 1 s	- - -
Sprache Musik	64 kbit/s 1.4 Mbit/s	10^{-1} 10^{-8}	< 0,25 s < 0,25 s	10 ms 10 ms
Graphiken Fotos	einige 100 kbit/s einige Mbit/s	$< 10^{-4}$ $< 10^{-4}$	< 1 s < 1 s	- -
Video (original) Video (komprimiert)	150 Mbit/s einige 10 Mbit/s	10^{-2} $< 10^{-8}$	< 0,25 s < 0,25 s	wenige ms wenige ms

Bild: Quantitative Anwendungsanforderungen

Zusätzliche Dienstmerkmale
Neben der Grundausstattung eines Dienstes wird eine Vielzahl zusätzlicher Funktionen (Supplementary Services, Service Attributes) bereitgestellt, welche entweder dem Benutzer des Dienstes oder dem Netzbetreiber dienen. Diese zusätzlichen Dienstmerkmale können auf verschiedene Art und Weise erbracht bzw. realisiert werden:
- Im Endgerät des Teilnehmers,
- In den Vermittlungseinrichtungen (Netzknoten),
- In speziellen Dienstzentralen (z. B. Dienste des sogenannten Intelligenten Netzes).

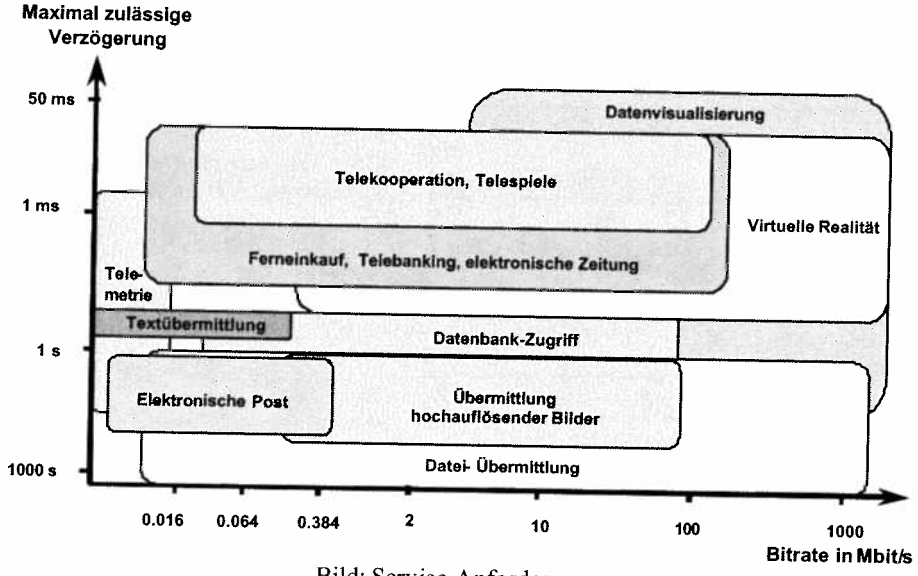


Bild: Service-Anforderungen

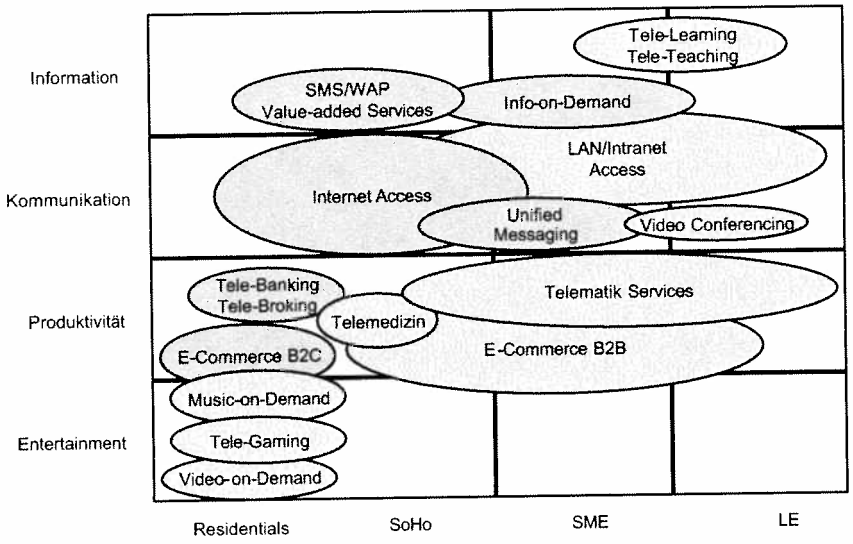
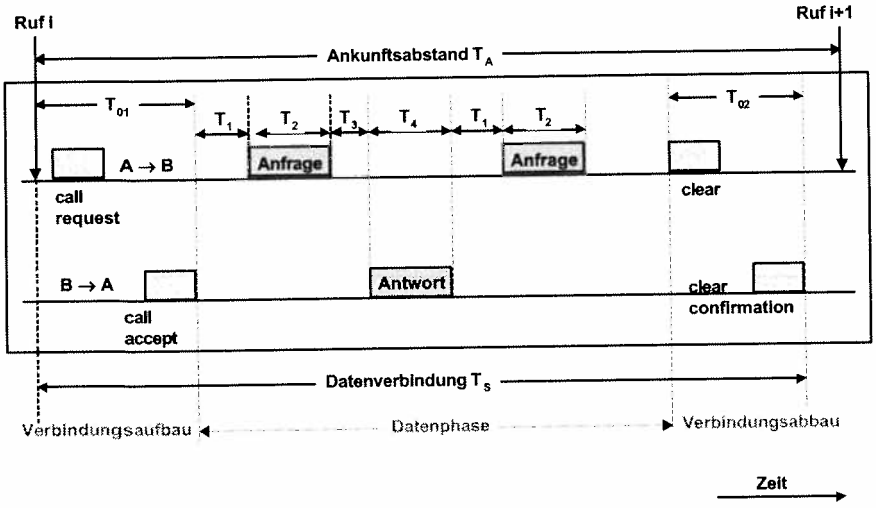
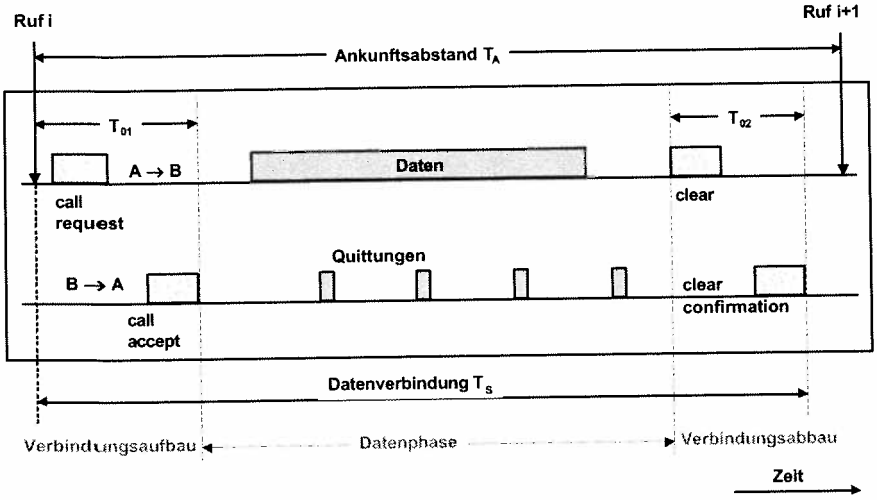


Bild: Marktklassifikation von Diensten



Massendatentransfer
Große Datenvolumen mit kurzen Quittungen in der Gegenrichtung oder eine kurze Anfrage mit einem großen Datenvolumen als Antwort.

Bild: Massendatenverkehr (Stapelverkehr)



Interaktiver Datenaustausch
In beide Richtungen unregelmäßige kurze Datenbursts, z.B. durch kurze Anfragen und Antworten.

Bild: Interaktiver Datenverkehr

Jitter

Die **Schwankung der Verzögerungszeit** (jitter) ist bei Paketnetzen grundsätzlich unvermeidlich und kann für den Anwender von besonderer Bedeutung sein. Sie wird durch die folgenden Begriffe charakterisiert:

- **Asynchrones Verhalten:** Die Verweildauer der Pakete zwischen Sender und Empfänger ist völlig offen und kann im Extremfall beliebig groß sein. Dies entspricht dem Begriff Best Effort. Bei der Übertragung von Rechnerdaten ist dieses Verhalten in der Regel akzeptabel.
- **Synchrones Verhalten:** Die Verweildauer der Pakete ist unbekannt und veränderlich, aber nach oben begrenzt. Der Grenzwert kann angegeben werden. Für die Sprach- und Bildübertragung in Paketnetzen ist synchrones Verhalten eine Mindestanforderung, die jedoch nicht hinreichend sein muss.
- **Isochrones Verhalten:** Die Verweildauer ist für alle Pakete gleich. Dieses Verhalten ist für die Sprach- und Bildübertragung in Paketnetzen geeignet.

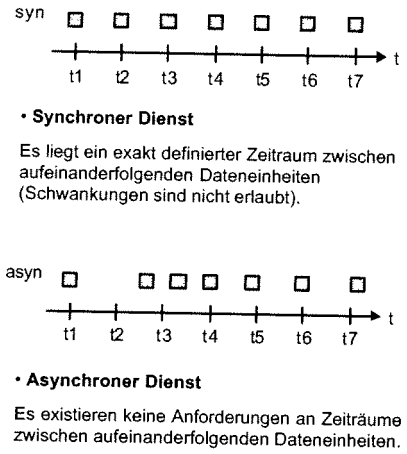
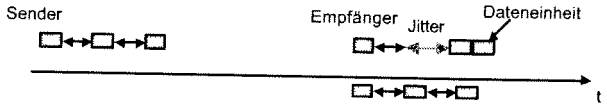


Bild: Synchroner und asynchroner Dienst

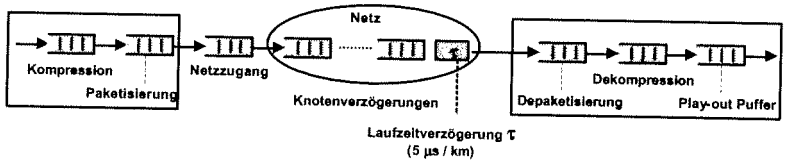


Jitter: Schwankung in der Verzögerung von Dateneinheiten

- Auch bei konstanter Senderate können die Dateneinheiten beim Empfänger mit variablen Zwischenabständen eintreffen
- Im Netz kann durch unterschiedliche Bedienung in den Zwischensystemen ein solcher Jitter verursacht werden

Bild: Verzögerungsschwankungen (Jitter)

Verzögerungskomponenten



Ende-zu-Ende Verzögerung
- 80 ms ermöglicht natürliche interaktive Kommunikation
- 100 - 120 ms ist tolerable
- Über 200 ms wird mühsam

- Ende-zu-Ende Laufzeitverzögerung bestimmt die verbleibende Zeit für die restlichen Verzögerungskomponenten
- Größe des Play-out Puffers ist bestimmt durch die maximale Verzögerungsschwankung

Bild: Ende-zu-Ende Verzögerung bei Echtzeit

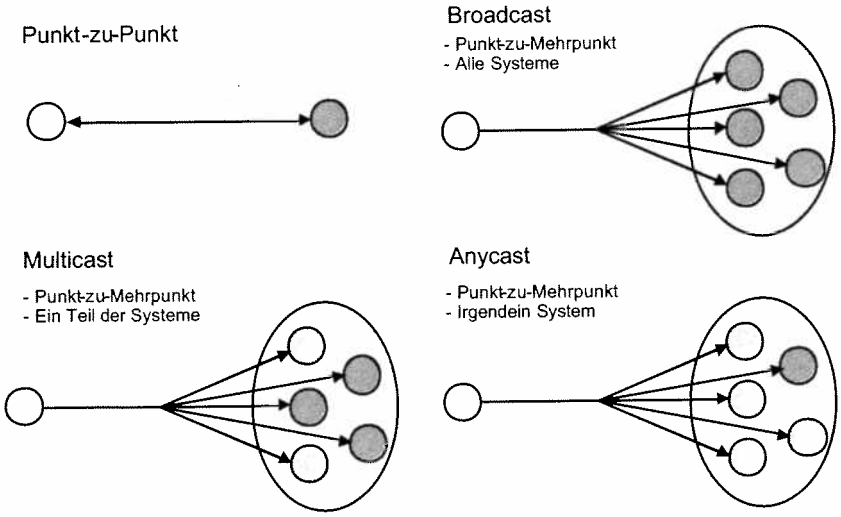


Bild: Kommunikationsformen

Kommunikationsbeziehungen

Eine Kommunikationsbeziehung (Kommunikationsstruktur, Kommunikationsmuster) gibt an, wie viele Teilnehmer in welcher Weise miteinander kommunizieren. Die einfachste Kommunikationsbeziehung besteht zwischen genau zwei Kommunikationspartnern, die bidirektional miteinander kommunizieren. Dies wird als Unicast bezeichnet und durch die Notation 1:1 gekennzeichnet. Unicast impliziert eine Punkt-zu-Punkt-Verbindung. Multicast Gruppenkommunikation) wird als 1:n und Broadcast als 1: m abgegeben.

Beim Multicast sendet 1 Sender an n Empfänger (Mitglieder der Gruppe). Beim Broadcast steht m für alle Teilnehmer in einem Netz. Beide Fälle beinhalten eine Punkt-zu-Mehrpunkt-Kommnunikation. Multicast ist in Rechnernetzen von zunehmender Bedeutung. Erweiterte Kommunikationsbeziehungen beschreiben die Kommunikation zwischen mehreren Teilnehmern. Kommunikationsbeziehungen dieser Art nehmen in der Praxis an Bedeutung zu.

Client-Server-Architekturen

Ein Netz kann aus Sicht der Anwendungen gleichberechtigte Teilnehmer miteinander verbinden. Solche Netze werden als **Peer-to-Peer-Netze** bezeichnet. Client-Server-Architekturen ordnen den Netzteilnehmern hingegen unterschiedliche Funktionen zu.

Ein Client ist ein Dienstnutzer, der Anfragen an einen Server (Diensterbringer) stellt. Der **Server** ermittelt und überträgt die Antwort an den Client. In der Praxis werden Server-Typen eingesetzt, die bestimmte Dienste erbringen und entsprechend benannt werden:

- **Dateiserver** (file server): speichert Dateien für eine Vielzahl von Clients und gibt diese auf Anfrage heraus.
- **Druckerserver** (print server): erledigt Druckaufträge für die im Netz existierenden Clients.
- **Datenbankserver** (database server): beinhaltet Datenbanken, die auf Anfrage von Clients abgefragt werden. Die Ergebnisse der Abfrage werden den Clients übermittelt.
- **Kommunikationsserver** (communications server): ermöglicht den Clients in einem Netz die Kommunikation in externe Netze.

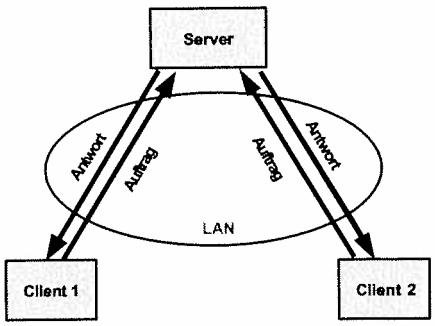


Bild: Client-Server Modell

Clients können für die Kommunikation mit einem bestimmten Servertyp ausgelegt sein. In der Regel können sie jedoch mit mehreren verschiedenartigen Servern kommunizieren.

Zur Festlegung der Aufgabenverteilung zwischen Client und Server wird ein vereinfachtes Schichtenmodell zugrunde gelegt. Die Schichten sind:

- **Darstellung** (presentation):
  beinhaltet die grafische Benutzeroberfläche, die die Interaktion des Anwenders mit der Anwendung ermöglicht.
- **Verarbeitung** (processing, application logic, business logic):
  beinhaltet die Anwendungsprogramme, die vom Anwender genutzt werden.
- **Datenhaltung** (data storage):
  beinhaltet Strukturen und Funktionen zur Speicherung und Manipulation von Daten für Anwendungsprogramme.

Die einfachste Verteilungsalternative besteht darin, Darstellung, Verarbeitung und Datenhaltung auf einem Zentralrechner auszuführen. Logisch findet also keine Verteilung statt, obwohl dezentrale Arbeitsplätze über ein Kommunikationssystem ~im einfachsten Fall eine sternförmige Punkt-zu-Punkt-Verkabelung, ein LAN kann ebenfalls verwendet werden) mit dem Zentralrechner kommunizieren.

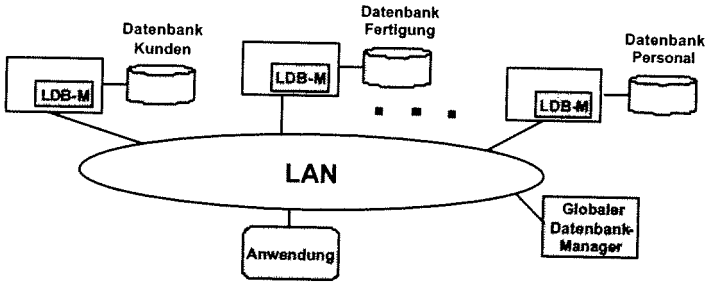


Bild: Verteilte Datenbank

Formen der Client-Server Modelle

- Basis Architektur (Clent-Server Architecture).
- Zwei-schichtige Client-Server-Architektur (two tier architecture).
- Drei-schichtige Client-Server-Architektur (three tier architecture).

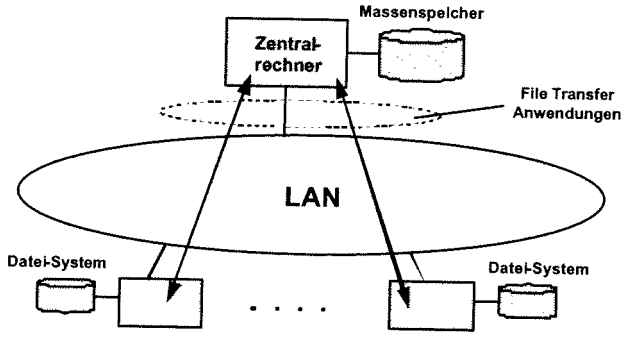


Bild: Verteilte Datenhaltung ohne Dateisystem

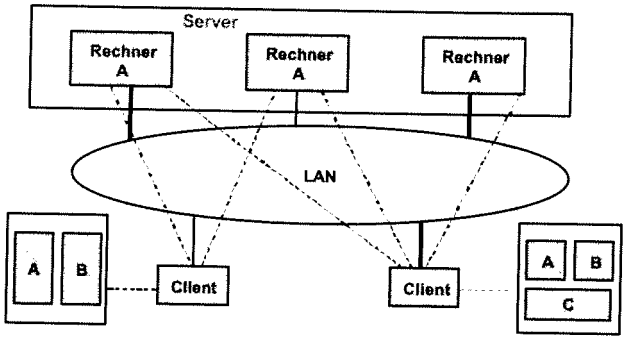


Bild: Verteilte Fenstertechnik

Zweischichtige Client-Server-Architektur

Client-Server-Architekturen (C/S-Architekturen) weisen Servern und Clients unterschiedliche Aufgaben zu. Zweischichtige C/S-Architekturen (two-tier architecture) überlassen dem Server die Datenhaltung. Bei der Variante fat client werden Darstellung und Verarbeitung vom Client erledigt. Beim fat server (gleichbedeutend mit thin client) übernimmt der Server zusätzlich die Verarbeitung.

Die über das Netz ausgeführten Funktionen sind für die beiden Fälle verschieden:

- **RFA (Remote File Access):** Zugriff auf eine entfernte Datei und deren Übertragung zum Client.
- **RDA (Remote Database Access):** Der Anwender sendet eine Datenbankanfrage an den Server.
- **Called Stored Procedures (gespeicherte Prozeduren):** Dies sind Anwendungsprogramme für die Datenbankabfrage, in die datenbankspezifische Anweisungen (z. B. SQL: Structured Query Language) eingebettet sind. Die Programme werden zusammen mit der Datenbank abgelegt. Dadurch muss der entfernte Benutzer lediglich den Aufruf der Called Stored Procedure mit zugehörigen Argumentwerten übertragen.

Dreischichtige Client-Server-Architektur

Dreischichtige C/S-Architekturen (three tier architecture) führen zwei Schichten mit Servern ein. Eine Server-Schicht ist mit Anwendungsservern (application server) besiedelt. Die andere mit Datenservern (data server). Die Clients sind über ein eigenes Netz mit den Anwendungsservern verbunden. Sie senden mittels RDA (Remote Data Access), RPC (Remote Procedure Call), Message Queueing (Nachrichten-Warteschlangen, Nachrichten werden nach dem E-Mail-Prinzip asynchron, also ohne auf Antwort zu warten, übertragen) oder Transaktionsverfahren Aufträge an die Anwendungsserver. Diese wenden sich bei Bedarf an die Datenserver. Anwendungs- und Datenserver sind untereinander durch ein eigenes Netz verbunden.

Anwendungsbereiche: Obwohl aus technischer Sicht die Kommunikation zwischen Anwendungsprozessen im Vordergrund steht, führt diese in vielen Fällen zur Kommunikation zwischen Personen. Beispiele sind Electronic Mail, Videokonferenzen oder Rundfunkübertragungen im Internet. Die Kommunikation zwischen technischen Prozessen über Rechnernetze ist ebenfalls von großer und zunehmender Bedeutung.

Multi-Service-Netze versus Single-Service-Netze: Das klassische Telefonnetz bietet im Prinzip genau einen Dienst, die Sprachkommunikation. Es ist genau auf diese Anwendung zugeschnitten und optimiert. Durch ISDN wurde das Telefonnetz zu einem Netz erweitert, das mehrere Dienste integriert. Der Begriff Multi-Service-Netz soll ausdrücken, dass ein Netz verschiedenartige Dienste (mit Daten sowie Sprach- und Bildsignalen) in einer einheitlichen Netz-Infrastruktur integriert. Dadurch ergeben sich für Betreiber wie für Anwender Vorteile. Der Aufwand für mehrere spezialisierte Netze wird vermieden und die Flexibilität der Nutzung wird erhöht. Eine aktuelle Entwicklungstendenz strebt ein Multi-Service-Netz über ein einheitliches Paket- oder Zellen-Netz an. Dies kann längerfristig zu einer Konvergenz von Rechner- und Telekommunikationsnetzen führen.

1.3 Grundlagen: Topologien und Netzstrukturen

Version Feb. 2004

- Geografische Netzstrukturen
- Bus, Stern, Baum, Ring, vermascht, hierarchisch
- Netzverfügbarkeit

Netzarchitekturen

Eine Netzarchitektur ist die vereinfachte Beschreibung des Netzaufbaus. Sie beschreibt die abstrakten Eigenschaften (im Gegensatz zu benutzerbezogenen Eigenschaften).

Dabei sind verschiedene Aspekte zu unterscheiden:

- Der Aufbau des verwendeten **Protokollstapels** (protocol stack) ist ein wichtiges Architekturmerkmal. Oft ist es sinnvoll und notwendig (zumindest auf einigen Schichten) Protokolle aus verschiedenen Protokollstapeln anzubieten.
- Die **topologische Struktur** ist ein weiteres, wichtiges Merkmal. Die Unterscheidung Transportnetz und Zugangsnetz (access network, ermöglicht den Zugang des Teilnehmers zum Transportnetz) weist darauf hin, dass beide Teile unterschiedliche Eigenschaften aufweisen müssen. Im Transportnetz werden von innen (teilnehmerfern) nach außen der Backbone, das Kernnetz (beim Telefonnetz das Fernnetz) und das periphere Netz (Ortsnetz) unterschieden. Der Backbone besteht aus relativ wenigen, aber sehr breitbandigen Verbindungen. Das periphere Netz weist viele, jedoch schmalbandige Verbindungen auf.
- Die **logische Struktur** eines Netzes betrachtet die Gliederung in Subnetze und die Funktion der zugehörigen Knoten. Client-Server-Architekturen werden je nach Anwendung mit unterschiedlichen logischen Strukturen realisiert.

Rechnernetze, Datennetze und verteilte Systeme

Ein **Datennetz** (data network) überträgt digitale Signale zwischen Paaren oder Gruppen von Anwendern. Dabei können Kommunikationsbeziehungen wahlfrei zwischen beliebigen Kommunikationspartnern hergestellt werden. Das Netz stellt den Anwendern die OSI-Schichten 1-3 zur Verfügung, d. h. das vom Netz vorgegebene Schicht-3-Protokoll ist vom Anwender einzuhalten.

Das Netz transportiert also Pakete für den Anwender, es interessiert sich jedoch nicht für deren Bedeutung und Wirkungen. Deshalb werden von verschiedenen Autoren auch die Begriffe Bearer Service (Trägerdienst), Netzdienst, Transportdienst und Übermittlungsdienst verwendet. Die Dienste eines Datennetzes können als netznah und anwendungsfern charakterisiert werden.

Ein **Rechnernetz** (computer network, Rechnerverbund) verbindet autonome Rechner. Es stellt den Anwendern Dienste bereit, die die OSI-Schichten 1-7 umfassen. Ziel der Rechnernetze ist die gemeinsame Nutzung von Ressourcen (resource sharing), die sich an verschiedenen Stellen im Netz befinden.

Ein Rechnernetz transportiert also nicht (anonyme) Pakete, sondern PDUs, die in Bezug auf den jeweiligen Dienst eine bestimmte Bedeutung beinhalten. Die auf Rechnernetzen ausgeführten Dienste werden verschiedentlich als Teledienste, Telematikdienste oder Kommunikationsdienste bezeichnet. Diese Dienste werden von den Anwendungen (Anwendungsprogrammen) genutzt. Sie können deshalb als anwendungsnah bezeichnet werden.

Ein verteiltes System (distributed system) verbindet autonome Rechner so, dass für den Benutzer die Abstraktion eines einzelnen, homogenen Systems repräsentiert wird. Dies bedeutet, dass die Verteilung **transparent** ist. Das System verbirgt Ort und Art der Ausführung seiner Funktionen.

In einem Rechnernetz ist sich der Anwender der Existenz und Erreichbarkeit verschiedener Rechner bewusst. Das Netz wird in der Regel heterogen sein, also verschiedenartige Rechner (Hardware, Betriebssystem) umfassen. Ein verteiltes System wird ebenfalls heterogene Komponenten enthalten. Ein verteiltes Betriebssystem verbirgt die Heterogenität und realisiert die Transparenz.

Rechnernetze und verteilte Systeme sind in der Praxis nicht sauber abzugrenzen. Zweck der Rechnernetze ist die **Kommunikation** (Austausch von Daten bzw. Informationen). **Koordination** (mehrfacher Informationsaustausch mit dem Zweck, ein abgestimmtes Verhalten der Partner zu finden) ist eine Erweiterung der Kommunikation. **Kooperation** (laufender Informationsaustausch mit dem Zweck, gemeinsam zu Ergebnissen zu kommen, die besser oder umfassender sind, als dies jeder Partner allein erreichen könnte) ist der Zweck der verteilten Systeme. Kooperation (Verteilung) ist auf Kommunikation angewiesen, während Kommunikation keine Verteilung impliziert.

Verteilung und Transparenz

Aus der Sicht des Betreibers von Rechnernetzen werden diese als Verbund von Ressourcen gesehen, die für viele Anwender verfügbar gemacht werden sollen (resource sharing).

Ziele sind:

- **Funktionsverbund:** Verschiedene Knoten enthalten spezifische Funktionen, die über das Netz anderen Knoten zur Verfügung gestellt werden.
- **Datenverbund:** Daten, die auf einem Knoten gespeichert sind, können auch von anderen Knoten genutzt werden.
- **Lastverbund:** Die Last (Anzahl der Verarbeitungsaufträge pro Zeiteinheit) eines Knotens kann auf andere, weniger belastete Knoten verteilt werden. Dadurch wird der Durchsatz (Anzahl der pro Zeiteinheit erledigten Verarbeitungsaufträge) für den Benutzer erhöht.
- **Verfügbarkeitsverbund:** Der Ausfall einzelner Knoten kann ohne wesentliche Leistungsreduktion toleriert werden, wenn die benötigten Funktionen und Daten redundant im Netz verfügbar sind.

Der Verbund kann auch aus der Sicht der **Verteilung** (distributed system) betrachtet werden.
Bei der **Datenverteilung** ergeben sich spezifische Probleme. Daten können durch **Partitionierung** (der Datenbestand wird in disjunkte, nichtüberlappende Teile zerlegt) oder **Replikation** (Kopien eines Datenbestandes werden auf anderen Knoten abgelegt) verteilt werden. Eine Replikation ermöglicht (im Gegensatz zur Partitionierung) einen Verfügbarkeitsverbund. Die Replikation kann jedoch zu **Inkonsistenz** führen (widersprüchliche Daten auf verschiedenen Knoten), was durch geeignete Maßnahmen verhindert bzw. beseitigt werden muss.
Aus Sicht des Anwenders soll die Verteilung möglichst **transparent** (nicht wahrnehmbar) sein. Da dies nicht in allen Belangen machbar oder sinnvoll ist, ist der Begriff Transparenz näher zu umschreiben:

- **Ortstransparenz** (location transparency): Der Ort der Ausführung ist für den Anwender transparent.
- **Zugriffstransparenz** (access transparency): Der Anwender bemerkt nicht, ob ein lokaler oder ein entfernter Zugriff erfolgt.
- **Leistungstransparenz** (performance transparency): Die Unterschiede in den Zugriffs- und Ausführungszeiten zwischen lokalen und entfernten Operationen sind für den Benutzer unwesentlich.
- **Fehlertransparenz** (failure transparency) Fehler, die auf die Verteilung zurückzuführen sind, bleiben dem Benutzer verborgen.

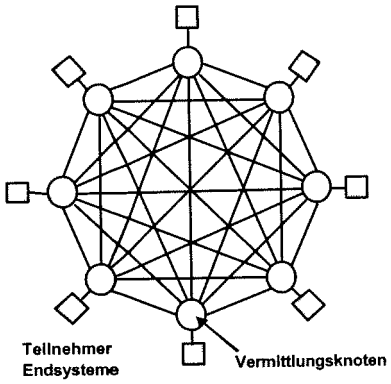


Bild: Vollvermaschtes Netz

Netzstrukturen haben die Aufgabe, die flächenhaft verteilten Quellen und Senken des Verkehrs in möglichst ökonomischer Form miteinander zu verbinden. Neben der rein topologischen Struktur spielen jedoch weitere Merkmale eine entscheidende Rolle, wie die Verteilung der Vermittlungsfunktionen oder der Grad an verteilter Intelligenz zur Verkehrslenkung.

Die **Topologie** eines Netzes beschreibt die geometrische Anordnung der Netzknoten und ihrer Verbindungen.
Unterschiedliche Topologien ergeben unterschiedliche Eigenschaften der damit aufgebauten Netze. Die Kenntnis der Vor- und Nachteile ist die Basis für die Auswahl einer im Einzelfall geeigneten Topologie. Die Betrachtung der geometrischen Anordnung allein ist dabei nicht ausreichend. Das Verhalten der Übertragungsstrecken muss nach Diffusionsnetz und Teilstreckennetz unterschieden werden.

Klassifikation von Topologien
Topologien lassen sich nach ihrer Dimension einteilen. Eine n-dimensionale Topologie lässt sich in einem n-dimensionalen Raum kreuzungsfrei aufzeichnen. **Eindimensionale Topologien** sind Bus, Ring und Stern. Sie werden primär bei lokalen Netzen verwendet. Ein Bus bildet ein Diffusionsnetz, während ein Ring (in der Regel) als Teilstreckennetz realisiert ist. In beiden Fällen ist jedoch die **Broadcast-Eigenschaft** vorhanden. Dies bedeutet, dass das von einer Station gesendete Signal unmittelbar (nur um die Laufzeit verzögert) von allen anderen Stationen empfangen wird.

Zweidimensionale Topologien sind Baum, Gitter und systolische Arrays. Die Baumtopologie ist für Rechnernetze ebenfalls wichtig, während andere zwei- (und auch mehr-) dimensionale Topologien für Parallelrechner genutzt werden.

Drei- und mehrdimensionale Topologien sind für Rechnernetze als vermaschte Topologien besonders wichtig. Bei der vollvermaschten Topologie ist jeder Netzknoten mit jedem anderen direkt verbunden. Bei einer Anzahl von n Netzknoten werden dafür n (n - 1)/2 Teilstrecken benötigt, was für große n nicht mehr praktikabel ist.

Netzstrukturen
Netzstrukturen haben die Aufgabe, die flächenhaft verteilten Quellen und Senken des Verkehrs in möglichst ökonomischer Form miteinander zu verbinden. Neben der rein topologischen Struktur spielen jedoch weitere Merkmale eine entscheidende Rolle, wie die Verteilung der Vermittlungsfunktionen, der Grad an verteilter Intelligenz zur Verkehrslenkung u.a.m. Im folgenden werden die wesentlichsten strukturellen Merkmale von Kommunikationsnetzen behandelt.

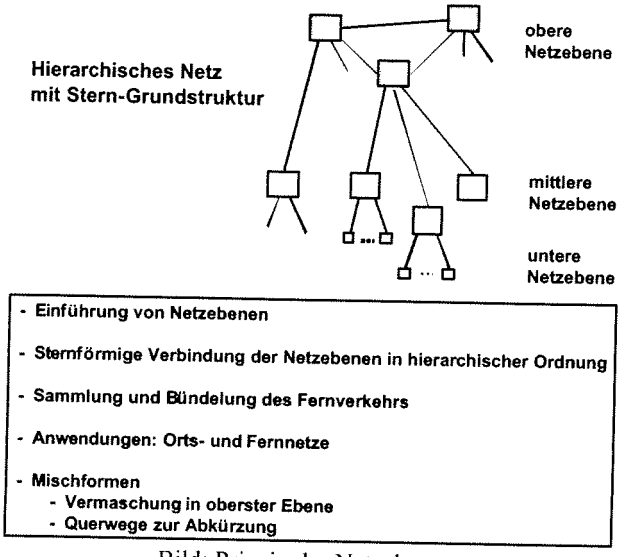


Bild: Prinzip der Netzebenen

Hierarchisches Netz mit Stern-Grundstruktur

- Einführung von Netzebenen,
- Sternförmige Verbindung der Netzebenen in hierarchischer Ordnung,
- Sammlung und Bündelung des Fernverkehrs,
- Anwendungen:
  - Orts- und Fernnetze,
  - Mischformen,
    - Vermaschung in der obersten Ebene,
    - Querwege zur Wegabkürzung.

Hierarchisches Netz mit Maschen-Grundstruktur

- unvollständige Vermaschung in oberer Netzebene
- verschiedenartige Strukturen im Anschlussbereich (Stern, Ring, Bus, ...).

Anwendung in derzeitigen öffentlichen Paketvermittlungsnetzen

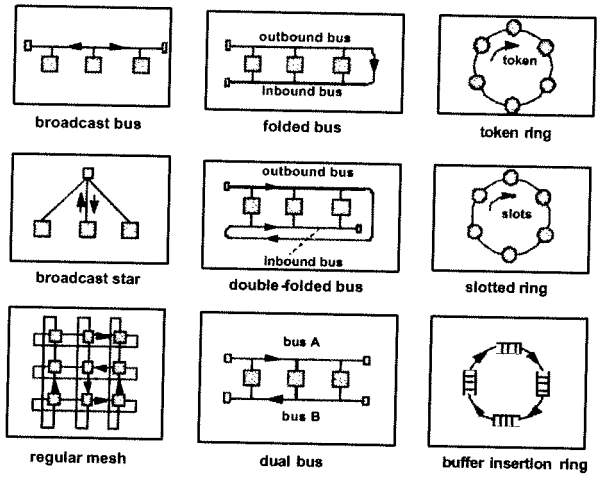


Bild: Netztopologien

Bei einem **Broacastnetz** (shared medium) wird das Signal eines Senders von allen angeschlossenen Empfängern unmittelbar (jedoch um die Signallaufzeit verzögert) empfangen. Jeder Empfänger muss selbst feststellen, ob er das Signal aufnimmt oder nicht.

Bei einem **Teilstreckennetz** läuft das Signal des Senders über (genau) eine Teilstrecke, an deren Ende ein Empfänger das Signal aufnimmt und (falls erforderlich) auf einer anderen Teilstrecke wieder aussendet.

Beispiele dazu sind:
Bussysteme: gefalteter Bus, doppelt-falteter Bus, Dualbus.
Ringnetze: Token Ring, Slotted Ring, Buffer-Insertion Ring.
Vermaschte Netze: Reguläre und irreguläre Vermaschung.

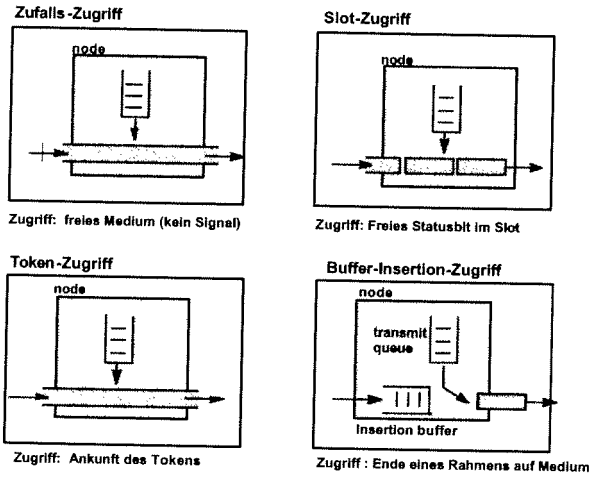


Bild: Zugriff auf gemeinsames Medium

Wichtige Zugriffsverfahren sind:

- Zufälliger Zugriff (Aloha, Slotted Aloha, Ethernet),
- Token Zugriff (Token Ring, Token Bus, FDDI),
- Slotted Zugriff (ATM-Ring),
- Insertion-Buffer Zugriff (Insertion Ring, IEEE 802.17).

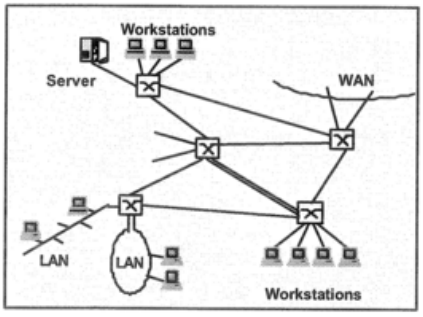


Bild: Allgemeines Maschennetz

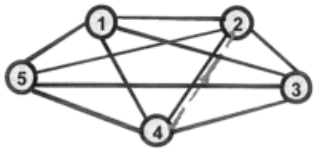


Bild: Maschennetz

- **Reines Maschennetz aus N Knoten**
- **Anzahl der N•(N - 1)/2 Verbindungswege**
- **Kürzestmögliche Verbindungen**
- **Unwirtschaftlich für großes N, wegen**
  - Anzahl der Verbindungsleitungen
  - schlechter Ausnutzung der Verbindungsleitungen

Anwendung
- in höheren Netzebenen

Bild: Maschennetz mit seinen Eigenschaften.

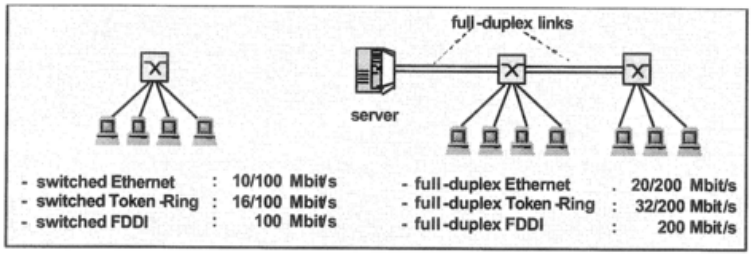


Bild: Sternnetz

- **Einführung eines Zentralknotens als Durchgangsknoten**
  d.h. Einführung einer höheren Netzebene
- **N Verbindungsleitungen**
- **2 Verbindungsleitungen pro Verbindung erforderlich**
- **unwirtschaftlich für großes N**

Anwendung
- in lokalen Netzen
- in Zugangsnetzen
- in zellulären Mobilfunknetzen
  (Funkkanalanbindung von Mobilstationen an Basisstation)

Bild: Sternnetz mit seinen Eigenschaften.

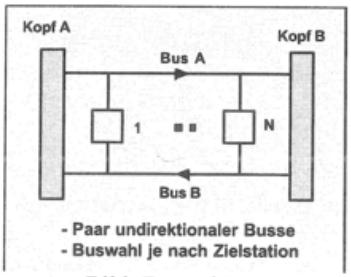


Bild: Doppel-Bus

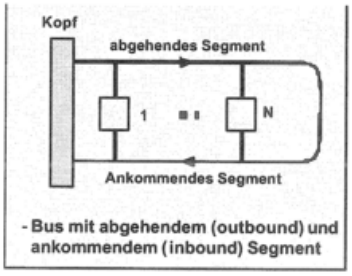


Bild: Gefalteter Bus

- **Zentraler Bus als Breitband-Übertragungssystem mit passiver oder aktiven Ankopplung**
- **Betrieb mit Vielfachzugriffsverfahren**
- **Anwendungen in lokalen Netzen mit Paketvermittlung**

Bild: Busnetz mit seinen Eigenschaften.

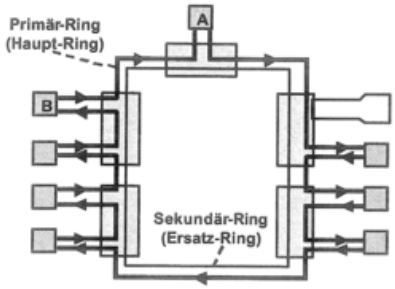


Bild: Ringnetz

- **Zentraler Ring als Breitband-Übertragungssystem mit aktiven Knoten**
- **Betrieb mit zentralem Takt und synchronem TDM oder dezentral im Paketmode (Token-Verfahren)**
- **Strukturelle/betriebliche Vorkehrungen bei Unterbrechung des Ringes möglich, um Teilbetrieb aufrechtzuerhalten**
- **Doppelringstruktur mit zwei gegenläufigen unidirektionalen Ringen zur Ausfallsicherung**
  (Selbstheilungsprinzip bei Unterbrechungen)
- **Anwendungen in lokalen Netzen mit Durchschaltevermittlung oder Paketvermittlung**

Bild: Ringnetz mit seinen Eigenschaften

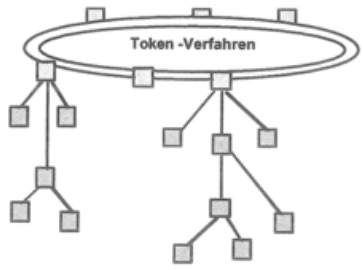
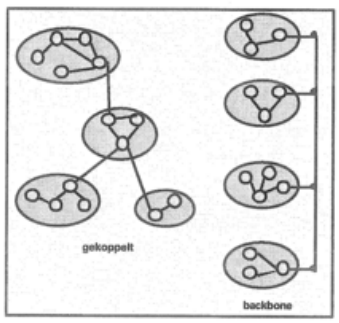


Bild: Ringnetz mit Baumverkabelung



Größere Netze müssen gekoppelt werden.

Bild: Gekoppelte Netze

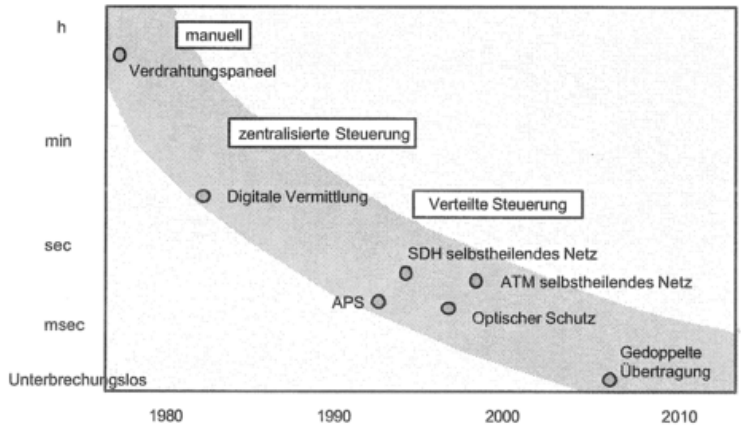
Bewertung von Topologien

Vor- und Nachteile verschiedener Topologien können anhand der folgenden Kriterien untersucht werden:

- **Verkabelungsaufwand:** Welche gesamte Kabellänge wird benötigt, wenn die geografische Anordnung der Netzknoten vorgegeben ist? Der Aufwand für das Einfügen eines zusätzlichen Netzknotens ist ein weiteres Kriterium.
- **Gesamtbandbreite:** Wenn die Bandbreite B aller Teilstrecken als gleich angenommen wird, kann die Gesamtbandbreite bei n Teilstrecken im günstigsten Fall n * B betragen.
- Effizienz: Darunter wird hier die Zahl der zu durchlaufenden Zwischenknoten verstanden. Der Aufwand für das Routing steigt mit der Anzahl der Zwischenknoten.
- **Ausfalltoleranz** (Robustheit): Beschreibt die Auswirkungen des Ausfalls einer Teilstrecke oder eines Netzknotens.

Günstige Bewertungen ergeben sich in den Fällen Bus (bei Verkabelungsaufwand und Effizienz) und voll vermaschte Topologie (bei Gesamtbandbreite und Effizienz und Ausfalltoleranz). Ungünstige Fälle sind der Bus (bei Gesamtbandbreite und Ausfalltoleranz), der Stern (insbesondere beim Ausfall der Station im Sternpunkt) und die vermaschte Topologie (beim Verkabelungsaufwand). Die Beurteilung wird komplizierter, wenn mehrere Kriterien zusammen betrachtet werden. Beispielsweise liefert die Baumtopologie einen guten Kompromiss zwischen Verkabelungsaufwand, Gesamtbandbreite und Effizienz insbesondere dann, wenn aus der Anwendung ein hierarchisch orientiertes Kommunikationsverhalten zu erwarten ist.

Schutzschaltungen



SDH : Synchronous Digital Hierarchy
ATM : Asynchronous Transfer Mode
APS : Automatic Protection Switching

Bild: Entwicklung von Netzschutzmechanismen

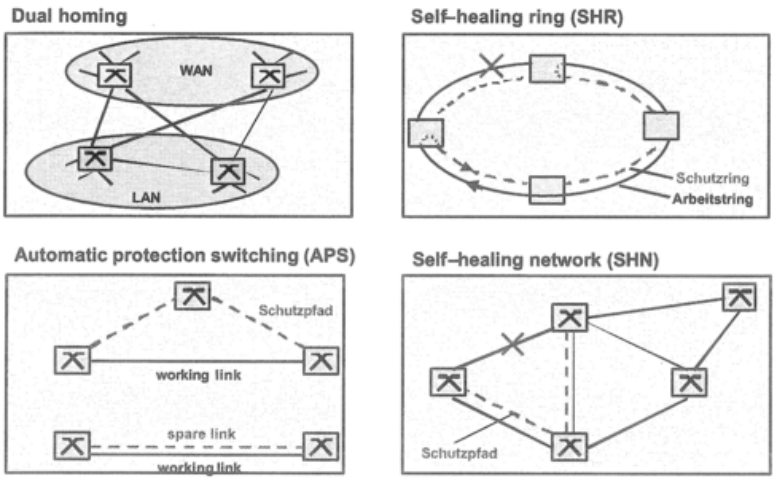
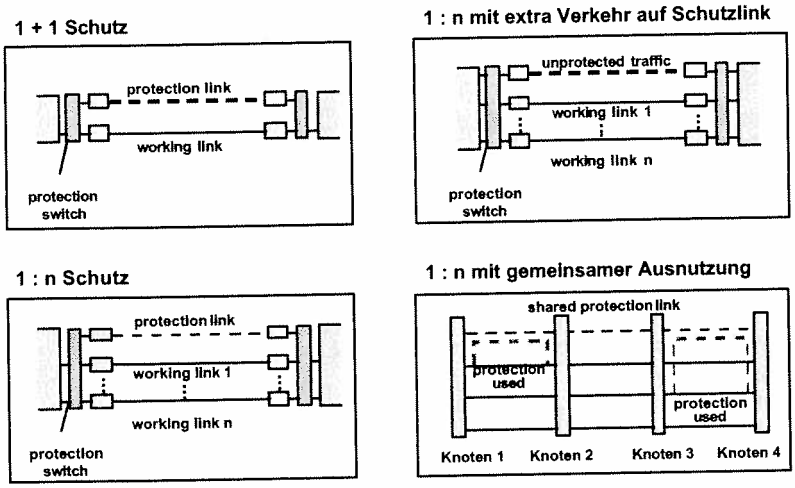


Bild: Netzschutzmechanismen

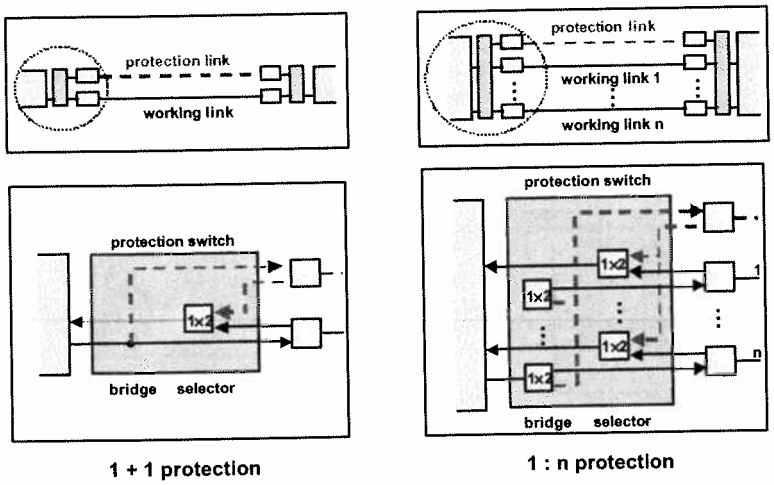
Es gibt vier Typen von Schutzschaltungen.

- Doppel-Netzanschluss (Dual-Homing),
- Leitungsschutz (Automatic Protection Switching),
- Selbstheilender Ring (Self-healing Ring),
- Selbstheilendes Netz (Self-healing Network).



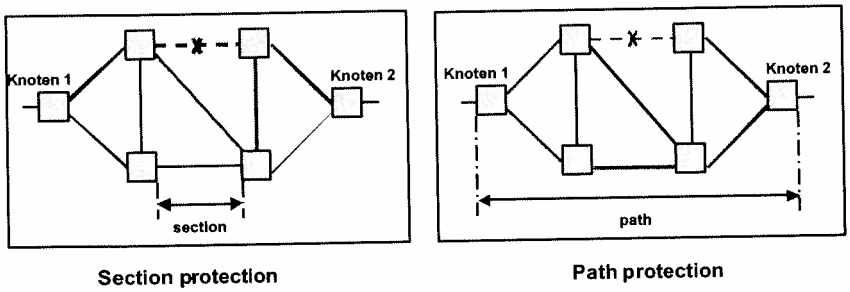
Beim Leitungsschutz werden folgende Konfigurationen betrachtet.

Bild: Automatic Protection Switching (APS)



Bei der Realisierung eines (1+1)-Schutzes wird das Übertragungssignal auf beide Leitungen ausgesendet und beim Empfänger selektiert. Beim (1+n)-Schutz sind Schalter an beiden Enden notwendig.

Bild: Realisierung von Automatic Protection Switching (APS)

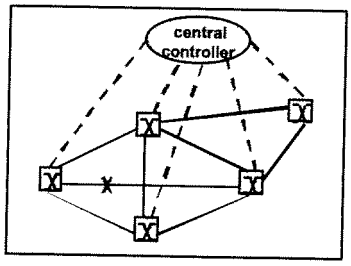


Bei Ende-zu-Ende Pfaden durch das Netz unterscheidet man zwei Arten von Schutzschaltungen: Abschnitts- und Pfadschutz. Im ersten Fall wird eine Ersatzschaltung über die ausgefallene Strecke gesucht. In zweiten Fall wird ein neuer Pfad gesucht. Die Vor- und Nachteile sind angegeben.

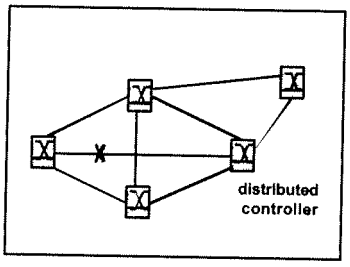
Restaurationsgeschwindigkeit	+
Algorithmische Komplexität	+
Netzauslastung	–

Restaurationsgeschwindigkeit	–
Algorithmische Komplexität	–
Netzauslastung	+

Bild: Abschnitt- und Pfadschutz



Zentrale Steuerung



Verteilte Steuerung

Zur Bestimmung von neuen Wegen durch das Netz kann eine zentrale oder dezentrale Steuerung eingesetzt werden. Vor- und Nachteile sind angegeben.

	Zentrale Steuerung	Verteilte Steuerung
Netzkomplexität	+	-
Standardisierungsbedarf	+	-
Lokaler Speicherplatz	+	-
Restaurationszeit	-	+
Netzverfügbarkeit	-	+
Steuerungsmehraufwand	-	+

Bild: Zentrale versus Dezentrale Steuerung

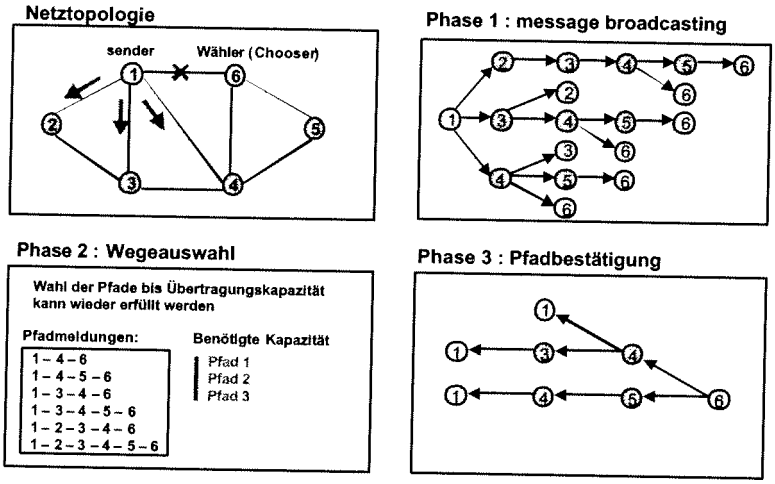


Bild: Selbstheilende Netze: Restaurationsprinzip

In Algorithmus für die dezentrale Steuerung geht wie folgt.

Phase 0:
Der Ausfall einer Leitung wird von Knoten 1 entdeckt (z.B. keine optische Pulse). Koten 1 bezeichnet man als Sender, Knoten 6 am anderen Ende als Wähler (chooser). Knoten 1 startet einen Broadcast über alle intakte Leitungen.

Phase 1:
Alle Knoten, die diese Meldung vorher noch nicht erhalten haben, senden sie weiter auf allen abgehenden Leitungen (nur nicht auf der Leitung, wo die Meldung angekommen war). Dabei wird die vorhandene Kapazität in der Knoten in der Meldung angegeben Im Algorithmus entsteht so einen Baum.

Phase 2:
Knoten 6 sammelt alle Wegmöglichkeiten und sucht so viele Pfade aus wie der Ersatzkapazität entspricht. Im Beispiel sind drei Pfade notwendig.

Phase 3:
Knoten 6 schickt unter Angabe der benötigten Kapazitäten auf jedem der ausgewählten Pfade eine Meldung zurück. Alle Zwischenknoten veranlassen die Durchschaltung der gewünschten Kapazität.

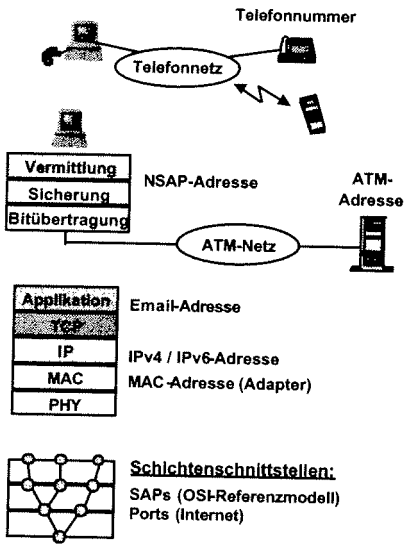
1.4 Grundlagen: Nummerierung und Adressierung

Version: Feb. 2004

Inhalt

- Nummerierung im Telefonnetz und ISDN (Integrated Services Digital Network)
- Adressierung zwischen Protokollschichten mit SAPs (Service Access Point) oder Ports
- Adressierung in OSI-Systemen
- Adressierung in ATM (Asynchronous Transfer Mode)
- Adressierung in IEEE LANs
- Adressierung im Internet (IPv4, IPv6)
- Adressierung im Internet (Email-Adresse, Adressauflösung, DNS, URL)

POTS	Telefonnetz
ISDN	Integrated Services Digital Network
NSAP	Network Service Access Point
ATM	Asynchronous Transfer Mode
Email	Electronic Mail
IPv4	Internet Protocol Version 4
IPv6	Internet Protocol Version 6
IEEE MAC	IEEE Medium Access Control
Identifier	interne Netzadressierung
SAP	Service Access Point (Protokoll-Pfade)



Der Aufbau von Kommunikationsbeziehungen erfolgt über Adressen, die der Lokalisierung von Endeinrichtungen, Teilnehmern oder Netzinstanzen dienen. Nummerierung und Adressierung hängen eng mit der Netzstruktur zusammen. Im folgenden wird in die Definition und Prinzipien von Nummerierung und Adressierung eingeführt.

1. Namensgebung,
2. Nummerierung,
3. Adressierung,
4. Labels.

- **1. Namensgebung**

Ein Name ist eine ortsunabhängige Kennung für Instanzen oder Einrichtungen eines Nachrichtennetzes. Der Bereich, innerhalb dessen Namen in eindeutiger Weise festgelegt sind, heißt Namensraum (name space). Die Gesamtheit der vergebenen Namen kann in einem Namenserver (name server) gespeichert sein, der der Netzverwaltung dient.

Namen sind i.a. aus alphanumerischen Zeichen aufgebaut. Verwandt mit dem Namensbegriff ist der Begriff „Kennung" (identifier). Je nach Anwendung werden unterschieden

- Teilnehmerkennung (subscriber identity),
- Gerätekennung (equipment identity).

2. Nummerierung

Die Nummerierung ist die wohl bekannteste Art, Teilnehmerendeinrichtungen oder Netze zu kennzeichnen. Die Nummerierung (numbering) verwendet dazu in der Regel Ziffernfolgen, gegebenenfalls ergänzt durch wenige Sonderzeichen (wie z.B. bei Tastwahl-Telefonen). Die Festlegung der Nummerierung erfolgt in einem Nummerierungsplan (numbering plan). Es werden verschiedene Arten von Nummerierungsprinzipien unterschieden:

Netzgebundene/Freie Nummerierung

- Bei der netzgebundenen Nummerierung richtet sich die Nummernvergabe nach der Netzstruktur; bei freier Nummerierung kann die Vergabe von Nummern ohne Rücksicht auf Netzstruktur oder Teilnehmerlage erfolgen.
- Hierarchische/Nichthierarchische Nummerierung. Bei der hierarchischen Nummerierung lehnt sich die Nummernvergabe an die Netzhierarchie.
- Nummerierungsbereich. Der Nummerierungsbereich (numbering area) ist der Bereich eines Nachrichtennetzes, innerhalb dessen die Nummerierung eindeutig ist.
- Kennzahl. Unter einer Kennzahl (Code) wird die Kennzeichnung eines Netzknotens, eines Nummerierungsbereiches, eines nationalen Netzes oder eines Dienstes verstanden.

Die Rufnummer (number) ist die Ziffernfolge zur Kennzeichnung eines Teilnehmeranschlusses.

Teilnehmerrufnummer	subscriber number	innerhalb eines Nummerierungsbereichs
Nationale Rufnummer	national number	innerhalb eines Landesnetzes
Internationale Rufnummer	international number	innerhalb des weltweiten Netzes
Durchwahlrufnummer	direct dialling-in number	Teilnehmerrufnummer einer Nebenstelle

3. Adressierung
Unter Adressierung (addressing) wird allgemein die Kennzeichnung von Instanzen innerhalb eines Kommunikationsnetzes mittels einer Adresse verstanden. Die Adresse besteht im allgemeinen aus alphanumerischen Zeichen und folgt einem allgemeingültigen Adressierungsschema innerhalb eines Adressierungsbereichs.

Hierarchische/Flache Adressierung
Die hierarchische Adressierung folgt nach einem baumförmig strukturierten Adressraum, der sich an der Netzstruktur orientieren kann. Bei flacher Adressierung erfolgt eine (weltweit) eindeutige Adressierung nach einem einstufigen Schema.

Spezielle Adressierungen
Die Adressierung kann sich auf unterschiedliche Kriterien beziehen wie
- Anschlussbezogene Adressierung(subscriber line addressing)
- Benutzerbezogene Adressierung (user addressing)
- Endgerätebezogene Adressierung(equipment addressing)
- Symbolische Adressierung (symbolic addressing)
- Unteradressierung (subaddressing)

Adressen sind (numerische) Werte, die einen Knoten in einem Netz eindeutig bestimmen. Je nach OSI-Schicht existieren verschiedene Typen von Adressen. Namen sind (logische) Werte, die an Stelle einer numerischen Adresse verwendet werden können. Adressen entsprechen Telefonnummern, Namen entsprechen dem Eigen- oder Firmennamen des Inhabers der Telefonnummer. Die Abbildung von Namen auf Adressen wird durch Namensdienste bzw. Verzeichnisdienste geleistet, die somit einem Telefonbuch entsprechen.

Adressen lassen sich abhängig von ihrem Typ einer Schicht des OSI-Modells zuordnen. OSI selbst ordnet den Schichten 3-6 Adressen zu, die als SAP (Service Access Point) in Verbindung mit der jeweiligen Schicht benannt sind:
- PSAP: Presentation SAP auf Schicht 6.
- SSAP: Session SAP auf Schicht 5.
- TSAP: Transport SAP auf Schicht 4.
- NSAP: Network-SAP auf Schicht 3.

NSAP ist die netzweit eindeutige Adresse eines Knotens; TSAP, SSAP und PSAP sind Selektoren. Sie geben an, welcher Anwendungsprozess gerade die genannte Schicht nutzt. Die gesamte Adresse eines Anwendungsprozesses ergibt sich also aus der Aneinanderreihung der einzelnen Adressen zu PSAP + SSAP + TSAP + NSAP.

Meistens stellt eine Adresse eine Individualadresse dar. Sie identifiziert also genau einen Teilnehmer. Weiter gibt es Gruppenadressen (für Multicast) und Broadcast-Adressen (für die Adressierung aller Teilnehmer in einem Netz). Ein Adressraum ist die Gesamtheit aller Adressen in einem Netz.

Adressen können lokal sein, sie sind dann nur innerhalb eines Teilnetzes (Subnetzes) eindeutig. Globale Adressen sind in einem gesamten Netz eindeutig. Adressräume können flach oder hierarchisch strukturiert sein. Bei flachen Adressräumen besteht kein Zusammenhang zwischen der Adresse und der geografischen Lage (Position) einer Station. Hierarchische Adressen bestehen aus einzelnen Teilen, die einem hierarchischen Aufbau eines Netzes entsprechen. Dann haben benachbarte Stationen weitgehend benachbarte Adressen. Von den nachfolgend behandelten Adressen sind MAC-Adressen flach, aber global (zumindest für U/L = 0); IP-, OSI-, ATM- und X. 121 -Adressen sind hierarchisch und global.

4. Labels
In dem oben behandelten Adressierungsschema bezeichnen die Adressen ein Endsystem (global oder lokal) eindeutig. Bei verbindungsloser Kommunikation muss jedes Paket (jede N-PDU) mit einer Zieladresse versehen sein. In verbindungsorientierten Netzen ist diese Forderung nach abgeschlossenem Verbindungsaufbau nicht mehr notwendig. Stattdessen können sich die Zwischensysteme (Router) darauf beschränken, für jede bestehende Verbindung logische Kanalnummern zu verwenden. Diese Nummern werden als Labels bezeichnet, sie sind nur lokal für jeweils eine Teilstrecke gültig (global gültige Labels wären nicht handhabbar und zu lang). Dabei muss das Zwischensystem lediglich die logische Nummer des Eingangskanals auf die des Ausgangskanals abbilden. Eine Verbindung zwischen zwei Endsystemen ist demnach eine Folge von Teilstrecken, von denen jede mit einem Label versehen ist. Eine solche Verbindung wird als virtuelle oder logische Verbindung

bezeichnet. Da lokale Labels kürzer sind als globale Adressen, wird die NPDU durch die Verwendung von Labels kürzer. Labels werden in unterschiedlichen Netzen verwendet.

Einige Labels und ihre Anwendung

Bezeichnung	Verwendung
LCN: Logical Channel Number	X.25
DLCI: Data Link Connection Identifier	Frame Relay
VPI/VCI: Virtual Channel Identifier/Virtual Path Identifier	ATM

Nummerierung im Telefonnetz und ISDN (Integrated Services Digital Network)

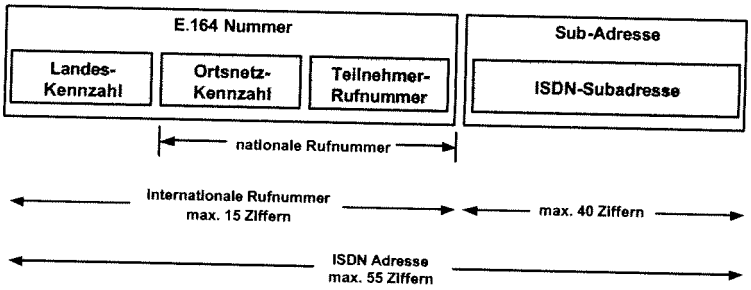


Bild: ISDN Adressstruktur nach E.164

Spezielle Formen der Kennzahlen sind:

- Landeskennzahl (country code)
  z.B. Österreich: 43, Frankreich: 33
- Ortsnetzkennzahl (area code)
  z.B. Wien: 1, Graz: 316,
  Bad Gleichenberg: 3159

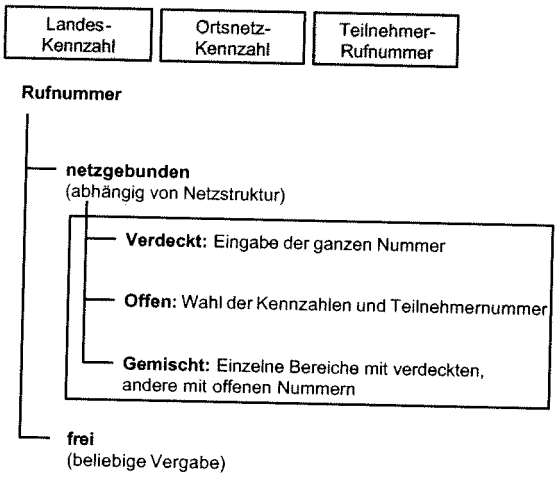


Bild: Rufnummernsysteme in der Telefonie

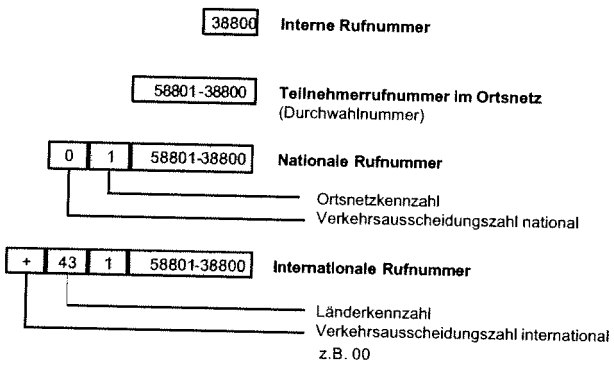


Bild: Telefonnetz - Offene Nummerierung

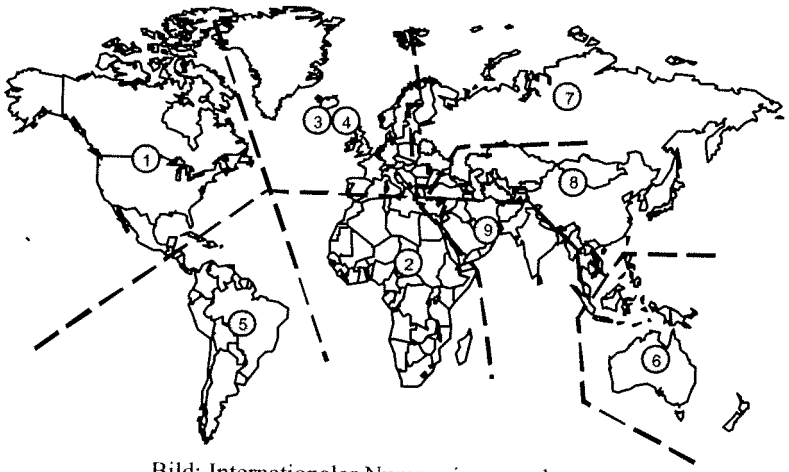


Bild: Internationaler Nummerierungsplan

Der erste Ziffer der Vorwahlnummer bestimmt die kontinentalen Bereiche des Nummerierungsplans nach E.164.

1: Nordamerika
2: Afrika
3: Europa
4: Europa
5: Süd-Amerika
6: Ozeanien
7: Russland
8: Asien
9: Mittelost

Bild: Nordamerikanischer Nummerierungsplan (Vorwahl 001)

Bei freier Nummerierung existiert für die Vorwahlnummer kein Zusammenhang bezüglich der geographischen Lage des Teilnehmers.

Anwendung:
Nord-Amerika.

Afrika 002

Ägypten	20
Algerien	213
Angola	244
Äthiopien	251
Benin	229
Botsuana	267
Burundi	257
Ivorküste	225
Dschibuti	253
Eritrea	291
Gabun	241
Gambia	220
Ghana	233
Guinea	224
Kamerun	237
Kap Verde	238
Kenia	254
Kongo	242
Liberia	231
Libyen	218
Malawi	265
Mauritius	230
Mosambik	258
Namibia	264
Niger	227
Nigeria	234
Ruanda	250
Sambia	260
Senegal	221
Simbabwe	263
Somalia	252
Sudan	249
Südafrika	27
Swasiland	268
Tunesien	216
Tschad	235
Uganda	256

Europa 003 / 004

Albanien	355
Andora	376
Armenien	374
Belarus	375
Belgien	32
Bosnien	387
Bulgarien	359
Dänemark	45
Deutschland	49
Finnland	358
Frankreich	33
Gibraltar	350
Griechenland	30
UK	44
Irland	353
Island	354
Italien	39
Jugoslawien	381
Kroatien	365
Lettland	371
Litauen	370
Luxemburg	352
Malta	356
Moldau	373
Monaco	377
Niederlande	33
Norwegen	47
Österreich	43
Polen	48
Portugal	351
Rumänien	40
Schweden	46
Schweiz	41
Slowakei	421
Slowenien	386
Spanien	34
Tschechien	429
Ukraine	380
Ungarn	36
Vatikan	39
Zypern	357

Süd-Amerika 005

Argentinien	54
Brasilien	55
Bolivien	591
Chile	56
Costa Rica	506
Ecuador	593
El Salvador	503
Guayana	592
Haiti	509
Honduras	504
Kuba	53
Mexiko	52
Nicaragua	5505
Panama	507
Peru	51
Surinam	597
Uruguay	598
Venezuela	58

Ozeanien 006

Australien	61
Indonesien	62
Malaysia	60
Neuseeland	64
Philippinen	63
Samoa	685
Thailand	66

Russland 007

Russland	7
Kasachstan	7
Tadschikistan	7

Fern-Asien 008

China	86
Hongkong	852
Japan	81
Korea	82
Laos	856
Taiwan	886
Vietnam	84

Nahost-Asien 009

Aserbaidschan	994
Bahrain	973
Georgien	995
Indien	91
Irak	964
Iran	98
Israel	972
Jemen	967
Jordanien	962
Libanon	961
Mongolei	976
Nepal	977
Oman	968
Pakistan	92
Saudi Arabien	966
Sri Lanka	94
Syrien	963
Türkei	90
Turkmenistan	993

Bild: Internationale Vorwahlnummern

Satellitennetze

881 0 / 1	ICO
881 2 / 3	Ellipso
881 4 / 5	
881 6 / 7	Iridium
881 8 / 9	Globalstar

Globale Netzbetreiber

882 10	BT
882 11	ST Telecommunications PTE
882 12	WorldCom
882 13	Telespazio
882 14	Verizon
882 15	Telstra
882 16	Thuraya
882 17	AT&T
882 18	Teledesic
882 19	Telecom Italia
882 20	ACeS
882 21	Ameritech
882 22	Cable & Wireless
882 23	Sita-Equant
882 24	Telia
882 25	Constellation Comms
882 26	SBC Communications Inc.
882 27	Williams Communications Inc.
882 28	Deutsche Telekom
882 29	Q-Tel (NZ) Ltd
882 30	Singapore Telecom
882 31	Telekom Malaysia

Bild: Vorwahlnummern von Satellitennetzen (881) und globalen Netzbetreiber (882)

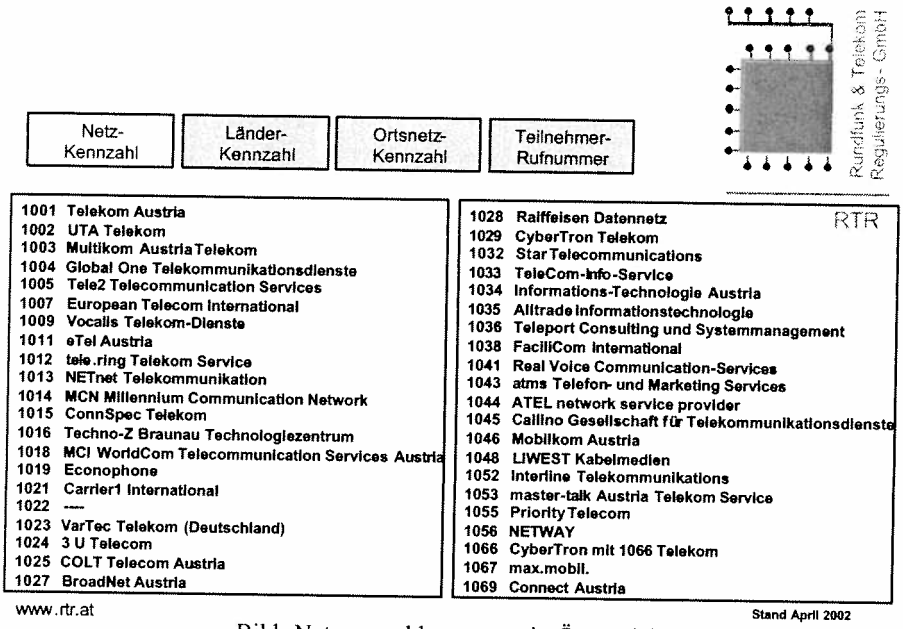


Bild: Netzvorwahlnummern in Österreich

Über **Netzvorwahlnummer** kann ein Netzbetreiber oder Netzanbieter nach eigener Wahl erreicht werden. Gehört der Netzanschluss dem Netzbetreiber selbst, ist die Netzkennzahl nicht notwendig.

Im Ortsvermittlungsknoten des Teilnehmers findet die Vermittlung der Verbindung zum gewählten Netz statt.

Bedingungen und Nummern werden in Österreich von der RTR (Rundfunk & Telekom Regulierungsbehörde) vorgegeben.

In den Ortvermittlungsknoten geschieht im allgemeinen auch die Trennung zwischen der Durchschaltevermittlung (Telefonnetz) und der Paketvermittlung (Internet, X.25, FR, ATM)

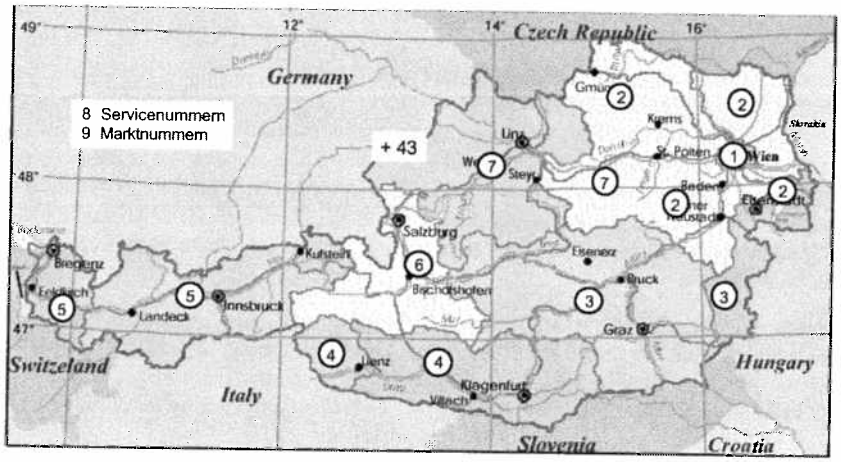


Bild: Festnetznummernplan in Österreich

Bei der **offenen Nummerierung** (open numbering) werden Kennzahlen und Verkehrsausscheidungszahlen (prefix) im Verkehr zwischen unterschiedlichen Nummerierungsbereichen angewandt. D.h. bei Ortsrufen müssen Landes- und Ortszahlen nicht mitgewählt werden bzw. bei einem Landesruf muss die Landeszahl nicht mitgewählt werden.

Bei der **verdeckten Nummerierung** (closed numbering) ist die Kennzahl fester Bestandteil der Rufnummer. D.h. auch bei Ortsrufen müssen Landes- und Ortszahlen mitgewählt werden.

Bei der **gemischten Nummerierung** (mixed numbering) ist der festen Mitwahl von Landes- und Ortszahlen von der geographischen Lage abhängig.

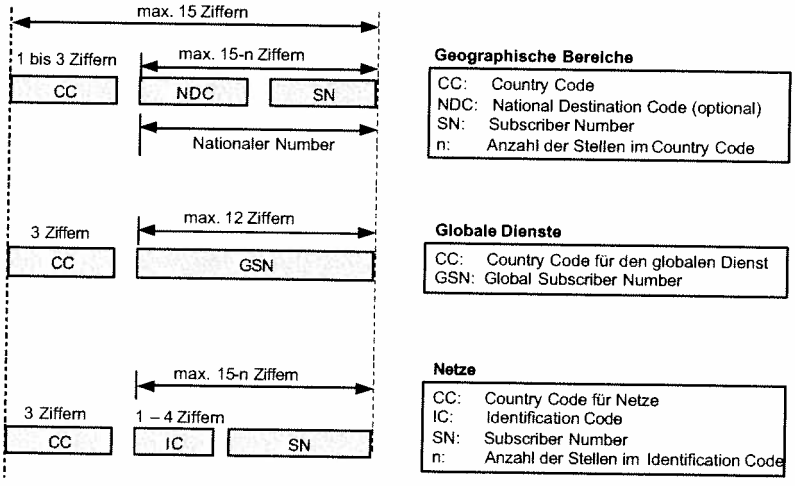


Bild: E.164 Nummernsystem

Das E.164 Nummernsystem legt für die maximal 15 Ziffern drei Nummerierungsmöglichkeiten fest:
- nach geographischen Bereichen,
- nach globalen Diensten,
- nach Netzen.

Je nach Verwendung ist die Einteilung der Ziffern verschieden.

GSM-Netze

650	GSM-Netz der tele.ring
664	GSM-Netz der Mobilkom Austria
676	GSM-Netz der T-Mobile Austria
699	GSM-Netz der Firma Connect Austria

Weitere Mobilfunknetze

660	Hutchison 3G Austria
663	Mobilfunknetz D der Mobilkom Austria
666	Pagerdienst der Mobilkom Austria
669	Pagerdienst der Mobilkom Austria
678	TETRA-Netz der TetraCall Bündelfunk
680	3G Mobile Telecommunications

Bild: Mobilnetzvorwahlnummern in Österreich

Europa 2xx

Albanien	276
Andora	213
Armenien	xxx
Belarus	257
Belgien	206
Bosnien	218
Bulgarien	284
Dänemark	233
Deutschland	262
Estland	248
Finnland	244
Frankreich	208
Georgien	282
Gibraltar	266
Griechenland	202
Irland	272
Island	274
Italien	222
Jugoslawien	220
Kroatien	219
Lettland	247
Litauen	246
Luxemburg	270
Malta	278
Moldau	259
Monaco	212
Niederlande	204
Norwegen	242
Österreich	232
Polen	260
Portugal	268
Rumänien	226
Russland	250
Schweden	240
Schweiz	228
Slowakei	231
Slowenien	293
Spanien	214
Türkei	286
Tschechien	230
UK	234 + 235
Ukraine	255
Ungarn	216
Zypern	280

Nordamerika 3xx

Haiti	372
Kanada	302
Kuba	368
Mexiko	334
USA	310-316

Asien 4xx

Afghanistan	412
Bangladesch	470
Bahrain	426
China	460
Hongkong	454
Indien	404
Irak	418
Iran	432
Israel	425
Japan	440-441
Jemen	421
Jordanien	416
Laos	457
Libanon	415
Mongolei	428
Nepal	429
Nord-Korea	467
Oman	422
Pakistan	410
Saudi Arabien	420
Sri Lanka	413
Süd-Korea	450
Syrien	417
Taiwan	466
Vietnam	452

Ozeanien 5xx

Australien	505
Indonesien	510
Malaysia	502
Neuseeland	530
Philippinen	515
Singapur	525
Thailand	520

Afrika 6xx

Ägypten	602
Algerien	603
Angola	631
Äthiopien	636
Benin	616
Botsuana	652
Burundi	642
Ivorküste	612
Dschibuti	638
Eritrea	636
Gabun	628
Gambia	607
Ghana	620
Guinea	611
Kamerun	624
Kap Verde	625
Kenia	639
Kongo	629
Liberia	618
Libyen	606
Malawi	650
Mauritius	617
Mosambik	643
Namibia	649
Niger	614
Nigeria	621
Ruanda	635
Sambia	645
Senegal	608
Simbabwe	648
Somalia	637
Sudan	634
Südafrika	655
Swasiland	653
Tansania	640
Tunesien	605
Tschad	622
Uganda	641

Süd-Amerika 7xx

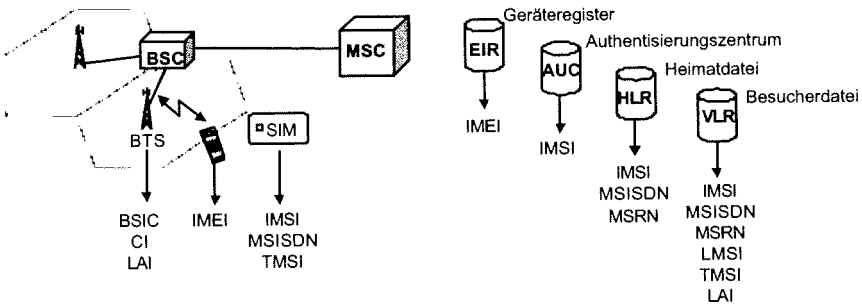
Argentinien	722
Brasilien	724
Bolivien	736
Chile	730
Costa Rica	712
Ecuador	740
El Salvador	706
Guayana	738
Honduras	708
Kolumbien	732
Nicaragua	710
Panama	714
Pararguay	744
Peru	716
Surinam	746
Uruguay	748
Venezuela	734

Bild: Mobilnetz-Ländervorwahl (E.212)

Die Mobilnetzvorwahlnummern werden nur zwischen Netzbetreibern verwendet. Sie haben für die Teilnehmer keine Bedeutung.

Als Vertreter für die Nummerierung und Adressierung in Mobilnetzen wird GSM (Global System for Mobile Communications) betrachtet. GSM besteht aus einem Zugangsnetz von Funkzellen mit Basisstationen (BTS, Base Station Transceiver), die über Controller (BSC, Base Station Controller) mit den Vermittlungsknoten (MSC, Mobile Switching Node) verbunden sind. Zur Realisation stehen vier Datenbanksysteme mit den Benutzerdaten zur Verfügung. Für die Adressierung hat jeder Mobilteilnehmer eine Telefonnummer sowie eine eindeutige, nicht öffentlichbekannte IMSI (International Mobile Subscriber Identity) auf der SIM-Karte. Die IMSI wird nur über das Netz geschickt, wenn beim Einbuchen ins Netz auf der SIM-Karte des Teilnehmers keine temporäre Nummer (TMSI, Temporary Mobile Subscriber Number) vorhanden ist. Diese Nummern sind zum Teil auch in den Heimat- und Besucherdateien zu finden.

In den Heimat- und Besucherdateien ist eine weitere wichtige Nummer zu finden. Die Aufenthaltsrufnummer (mobile station roaming number, MSRN) ist die Nummer, die einem Mobilteilnehmer vorübergehend zugeordnet wird und angibt, in welchem Netzteil sich dieser Teilnehmer momentan aufhält. Sie besteht aus Landeskennzahl, Netzkennzahl des besuchten Netzes und einer Teilnehmernummer innerhalb des besuchten Netzes. Sie wird von der Aufenthaltsdatei (visiting location register, VLR) vergeben.



SIM	- Subscriber Identity Module
EIR	- Equipment Identification Register
AUC	- Authentication Centre
HLR	- Home Location Register
VLS	- Visitor Location Register
BSC	- Base Station Controller
BTS	- Base Transceiver Station
MSC	- Mobile Switching Centre

MSISDN	- Mobile Subscriber ISDN Number
TMSI	- Temporary Mobile Subscriber Identity
MSRN	- Mobile Station Roaming Number
LMSI	- Local Mobile Station Identity
IMEI	- International Mobile Equipment Identity
IMSI	- International Mobile Subscriber Identity
BSIC	- Base Transceiver Station Identity Code
CI	- Cell Identity
LAI	- Location Area Identity

Bild: Nummern und Adressen in GSM

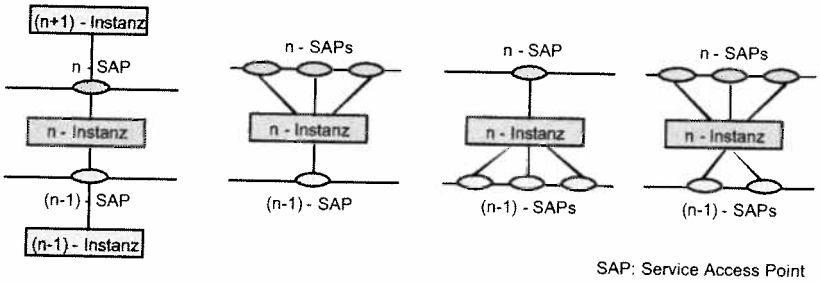
Die Identität des Mobilgerätes (International Mobile Equipment Identifier, IMEI) ist im Geräteregister abgelegt.

In einem Mobilnetz selbst müssen alle Netzelemente adressierbar sein. Dies sind unter anderen:

- Zellen (CI, Identifier),
- organisatorisch zusammengefasste Zellen für das Suchen eines Teilnehmers (LAI, Location Area Identifier),
- Basisstationen (Base Station Identification Code, BSIC).
-
- Das Authentisierungszentrum bereitet die Informationsdaten vor, die zur Authentisierung eines Teilnehmers durch die Heimatdatei (HLR, Home Register Location) benötigt werden.

Adressierung zwischen OSI-Protokollschichten (SAPs, Service Access Point)

Services	SAP
Application	-
Presentation	P - SAP
Session	S - SAP
Transport	T - SAP
Network	N - SAP
DataLink	DL - SAP
PHysical	PH - SAP



SAP: Service Access Point

Bild: Service Access Points

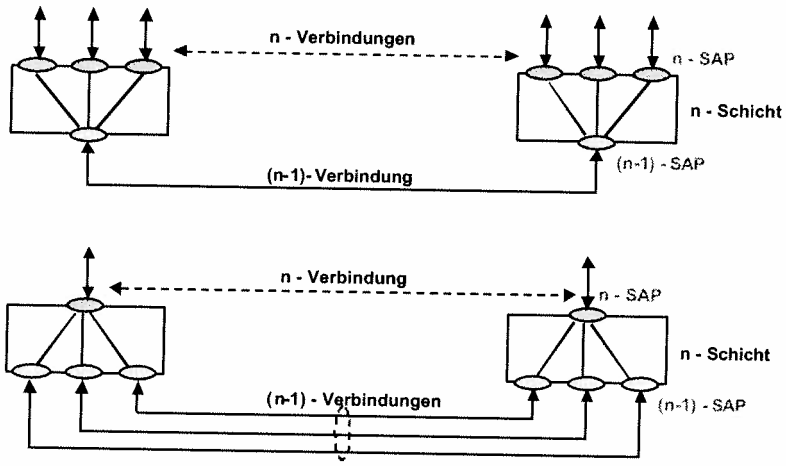


Bild: Logische Verbindungen zwischen SAPs

In Kommunikationsprotokollen gibt es Adressen, die als SAP (Service Access Point) in Verbindung mit der jeweiligen Schicht benannt sind:

- PSAP: Presentation-SAP auf Schicht 6.
- SSAP: Session-SAP auf Schicht 5.
- TSAP: Transport-SAP auf Schicht 4.
- NSAP: Network-SAP auf Schicht 3.

NSAP ist die netzweit eindeutige Adresse eines Knotens; TSAP, SSAP und PSAP sind Selektoren. Sie geben an, welcher Anwendungsprozess gerade die genannte Schicht nutzt. Die gesamte Adresse eines Anwendungsprozesses ergibt sich also aus der Aneinanderreihung der einzelnen Adressen zu PSAP + SSAP + TSAP + NSAP.

Adressierung zwischen Internet-Protokollschichten (Sockets)

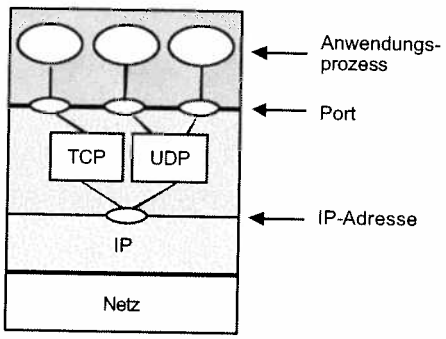


Bild: Transport-Adressen im Internet

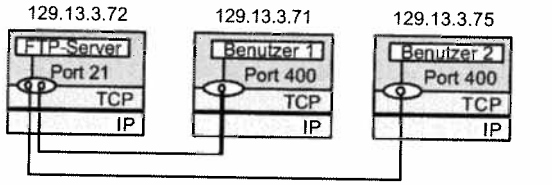


Bild: Adressierung in TCP (IP-Adresse + Port-Adresse)

Im Internet geschieht die Adressierung der Anwendungsprozesse über die Kette:

- IP-Adresse,
- Port-Nummer (Well-known Ports oder anwenderspezifizierte Ports).

Dabei kann ein Port über verschiedene Protokolle erreicht werden. Dieses Protokoll ist durch eine Protokollnummer spezifiziert. Die Protokollnummer befindet sich bei IPv4 direkt im Header. Bei IPv6 ist das Protokoll im Header-Extention vorhanden. Die Portnummer ist im TCP oder UDP-Header zu finden.

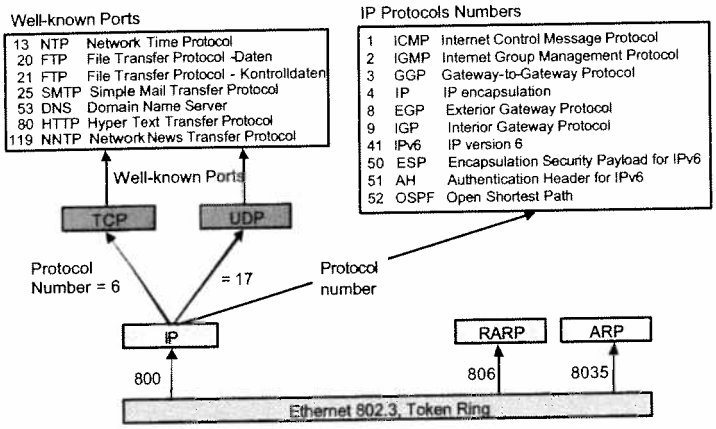


Bild: Adressierung von Internetanwendungen

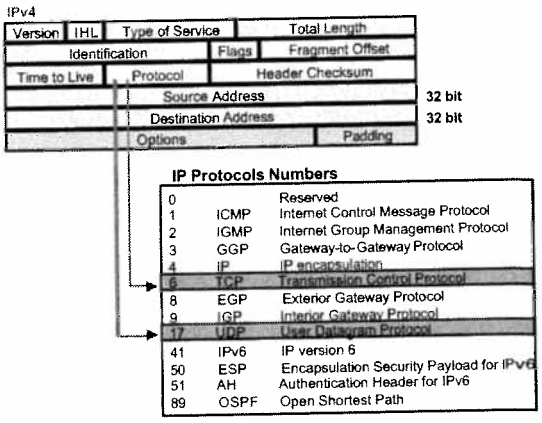


Bild: IPv4 Header und Protokollnummern

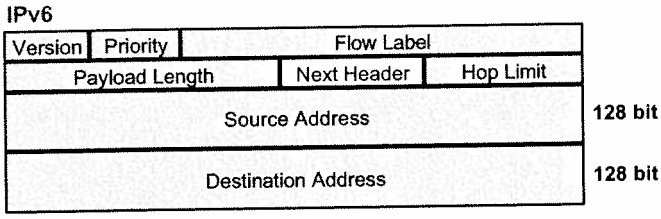


Bild: IPv6 Header

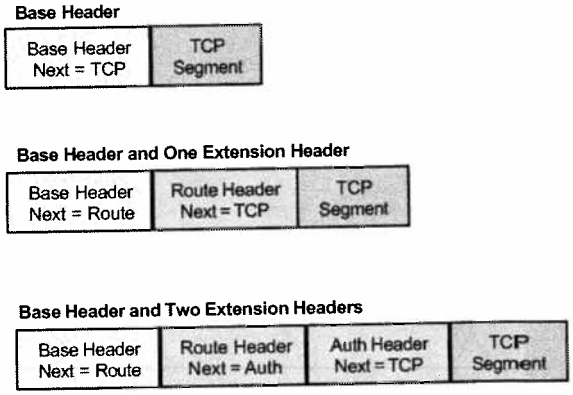


Bild: Extension Header in IPv6

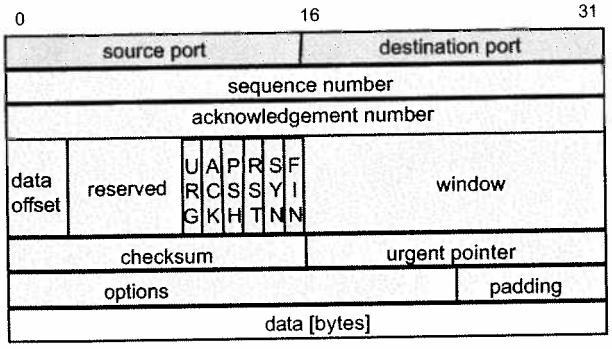


Bild: TCP Header

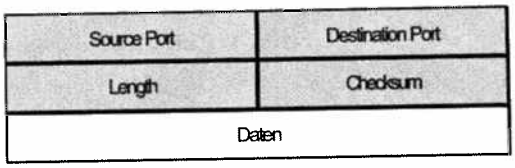
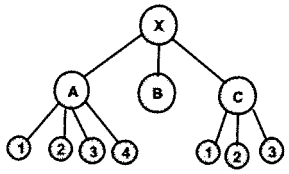


Bild: UDP-Header

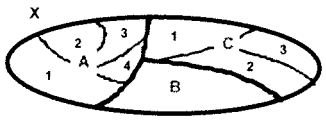
20	FTP (Data), File Transfer Protocol	(TCP)
21	FTP (Control)	(TCP)
23	TELNET, Terminal Emulation	(TCP)
25	SMTP, Simple Mail Transfer Protocol	(TCP)
53	DOMAIN, Domain Name Server	(UDP)
67	BOOTPS, Bootstrap Protocol Server	(UDP)
68	BOOTPC, Bootstrap Protocol Client	(UDP)
69	TFTP, Trivial File Transfer Protocol	(UDP)
80	HTTP Hypertext Transfer Protocol (default port)	(TCP)
111	SUN RPC, Run Remote Procedure Call	(TCP)
161	SNMP, Simple Network Management Protocol	(UDP)

Bild: Well Known Ports

Adressierung in OSI-Systemen



Hierarchische Struktur



Netzaufteilung

ISO-Adressierungsschema

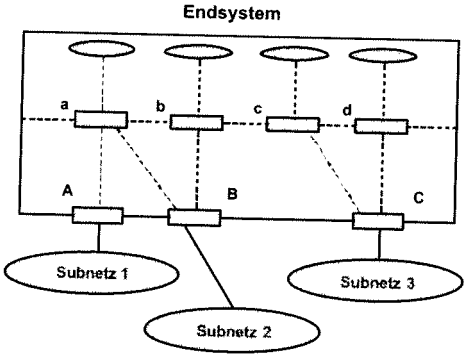
In ISO ist ein allgemeingültiges Adressierungsschema definiert, welches folgende Forderungen genügt:

- Integration bestehender Adressierungsschemata (ITU, nationale Festlegungen),
- Strukturiertheit,
- Lokale Adressierungsmö glichkeit in abgegrenzten Teilbereichen.

Merkmale:

- Einteilung in mehrere Adressierungsbereiche (Adressierungsdomänen)
- Verfeinerung in Teildomänen möglich Adressierung innerhalb der Domänen durch eine Adressierungsverwaltung, welche verantwortlich ist für die weitere Unterteilung und Adressvergabe
- Codierung in Form von Dezimalziffern oder binär

Bild: OSI-Domänen und Subnetze



NSAP: Network Service Access Point
SNPA: Subnetwork Point of Attachment

Bild: OSI-Adressierungskonzept

Innerhalb dieses Adressierungsschemas können unterschieden werden:

- Netzadresse (network address)
  Kennzeichnung des Dienstzugangspunktes (SAP) der Vermittlungsschicht im OSI-Referenzmodell
- Quell-, Zieladresse (source/destination address)
  Adresse des Absenders/Empfängers von Nachrichten
- Gruppen-/Rundrufadresse (multicast/broadcast address)
- Adresse, unter der eine Gruppe oder alle Endeinrichtungen eines Netzbereiches angesprochen werden können

Die Adressen sind in einem **Adressverzeichnis** (directory) aufgeführt.

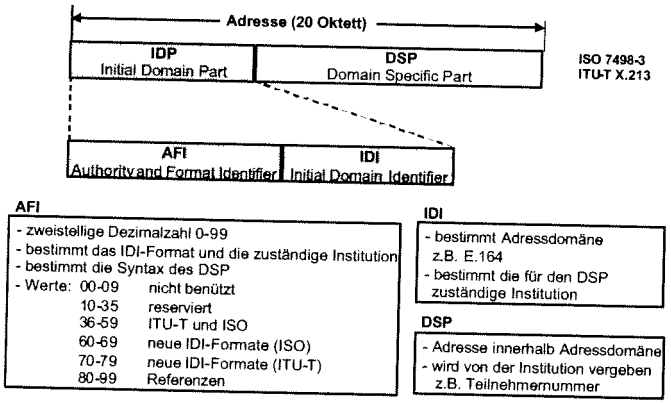


Bild: Adress-Struktur nach OSI

Adressierung nach OSI

Die verwendete Adressierung ist auch in X.213 festgelegt. Dort wird ein hierarchischer Aufbau der **NSAP-Adresse** (Network Service Access Point) beschrieben, der diese Felder enthält:

- IDP (Initial Domain Part), bestehend aus AFI und IDI.
- AFI (Authority Format Identifier) enthält eine zweistellige Dezimalzahl (0-99), die das IDI-Format und die dafür zuständige Institution sowie die Syntax des DSP bestimmt.
- IDI (Initial Doniain Identifier) gibt die Adressendomäne (beispielsweise DM ICD oder E.164 und die für den DSP zuständige Institution an. Die genaue Bedeutung des IDI folgt aus dem angegebenen AFI-Wert.

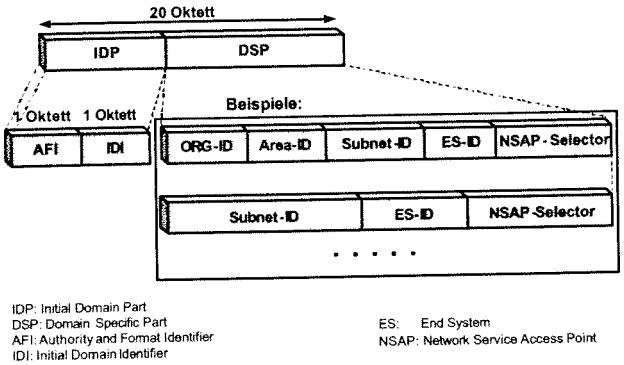


Bild: Network Service Access Point (NSAP)

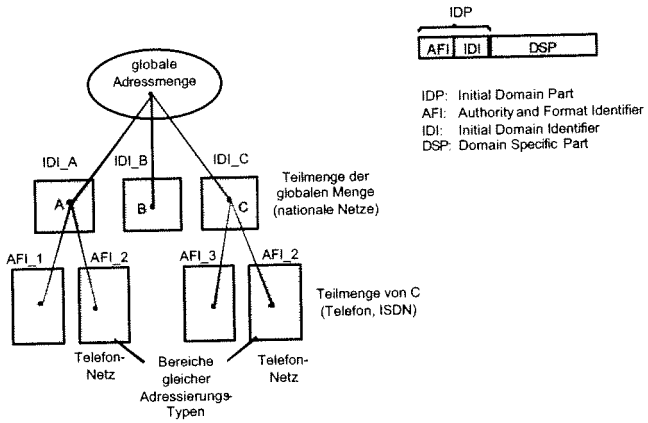


Bild: Adressierungssystem

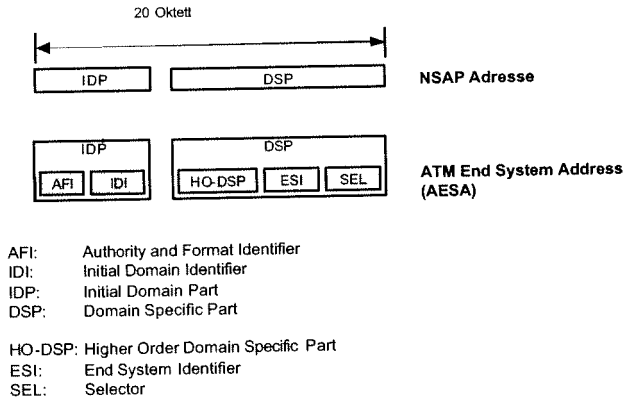


Bild: Schema der NSAP Adresse

DSP (Domain Specific Part), Adresse innerhalb der Adressendomäne. Diese wird von der dafür zuständigen Institution vergeben und kann die Adresse eines Teilnehmers sein.

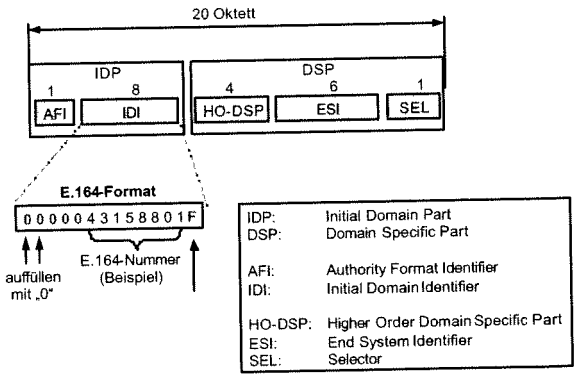


Bild: NSAP Adresse nach E.164

Adressierung in ATM-Systemen

In ATM-Systemen bilden die Felder AFI und IDI zusammen den IDP (Initial Domain Part). Der DSP (Domain Specific Part) besteht aus HO-DSP, ESI und SEL. Der HO-DSP identifiziert einen Teil eines Adressraums, also ein Subnetz. Der ESI benennt ein bestimmtes Endsystem irrt Subnetz. Das SEL-Feld kann durch das Endsystem interpretiert und für die Auswahl eines bestimmten Anwendungsprozesses benutzt werden.

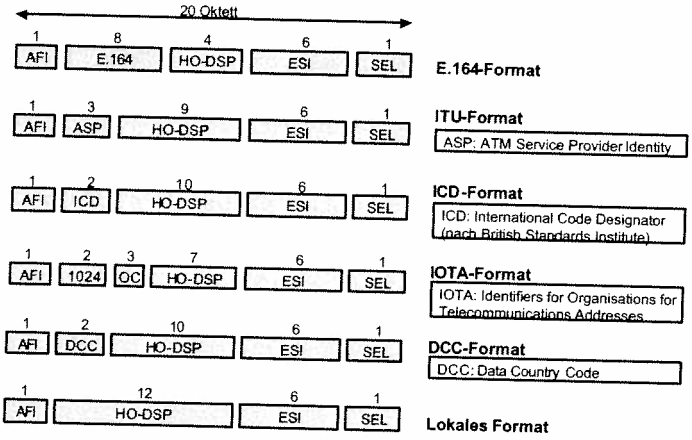


Bild: AESA: ATM End System Address

ATM-Adressen sind ein Beispiel für OSI-Adressen. Für die Realisierung weltweiter ATM-Netze wurden mehrere Adressformate vorgesehen. Das **DCC-Format** (Data Country Code) enthält Ländercodes. Das **ICD-Format** (International Code Designator) identifiziert im Feld ICD eine internationale Organisation eindeutig. Der Inhalt dieses Feldes wird vom BSI (British Standards Institute) zugeteilt. Das E.164-Format enthält im IDI-Feld eine E.164 Nummer. Diese besteht aus 15 Dezimalziffern, die eine Landeskennung und eine nationale Kennung (National Significant Number) repräsentieren. Bei Verwendung einer E.164-Nummer sind ATM-Systeme weltweit eindeutig adressierbar.

X.121-Adressen

Adressen nach der Empfehlung X.121 werden im Packet Level Protocol von X.25 zur Adressierung des Empfängers. Sie können ebenfalls in Frame Relay genutzt werden. Die Adresse besteht aus maximal 14 Dezimalziffern. Das Feld PSN erlaubt die Auswahl eines bestimmten Netzes (Netzbetreibers) in einem Land.

Adressierung in IEEE LANs
Struktur der IEEE MAC-Adresse

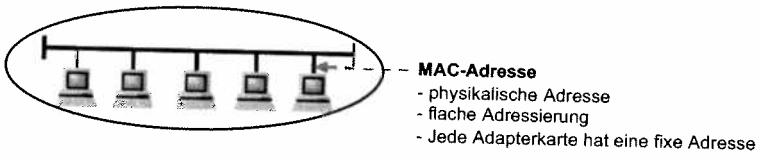


Bild: IEEE MAC-Adressen

MAC-Adressen sind **Hardwareadressen** (physikalische Adressen). Sie sind der Hardware des Netzadapters in einem Netzknoten zugeordnet. Eine MAC-Adresse muss innerhalb eines Netzes, in dem Rahmen der Schicht 2 übertragen werden, eindeutig sein. Häufig werden MAC-Adressen jedoch global eindeutig vergeben, insbesondere dann, wenn - wie üblich - das Adressierungsschema nach IEEE 802 verwendet wird.

Wichtig ist, dass die MAC-Adressen keine Information darüber enthalten, wo sich die entsprechenden Stationen im LAN geographisch befinden.

Um keinen Wildwuchs an unterschiedlichen MAC-Adressen aufkommen zu lassen, standardisierte das IEEE-Komitee 802 die physikalischen LAN-Adressen. Die erste Festlegung betraf hierbei die Länge des Adressfeldes im MAC-Header. Zuerst wurden sowohl 16- als auch 48-Bit Adressen vorgesehen (ausgenommen 802.6-Standard). Die Adressen mit 16 Bit Länge haben sich nicht durchgesetzt und wurden sogar aus dem Standard herausgenommen. Einzig beim Standard IEEE 802.6 (DQDB) besteht die Möglichkeit, mit 16-, 48- oder 64-Bit-Adressen zu arbeiten. Die größte Bedeutung kommt der MAC-Adresse mit 48 Bit Länge zu. Die 48-Bit-Adressen werden global eindeutig vergeben. Dazu teilt IEEE jedem Hersteller von Netzadaptern einen Block von herstellerspezifischen Adressteilen (OUI, Organisationally Unique Identifier) zu. Der Hersteller ergänzt diesen Teil für jeden hergestellten Adapter mit einer laufenden Nummer. IEEE hat für zukünftige Netze auch 64-Bit-Adressen unter der Bezeichnung EUI-64 definiert, die bisherigen 48-Bit-Adressen werden als EUI-48 bezeichnet.

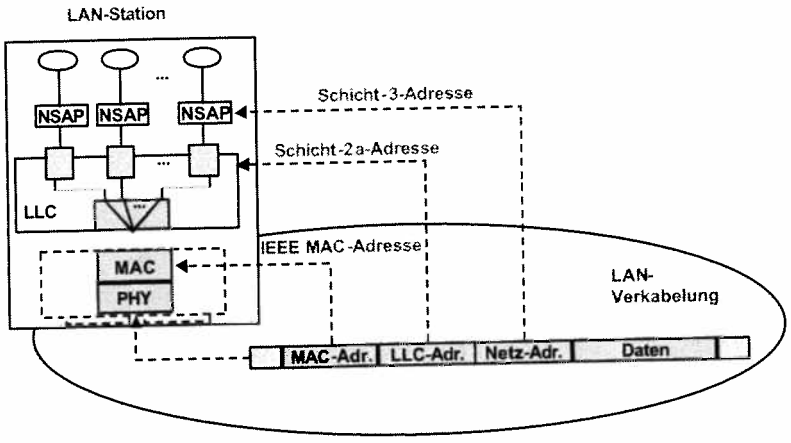


Bild: LAN-Adressierung

Logisch gesehen besteht die Kommunikation im LAN im Datenaustausch zwischen zwei Kommunikationspuffern innerhalb der LLC-Schicht. Dafür müssen die Datenrahmen zuerst zwischen entsprechenden LAN-Adapterkarten ausgetauscht werden.

Das prägnante Merkmal der MAC-Teilschicht ist die MAC-Adresse, mit der die entsprechende LAN-Adapterkarte addressiert wird. In jedem MAC-Rahmen muss sowohl eine MAC-Quelladresse als auch eine MAC-Zieladresse enthalten sein. Eine MAC-Adresse ist als eine physikalische LAN-Adresse zu interpretieren.

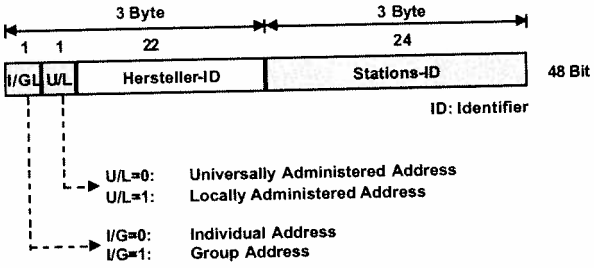


Bild: Struktur der IEEE MAC-Adresse

Ein LAN-Adapter-Hersteller muss eine von der IEEE einen Adressblock, bestehend aus mehreren Adressen, kaufen und hat dadurch die Gewissheit, dass die LAN-Adapterkarte, die er herstellt, weltweit eindeutig adressierbar ist. Die ersten drei Bytes der MAC-Adresse enthalten einen Festwert als Hersteller-Identifikator (ID), der den Hersteller weltweit eindeutig kennzeichnet. Diese Identifikator wird auch als OUI-Code (Organisationally Unique Identifier) bezeichnet. Die restlichen drei Bytes dienen als Stations-Identifikator und können von der Firma frei vergeben werden. Die Stations-ID ist also eine Art Kartennummer. Ein Hersteller kann damit bei einem festen Hersteller-ID bis zu 2^{24} LAN-Adapterkarten mit unterschiedlichen Nummern (Adressen) versehen.

Gruppenadresse

In jedem LAN muss auch die Möglichkeit bestehen, einen MAC-Frame einmalig an mehrere Stationen zu verschicken. Dies setzt eine Gruppenadressierung voraus. Um eine derartige Adressierung zu unterstützen, haben in der MAC-Adresse die ersten zwei Bits eine besondere Bedeutung.

Das **I/G-Bit** legt fest, ob es sich um eine individuelle MAC-Adresse (I: Individuum) oder eine Gruppenadresse (G: Gruppe) handelt. Wird I/G = 0 gesetzt, dann stellt die MAC-Adresse eine individuelle Adresse dar und deutet nur auf eine Station hin. Dagegen stellt im Fall I/G = 1 die MAC-Adresse eine Gruppenadresse dar. Bei einer MAC-Ziel-Adresse als Gruppenadresse kann die Stations-ID eine Bitkombination enthalten, mit der eine logische Gruppe von Stationen gekennzeichnet wird. Ein Sonderfall ist eine Gruppe, die aus allen LAN-Stationen besteht. Dazu wird eine Sonder-Gruppenadresse verwendet, die als Multicast- oder Broadcast-Adresse bezeichnet wird, bei der sämtliche Bits der Stations-ID gleich Eins sind. Ein MAC-Frame mit einer Broadcast-Adresse wird von allen LAN-Adapterkarten aufgenommen.

Das **G/L-Bit** markiert, ob die gegebene MAC-Adresse eine globale (G) oder lokale (L) Bedeutung hat. Ist G/L = 1, bedeutet dies, dass die Adresse durch IEEE vergeben wurde. In diesem Fall hat diese Adresse globale Bedeutung, d.h. sie ist weltweit eindeutig. Ist G/L = 0, besteht für den Hersteller einer LAN-Adapterkarte die Möglichkeit, die Adressen für die eigenen Karten unabhängig von den IEEE-Adressen selbst zu vergeben. Derartige Adressen haben nur lokale Bedeutung und können weltweit nicht eindeutig sein.

Ein Problem resultiert aus der Darstellung und die Übermittlung der Bits von MAC-Adressen bei den unterschiedlichen MAC-Zugriffsverfahren. So wird bei IEEE 802.3 (CSMA/CD) und IEEE 802.4 (Token Bus) das niederwertige Bit jedes Bytes zuerst übertragen, dagegen bei IEEE 802.5 (Token Ring) und FDDI wird das höchstwertige Bit zuerst übertragen. Dies kann durchaus dazu führen, dass bei einem Übergang von einem 802.3 LAN zu einem FDDI jede MAC-Adresse entsprechend umgestellt werden muss. Diese Situation ist vor allem in den Kopplungselementen zwischen zwei unterschiedlichen LANs zu beachten.

Adressierung im Internet mit IPv4

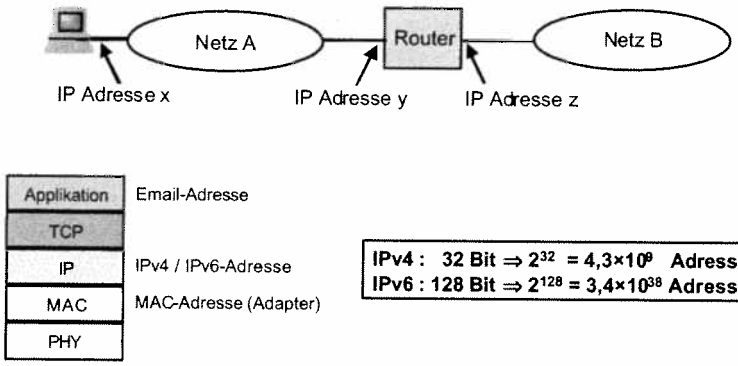
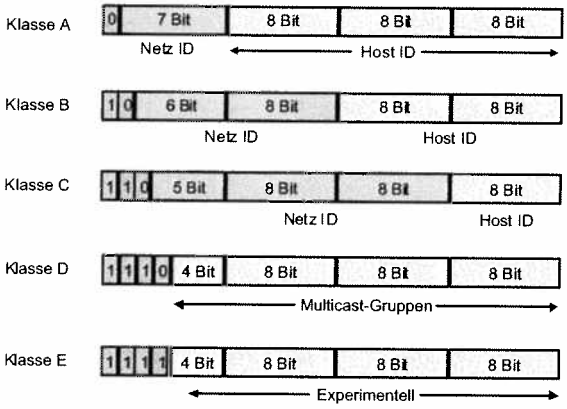
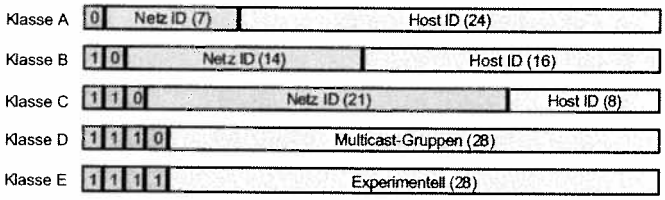


Bild: Verwendung von IP-Adressen

Adressierung nach TCP/IP
TCP/IP kennt IP-Adressen und Portnummern. **IP-Adressen** sind die Adressen der Netzschicht im TCP/IP-Protokollstapel. Sie bestehen aus 32 bit (4 Byte, in der IP-Version 4, kurz IPv4) bzw. 128 bit (16 Byte in IPv6). **Portnummern** werden von TCP und UDP zur Adressierung des darüber liegenden Dienstes benutzt. Sie sind also der OSI-Schicht 4 zuzuordnen. Im OSI-Referenzmodell ist der TSAP das Äquivalent zur Portnummer.

Internet-Adressen
Jedes Endsystem (Rechner, Router) im Netz wird beim Einsatz der Protokollfamilie TCP/IP durch eine logische IP-Adresse identifiziert. Für alle Endsysteme und Netzkomponenten, die unter Verwendung von TCP/IP kommunizieren, ist eine eindeutige IP-Adresse erforderlich. Jede IP-Adresse (sog. Unicast-Adresse) hat im allgemeinen folgende Struktur: Netz-ID , Host-ID (ID = Identifkation). Die Netz-ID (auch als Netz-ID bezeichnet) identifiziert sämtliche Systeme, die sich im gleichen Netz befinden. Alle Systeme im gleichen Netz müssen dieselbe Netz-ID tragen. Die Host-ID identifiziert ein beliebiges Endsystem (Arbeitsstation, Server, Router, ...) im Netz. Die Identifikation Host-ID muss für jedes einzelne Endsystem in einem Netz (d.h. für eine Netz-ID) eindeutig sein. Eine IP-Adresse bestimmt weltweit eindeutig einen Rechner. Es werden fünf Klassen von IP-Adressen definiert, um den Aufbau der Netze unterschiedlicher Größe zu ermöglichen. Die Adresse einer Klasse legt fest, welche Bits für die Netz-ID und welche für die Host-ID verwendet werden. Sie bestimmt ebenfalls die mögliche Anzahl der Netze und Endsysteme (Hosts).





Klasse	Anzahl Netze	Anzahl Hosts	Adressbereich
A	126 (2^7-2)	16.777.214 ($2^{24}-2$)	1.0.0.0 – 126.0.0.0
B	16.384 (2^{14})	65.534 ($2^{16}-2$)	128.0.0.0 – 191.255.0.0
C	2.097.152 (2^{21})	254 (2^8-2)	192.0.0.0 – 223.255.255.0
D			224.0.0.0 – 239.255.255.255
E			240.0.0.0 – 255.255.255.254

Bild: IPv4-Adressklassen

- **Klasse A (Class A)**
  Die Adressen dieser Klasse werden Netzen mit einer sehr großen Anzahl von Endsystemen zugewiesen. Das höchstwertigste Bit einer Adresse der Klasse A ist immer auf 0 gesetzt. Die nächsten sieben Bits schließen die Netz-ID ab. Die restlichen 24 Bits (d.h. die restlichen 3 Bytes) bilden die Host-ID. Dies ermöglicht, 2^7 = 126 Netze und circa 17 Millionen von Endsystemen pro Netz zu identifizieren.
- **Klasse B (Class B)**
  Die Adressen dieser Klasse werden mittelgroßen und großen Netzen zugewiesen. Die zwei höchstwertigen Bits einer Adresse der Klasse B sind immer auf 10 gesetzt. Die weiteren 14 Bits (zur Vervollständigung der ersten beiden Bytes) stellen die Netz-ID dar. Die letzten 2 Bytes bilden die Host-ID. Dies ermöglicht, 2^{14} = 16 384 Netze und circa 65 000 Endsysteme pro Netz zu identifizieren.
- **Klasse C (Class C)**
  Die Adressen dieser Klasse C werden für kleine Netze (wie z.B. LANs) verwendet. Die 3 höchstwertigen Bits einer Adresse der Klasse C sind immer auf 110 gesetzt. Die weiteren 21 Bits (zur Vervollständigung der ersten 3 Bytes) stellen die

Netz-ID dar. Das letzte Byte bildet die Host-ID. Dies ermöglicht, etwa 2 Millionen Netze und 254 Endsysteme pro Netz zu identifizieren.

- **Klasse D (Class D)**
  Die Adressen dieser Klasse D werden für den Einsatz bei Multicast-Gruppen (als geschlossene Benutzergruppen) verwendet. Eine Multicast-Adresse wird in der Regel mehreren Endsystemen zugeordnet. Die 4 höchstwertigen Bits einer Multicast-Adresse sind immer auf 1110 gesetzt. Die restlichen Bits bezeichnen eine Gruppe von Endsystemen. Die Multicast-Adressen enthalten keine Netz- bzw. Host-ID-Bits. Die IP-Pakete werden an eine ausgewählte Gruppe der Endsysteme in einem Netz weitergeleitet. Eine Multicast-Adresse repräsentiert im Grunde genommen bei der Multicast-Verteilung eine Tabelle mit IP-Adressen einer Gruppe von Endsystemen.
- **Klasse E (Class E)**
  Die Klasse E stellt eine experimentelle Adresse dar und ist nicht für den normalen Gebrauch bestimmt.

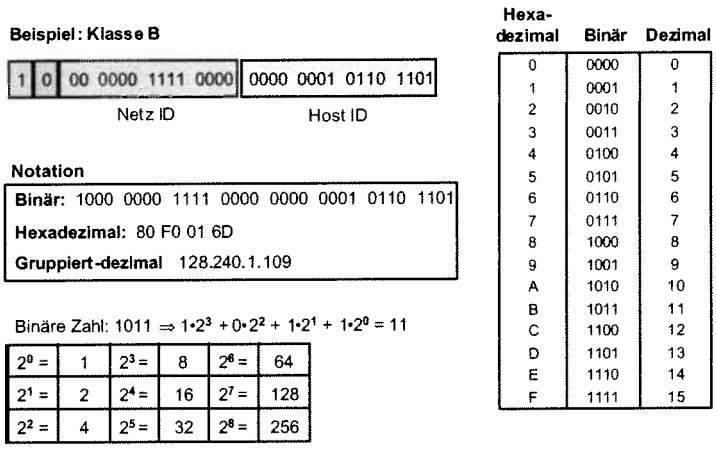


Bild: IPv4-Adresse

Darstellung von IP-Adressen

Jede IP-Adresse ist 32 Bit lang und besteht aus vier Feldern von je 8 Bit Länge, auch Bytes genannt. Die einzelnen Bytes werden durch Punkte voneinander getrennt. Ein Byte repräsentiert eine Dezimalzahl zwischen 0 und 255.

Bei dieser Adressvergabe unterscheidet man drei Klassen von Netzen. Je nach Anzahl der im Netz vorgesehenen TCP/IP-Hosts bekommt man eine Adresse einer entsprechenden Klasse zugeteilt. Über die Netzadresse wird, unter anderem, eine Unterteilung in verschiedene Anwendungen (Wissenschaft, Militär ..) und in Installationsorte (USA, Europa ...) vorgenommen.

Es können weltweit maximal 2^7-2 = 126 Netze der Klasse A existieren. Die IP-Adressen mit den Bit-Kombinationen "Alle Bits 0" und "Alle Bits l" sind ungültige IP-Adressen. Bei einem Netz der Klasse A können 2^{24} -2 Stationen adressiert werden. Bei einem Netz der Klasse B wird eine IP-Adresse vergeben, die die ersten 16 Bit (14 Bit) festlegt. Hier können nur noch 2^{16}-2 IP-Adressen innerhalb eines Netzes vergeben werden. Einem Betreiber eines Klasse-C-Netzes bleiben genau 254 Adressen, die er seinen im Netz befindlichen Endsystemen (Hosts) zuordnen kann.

Neben dieser klassenbasierten Einteilung von IP-Adressen findet insbesondere bei ISPs eine bitweise Beschreibung des Netzschemas Verwendung, das Grundlage des Classless Inter-Domain Routing CIDR geworden ist.

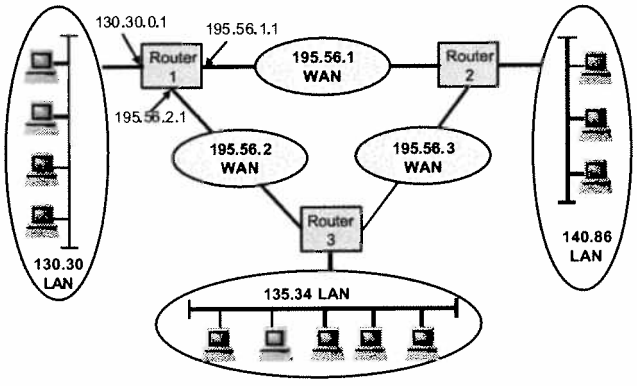


Bild: Router-Netz

Wie im Bild zu sehen ist, muss dem WAN auch eine Subnetz-ID zugeordnet werden, wenn die lokalen Netze mit Hilfe von Routern standortübergreifend über ein WAN verbunden sind. Zwischen diesen beiden Routern werden IP-Pakete über das WAN übermitttelt, so dass die Router-Ports seitens des WANs durch die eindeutigen IP-Adressen identifiziert werden. Da sich unterwegs zwischen den beiden Routern im WAN kein Router mehr befindet, muss das ganze WAN aus der Routing-Sicht als ein Subnetz gesehen werden. Damit muss dem WAN (formal!) eine Netz-ID zugeteilt werden. In diesem Fall stellt das WAN nur eine Verbindung für den Datenaustausch zwischen den Routern zur Verfügung.

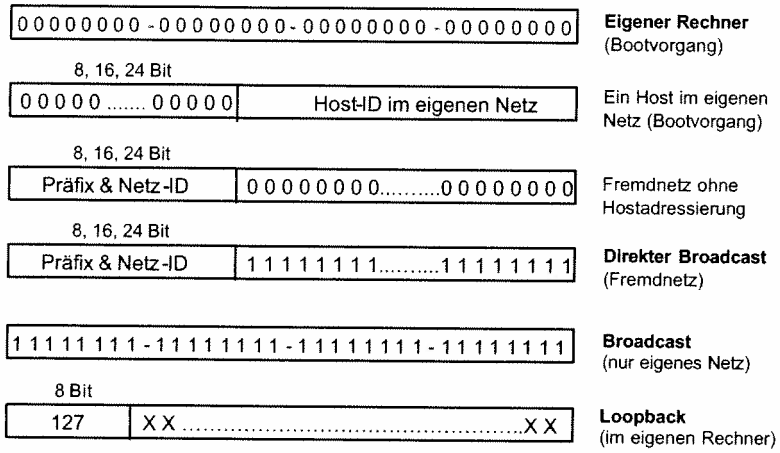


Bild: Spezielle IPv4-Adressen

Vergabe von IP-Adressen

Bei der Vergabe von IP-Adressen muss vordringlich darauf geachtet werden, dass die Adressen aller in einem physikalischen Netz liegenden Endsysteme (Stationen) sich nur in dem Netz-ID-Teil unterscheiden und dass keine IP-Adresse doppelt vorkommt. Für die Nutzung des IP-Adressraums gelten darüber hinaus einige weitere Einschränkungen, auf die wir im folgenden kurz eingehen möchten. Diese betreffen die Verwendung bestimmter Netz-Adressbereiche sowie die Vergabe lokaler IP-Adressen als Host- bzw. Interface-ID. Generell können unterschieden werden:

- (lokale) IP-Netzadressen,
- (lokale) IP-Broadcastadressen,
- Loopback-Adresse sowie
- private IP-Adressbereiche.

Klasse	Netzmaske	IP Adresse	Netz ID	Host ID	Host-Adressen
A	255.0.0.0	34.63.1.132	34.0.0.0	0.63.1.132	0.0.1 -- 255.255.254
B	255.255.0.0	148.33.22.5	148.33.0.0	0.0.22.5	0.1 -- 255.254
C	255.255.255.0	195.1.1.34	195.1.1.0	0.0.0.34	1 -- 254

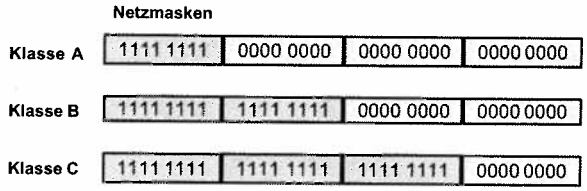


Bild: Netz und Host IPv4-Adressen

Standard-Subnetz-Maske

Eine Subnetz-Maske (Subnet Mask) kann eine Standard-Subnetz-Maske (Default Subnet Mask) bzw. eine benutzerdefinierte Subnetz-Maske darstellen. Wird ein physikalisches Netz nicht auf die Subnetze (Teilnetze) aufgeteilt, so verwendet man in diesem Fall eine Standardmaske. Wird ein physikalisches Netz auf mehrere Subnetze (Teilnetze) aufgeteilt, so muss eine Subnetz-Maske vom Benutzer definiert werden. Auf diese Möglichkeit gehen wir später ein. Zunächst wird die Bedeutung einer Standardmaske näher erläutert.

Eine Standard-Subnetz-Maske ist eine 32-Bit-Kombination, die verwendet wird, um

- einen Teil der IP-Adresse auszublenden und auf diese Weise die Netz-ID von der Host-ID zu unterscheiden
- festzustellen, ob der Ziel-Host sich in demselben Netz oder einem anderen (Remote-) Netz befindet.

Jeder Host in einem TCP/IP-Netz benötigt eine Subnetz-Maske, d.h. entweder

- eine Standardmaske, falls keine Aufteilung des physikalischen Netzes vorgenommen wird, oder
- eine benutzerdefinierte Subnetz-Maske, falls das physikalische Netz auf mehrere Subnetze aufgeteilt wird.

Die Struktur der Standard-Subnetz-Maske ist von der Klasse der IP-Adresse abhängig. Wie hier ersichtlich ist, werden alle Bits, die zu einer Netz-ID gehören, auf 1 gesetzt. Der Dezimalwert jedes Bytes beträgt jeweils 255. Alle Bits, die zur Host-ID gehören, werden auf 0 gesetzt.

Um die Identifikation des Zielnetzes (d.h. Ziel-Netz-ID) aus einer IP-Adresse herauszufiltern, wird eine Operation Bitweise_AND für IP-Adresse und Subnetz-Maske ausgeführt. Die Operation Bitweise_AND besteht darin, dass jedes einzelne Bit der IP-Adresse mit dem entsprechenden Bit in der Subnetz-Maske verglichen wird. Wenn beide Bits 1 sind, ist das resultierende Bit ebenfalls 1. Wenn eine andere Kombination von Bits vorliegt, ist das resultierende Bit 0. Die Operation Bitweise_AND wird als ein rechnerinterner Prozess durchgeführt, so dass der Benutzer keinen Einfluss auf dessen Durchführung hat.

Bis 1992:
- keine Zusammenhang zwischen Adressen und geographischen Bereichen
- dadurch große Routing-Tabellen

Zuweisung der restlichen Klasse C Adressen

Region	Adressbereich
Multi-regional	192.0.0.0 – 193.255.255.255
Europa	194.0.0.0 – 195.255.255.255
Weitere geographische Bereiche	196.0.0.0 – 197.255.255.255
Nordamerika	198.0.0.0 – 199.255.255.255
Zentral- und Südamerika	200.0.0.0 – 201.255.255.255
Ozeanien	202.0.0.0 – 203.255.255.255
Weitere geographische Bereiche	204.0.0.0 – 205.255.255.255
Weitere geographische Bereiche	206.0.0.0 – 207.255.255.255

Bild: Zusammenfassung von Klasse-C Adressen

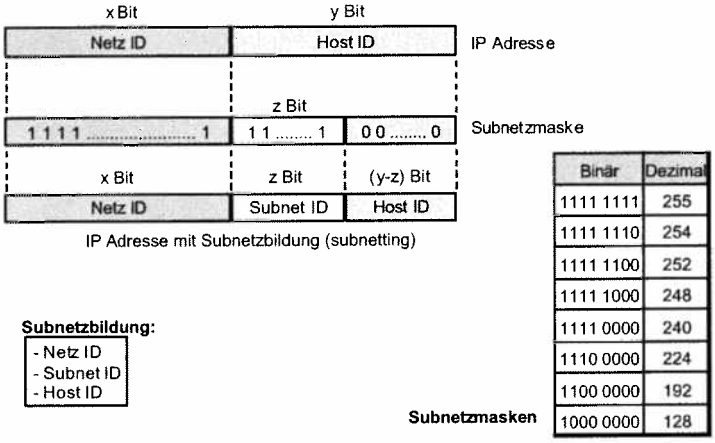


Bild: Subnetzbildung (Subnetting)

Bildung von Subnetzen

Ein Subnetz stellt eine geschlossene Gruppe der Endsysteme (Hosts) dar, und diese Gruppe wird mit einer Subnetz-ID identifiziert. Wird ein physikalisches Netz auf mehrere Teilnetze aufgeteilt, so bezeichnet man diese Teilnetze als Subnetze. Das ganze physikalische Netz kann auch als ein Sonder-Subnetz gesehen werden. Die Subnetze entstehen, wenn autonome Netze in mehrere physikalische oder logische Netze aufgeteilt werden. Zu einem Subnetz können auch mehrere physikalische Netze zusammengefasst werden. Dieser Gruppe von physikalischen Netzen muss eine gemeinsame Subnetz-ID zugewiesen werden.

Innerhalb von physikalischen LANs werden oft geschlossene Gruppen der Endsysteme gebildet. Diese Gruppen werden als virtuelle LANs (VLANs) bezeichnet. Ein virtuelles LAN kann als ein logisches Subnetz innerhalb eines physikalischen LANs interpretiert werden. Somit muss jedem virtuellen LAN auch eine Subnetz-ID zugewiesen werden.

Die großen TCP/IP-Netze werden aus organisatorischen bzw. politischen Gründen oft auf kleinere Subnetze aufgeteilt werden, was man als Strukturierung bezeichnet. Diese Subnetze werden oft IP-Subnetze genannt. Für die Vernetzung von einzelnen IP-Subnetzen miteinander können IP-Router bzw. IP-Switches (d.h. Layer-3-Switches) eingesetzt werden.

Um ein Netz in Subnetze unterteilen zu können, muss jedes Subnetz eine andere Identifikation (ID) verwenden. Eine eindeutige Subnetz-ID wird geschaffen, indem man die Bits der Host-ID in zwei Bereiche aufteilt. Ein Bereich wird verwendet, um das Subnetz als eindeutige und selbständige Gruppe der Endsysteme zu identifizieren, der andere Bereich wird zur Identifizierung der Hosts in diesem Subnetz verwendet.

Eine solche Aufteilung der Host-ID in der IP-Adresse wird auch als Subnetting oder Subnetworking bezeichnet.
- Jeder Abteilung (Organisation) kann ein getrenntes Subnetz zugeordnet werden.
- Unterschiedliche LAN-Technologien (beispielsweise Ethernet und Token-Ring) können als unterschiedliche Subnetze definiert und dementsprechend über Router verbunden werden.
- Die Belastung des Netzes kann reduziert werden, indem man den Verkehr zu den einzelnen Subnetzen einschränkt.

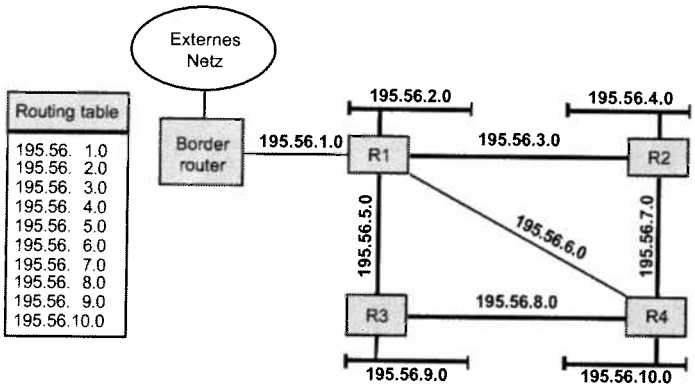


Bild: Netzklasse C ohne Subnetzbildung

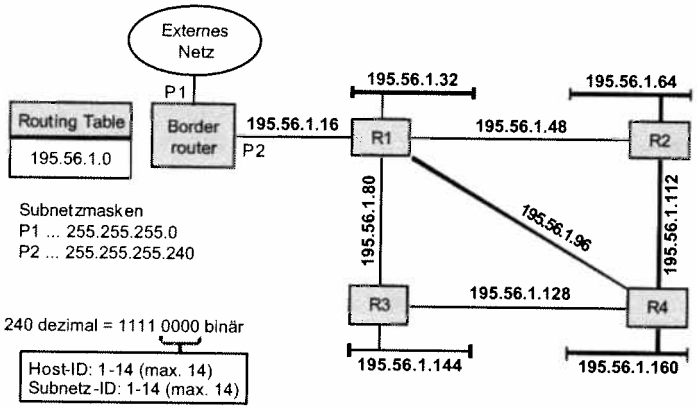


Bild: Netzklasse C mit Subnetzbildung

Natürliche Subnetzmasken

Netzklasse A :	255.0.0.0
Netzklasse B :	255.255.0.0
Netzklasse C :	255.255.255.0

8-Bit Masken

Binär	Dezimal
1111 1111	255
1111 1110	254
1111 1100	252
1111 1000	248
1111 0000	240
1110 0000	224
1100 0000	192
1000 0000	128

0000 1001 0100 0011 0010 0110 0000 0001	9.67.38.1	Klasse A Adresse
1111 1111 1111 1111 1111 1111 11xx xxxx	255.255.255.192	Subnetzmaske
0000 1001 0100 0011 0010 0110 00xx xxxx	9.67.38.0	Subnetzbasisadresse
xxxx xxxx 0100 0011 0010 0110 00xx xxxx	68760	Subnetznummer

Klasse A ← Subnetz → Host

Bild: Subnetzmasken

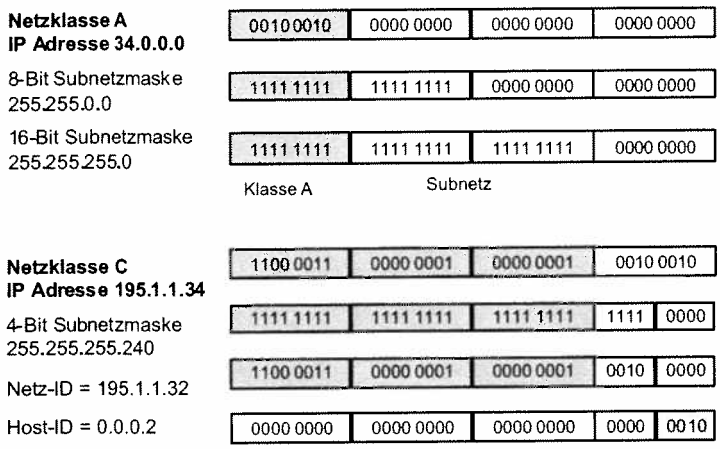


Bild: Subnetzbildung

Benutzerdefinierte Subnetz-Maske

Die Festlegung einer benutzerdefinierten Subnetz-Maske ist erforderlich, wenn ein physikalisches Netz vom Benutzer in mehrere Subnetze aufgeteilt wird. Bevor eine Subnetz-Maske festgelegt wird, ermittelt man zuerst

- die Anzahl der Subnetze,
- die Anzahl der Hosts pro Subnetz.

Bestimmen von Subnetz-IDs und Host-IDs

Die Subnetz-II)s bestimmen diese Host-ID-Bits, über die sich die Subnetz-Maske erstreckt. Um eine Subnetz-ID zu bestimmen, werden zunächst die möglichen Bitkombinationen untersucht und dann in das Dezimalformat konvertiert.

Folgende Schritte sind nötig:

- Alle möglichen Bitkombinationen der durch die Subnetz-Maske belegten Bits werden ermittelt.
- Alle Bitkombinationen, die entweder nur 0 oder nur 1 enthalten, sind ungültig.
- Die Bitkombinationen "Alle Bits 0" und "Alle Bits l" sind ungültige IP-Adressen. Die Kombination "Alle Bits C' ist reserviert und hat die Bedeutung "nur dieses Netz ". Mit der Kombination "Alle Bits l" wird eine Subnetz-Maske identifiziert.
- Die restlichen Kombinationen (über das ganze Byte) werden in das Dezimalformat konvertiert. Jeder Dezimalwert stellt ein einzelnes Subnetz-ID dar.

Nach der Festlegung von Subnetz-IDs müssen die Host-IDs in den einzelnen Subnetzen bestimmt werden. Um Host-IDs innerhalb eines Subnetzes zu bestimmen, muss man zuerst berechnen, wie viele Bits für die Host-ID zur Verfügung stehen.

Subnetzmaske: 255.255.255.192 (1100 0000)
Subnetze : $2^2 - 2 = 2$
Hosts pro Subnetz : $2^6 - 2 = 62$

Subnetz 1:	195.1.1	01 00 0000	Netz ID = 195.1.1.64
Subnetz 2:		10 00 0000	Netz ID = 195.1.1.128

- Nicht erlaubt ist Subnetz 0 (Netz ID.0)
- Nicht erlaubt ist Subnetz-Broadcast (Netz ID.192)
- 124 von 254 Host-Adressen werden verwendet (48,8%)

Bild: Netzklasse C - Adresse 195.1.1.0 /26

Subnetzmaske: 255.255.255.224 (1110 0000)
Subnetze : $2^3 - 2 = 6$
Hosts pro Subnetz : $2^5 - 2 = 30$

Subnetz 1:	195.1.1	001 0 0000	Netz ID = 195.1.1.32
Subnetz 2:		010 0 0000	Netz ID = 195.1.1.64
Subnetz 3:		011 0 0000	Netz ID = 195.1.1.96
Subnetz 4:		100 0 0000	Netz ID = 195.1.1.128
Subnetz 5:		101 0 0000	Netz ID = 195.1.1.160
Subnetz 6:		110 0 0000	Netz ID = 195.1.1.192

- Nicht erlaubt ist Subnetz 0 (Netz ID .0)
- Nicht erlaubt ist Subnetzbroadcast (Netz ID .224)
- 180 von 254 Host-Adressen werden verwendet (70,8%)

Bild: Netzklasse C - Adresse 195.1.1.0 /27

Subnetzmaske: 255.255.255.240
(1111 0000)
Subnetze : $2^4 - 2 = 14$
Hosts pro Subnetz : $2^4 - 2 = 14$

- Nicht erlaubt ist
  Subnetz 0 (Netz ID .0)
  Subnetzbroadcast (Netz ID .240)
- 196 von 254 Host-Adressen
  werden verwendet (77,2%)

Subnetz	Subnetz-ID	Subnetz-ID
1	195.1.1. 0001 | 0000	195.1.1.16
2	195.1.1. 0010 | 0000	195.1.1.32
3	195.1.1. 0011 | 0000	195.1.1.48
4	195.1.1. 0100 | 0000	195.1.1.64
5	195.1.1. 0101 | 0000	195.1.1.80
6	195.1.1. 0110 | 0000	195.1.1.96
7	195.1.1. 0111 | 0000	195.1.1.112
8	195.1.1. 1000 | 0000	195.1.1.128
9	195.1.1. 1001 | 0000	195.1.1.144
10	195.1.1. 1010 | 0000	195.1.1.160
11	195.1.1. 1011 | 0000	195.1.1.176
12	195.1.1. 1100 | 0000	195.1.1.192
13	195.1.1. 1101 | 0000	195.1.1.208
14	195.1.1. 1110 | 0000	195.1.1.224

Bild: Netzklasse C - Adresse 195.1.1.0 /28

Subnetzmaske: 255.255.255.248
(1111 1000)
Subnetze : $2^5 - 2 = 30$
Hosts pro Subnetz : $2^3 - 2 = 6$

14 • 2 Subnetze

- Nicht erlaubt ist
  Subnetz 0 (Netz ID .0)
  Subnetzbroadcast (Netz ID .248)
- 180 von 254 Host-Adressen
  werden verwendet (70,8%)

Subnetz	Subnetz-ID	Subnetz-ID
1	195.1.1. 0000 1 | 000	195.1.1.8
2	195.1.1. 0001 0 | 000	195.1.1.16
3	195.1.1. 0001 1 | 000	195.1.1.24
4	195.1.1. 0010 0 | 000	195.1.1.32
5	195.1.1. 0010 1 | 000	195.1.1.40
6	195.1.1. 0011 0 | 000	195.1.1.48
7	195.1.1. 0011 1 | 000	195.1.1.64
24	195.1.1. 1100 0 | 000	195.1.1.194
25	195.1.1. 1100 1 | 000	195.1.1.202
26	195.1.1. 1101 0 | 000	195.1.1.210
27	195.1.1. 1101 1 | 000	195.1.1.216
28	195.1.1. 1110 0 | 000	195.1.1.224
29	195.1.1. 1110 1 | 000	195.1.1.232
30	195.1.1. 1111 0 | 000	195.1.1.240

2•1 +14•2 = 30 Subnetze

Bild: Netzklasse C - Adresse 195.1.1.0 /29

Subnetzmaske: 255.255.255.252
(1111 1100)
Subnetze : $2^6 - 2 = 62$
Hosts pro Subnetz : $2^2 - 2 = 2$

14 • 4 Subnetze

- Nicht erlaubt ist
  Subnetz 0 (Netz ID .0)
  Subnetzbroadcast (Netz ID .252)
- 124 von 254 Host-Adressen
  werden verwendet (48,8%)

Subnetz	Subnetz-ID	Subnetz-ID
1	195.1.1. 0000 01 | 00	195.1.1.4
2	195.1.1. 0000 10 | 00	195.1.1.8
3	195.1.1. 0000 11 | 00	195.1.1.12
4	195.1.1. 0001 00 | 00	195.1.1.16
5	195.1.1. 0001 01 | 00	195.1.1.20
6	195.1.1. 0001 10 | 00	195.1.1.24
7	195.1.1. 0001 11 | 00	195.1.1.28
56	195.1.1. 1110 00 | 00	195.1.1.224
57	195.1.1. 1110 01 | 00	195.1.1.228
58	195.1.1. 1110 10 | 00	195.1.1.232
59	195.1.1. 1110 11 | 00	195.1.1.236
60	195.1.1. 1111 00 | 00	195.1.1.240
61	195.1.1. 1111 01 | 00	195.1.1.244
62	195.1.1. 1111 10 | 00	195.1.1.248

2•3 +14•4 = 62 Subnetze

Bild: Netzklasse C - Adresse 195.1.1.0 /30

Subnetzmaske: 255.255.255.240 (1111 0000)

Subnetze: $2^4 - 2 = 14$
Hosts pro Subnetz : $2^4 - 2 = 14$

Subnetz 1

Host number		
	195.1.1. 0001 | 0000	Netz ID = 195.1.1.16
Host 1	195.1.1. 0001 | 0001	Host ID = 195.1.1.17
Host 2	195.1.1. 0001 | 0010	Host ID = 195.1.1.18
----------	195.1.1. 0001 | ------	----------
Host 14	195.1.1. 0001 | 1110	Host ID = 195.1.1.30
Broadcast	195.1.1. 0001 | 1111	Broadcast ID = 195.1.1.31

Subnetz 2

Host number		
	195.1.1. 0010 | 0000	Netz ID = 195.1.1.32
Host 1	195.1.1. 0010 | 0001	Host ID = 195.1.1.33
Host 2	195.1.1. 0010 | 0010	Host ID = 195.1.1.34
----------	195.1.1. 0010 | ------	----------
Host 14	195.1.1. 0010 | 1110	Host ID = 195.1.1.46
Broadcast	195.1.1. 0010 | 1111	Broadcast ID = 195.1.1.47

4-Bit Subnetzmaske

Subnetzmaske: 255.255.255.240 (1111 0000)
Subnetze : $2^4 - 2 = 14$
Hosts pro Subnetz : $2^4 - 2 = 14$

195.1.1.0	**Subnetz 0** (Ungültige Host-Adressen)
195.1.1.1	
195.1.1.2	

195.1.1.15	

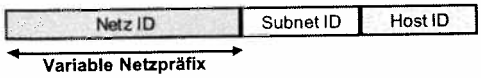
195.1.1.16	(Ungültige Host-Adressen) **Subnetz 1**
195.1.1.32	**Subnetz 2**
195.1.1.48	**Subnetz 3**
--------	--------
195.1.1.224	**Subnetz 14**

195.1.1.31	**Broadcast** (Ungültige Host-Adressen) **in Subnetz 1**
195.1.1.47	**in Subnetz 2**
195.1.1.63	**in Subnetz 3**
--------	--------
195.1.1.239	**in Subnetz 14**

195.1.1.240	(Ungültige Host-Adressen)
195.1.1.241	

195.1.1.254	
195.1.1.255	**Broadcast in allen Subnetzen**

Bild: Netzklasse C - Adresse 195.1.1.0 /28



Ersetzen der festen Netzklassen durch Netz-Präfixe variabler Länge (13 bis 27 Bit)

Beispiel: 129.24.12.0/14
Die ersten 14 Bit der IP-Adresse werden für die Netz-Identifikation verwendet

Einsatz in Verbindung mit hierarchischem Routing
- Backbone-Router betrachtet nur z.B. die ersten 13 Bit (kleine Routing-Tabellen, wenig Rechenaufwand)
- Router eines angeschlossenen Providers z.B. die ersten 15 Bit
- Router in einem Firmennetz mit 128 Hosts betrachtet 25 Bit

Durch geschickte Adressvergabe können mehrere ursprüngliche Netze der Klasse C durch ein einziges Präfix zusammengefasst werden

Bild: Variable Netzmaske

Wiederholte Zusammenfassung führt zu kürzeren Präfixes der IP-Adressen

Vorteil: Reduzierung der Grösse von Routingtabellen
Auffinden des „Longest Matching Prefix"

Class C ist auch nach dem geographischem Vorkommen unterteilt
Europa: 194.0.0.0 – 195.255.255.255

CIDR und Subnetze

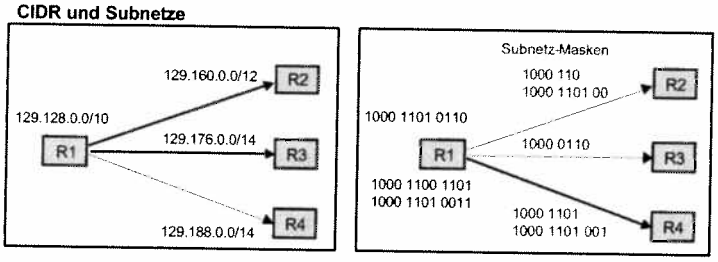


Bild: CIDR: Classless Inter-Domain Routing

Adressierung im Internet mit IPv6

Adressstruktur von IPv6

Bereits Anfang der 90er Jahre war festzustellen, dass der auf dem Protokoll IPv4 basierende Adressraum bei dem weiteren rapiden Internet-Wachstum bald zu knapp sein würde. Einer der Hauptgründe, ein neues IP-Protokoll zu entwickeln, war die Erweiterung der Adressierung. Die Adresslänge in IPv6 wird auf das Vielfache - jeweils 128 Bits für Quell- und Zieladresse - im Vergleich zu der Adresslänge 32 Bits beim IP4 erweitert. Somit sind im Prinzip 2^{128} Adressen beim IPv6 verfügbar. Dies bedeutet die Vergrößerung des Adressraums um den Faktor 2^{96}. Ähnlich wie beim Protokoll IP4 identifiziert eine IP-Adresse nicht eine ganze Station, sondern deren Interface als ein physikalischer Port (Netzanschluss). Beispielsweise werden einer Station, die an zwei Netzen (Dual Homing) angeschlossen ist, zwei IP-Adressen zugeteilt.

Im allgemeinen wird zwischen folgenden Kategorien von IPv6-Adressen unterschieden:

- Unicast
- Multicast
- Anycast

Die Unicast-Adressen werden für die Unterstützung von Punkt-zu-Punkt-Verbindungen verwendet. Somit repräsentiert dieser Typ die häufigste Adressierungsart, bei der ein Quellsystem die Daten an ein direkt angegebenes Zielsystem sendet. Eine Unicast-Adresse identifiziert einen Interface in einer Station.

Eine Multicast-Adresse identifiziert eine Gruppe von Interfaces. Ein Paket mit einer Multicast-Adresse wird an die Interfaces aller Stationen einer Gruppe direkt übermittelt.

Eine Anycast-Adresse identifiziert ebenfalls eine Gruppe von Stationen, genauer gesagt eine Gruppe von Prozessen. Der Unterschied zwischen Multicast- und Anycast-Adressen besteht in der Übermittlung von Paketen. Die Anycast-Adressen ermöglichen den Versand von Paketen über eine festgelegte Stelle an alle Stationen aus einer Gruppe. Ein Paket mit einer AnycastAdresse wird zuerst an eine Station aus der Gruppe (z.B. einen speziellen dedizierten-Router) übergeben, die im nächsten Schritt das empfangene Paket an die weiteren Stationen aus dieser Gruppe verteilt. Die AnycastAdressen unterstützen also eine Art der Verteilung der Pakete und erlauben, unterschiedliche Rechner zu einer funktionellen Gruppe zusammenzufassen.

IPv4: gruppiert dezimal (Dotted-Decimal): **195.30.40.50**

IPv6: gruppiert hexadezimal (Colon-Hex)

ABCD:0000:0000:0000:1234:0000:0000:EFFF

- Nullen am Anfang jeder Gruppe dürfen weggelassen werden
- Nur eine Null-Zwischengruppe darf weggelassen werden
  ABCD::1234 :0000:0000:EFFF
  ABCD:0000:0000:0000:1234::EFFF
- Letzte 4 Byte (32 Bit) können auch gruppiert dezimal (dotted-decimal) geschrieben werden (Kompatibilität mit IPv4)
  ::195.30.40.50
- Präfix Angabe durch /Maskenlänge
  1234:ABDC:0007:0000:0000:0000:0000:0000 /40
  1234:ADCB:7::/40

Bild: IP-Adressendarstellung

Darstellung von IPv6-Adressen

Die IPv6-Adressen haben im allgemeinen folgende Form:
X:X:X:X:X:X:X:X
wobei jedes X-Zeichen einen 16-Bit-Wert in hexadezimaler Schreibweise darstellt. Eine IPv6-Adresse kann also folgendermaßen aussehen
ADCF:0005:0000:0000:0000:0000:0600:FEDC
Die führenden Nullen können weggelassen werden. Somit ist es erlaubt, z.B.
0 statt 0000 5 statt 0005 600 statt 0600
zu schreiben. Hierdurch lässt sich die bereits erwähnte Adresse nun in der gekürzten Form
ADCF:5:0:0:0:0:600:FEDC
darstellen.

Ebenso können mehrere aufeinanderfolgende Null-Werte unterdrückt und durch "::" abgekürzt werden. Eine korrekte Schreibweise für die eben gezeigte Adresse wäre damit auch:
ADCF:5::600:FEDC

Volle Darstellung

- ADCF:BA56:600:FEDC:0:0:0:0
- 0:0:0:0:ADCF:BA56:600:FEDC
- 0:0:0:ADCF:BA56:0:0:0

Vereinfachte Darstellung

- ADCF:BA56:600:FEDC::
- ::ADCF:BA56:600:FEDC
- ::ADCF:BA56:0:0:0 oder
- 0:0:0:ADCF:BA56::

Das Symbol "::" darf nur an einer Seite der Adresse verwendet werden. Die Darstellung
::ADCF:BA56:: als 0:0:0:ADCF:BA56:0:0:0
ist nicht eindeutig.

- **128 Bit (feste Länge)**
- $2^{128} = 3.4 \times 10^{38}$ Adressen ⇒ $665*10^{21}$ Adressen pro m^2 der Erdoberfläche
- 128 Bit anstatt 32 Bit
  ⇒ 340 282 366 920 938 463 463 374 607 431 768 211 456 ($3*10^{38}$) Hosts
  ⇒ 665 570 793 348 866 943 898 599 Hosts pro m^2 der Erdoberfläche
- Bei einer Adresszuweisungsrate von 10^6 /µs, würde es 20 Jahre dauern

- 32 Bit ⇒ 4×10^9 Hosts (durch die Klasseneinteilung sind nicht alle Adressen vorhanden)
- Hierarchische Zuweisung ⇒ verschnitt wie in der Telefonie
- Erwartete Ausnutzungsgrad von $8*10^{17}$ bis $2*10^{33}$ Adressen
- $8*10^{17}$ ⇒ 1 564 Adressen pro m^2 der Erdoberfläche
- 85% noch nicht zugeordnet

- mehrere Schnittstellen (Interfaces) pro Host und mehrere Adressen pro Schnittstelle
- Unicast, Multicast, Anycast
- Adressenzuweisung: Provider-basierend, lokal pro Netzbereich, lokal pro Anschluss

Bild: Anzahl IPv6-Adressen

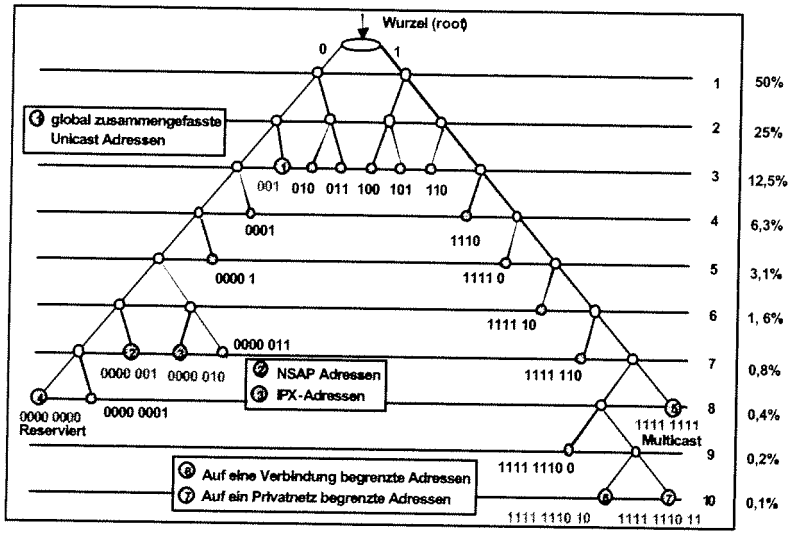


Bild: IPv6: Binäre Präfixwerten

Aufteilung des IPv6-Adressraums

Im Gegensatz zur einfachen Unterteilung von Adressen nach Klassen A bis E in Netzen beim IPv4-Einsatz ist die Unterscheidung von Adresstypen beim Protokoll IPv6 sehr flexibel und somit aufwendiger. Um welchen Adresstyp es sich handelt, bestimmt ein sogenannter Formatpräfix, der eine variable Länge besitzt und durch die ersten (von links gelesen) Bits bestimmt wird. Durch den Präfix-Einsatz kann der ganze Adressraum auf bestimmte Adressklassen aufgeteilt werden. Mit dessen Hilfe lassen sich bestimmte Spezialadressen kennzeichnen, wie z.B. Multicast, Aggregatable Global, Link Local Use oder Site Local Use.

Beim Protokoll IPv6 wird im allgemeinen unterscheiden zwischen

- Unicast-Adressen,
- Multicast-Adressen.

Zwei Unicast-Adressen legen eine Punkt-zu-Punkt Verbindung fest, so dass dieser Typ von Adressen am häufigsten verwendet wird. Eine Unicast-Adresse identifiziert eindeutig einen physikalischen Anschlussport (Interface) in einer Station. Ist eine Systemkomponente (z.B. ein Server bzw. ein Router) über mehrere Netze erreichbar, d.h. wird sie an mehreren Netzen angeschlossen, muss jedem Anschlussport eine Unicast-Adresse zugeteilt werden. Enthält eine Systemkomponente zwei Adressen, wird sie als Dual-Homing bezeichnet.

Es werden auch einige Adressformate reserviert, um die anderen bekannten Adressen in die IPv6-Adressen einbetten zu können. Hierzu gehören die IPv6-Adressen für die Übertragung:

- von NSAP-Adressen, d.h. OSI-Adressen (Präfix 0000 001),
- von IPX-Adressen (Präfix 0000 010).

Unicast-Adressen von IPv6

Unter den Unicast-Adressen sind wiederum folgende Klassen zu unterscheiden:

- **Provider Based Global Unicast Addresses:** Diese Klasse von Adressen werden für normale Punkt-zu-Punkt-Kommunikation verwendet und unterscheidet sich von anderen Adressen durch das Präfix 010. Ein Achtel des Adressraums wird für diese Klasse eingeräumt und dem Präfix nur 3 Bits zugeordnet.
- **Aggregatable Global Unicast Addresses:** Diese aggregierbaren globalen Unicast-Adressen unterscheiden sich von anderen Adressen durch das Präfix 001 und sind auch für normale Punktzu-Punkt-Verbindungen vorgesehen.
- **Adressen von lokaler Bedeutung:** Hierbei werden zwei Arten definiert:
  - Link Local Use Unicast Addresses,
  - Site Local Use Unicast Addresses.

Diese Adressen können nur ohne Internet-Anbindung verwendet werden.

- Spezielle Unicast-Adressen: Zu dieser Klasse gehören vor allem:
- IPv4-kompatible IPv6-Adressen und
- IPv4-mapped IPv6-Adressen.

Diese Adressen werden für die Kommunikation zwischen den Endsystemen mit dem klassischen Protokoll IP4 und den Endsystemen mit dem neuen Protokoll IPv6 verwendet. Diese speziellen Adressen sind von großer Bedeutung bei der Migration zum IPv6-Einsatz, insbesondere wenn die beiden Protokolle in einem Netz implementiert werden.

Die einzelnen Typen von Unicast-Adressen werden nun näher dargestellt.

Provider-basierte globale Unicast-Adressen

Eines der größten Probleme beim Protokoll IPv4 ist der Umfang von Routing-Tabellen in großen Netzen und die damit verbundenen Leistungseinbußen. Dies ergibt sich aus der klassenbasierten Aufteilung der Internet-Adressen nach dem Protokoll IPv4, was durch die Einführung des Classless Inter Domain Routing (CIDR) jedoch abgemildert werden konnte. Bei diesen Adressen wird der ganze Adressraum direkt auf die einzelnen Netze aufgeteilt, ohne irgendwelche Verweise auf die Lokation der Netze auf der Erdkugel zu geben.

Die IPv4-Adressen haben den Nachteil, dass sie keine Hierarchie in dem Hierarchien Sinne bilden, dass es möglich wäre, auf die Lokation eines Netzes auf der Erdkugel zu verweisen. Durch eine mehrstufige Strukturierung von Adressen und Bildung

einer Hierarchie von Subnetzen lässt sich das Wachsen von Routing-Tabellen noch in akzeptierten Grenzen halten und damit auch die Verzögerung der Pakete in Routern.

Die Provider-basierten Unicast-Adressen werden von anderen Klassen von Adressen durch das Präfix 010 unterschieden. Diese Adressen werden in erster Linie von den jeweiligen internationalen Organisationen verwaltet. Registry-ID (kurz Reg-ID) bezieht sich auf die internationale "Registrierungs"-Organisation, bei der diese Adresse registriert wird.

Beispielsweise gelten zur Zeit. folgende Reg-ID-Zuweisungen:

- Reg-ID = 10000: ICAN (Internet Corporation for Assigned Names and Numbers - http://www.icann.org/),
- Reg-ID = 01000: RIPE (Reseau IP European, Regional Internet Registryfor Europe - http://www.ripe.net/),
- Reg-ID = 11000: InterNIC (Internet Information Center),
- Reg-ID = 00 100: APNIC (Asia Pacific Internet Information Center).

Durch die n-Bit-Angabe im Feld Provider-ID wird der Anbieter der Internet-Dienste identifiziert. Die Länge der Provider-ID kann variabel sein. Dadurch kann jede der bereits erwähnten internationalen Organisationen Provider-IDs von beliebiger Länge zulassen und auf diese Art und Weise verschiedene Klassen von Anbietern bilden. Wird eine kurze Provider-ID (n klein) einem großen weltweit agierenden Anbieter zugewiesen, so kann er eine große Anzahl von Netzbetreibern mit Subscriber-ID (56-n Bits) definieren. Eine Subscriber-ID stellt die Identifikation des Betreibers eines privaten Netzes dar und ist mit der Netz-ID bei der IPv4-Adresse zu vergleichen.

Eine internationale Organisation für die Registrierung von IPv6-Adressen kann mehrere nationale Organisationen mit den Adressen versorgen. Eine internationale Organisation kann mehrere nationale Organisationen für die Vergabe von Adressen koordinieren. Diese nationalen Organisationen werden mit National-Registry-ID) identifiziert.

Die letzten 64 Bits jeder Adresse werden als Intra-Subscriber bezeichnet und definieren die interne Netzstruktur bei einem Netzbetreiber. Für die Identifikation der Subnetze dient Subnet-ID. Die letzten 48-Bits als Interface-ID ermöglichen es, die Endsysteme in einem Subnetz zu identifizieren.

An dieser Stelle ist darauf hinzuweisen, dass man beim Protokoll IPv6 von Interface-ID statt Host-ID spricht. Die Interface-ID in der IPv6-Adresse entspricht vollkommen der Host-ID in der IPv4-Adresse. Ist ein Endsystem an unterschiedliche Netze (WANs bzw. LANs) angeschlossen, so hat es mehrere physikalische Ports und somit auch mehrere Interface-IDs. Ein Interface-ID ist somit als eine physikalische Netzadresse zu interpretieren.

Die öffentliche Struktur der Adresse beschreiben die Teile: Registry-ID, National Registry-ID und Provider-ID. Diese Angaben ermöglichen, im Gegensatz zur IPv4-Adresse, eine Provider-basierte globale IPv6-Adresse auf der Erdkugel schnell zu lokalisieren. Durch die Lokalisierung von Adressen ist u.a. das weltweit hierarchische Routing möglich, so dass die IPv6-Pakete oft über die von vornherein bekannten internationalen Routen transportiert werden können.

An dieser Stelle ist eine Besonderheit von IPv4-Adressen hervorzuheben: Die Interface-ID repräsentiert eine Netzadresse eines Ports im Endsystem und enthält 48 Bits. Jede physikalische Adresse in Shared Medium LANs (d.h. jede MAC-Adresse) ist ebenfalls 48 Bits lang. Im Feld Interface-ID kann eine MAC-Adresse eingebettet werden.

Somit weist jede IPv6-Adresse zwei wichtige Besonderheiten auf

- sie ist weltweit eindeutig,
- sie enthält die physikalische Netzadresse des Endsystems.

Im Gegensatz zu den IPv4-Adressen ist in den IPv6-Adressen die Zuordnung IPv6-Adresse zu MAC-Adresse enthalten - der große Vorteil von IPv6-Adressen (möglicherweise aber auch ihr größter Nachteil). Aus diesem Grund ist das Hilfsprotokoll ARP beim Protokoll IPv6 nicht notwendig, was auch bestimmte Auswirkungen auf die Funktionsweise von IPv6-Routem hat.

Da IPv6-Adressen die physikalische Netzadresse bereits enthalten, ist eine automatische Adresskonfiguration (sog. Stateless Autoconfiguration) möglich.

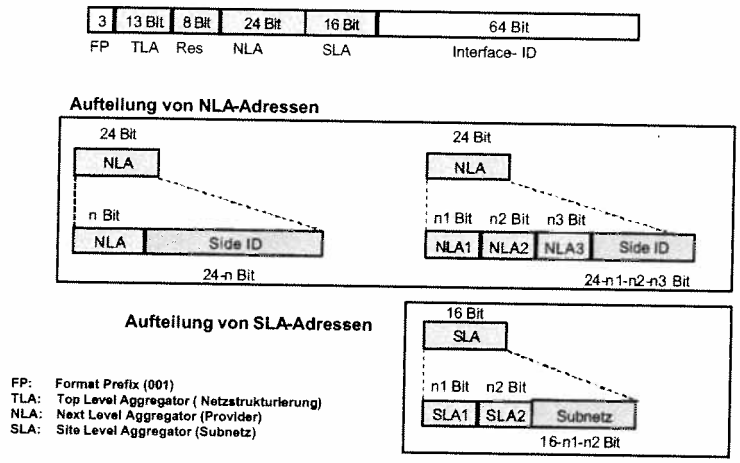


Bild: IPv6-Adressstruktur

Aggregierbare globale Unicast-Adressen

Eine zweite Klasse von IPv6-Adressen für die Punkt-zu-Punkt-Kommunikation bilden sogenannte aggregierbare globale Unicast-Adressen (Aggregatable Global Unicast Addresses). Diese Adressen werden im Internet-Standard RFC 2374 festgelegt und sollten die Provider-basierten globalen Adressen ersetzen. Im folgenden werden sie kurz AG-Unicast-Adressen (AG: Aggregierbar Global) genannt..

Beim Entwurf von AG-Unicast-Adressen wurde davon ausgegangen, dass die gesamte Internet-Welt organisatorisch gesehen eine hierarchische Aggregation Struktur aufweist. An der Spitze dieser Hierarchie (Top Level) stehen internationale und nationale Organisationen wie z.B. Anbieter der Netz- bzw. Internet-Dienste.

Der ganze Raum von AG-Unicast-Adressen wird zunächst auf jene Top-Level-Organisationen aufgeteilt, die als internationale Verwaltungen von IPv6-Adressen fungieren. Hierfür dient die Angabe TLA-ID (Top Level Aggregation Identifier) in den AG-Unicast-Adressen. Die TLA-ID in den AG-Unicast-Adressen entsprechen vollkommen der Registry-ID in den Provider-basierten Unicast-Adressen.

Die nächste Stufe (Next Level) in dieser Hierarchie bilden weitere Organisationen, die einerseits als Verwaltungen von IPv6-Adressen bzw. als Anbieter der Netz- und Internet-Dienste fungieren können. Diese Organisationen können ebenfalls in einer Hierarchie zueinander stehen. Auf der letzten Stufe stehen individuelle Institutionen als "Endbenutzer" der Internetdienste. Die eben geschilderte Hierarchie im Bereich der Internet-Welt findet in den AG-Unicast-Adressen ihre Berücksichtigung.

Die einzelnen Angaben in den AG-Unicast-Adressen haben hier folgende Bedeutung:

- **Format Präfix:** Die Bitkombination 001 dient den AG-Unicast-Adressen als Identifikation und ermöglicht, diesen Adresstyp von anderen Adresstypen zu unterscheiden.
- **NLA-ID (Next Level Aggregation Identifier):** Eine Top-Level-Organisation mit einem Identifikator TLA-ID kann ihren Adressraum an die weiteren Organisationen der nächsten Hierarchiestufe mit Hilfe des Identifikators NLA-ID aufteilen. Der NLA-ID kann weiter strukturiert werden, so dass sich die hierarchische Struktur zwischen den einzelnen Organisationen in den Adressen abbilden lässt. Diese Struktur stellt quasi eine öffentliche Struktur innerhalb der Internet-Welt dar.
- **SLA-ID (Site Level Aggregation Identifier):** An dieser Stelle wird die Identifikation einer individuellen Organisation (eines Kunden) als Endbenutzer angegeben. Der SLA-ID-Inhalt kann weiter hierarchisch strukturiert, um eine Subnetz-Hierarchie innerhalb eines physikalischen großen Netzes adressieren zu können. Man kann hier von einer privaten Struktur sprechen.
- **Interface-ID (Interface Identifier):** Dieses Feld enthält den Identifikator eines physikalischen Ports in einem Endsystem, einen Router etc. Im allgemeinen ist die Interface-ID als eine physikalische (auch sog. Link-) Netzadresse eines Ports in einem Endsystem zu interpretieren.

Der Adressraum einer Top-Level-Organisation TLA-ID kann mit dem Identifikator TLA-ID auf Teil-Adressräume von weiteren (z.B. nationalen) Organisationen aufgeteilt werden. Mit einem Identifikator NLA-ID kann entweder eine Organisation oder eine hierarchische Struktur von Organisationen identifiziert werden. Im allgemeinen können die Angaben NLA-ID und SLA-ID weiter strukturiert werden. Durch die Strukturierung der N-LA-ID lässt sich eine weitgehende Hierarchie innerhalb der öffentlichen Struktur aufstellen. Durch die weitere Strukturierung der SLA-ID lässt sich die Netzstruktur eines Netzbetreibers hierarchisch strukturieren.

Der NLA-ID kann als Adressraum mit der Länge von 24 Bits weiter strukturiert werden, um eine hierarchische Struktur von Organisationen in Adressen zu berücksichtigen. Aufgrund der so strukturierten globalen Adressen lässt sich Routing in großen Level-Netzen vereinfachen.

Hat eine Next-Level-Organisation A_i (z.B. eine nationale Organisation) von der Top-Level-Organisation mit TLA-ID eine Identifikation NLA-ID erhalten, so kann diese Organisation A_i für sich die ersten m Bits vom NLA-ID als eigener Identifikator NLADI-ID reservieren. Das restliche 24-m Bits lange Feld, Site-ID, stellt einen Adressraum dar, der wiederum aufgeteilt werden kann. Somit können weitere Organisationen (Institutionen, Provider) B_j, j = 1, 2, ... sich den (24-m)-Bit-langen Adressraum teilen. Jede dieser Organisationen kann wiederum einen Identifikator NLA2-ID mit n Bits für sich festlegen und die restlichen 24-m-n Bits als Adressraum an weitere Organisationen C_k, k = 1, 2, ... zur Verfügung stellen. Diese Organisation C_k

kann einen o Bits langen Identifikator NLA2-ID) als eigene "Vorwahl" nutzen und die restlichen 24-m-n-o Bits als Adressraum für individuelle Organisationen bzw. Unternehmen nutzen.

Es lässt sich auf die gleiche Weise auch das Feld NLA-ID strukturieren. Private Netzstrukturen können somit auf Grundlage der Identifikator Site-ID im Feld NLA-ID gekennzeichnet und hierarchisch adressiert werden.

Eine Organisation in ihrer weltweit verteilten Netzstruktur kann die Komponenten effektiv adressieren. Hierfür nutzt sie das Feld SLA-ID als einen eigenen Adressraum. Mit dem Identifikator SLA1-ID kann sie die Standorte auf den einzelnen Kontinenten kennzeichnen. Der Rest als Subnet-ID kann wiederum in SLA2-ID) und Subnet-ID aufgeteilt werden. Der Identifikator SLA2-ID) kann dem Standort innerhalb eines Landes zugeteilt werden. Das Feld Subnet-ID ermöglicht es, die einzelnen Subnetze innerhalb eines Landes zu identifizieren.

Man kann sich auch andere Beispiele für die SLA-ID-Aufteilung vorstellen. Handelt es sich um eine Netzstruktur innerhalb eines Standortes, wie dies häufig der Fall sein wird, so setzt sich diese Netzstruktur aus den Teilnetzen innerhalb einzelner Gebäude zusammen. Ein Teilnetz in einem Gebäude enthält einige Subnetze, wie z.B. Etagennetze bzw. virtuelle LANs. Um die Komponenten innerhalb einer solchen Netzstruktur effektiv zu identifizieren, kann das Feld NLA-ID einer Adresse ähnlich aufgeteilt werden. Dies würde weitgehend der Subnetzbildung beim Protokoll IPv4 entsprechen.

Wie hier geschildert wurde, lässt sich jede AG-Unicast-Adresse mehrstufig strukturieren. Dadurch lassen sich sowohl große als auch kleine Organisationen bzw. Anbieter der Internet-Dienste definieren.

Globale Unicast IPv6-Adressen und MAC-Adressen in LANs

Beim Routing von IPv6-Paketen in IPv4-Netze ist folgendes Problem zu lösen: Der letzte Router auf einem Datenpfad erhält ein IP-Paket, das zu einem Endsystem im LAN weitergeleitet werden soll, aber im IP-Paket ist nur Ziel-IP-Adresse enthalten. Der Router (als der letzte unterwegs) muss ins LAN den vollständigen MAC-Frame mit der Ziel-MAC-Adresse wegsenden. Um die richtige Ziel-MAC-Adresse (d.h. physikalische Host-Adresse) zu ermitteln, nutzt der Router das Hilfsprotokoll ARP (Address Resolution Protocol). Dieses Protokoll hat die Aufgabe, die Zuordnung: Ziel-IP-Adresse zu Ziel-MAC-Adresse zu bestimmen.

Auf die Funktion des Hilfsprotokolls ARP könnte man verzichten, wenn eine Protokolladresse den Bezug zur entsprechenden physikalischen Adresse hätte. Dieser Ansatz wird bei den globalen Unicast-IPv6-Adressen verfolgt. Hier wird eine MAC-Adresse im Feld Interface-ID eingebettet. Damit lässt sich die MAC-Adresse als physikalische LAN-Adresse aus der IPv6-Protokolladresse direkt ableiten, so dass man auf das Protokoll ARP beim IPv6 vollkommen verzichten kann.

Beim Einkapseln ins Feld Interface-ID wird die MAC-Adresse aufgeteilt. Der erste Teil Hersteller-ID (Company-ID) wird direkt nach dem Feld SLA-ID untergebracht danach folgen zwei Füll-Bytes mit den Bitkombinationen x'FF' und x'FE', und anschließend wird die Manufacturer-Selected Extension ID eingetragen.

Unicast-Adressen von lokaler Bedeutung

Wie bereits erwähnt, werden zwei Arten von Unicast-Adressen für lokale Nutzung definiert:

- Link Local Use Unicast Addresses
- Site Local Use Unicast Addresses

Es handelt sich bei Link Local Use Unicast Addresse (kurz LLU-Unicast-Adresse) um eine unstrukturierte Adresse. Da die LLU-Unicast-Adressen keine Identifikation von Subnetzen enthalten, können sie nur innerhalb isolierter IPv6-Subnetze verwendet werden. Die LLU-Unicast-Adressen dürfen von Routern nicht weitergeleitet werden, z.B. können sie nicht ins Internet geschickt werden.

Site Local Use Unicast Addresses (kurz SLU-Unicast-Adressen) sind strukturiert. Da die SLU-Unicast-Adressen keine weitere Identifikation höherer Hierarchie als Subnetz-IDs enthalten, können sie nur innerhalb einer Gruppe von IPv6-Subnetzen innerhalb eines isolierten Standorts (Site) verwendet werden. Die SLU-Unicast-Adressen ermöglichen, innerhalb einer nicht an das globale Internet angeschlossenen Organisation eindeutige Adressen zu vergeben, ohne dafür global eindeutige Adressen verwenden zu müssen. Die SLU-UnicastAdressen sind nur innerhalb einer Organisation eindeutig und dürfen von Routern nach außen (z.B. ins Internet) nicht weitergeleitet werden.

Spezielle Unicast-Adressen von IPv6

Beim IPv6 werden einige spezielle Unicast-Adressen eingeführt. Es handelt sich hierbei um:

- unspezifizierte Adressen (Unspecified Addresses),
- Loopback-Addressen,
- IPv6-Adressen mit eingekapselten IPv4-Adressen.

Diese unspezifizierte Adresse ist 0:0:0:0:0:0:0:0 (oder einfach "::") und kann z.B. als Absenderadresse eines Endsystems verwendet werden, dem die Adresse(n) noch nicht zugeteilt wurde(n). Dies ist z.B. der Fall, wenn ein Endsystem ein IP-Paket sendet, damit es die eigene IP-Adresse erfährt.

Die Loopback-Adresse ist 0:0:0:0:0:0:0:1 (oder einfach "::1") und wird in IP-Paketen genutzt, die zwischen den Programmen innerhalb eines Rechner (z.B. beim Testen) ausgetauscht werden. Diese Adresse kann weder Quell- noch Zieladresse von Paketen sein, die ein Endsystem bzw. einen Router verlassen.

Es werden zwei Arten von IPv6-Adressen mit eingekapselten IPv4- Adressen unterschieden:

- IPv4-kompatible IPv6-Adressen
- IPv4-mapped IPv6-Adressen

Diese Unicast-Adressen werden als IPv4-basierte Adressen bezeichnet.

Wie hier zu sehen ist, ergänzen die beiden Adresstypen eine 32-Bit-lange alte" IPv4-Adresse zu der vollen Länge der IPv6-Adresse. Diese Adresstypen werden mit Hilfe des 80-Bit-langen Präfixes 000 ... 0 identifiziert. Die nächsten 16-Bits ermöglichen es, diese beiden Adresstypen voneinander zu unterscheiden. Diese IPv4-basierten IPv6-Adressen werden bei der Migration zum IPv6-Einsatz verwenden, d.h. in Netzen, in denen die Systemkomponenten mit dem Protokoll entweder IPv4 oder IPv6 bzw. mit den beiden Protokollen IP4 und IPv6 betrieben werden.

Multicast- und Anycast-Adressen

Eine Multicast-Adresse identifiziert eine Gruppe von Systemen. Ein Paket, das an eine Multicast-Adresse gesendet werden soll, wird normalerweise an alle Systeme der Gruppe gesendet. Beim IPv6 gibt es keine BroadcastAdressen. Diese Funktion wird durch Multicast-Adressen erfüllt. Die Broadcast-Adresse entspricht somit der "All-Nodes"-Multicast-Adresse.

Die einzelnen Angaben haben hier folgende Bedeutung:

- Präfix: Die Bitkombination 1111 1111 deutet auf eine Multicast-Adresse hin.
- Flags: Die ersten drei Bits sind zur Zeit reserviert und müssen auf 0 gesetzt werden. Das Bit T hat folgende Bedeutung:
- T = 0: eine ständig zugeordnete (d.h. well-known) Multicast-Adresse,
- T = 0: eine temporär zugeordnete Multicast-Adresse.
- Scope (Gültigkeitsbereich): Hier wird der Gültigkeitsbereich eines Multicast-Paketes angegeben.
- Group-ID (Gruppen-ID): Dieses Feld kennzeichnet unabhängig vom Scope-Wert ob es sich bei der Multicast-Adresse um eine permanente oder um eine nur vorübergehend gültige Adresse handelt.

Multicast-Adressen dürfen nicht als Quell-Adressen erscheinen.

Adressierung im Internet (Email-Adresse, Adressauflösung, DNS, URL)

Adressauflösung

Da im Ablauf eines Kommunikationsvorgangs mehrere OSI-Schichten beteiligt sind, werden auch die Adressen dieser Schichten benötigt. Beim Übergang zwischen Schichten müssen demzufolge Adressen ineinander abgebildet werden, dieser Vorgang wird als **Adressauflösung** (address resolution) bezeichnet. Auf den höheren Schichten wird dies durch Verzeichnisdienste geleistet. Die Abbildung von Netzadressen in Hardwareadressen wird durch ARP (Address Resolution Protocol realisiert.

Adresszuweisung

Die einem Endsystem zugewiesene Adresse muss diesem mitgeteilt werden. Dafür gibt es grundsätzlich drei Möglichkeiten:

- Die Adresse wird **im Endsystem gespeichert.** Dies kann per Hardware (Schalter, PROM) oder Software (Festplatte) geschehen. Im einfachsten Fall erfolgt die Zuweisung lokal und manuell.
- Die Adresse wird in einem LAN-Server gespeichert und dem Endsystem auf Anfrage bzw. beim Booten mitgeteilt. Dies ist bei Endsystemen ohne permanente Speicher (Festplatte) sinnvoll, aber auch für die zentrale Konfiguration der Adressen (und weiterer kommunikationsrelevanter Informationen) über ein LAN. Hierfür sind die Protokolle BOOTP und DHCP verwendbar. PPP ermöglicht ebenfalls eine Adresszuweisung.
- Die Adresse muss nicht explizit mitgeteilt werden. Damit kann ein beliebiges Endgerät an das Netz angeschlossen und sofort genutzt werden (plug and play). Dies trifft für die MAC-Adresse von Ethernet-Adaptern zu, die nach IEEE 802 eindeutig einem bestimmten Adapter zugeordnet ist. Vorstellbar ist auch ein Verfahren, das eine noch nicht benutzte Adresse ermittelt und einem neuen Endsystem zuweist.

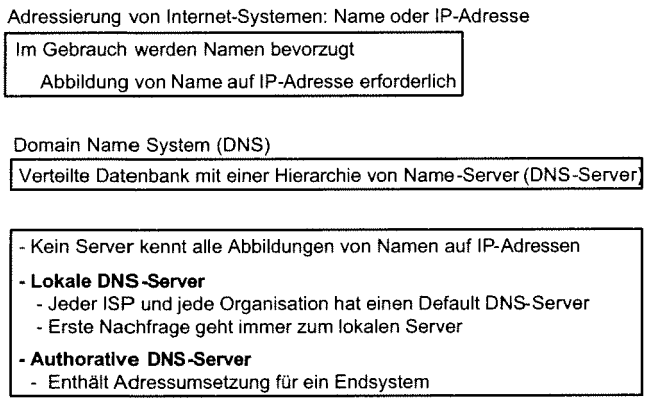


Bild: Namensdienst: Domain Name System (DNS)

Domain Name System

Bei der bisherigen Darstellung der Kommunikationsprinzipien in TCP/IP-Netzen wurde unterstellt, dass die IP-Adresse des Partners gegeben ist. Dies ist aber normalerweise nicht der Fall. Beim Aufruf einer WWW-Seite wird diese in Form eines sog. Uniform Resource Locators (URL) angesprochen. Teil dieser URL-Adresse ist der Name des Rechners (und der Domäne), der als WWW-Server dient. Um Rechnernamen in IP-Adressen zu konvertieren, wurde das Domain Name System (DNS) entwickelt, das ein weltweit verteiltes Verzeichnis von Internet-Namen darstellt.

Das System DNS ist so ausgelegt, dass sich die Benutzer die IP-Adressen von Rechnern nicht merken müssen, sondern statt dessen deren Namen verwenden können, um entfernte Rechner in TCP/IP-Netzen zu lokalisieren und um diese Verbindungen herzustellen. Obwohl DNS eigentlich für das Internet entwickelt wurde, lässt es sich auch in privaten TCP/IP-basierten Netzen einsetzen, wobei auch eine Ankoppelung an das Internet möglich ist.

Vor der Implementierung von DNS wurde die Zuordnung von IP-Adressen zu den Namen in einer zentralen Host-Tabelle (auch Host-Datei genannt) abgespeichert. Jede Host-Tabelle enthält eine Liste mit Host-Namen (Namen von Rechnern bzw. von anderen TCP/IP-Endsystemen) mit deren IP-Adressen. Mit dem ständigen Zuwachs an Rechnern in einem Netz und durch Integration einer immer größeren Zahl von Netzen in größeren Netzen wurde deutlich, dass die Ermittlung von IP-Adressen über zentrale Host-Tabellen keine richtige Lösung mehr ist. In einem großen Netz kann die Namensvergabe nicht den Entscheidungen der einzelnen Benutzer überlassen werden. Ein großes Netz wäre dann kaum noch zu verwalten. Das primäre DNS-Ziel war es, die Host-Tabellen durch eine verteilte und vernetzte Datenbank zu ersetzen. Mit der DNS-Hilfe ist es möglich, die Host-Namen - im gesamten Internet sowie in den privaten TCP/IP-basierten Netzen - so zu verwalten, dass sie weltweit eindeutig sind.

Ermittlung von Ziel-IP-Adressen

Ein DNS-System wird durch die Interaktion von zwei Komponenten implementiert:

- Resolver,
- Name-Server.

Das DNS funktioniert nach dem Client/Server-Prinzip. Der Resolver ist die Client-Software auf dem Rechner eines Benutzers, die DNS-Server abfragt, um Rechnernamen in IP-Adressen zu übersetzen. Der DNS-Server ist ein Programm in einem

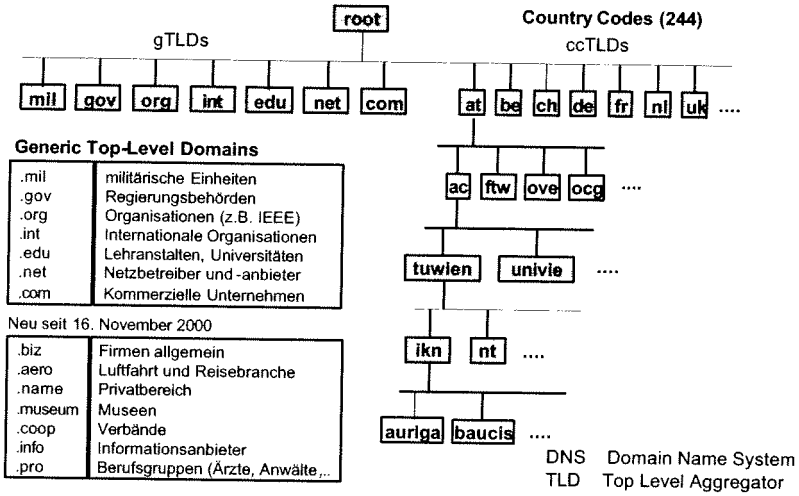
dedizierten Rechner, das auf eine Datei mit Host-Namen und ihren zugehörigen IP-Adressen zugreift, um die entsprechenden Anfragen des Resolvers zu beantworten. Somit sind Resolver Clients, die auf Name-Server zugreifen.

Mittels Name-Server Referrals ermittelt der Resolver einer Ziel-IP-Adresse über folgende Schritte:

1. Die Anwendung im Quellrechner (hier z.B. WWW-Browser) leitet eine Abfrage (Query) an den Resolver.
2. Der Resolver leitet die Abfrage an den lokalen Name-Server 1 weiter.

   Jeder Name-Server verfügt über eine Datenbank, in der u.a. die Zuordnungen Host-Name zu IP-Adresse enthalten sind. Es handelt sich hierbei nur um die Zuordnungen vom Host in einer Domain (Domäne), für die dieser Name-Server autorisiert ist. Ein Server kann ebenfalls über einen Cache verfügen, in dem er u.a. auch die Zuordnungen Host-Name zu IP-Adresse über eine festgelegte Zeit (z.B. 2 Tage) speichert. Diese Zuordnungen betreffen aber die fremden Hosts, die sich außerhalb seiner Domain befinden. Diese Zuordnungen repräsentieren einfach die Ergebnisse von früheren Abfragen. Antworten aus seinem Cache kennzeichnet der Name-Server als "not-authoritive Answer".

   a) Der lokale Name-Server findet die gesuchte Zuordnung Host-Name zu IP-Adresse weder in seiner eigenen Datenbank noch im Cache, so dass er diese Abfrage an einen übergeordneten Name-Server 2 weiterleitet.
   b) Name-Server 2 verweist den Name-Server 1 auf andere Name-Server, hier auf den Name-Server 3 im Zielnetz 2.
   c) Der lokale Name-Server 1 richtet die Abfrage an Name-Server 3 im Zielnetz.
   d) Name-Server 3 sendet die gesuchte Zuordnung.
3. Der lokale Name-Server 1 sendet die gesuchte Zuordnung an den Resolver im Rechner X. Der Resolver speichert diese Information in seinem Cache für eine eventuelle zukünftigen Nachfrage ab.
4. In diesem Schritt wird die gesuchte IP-Adresse der Anwendung übergeben.



Aufbau des DNS-Namensraums

Bei DNS handelt es sich um eine baumförmige weltweite Vernetzung einzelner Name-Server, die eine weltweit verteilte Datenbank bilden. Sie wird auch als DNS-Datenbank bezeichnet. Jedes Datenelement in einer verteilten DNS-Datenbank ist über einen Namen indiziert. Diese Namen sind im Grunde genommen nur Pfade in einem großen Baum. Dieser Baum besitzt ganz oben eine einzige Wurzel (Root), die man einfach "Root" nennt. Genau wie bei jedem anderen Dateisystem kann der DNS-Baum mehrere Abzweigungen haben, die als Knoten (nodes) dargestellt werden.

Bild: DNS hierarchische Namenstruktur

Jeder Knoten des Baumes repräsentiert eine Domain (Domäne) und stellt einen Teil der gesamten Datenbank dar, also wie ein Verzeichnis in einem Dateisystem. Jede Domain (sowie jedes Verzeichnis) kann in weitere Teile untergliedert werden. Diese Teile werden im DNS als Subdomains bezeichnet und entsprechen den Unterverzeichnissen eines Dateisystems. Eine Subdomain wird, genau wie ein Unterverzeichnis, als Unterknoten (Sohn) des übergeordneten Knotens (Vater) interpretiert. Jeder Knoten des Baumes wird mit einem einfachen Namen versehen. Dieser Name kann bis zu 63 Zeichen lang sein. Dabei ist für die Root der Name „." reserviert.

Der vollständige Domain-Name im Baum (Full Qualified Domain Name) FQDN besteht aus den Namen einzelner Knoten bis zur Root. Dies bedeutet, dass der Name eines Knoten sich aus den einzelnen Namen im Pfad zusammensetzt, wobei diese einzelnen Namen durch einen Punkt voneinander getrennt werden.

Der FQDN eines Knotens kann so interpretiert werden, dass er drei Bestandteile beinhaltet:
- den Hostnamen (bzw. dessen Alias-Namen),
- den Domain-Namen (einschließlich evtl. Subdomänen) und
- das Domain-Suffix.

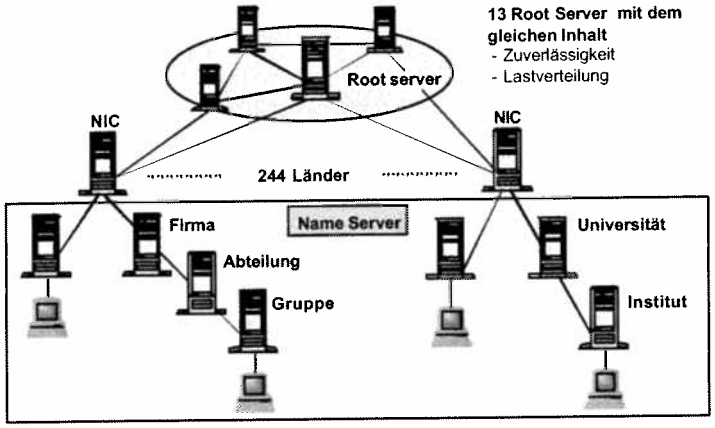


Bild: Domain Server System Hierarchie

Eines der Hauptziele beim Entwurf von DNS war die Dezentralisierung der Administration. Dieses Ziel wird durch sogenannte Delegierung erreicht. Das Delegieren von Domains funktioniert so ähnlich wie das Delegieren in der Arbeit. Ein Projektleiter kann ein großes Projekt in kleinere Aufgaben unterteilen und die Verantwortung für jede dieser Teilaufgaben an verschiedene Mitarbeiter übergeben (delegieren). Auf die gleiche Weise kann eine Organisation, die eine Domain administriert, diese in Subdomains aufteilen. Jede dieser Subdomains kann an andere Organisationen delegiert werden. Dies bedeutet, dass die Organisation, der die Verantwortung dieser Domain übertragen wurde, für die Pflege aller Daten der Subdomain verantwortlich ist. Die Daten der Subdomain können unabhängig geändert und sogar in weitere Subdomains aufgeteilt werden, die sich dann wieder weiterdelegieren lassen. Die übergeordnete Domain enthält nur Zeiger auf die Quellen mit den Daten der Subdomain, so dass Anfragen entsprechend weitergeleitet werden können.

Die oberste Ebene des DNS-Namensraums wird vom InterNIC (Internet Network Information Center) verwaltet. Das InterNIC übergibt die Verantwortung sowohl an öffentliche Organisationen als auch an private Unternehmen für die Verwaltung von deren Domains im DNS-Namensraum. Die Organisationen und Unternehmen setzen DNS-Server zum Verwalten der Namenzuordnungen zu IP-Adressen von Rechnern und anderen Endsystemen in deren Domains ein.

Die oberste Ebene des Domain-Namensraums wird in drei Hauptgruppen unterteilt:

- Domains von Organisationen: dreistelliger Name, der die Hauptfunktion bzw. -Aktivität der Organisation in der Domain angibt. Die meisten Organisationen in den USA sind in einer solchen Domain vertreten.
- Geographische Domains mit einem festgelegten zweistelligen Länderkennzeichen.
- arpa-Domain, eine besondere Domain mit dem Namen in-addr.arpa wurde für die Zuordnung von IP-Adressen zu Rechnernamen eingerichtet.

Die Organisationen und Unternehmen, denen das InterNIC einen Bereich des Domain-Namensraums zugewiesen hat, sind für das Benennen der Rechner und anderer Endsysteme in der ihnen zugeteilten Domain verantwortlich.

Primary Name Server (Master)
Datenbank mit autorisierten Daten
Datenbank Eintragungen

Secondary Name Server (Slave)
Datenbank mit autorisierten Daten
Aktualisierungen vom Master

Caching Server
Keine autorisierte Daten
Entfernung von Daten: time-to-live field (32 Bit)

Bild: DNS Server Typen

Um die Administration der Netze zu vereinfachen und sowohl Datensicherheit als auch Betriebssicherheit zu gewährleisten, können zwei Arten von Name-Server in einer DNS-Zone zur Verfügung gestellt werden:

- Primäre (primary) Name-Server und
- sekundäre (secondary) Name-Server.

Ein primärer Name-Server erhält die Daten für die Zonen, über die er die Autorität besitzt, aus Dateien, die auf dem Host liegen, auf dem der Server läuft. Die Dateien, aus denen der primäre Name-Server seine Zonendaten liest, werden Zonendateien genannt. Bei Änderungen an den Zonendaten, z.B. durch Hinzufügen von Hosts zur Zone, müssen diese Änderungen auf dem primären Name-Server vorgenommen werden, so dass die neuen Daten in die lokale Zonendatei eingetragen werden.

Ein sekundärer Name-Server erhält seine Zonendaten von einem primären Name-Server. Beim Start stellt der sekundäre Name-Server den Kontakt mit dem primären Name-Server her, um seine Zonendaten zu aktualisieren. Dieser Vorgang wird als Zonentransfer bezeichnet. Während eines Zonentransfers sendet der primäre Name-Server eine Kopie der Zonendatei an den sekundären Name-Server.

Generell sollte man den primären und den sekundären Name-Server in verschiedenen Subnetzen installieren, damit die DNS-Namensabfragen auch dann unterstützt werden können, wenn ein Subnetz ausfällt.

Aufbau

- Hierarchie von Name-Server, dadurch Skalierbarkeit gegeben
- Kein Name-Server verfügt über die kompletten Daten

Typen von Name-Server

- **Lokale Name-Server**
  z.B. ISP, Universität, Firma etc. besitzt lokalen Name-Server
- **Root-Server**
  einige wenige solche Server existieren weltweit
- **Authorisierte Name-Server**
  Jedes System ist bei einem solchen Server registriert
  Oft geographisch mit lokalen Name-Server zusammen

Für jede Hierarchiestufe (= Domäne) gilt

- Sie besitzt die Authorität zur Namensvergabe innerhalb dieser Domäne
- Sie verfügt über Name-Server, die für die nächst tiefere Ebene zuständig sind
- Ein Root-Server ist bekannt

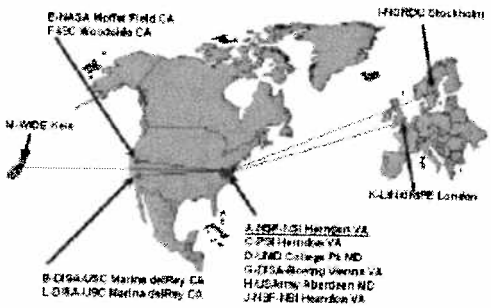
Bild: Name-Server

Root Server enthalten nur Einträge für TLDs (generische und Länder TLDs)

Allgemein:

- jeder Nameserver enthält nur die Einträge für die er verantwortlich ist (autorative)
- darüber hinaus auch noch zwischengespeicherte Einträge von vorhergehenden Anfragen
- Timeout legt fest wie lange Einträge zwischengespeichert werden (typisch mehrere Tage)

Bild: Root Server and Registrierung von TLDs



Lokation der DNS Root-Server
http://www.wia.org/

Weltweit gibt es 13 Root-Server

Aufgaben

- Kontaktiert Autorative Name Server, falls Adressumsetzung unbekannt
- Gibt Adressumsetzung dem lokalen Name- Server bekannt

Bild: Verteiltes Netz von DNS Root-Server

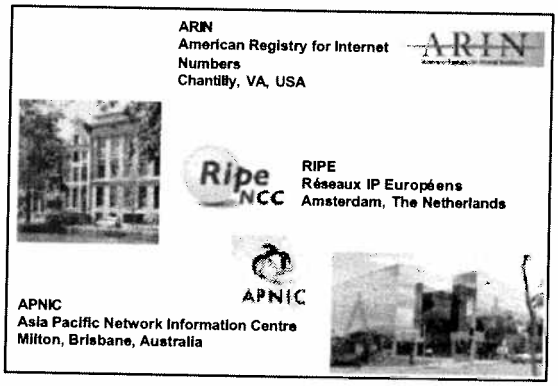


Bild: Registrierung von NLAs

DNS-Zonen und Name-Server

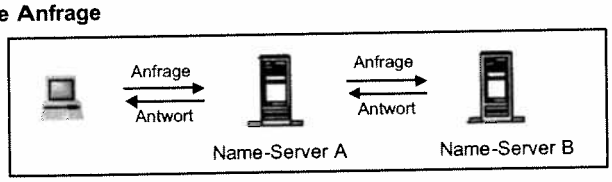
Ein Name-Server stellt einen dedizierten Rechner dar, in dem die Informationen (als Ressource Records) über den Domain-Namensraum gespeichert werden. Ganz allgemein enthalten Name-Server vollständige Informationen über einen Teil des Domain-Namensraums. Dieser Teil wird Zone genannt und man sagt, dass der Name-Server "die Autorität" über die Zone besitzt. Die Name-Server können auch die Autorität über mehrere Zonen besitzen.

Der Unterschied zwischen einer Zone und einer Domain besteht darin, dass der Name-Server einer Zone nur solche Namen und Daten einer Domain enthält, die in ihre Subdomains nicht delegiert wurden. Somit handelt es sich bei einer Zone nur um einen Bereich einer DNS-Domain. In kleinen Unternehmen kann eine Zone die gesamte Domain umfassen. Die DNS-Server können in der (Root)-Domain, der Zone und den Subdomains eines TCP/IP-Netzes installiert werden, also überall dort, wo ein DNS-Server zum Verwalten der DNS-Daten sowie des Datenverkehrs aufgrund von DNS-Namensabfragen benötigt wird.

Das Aufteilen einer Domain in Zonen und Subdomains hat den Vorteil, Verwaltungsaufgaben den verschiedenen organisatorischen Gruppen zuordnen zu können. Bei der DNS-Server-Datenbank handelt es sich um einen Satz von Dateien, die die

Zuordnungen der Host-Namen zu den IP-Adressen sowie andere DNS-Informationsdaten für die Rechner in einem TCP/IP-Netz enthalten.

Rekursive Anfrage



Iterative Anfrage

Kann in jeder Stufe der Abfragekette angewandt werden

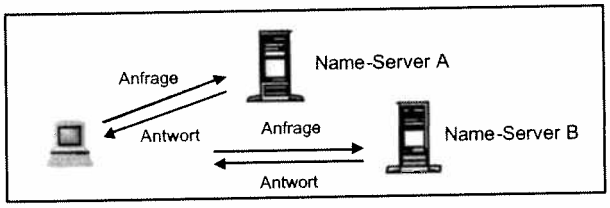


Bild: Typen von DNS-Anfragen

Prinzip der Namensauflösung

Die Name-Server gehen bei der Gewinnung von Daten aus dem DNS-Namensraum äußerst geschickt vor. Sie können nicht nur die notwendigen Informationen aus Zonen liefern, über die sie, die Autorität besitzen, sondern auch den DNS-Namensraum nach Daten absuchen, für die sie nicht verantwortlich sind. Dieser Prozess wird als Namensauflösung (name resolution) oder einfach nur als Auflösung (resolution) bezeichnet.

Weil der Namensraum wie ein auf den Kopf gestellter Baum strukturiert ist, kann ein Name-Server eine Abfrage nach jedem beliebigen Namen im DNS-Namensraum an einen Root-Name-Server richten, der ihm dann den Weg weisen wird.

Der Root-Name-Server weiß, wo die einzelnen Top-Level-Domains Name-Server zu finden sind. Für jede Abfrage auf einen beliebigen Domain-Namen hin kann der Root-Name-Server zumindest die Namen und Adressen des Naine-Servers zurückgeben, der für die Top-Level-Domain die Verantwortung trägt, in der dieser Domain-Name liegt. Diese Top-Level-NameServer können eine Liste von Name-Servern zurückgeben, die für die Second-Level-Domain verantwortlich sind. Jeder abgefragte Name-Server liefert genaue Angaben darüber, wie man der gesuchten Information näher kommt, oder erteilt selbst die gewünschte Antwort.

Die Root-Name-Server sind für die Auflösung sehr wichtig. Würden alle Root-Name-Server im Internet für eine längere Zeit nicht erreichbar sein, wäre auch jegliche Auflösung von Namen unmöglich. Um sich hiervor zu schützen, besitzt das Internet mehrere Root-Name-Server die über verschiedene Teile des Netzes weltweit verteilt sind.

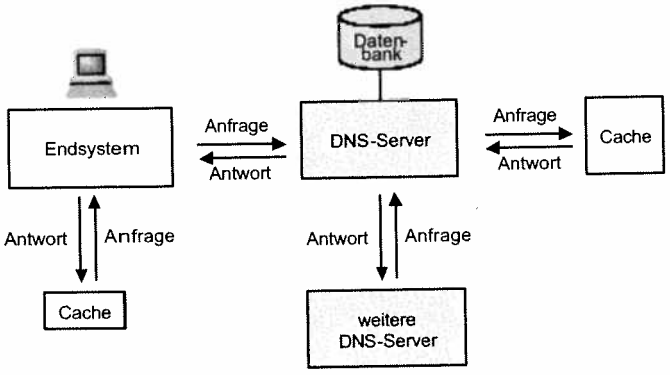


Bild: Domain Server System Abfrage

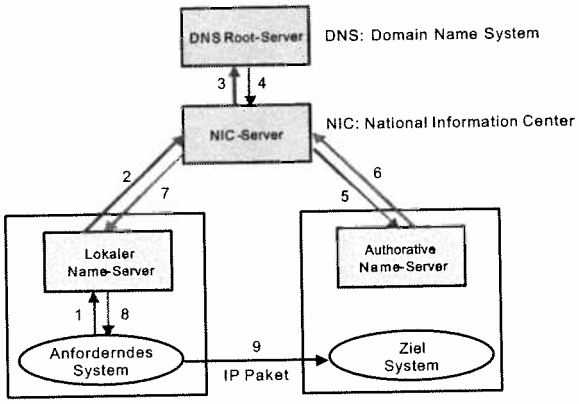


Bild: Allgemeiner Ablauf einer DNS-Abfrage

Auflösung von IP-Adressen auf Host-Namen

Oft kommt es vor, dass ein Benutzer nur über die IP-Adresse eines Rechners verfügt, jedoch den der entsprechenden IP-Adresse zugeordneten Host-Namen benötigt. In diesem Fall wird nach der Zuordnung IP-Adresse zu Host-Name gefragt. Die Abbildung von Adressen auf Namen wird benutzt, um Ausgaben zu erzeugen, die für den Anwender einfacher zu lesen und zu interpretieren sind (beispielsweise in Log-Dateien). Darüber hinaus wird dieses Verfahren auch bei der Fehlerbehebung in TCP/IP-Netzen angewendet.

Zur Verwaltung der Zuordnungen von IP-Adressen zu Host-Namen durch DNS-Server wurde eine besondere Domain in-addr.arpa durch InterNIC eingerichtet. Beim Eintragen der Zuordnungen von IP-Adressen zu Host-Namen werden diese Knotennummern entsprechend belegt. Da die Hierarchien von IP-Adressen und Host-Namen umgekehrt sind, muss dies die Organisation der Domain in-addr.arpa berücksichtigen.

Die Knoten der Domain in-addr.arpa sind nach den Zahlen in der für IP-Adressen übliche Repräsentation benannt. Die Domain in-addr.arpa kann beispielsweise bis zu 256 Subdomains besitzen, von denen jede einzelne einem möglichen Wert des

letzten Bytes einer IP-Adresse entspricht. Jede dieser Subdomains kann wiederum 256 Subdomains aufweisen, die jeweils wiederum mit jedem möglichen Wert des zweiten (von rechts) Byte von IP-Adressen übereinstimmen. Schließlich werden - auf der vierten Unterteilungsstufe - den Knoten die entsprechenden Resource Records zugeteilt, die den vollen Host-Namen (FQDN) der jeweiligen IP-Adresse aufweisen.

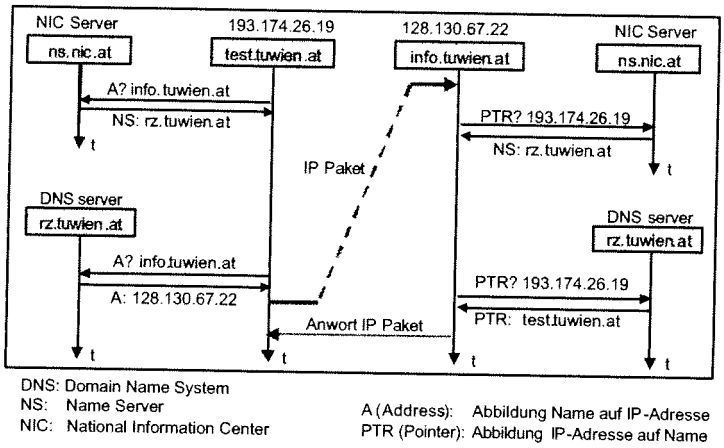


Bild: Beispiel einer DNS Anfrage

Name-Server und Internet-Anbindung

Heutzutage werden private Netze oft mit dem Internet verbunden, um auf die externen Ressourcen im globalen Netz zuzugreifen (z.B. WWW-Anwendungen). Dies verlangt jedoch eine sorgfältige Planung, um potentielle Sicherheitsrisiken zu vermeiden, die durch das Öffnen des privaten Netzes für fremde Benutzer entstehen können.

Eine häufige Schutzmaßnahme ist daher der Einsatz eines als Firewall bezeichneten Rechners. Unter einer Firewall versteht man einen Rechner, der nur die Ausführung bestimmter Operationen oder Programme über das Internet erlaubt. Eine Firewall-Konfiguration kann, je nach den besonderen Anforderungen des jeweiligen Unternehmens, sehr einfach oder extrem komplex sein. Hier wird versucht, zu zeigen, dass das Konzept für den DNS-Einsatz mit dem Firewall-Konzept eng zusammenhängt.

Bei einer Lösung eines Unternehmensnetzes wird das Netz in zwei logischen Teilen aufgeteilt wurde:

- interner Netzteil,
- externer Netzteil.

Der interne Netzteil enthält einen internen DNS-Server, der hauptsächlich durch die interne Kommunikation in Anspruch genommen wird. Der externe DNS-Server wird bei der Kommunikation über das Internet verwendet.

Die Firewall schützt den internen Netzteil gegen Zugriffe durch fremde Benutzer vom Internet, wobei den Rechnern im internen Netzteil der Zugriff auf Ressourcen im Internet gewährt wird. Die externen Server erlauben den Rechnern außerhalb des internen Netzteils, auf durch öffentliche Dienste zur Verfügung gestellte Ressourcen zuzugreifen.

Diese externen Server müssen jedoch genau überwacht und gesichert werden, da sie direkt mit dem Internet verbunden sind und keine Zugriffskontrolle durch die Firewall ausüben. Der Eingangs-Router kann speziell erweitert (Filterfunktion für IP-Pakete) und zur Überwachung des Zugriffs von außen auf die externen Server eingesetzt werden.

Die DNS-Dienste für die externen und internen Netze sollten vollständig voneinander getrennt sein, damit die Rechner außerhalb des internen Netzteils daran gehindert werden, die Namen und IP-Adressen von im internen Netzteil befindlichen Ressourcen ausfindig zu machen. Dadurch wird sichergestellt, dass die einzigen extern verfügbaren Informationen die Namen und IP-Adressen der externen Server (DNS- und WWW-Server) sind, die für die Bereitstellung öffentlicher Dienste des Unternehmens konfiguriert wurden.

Den Rechnern aus dem internen Netzteil, die die Ermittlung von IP-Adressen auf den Internet-Zugriff fordern, müssen normalerweise die notwendigen Interaktionen mit den DNS-Servern im öffentlichen Internet ermöglicht werden. Aus diesem Grund sollte die Fähigkeit zum Datenaustausch außerhalb des internen Unternehmensnetzes nur bestimmten DNS-Servern eingeräumt werden. Ein DNS-Server, der zur Auswertung einer DNS-Abfrage außerhalb des privaten Netzes nach entsprechenden Daten sucht, wird als Forwarder bezeichnet.

Nachdem ein externer DNS-Server als Forwarder eingerichtet wurde, sollten alle anderen DNS-Server im Netz für die Verwendung der Forwarder zur Auswertung von fremden Namen außerhalb des internen Netzes konfiguriert werden. Wenn ein Name-Server, der für die Verwendung eines Forwarders konfiguriert wurde, eine Abfrage erhält und diese anhand seiner Zonendateien nicht beantworten kann, gibt er die Abfrage an den Forwarder zurück. Daraufhin übernimmt der Forwarder die

notwendigen Schritte, die zur Antwort auf diese Abfrage führen. In diesem Fall richtet er die Abfrage an einen übergeordneten Name-Server im Internet und gibt die erhaltene Antwort an den richtigen Name-Server im internen Netzteil zurück.

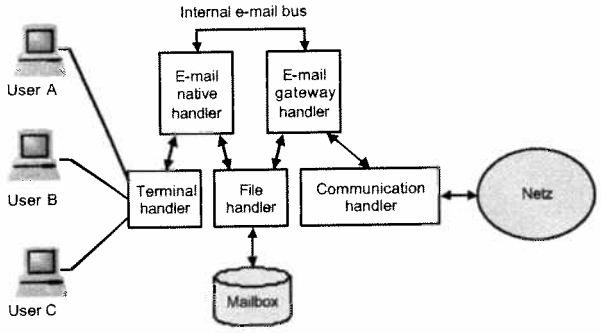


Bild: E-mail System Modell für ein Netz

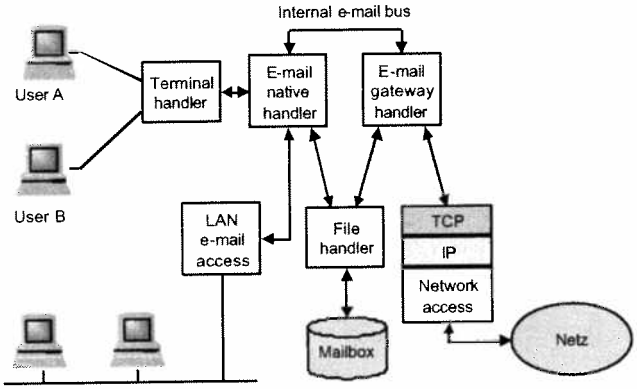


Bild: E-mail System Modell für den LAN Zugang

Dynamische Vergabe und Ermittlung von IP-Adressen

Durch die Vergabe von IP-Adressen können Rechner in IP-Netzen und speziell im Internet angesprochen werden. Im intuitiven Umgang sind IP-Adressen jedoch nicht sprechend genug. Es ist sinnvoll, statt einer IP-Adresse einen Rechner über seinen Namen zu adressieren. Dies kann im Prinzip durch eine statische Tabelle - die Host-Datei - erfolgen; sobald aber eine Vielzahl Rechner in entfernten IP-Netzen, d.h. speziell im Internet, erreicht werden sollen, wird die Pflege der Host-Dateien schnell unhandlich.
Um das Problem der dynamischen Namensauflösung im Internet zu lösen, wurde das Domain Name System (DNS) geschaffen. Das Domain Name System stellt eine verteilte Datenbank dar, die im Grunde genommen mit ihrem Informationsgehalt das Internet abbildet..

Entsprechend der Bedeutung des DNS für das Internet hat sich die Vergabe dynamischer IP-Adressen im Intranet entwickelt. Über das Dynamic Host Configuration Protocol (DHCP) kann eine dynamische und konsistente Vergabe von IP-Adressen und anderen wichtigen IP-Informationen für Rechner im Intranet erreicht werden.

1.5 Grundlagen: Kommunikationsverfahren

Version: Feb. 2004

- Aufbau einer Kommunikationsstrecke
- Systemkomponente einer Kommunikationsstrecke
- Begriffe Quellen-, Leitungs-, Kanalcodierung
- Begriffe Störungen, Fehlersicherung
- Begriffe Signale, Bits, Rahmen, Pakete, Nachrichten
- Datenmodems
- xSDL-Systeme

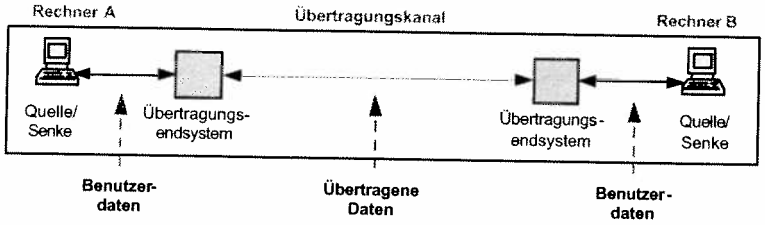


Bild: Kommunikationsmodell

Das einfache Kommunikationsmodell betrachtet einen Übertragungskanal zwischen zwei Übertragungsendsystemen. Dabei werden Benutzerdaten einfach als übertragene Daten transportiert ohne die Einzelheiten der physikalischen Übertragung zu berücksichtigen.

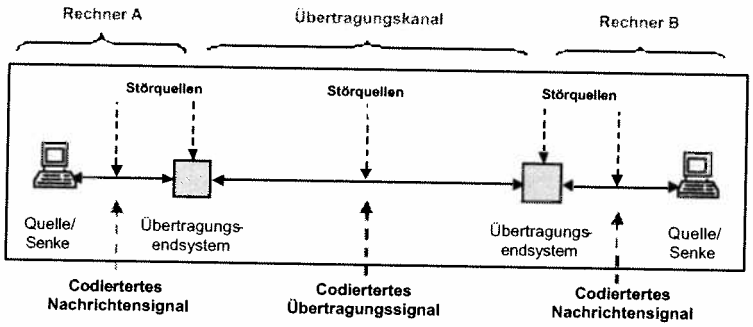


Bild: Übertragungstechnisches Modell

Das übertragungstechnische Modell konzentriert sich auf die Übertragung zwischen zwei Übertragungsendsystemen. Dazu werden codierte Nachrichtensignale als codierte Übertragungssignale zwischen beiden Endsystemen ausgetauscht. Dabei müssen alle Störeinflüsse betrachtet werden.

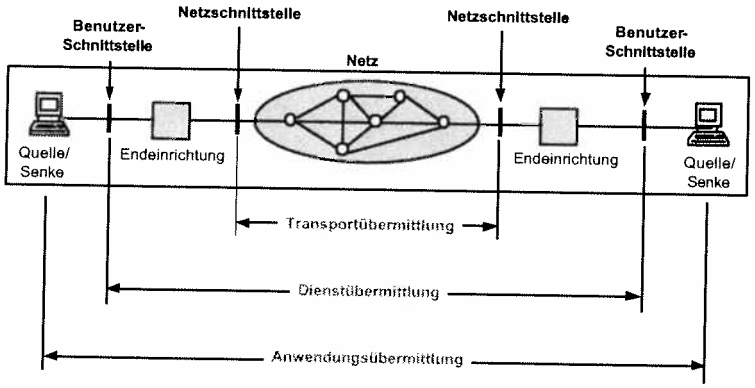


Bild: Netztechnisches Modell

Das netztechnische Modell betrachtet die Netzeigenschaften. In erster Linie gibt es Benutzer- und Netzschnittstellen. Zwischen den Netzschnittstellen findet die Transportübermittlung statt. Zwischen den Benutzerschnittstellen spricht man von der Dienstübermittlung und zwischen den Anwendungssystemen ist die Anwendungsübermittlung angesiedelt. Wichtig ist, dass die Transportübermittlung sich zusammensetzt aus einer Aneinanderreihung von Transport- oder Übertragungskanälen.

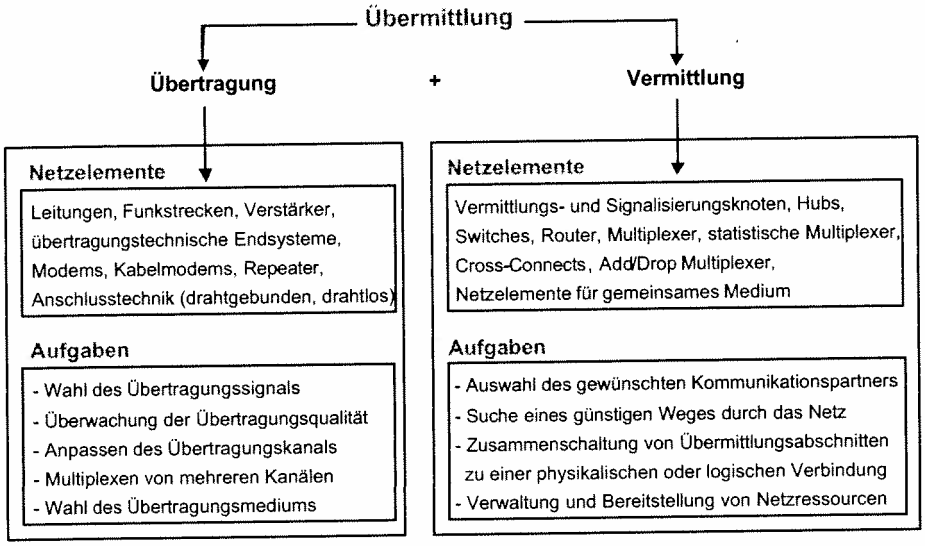


Bild: Übertragung und Vermittlung

Die Kombination von Übertragung und Vermittlung wird als Übermittlung bezeichnet. Jeder Bereich hat spezielle Netzelemente und Aufgaben.

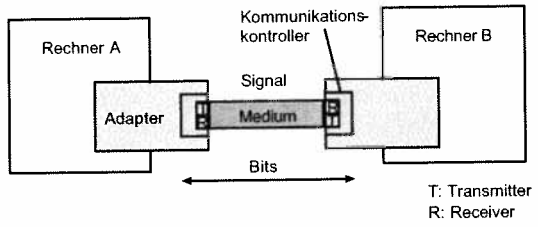


Bild: Datenkommunikation

Einfaches Szenario: Zwei direkt benachbarte Rechner kommunizieren über ein Medium (z. B. Kupferadern, Radiowellen oder Glasfaser).

- Anschluss der Rechner an das Medium über Adapter,
- Kommunikationskontroller auf dem Adapter regelt den Ablauf der Kommunikation.

Folgende Probleme sind unter anderem zu lösen

- Codierung der Signale,
- Organisation der Übertragung

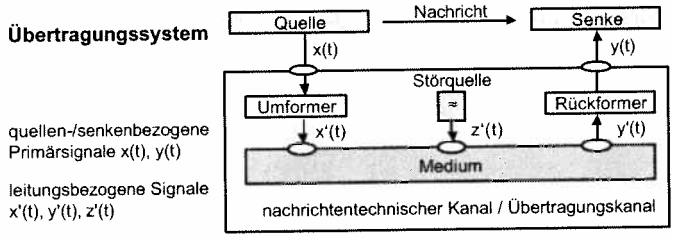


Bild: Übertragungskanal / Übertragungssystem

Für die mathematische Beschreibung des Übertragungskanals werden die Primärsignale an der Quelle und an der Senke durch zeitliche Signalverläufe x(t) bzw. y(t) beschrieben. Die leitungsbezogene Signale sind x'(t) und y'(t). Störungen werden durch Überlagerung von z'(t) und x'(t) berücksichtigt.

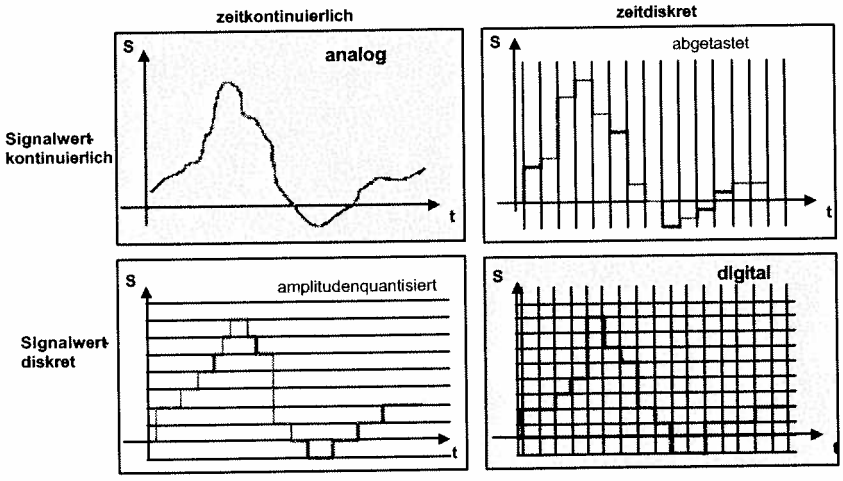


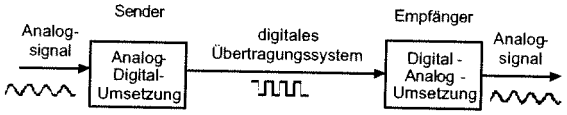
Bild: Signalquellen

Analoges Signal: Kontinuierlich in Zeit und Signalwert.

Digitales Signal: Diskret in Zeit und Signalwert.

Sprache	analog digital	3 kHz	GSM 13 kbit/s Telefonie 64 kbit/s, 32 kbit/s, ... 9,6 kbit/s
Audio	analog digital	20 kHz	CD-Qualität 4 bis 6 Mbit/s MP3-komprimiert etwa 128 kbit/s
Video	analog digital	5-6 MHz	Fernsehen in Studioqualität 60 / 100 Mbit/s Video (unkomprimiert) 100 - 600 Mbit/s Video (komprimiert) 2 - 100 Mbit/s HDTV (unkomprimiert) 1500 Mbit/s HDTV (komprimiert) 150 Mbit/s
Text	digital		50 kbit/s -10 Mbit/s
Daten	digital		Datentransfer 1 - 150 Mbit/s Telekonferenzen < 150 Mbit/s
Bilder	digital		Graphiken einige 100 kbit/s Fotos einige Mbit/s Hochauflösende Bilder < 150 Mbit/s

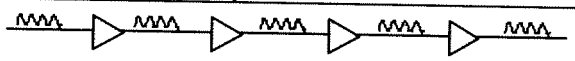
Bild: Zeitabhängige Signale



- **Übertragung analoger Signale über digitale Übertragungssysteme:**
  Umwandlung
  - wertkontinuierlich → wertdiskret (Quantisierung)
  - zeitkontinuierlich → zeitdiskret (Abtastung)
- **Ziel:** Rekonstruierbarkeit des originalen Signals beim Empfänger

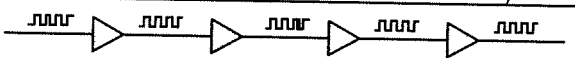
Bild: Digitalisierung analoger Signale

Übertragung von analogen Signalen



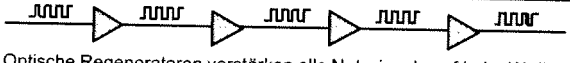
- Regeneratoren verstärken Nutz- und Rauschsignal
- Dadurch wird das analoge Nutzsignal immer schlechter
- **Beim Empfänger:** schlechtere Qualität **als das gesendete Nutzsignal**

Übertragung von digitalen Signalen (elektronische Verstärker)



- Regeneratoren können das digitale Nutzsignal vollständig rekonstruieren
- 3R-Regeneration: Amplitude, Impulsform, zeitliche Lage
- **Beim Empfänger:** gleiche Qualität **wie das gesendete Nutzsignal**

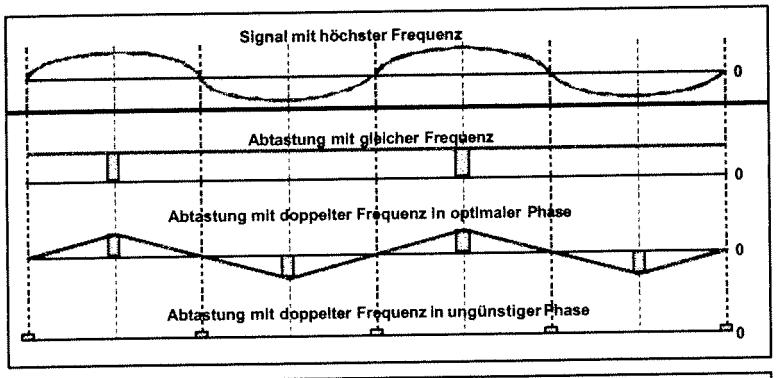
Übertragung von digitalen Signalen (optische Verstärker)



- Optische Regeneratoren verstärken alle Nutzsignale auf jeder Wellenlänge gleichzeitig, aber dafür nur in der Amplitude (1R Regeneration)
- In regelmäßigen Abständen müssen alle Nutzsignale im einzelnen elektronisch rekonstruiert werden (optische 3R- Regeneratoren in Labors verfügbar)
- **Beim Empfänger:** gleiche Qualität **wie das gesendete Nutzsignal**

Bild: Vorteile digitaler Übertragungssysteme

Im Bild sind die Unterschiede zwischen der analogen und digitalen Übertragung angegeben. Im wesentlichem geht es darum, dass digitale Signale beliebig oft regeneriert werden können, sodass am Empfänger das gesendete Signal komplett rekonstruiert werden kann. Vollständige Regeneration (3R-Regenation) rekonstruiert die Amplitude, die Impulsform und die zeitliche Lage des Pulses. Zu unterscheiden sind elektronische oder optische Verstärker, wobei heute die optischen Verstärker nur eine 1R-Regeneration (Amplitude) schaffen.



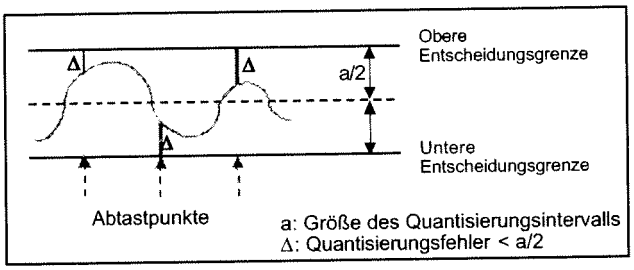
Zur fehlerfreien Rekonstruktion des Signalverlaufs der abgetasteten Analogsignale ist eine Mindestabtasthäufigkeit (Abtastfrequenz f_A) bei periodischem Abtastzyklus erforderlich

Die Abtastfrequenz f_A muss mehr als doppelt so hoch sein wie die höchste im abzutastenden Signal vorkommende Grenzfrequenz (f_S): $f_A > 2f_S$

Bild: Abtasttheorem nach Shannon

Die vollständige Rekonstruktion basiert auf das Abtasttheorem von Shannon. Dabei kann ein Signal wiedergewonnen werden, wenn die Abtastfrequenz doppelt zu hoch ist als die höchste Frequenzkomponente im Ursprungsignal.

Beispiel: Telefonsignale im Frequenzband 300 bis 3400 Hz werden mit 8 kHz abgetastet.



- Wertebereich des Analogsignals wird in endliche Anzahl von Quantisierungsintervallen eingeteilt, denen jeweils ein fester diskreter Wert zugeordnet wird
- Anstelle des ursprünglichen Analogsignals wird das mit dem Quantisierungsfehler $\Delta < a/2$ behaftete digitale Signal übertragen

Zuordnung des Mittelwerts des Intervalls beim Empfänger

Beispiel: Pulse Code Modulation (PCM)

Bild: Quantisierung und Codierung

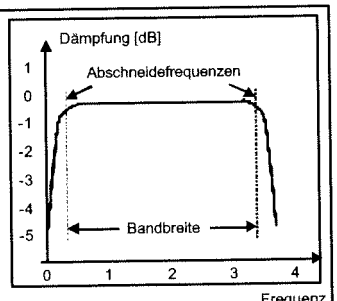
Bei der Digitalisierung der Signale mit Hilfe einer Quantisierung entsteht der sogenannte Quantisierungsfehler, der als Mittelwert bleibt. Bei der Codierung von mehreren Amplitudenstufen entsteht die Pulse Code Modulation (PCM), die bei Digitaltelefonie (z.B. ISDN) verwendet wird. Eine mit 8 kHz abgetastete Sprachprobe wird mit 8 Bit codiert, so dass ein konstanter Sprachstrom mit 64 kbit/s generiert wird.

Schon 1924 hat H. Nyquist die Existenz einer fundamentalen Grenze der Datenrate eines Kanals erkannt und eine Gleichung abgeleitet, die die maximale Datenrate für einen rauschfreien Kanal mit eingeschränkter Bandbreite angibt. 1948 führte Claude Shannon die Arbeit von Nyquist fort und entwickelte eine Gleichung für einen Kanal aus mit zufälligem (thermodynamischem) Rauschen (Shannon, 1948).

Maximale Datenrate D für einen rauschfreien Kanal mit eingeschränkter Bandbreite

$D = 2 \cdot B \cdot \log_2(N)$ [bit/s]

- B: Bandbreite des Kanals [Hz]
- N: diskrete Signalstufen



Beispiel:

- Kanal mit 3000 Hz, binäres Signal (N =2)
- maximale Datenrate: 6 kbit/s

Bild: Nyquist-Theorem

Nyquist bewies, wenn ein beliebiges Signal durch einen Tiefpassfilter der Bandbreite B geführt wird, das gefilterte Signal vollständig durch 2B Abtastwerte pro Sekunde wiederhergestellt werden kann. Mehr als 2B Abtastwerte pro Sekunde sind überflüssig da Anteile mit höherer Frequenz, die durch eine höhere Abtastrate entdeckt werden konnten, bereits ausgefiltert wurden. Besteht ein Signal aus N diskreten Stufen, lautet das Nyquist-Theorem wie im Bild angegeben.

Ein rauschfreier 3-kHz-Kanal kann beispielsweise binäre (d.h. zweistufige) Signale mit einer maximalen Rate von 6 kbit/s übertragen.

Maximale erzielbare Bitrate C hängt vom Signal-Rausch-Abstand ab

$C = B \cdot \log_2 (1 + S / N)$ [bit/s]

- B: Kanalbandbreite
- S: Energie des Signals
- N: Energie der Störquelle (Energie ~ Quadrat der Amplitude)

Beispiel

3000 Hz Kanal
SNR (signal-to-noise ratio) [dB] = 30 dB = $10 \log_{10}$(S/N) dB $\Rightarrow$ S/N = 1000
C = 3000 ($\log_2$ (1+1000)) ≈ 3000 • 10 = 30 kbit/s

Bild: Kanalkapazität nach Shannon

Bis jetzt wurde ein rauschfreier Kanal betrachtet. Ist zufälliges Rauschen vorhanden, verschlechtert sich die Situation sehr schnell. Der Umfang des vorhandenen thermischen Rauschens wird durch das Verhältnis vom Signal S zum Rauschsignal N (d.h durch den Rauschabstand S/N) bestimmt.

Normalerweise wird nicht dieses Verhältnis angegeben, sondern der Wert $10 \log_{10}$ S/N. Diese Einheiten werden Dezibel (dB) genannt. Ein Verhältnis S/N von 10 ist 10 dB, ein Wert von 100 ergibt 20 dB, ein Wert von 1.000 ergibt 30 dB usw.

Die Hersteller von Stereoverstärkern geben die Bandbreite (den Frequenzbereich), über den sich ihr Produkt linear verhalt, durch die jeweilige Frequenz von 3 dB an. An diesen Punkten wird die Verstärkung ungefähr halbiert. Shannons wichtigste Erkenntnis ist die, dass die maximale Datenrate eines rauschenden Kanals mit einer Bandbreite von B Hz und einem Rauschabstand von S/N wie im Bild angegeben.

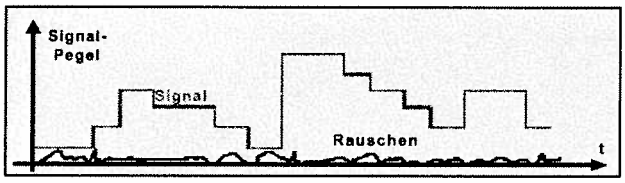
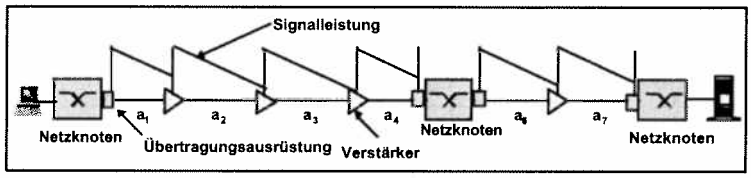


Bild: Kanalkapazität (Shannon)

So kann z.B. ein Kanal mit 3 kHz Bandbreite und einem Rauschabstand von 30 dB (typische Parameter des Telefonsystems) nie mehr als 30 kbit/s übertragen, gleichgültig, wie viele oder wenn die Signalstufen benutzt werden und wie oft oder selten Abtastwerte abgenommen werden. Shannons Ergebnis wurde mit Argumenten der Informationstheorie abgeleitet und ist auf jeden Kanal, der dem Gaußschen (thermischen) Rauschen unterliegt, anwendbar.



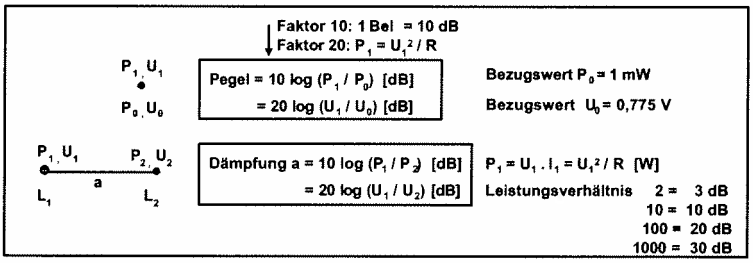


Bild: Pegel und Dämpfung

Die Einheit Dezibel (dB) ist eine wichtige Größe in der Elektrotechnik. Es wird dadurch ein logarithmisches Leistungsverhältnis definiert, z.B. Signal-zu-Rausch Leistung. Allgemein gilt: L = 10 lg (P1/P2) in dB.

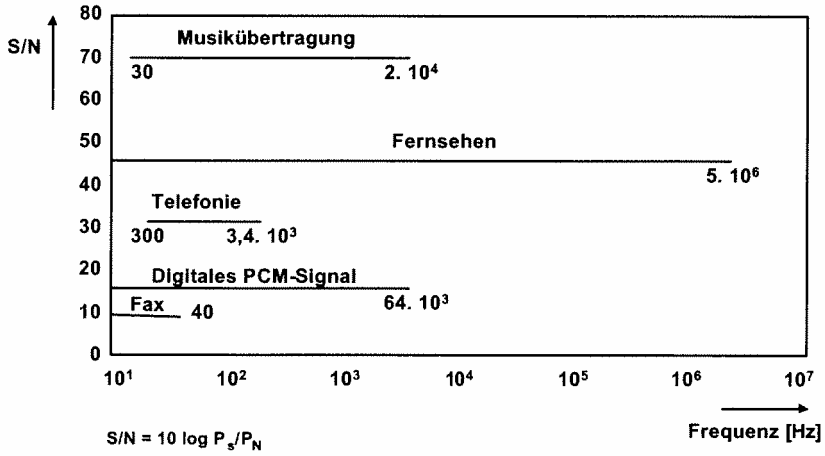


Bild: Dynamik und Bandbreite von Signalquellen

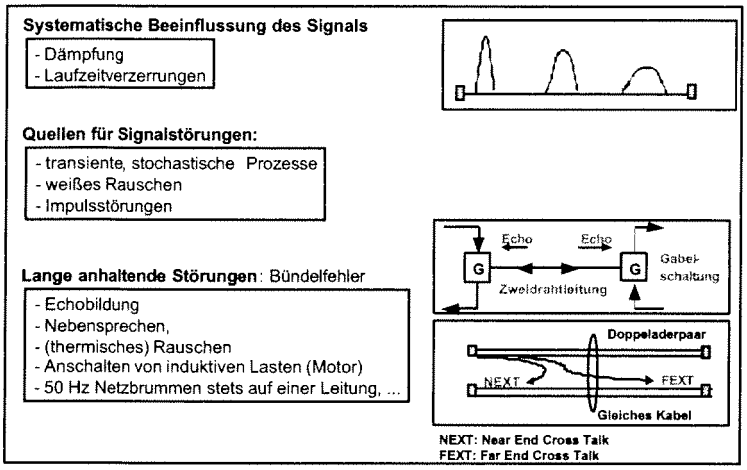


Bild: Übertragungsstörungsursachen durch Rauschen

Elektrische Signale sind störungsanfällig. Neben Übertragungstechnischer Beeinflussung der Signalpulsform durch Dämpfung und Laufzeitverzerrung, gibt es zahlreiche beeintrachtende Signalstörungen von außen.

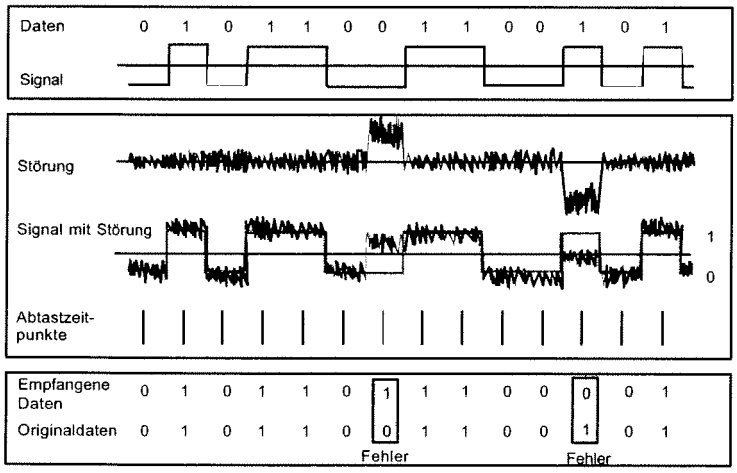


Bild: Übertragungsstörung durch Rauschen

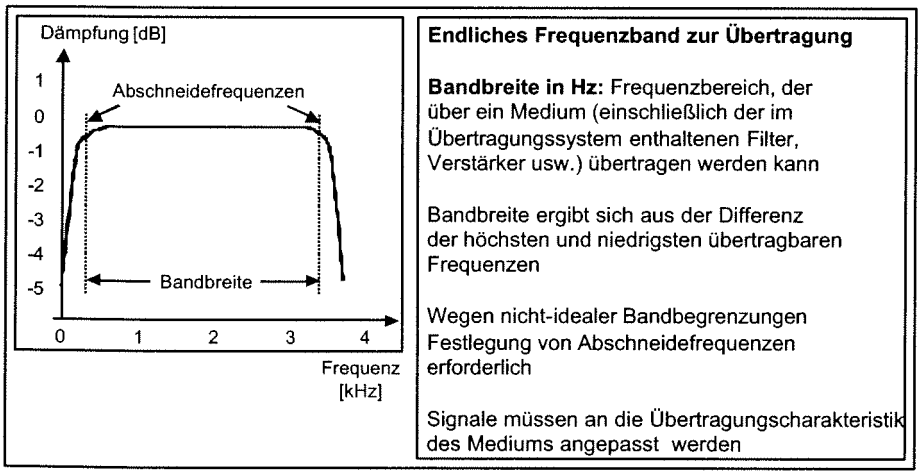


Bild: Bandbegrenztes Medium

Zur Übertragung benötigt man ein Frequenzband, das durch sogenannte Abschneidefrequenzen begrenzt wird. Man spricht von einer bandbegrenzten Übertragung. Die Begrenzung wird durch Filter realisiert: Tiefpass, Hochpass und Bandpass.

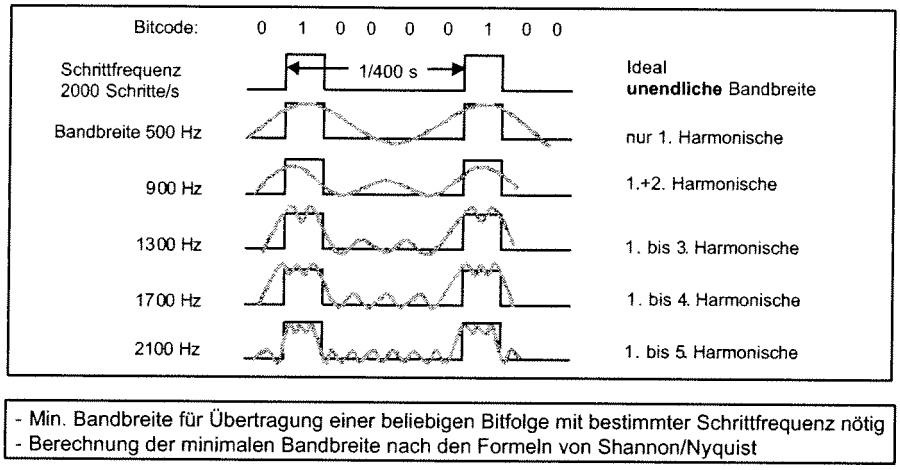


Bild: Bandbreite und digitales Signal

Codierung und Modulation

Eine Codierung kann unter anderem folgende **Ziele** verfolgen:

- Darstellung alphanumerischer **Zeichen** in einer standardisierten Form. Beispielsweise wird das lateinische Alphabet häufig durch den ASCII-Code dargestellt.
- Codierung von **Zahlen,** Zahlenwerte können prozessorintern unterschiedlich dargestellt sein. Für ihre Übertragung in Netzen sind ebenfalls standardisierte Codes erforderlich.
- Codierung von **Symbolen** (beliebige Zeichen, einzelne Bits oder Bitketten) zur Übertragung über einen physikalischen Kanal.
- Codierung von **Signalen** der realen Welt (z.B. Sprache, Bilder) so, dass zur Übertragung eine möglichst geringe Bandbreite benötigt wird.

Reale Signale (z.B. Sprache: Schallwellen, Bilder: zweidimensionale Verteilung der Lichtintensität) werden in der Regel zuerst in eine analoge elektrische Darstellung gebracht. Die Spannungsverläufe sind also kontinuierlich. Für die Verarbeitung und Übertragung werden jedoch meistens und noch zunehmend digitale (wertediskrete) Darstellungen bevorzugt. Zur Umwandlung zwischen den Signaldarstellungen existieren verschiedene Verfahren.

Im Hinblick auf die Signalübertragung unterscheidet man die folgenden Codierungsarten: Leitungscodierung, Kanalcodierung und Quellencodierung. Die Codierungsarten erfüllen unterschiedliche Aufgaben. Die gestellten Anforderungen unterscheiden sich ebenfalls. Wenn alle Codierungsarten eingesetzt werden (beispielsweise bei der Sprach- oder Bildübertragung über Paketnetze) ist beim Sender die Folge Quellen-, Kanal- und Leitungscodierung zu durchlaufen. Beim Empfänger ist die Reihenfolge umgekehrt.

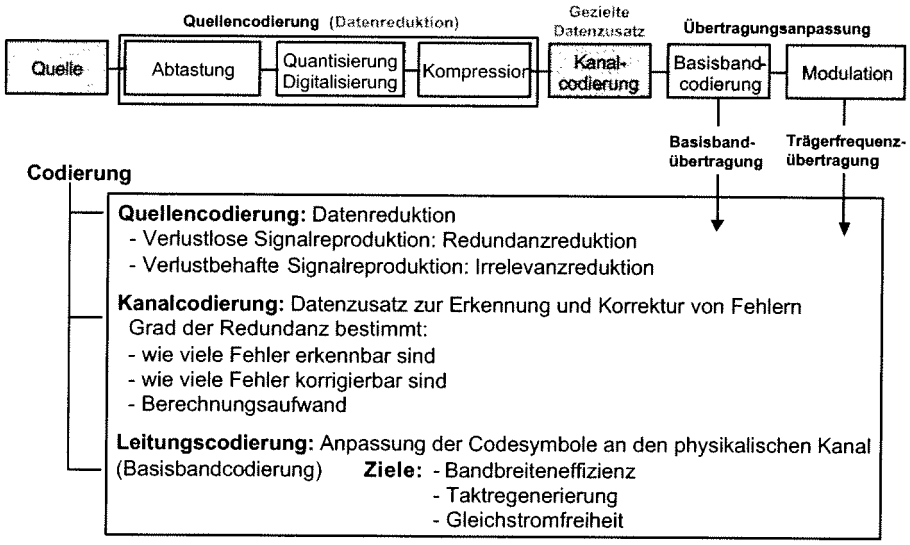


Bild: Codierung: Quellen-, Kanal- und Leitungscodierung

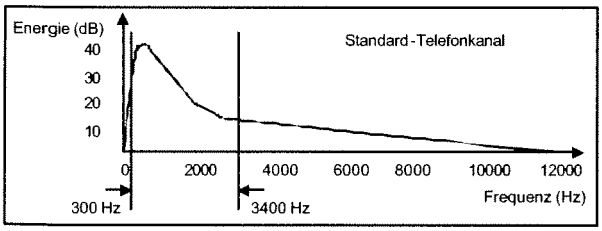
Quellencodierung/Datenkompression (source coding, data compression)
Bei der Kanalcodierung wird die zu übertragende Datenmenge vergrößert. Die Datenkompression verfolgt hingegen das Ziel, die Datenmenge zu reduzieren. Verfahren zur Datenkompression lassen sich einteilen in Entropiecodierung, Quellencodierung und hybride Codierung. Die Entropiecodierung ist verlustfrei, d. h. die Originaldaten können exakt wiederhergestellt werden. Dazu entfernt der Sender die im Signal enthaltene Redundanz, der Empfänger fügt sie wieder hinzu. Beispielsweise kann eine Folge n gleicher Zeichen durch ein Zeichen und den Wiederholungsfaktor n übertragen werden. Die Quellencodierung verwendet Wissen über die zu codierenden Signale. Sie entfernt die im Signal enthaltene Irrelevanz (dies sind Anteile, die der Empfänger nicht oder nur schlecht wahrnehmen kann, z. B. Farbverläufe bei rasch veränderlichen Kanten in Bildern). Die Quellencodierung ist meistens verlustbehaftet, erreicht aber dafür wesentlich höhere Kornpressionsgrade als die Entropiecodierung.

Kanalcodierung (channel coding)
Ziel der Kanalcodierung ist es, die Kommunikation gegen Übertragungsfehler zu sichern. Dazu werden die Daten als Codewörter codiert, die den Eigenschaften des Übertragungskanals angepasst sind. Grundsätzlich kann die Kanalcodierung fehlererkennende oder fehlerkorrigierende Codes verwenden (error detection bzw. error correction). Damit Fehler erkannt bzw. korrigiert werden können, müssen die Nutzdaten durch redundante Daten ergänzt werden, die aus den Nutzdaten abgeleitet sind und zusammen mit diesen übertragen werden. Der Empfänger kann dann die von ihm empfangenen, redundanten Daten mit denen vergleichen, die er selbst aus den empfangenen Nutzdaten berechnet hat. Wenn er dabei Unterschiede feststellt, kann er davon ausgehen, dass Übertragungsfehler aufgetreten sind.

Leitungscodierung (line coding)
Die Leitungscodierung ordnet einem oder mehreren Bits ein **bestimmtes Symbol (Signalelement)** zu, das auf der Leitung übertragen wird.

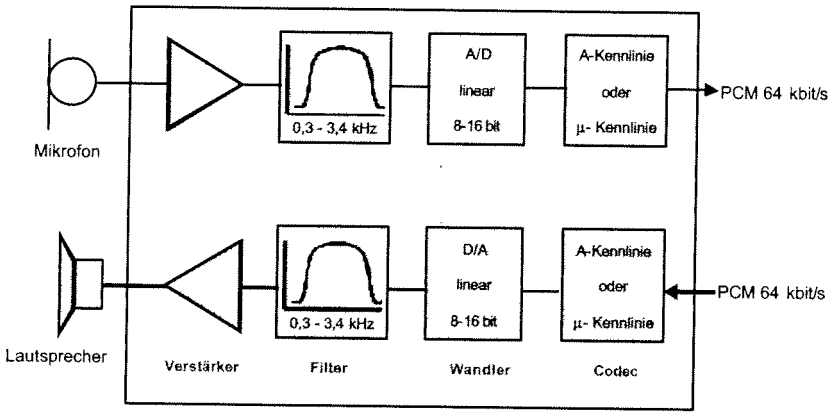
Dabei sollen die folgenden Kriterien bestmöglich erfüllt werden:
- **Bandbreiteneffizienz:** Die für eine vorgegebene Datenrate (Anzahl der pro Zeiteinheit zu übertragenden Datenbits) erforderliche Bandbreite soll möglichst gering sein bzw. die auf einer Leitung mit gegebener Bandbreite mögliche Datenrate soll maximal sein.
- **Taktregenerierbarkeit:** Der Empfänger muss die Symbolzeiten (die Anfangs- und Endzeitpunkte eines Symbols) aus dem empfangenen Signal wiedergewinnen, da ihm der ursprüngliche Sendetakt nicht zur Verfügung steht.
- **Gleichspannungsanteil:** Bei der Übertragung über Leitungen, die keine Gleichspannungen übertragen können (deren untere Grenzfrequenz also größer als null ist), darf im Frequenzspektrum des Sendesignals der Wert null nicht vorkommen. Andernfalls ist es für den Empfänger schwierig bis unmöglich, das Signal korrekt zu erkennen.

Im einfachsten Fall werden für Leitungscodes zweiwertige Symbole mit unipolaren (U+, 0) oder bipolaren (U+, U-) Spannungspegeln verwendet. Der Spannungspegel kann für die Symboldauer konstant sein oder er kann sich zu bestimmten Zeitpunkten ändern. Für verfeinerte Codes werden mehrwertige (ternäre, quaternäre) Spannungspegel verwendet. Zudem können Bitketten der Länge n in Symbolketten der Länge m (m ≠ n) abgebildet werden. Für einige wichtige Codes sind Zeitdiagramme der Pegelverläufe zusammengestellt.



- Frequenzbereich: 300 - 3400 Hz = 3,1 kHz Bandbreite
- Abtastfrequenz höher als 6,8 kHz (Shannon-Abtasttheorem)
- Abtastfrequenz für PCM-Digitalisierung: f_A = 8 kHz
- Abtastperiode: $T_A = 1/f_A = 1/(8000\ Hz) = 125\ \mu s$
- 256 Quantisierungsintervalle, d.h. 8 Bit für binäre Codierung
- Bitrate für digitalisierten Fernsprechkanal: 8 kHz • 8 bit = 64 kbit/s

Bild: Pulse Code Modulation (PCM)



A/D: Analog/digital-Wandler
D/A: Digital/analog -Wandler
Codec: Codierer / Decodierer
PCM : Pulse Code Modulation

Bild: Codierung und Decodierung von Sprache

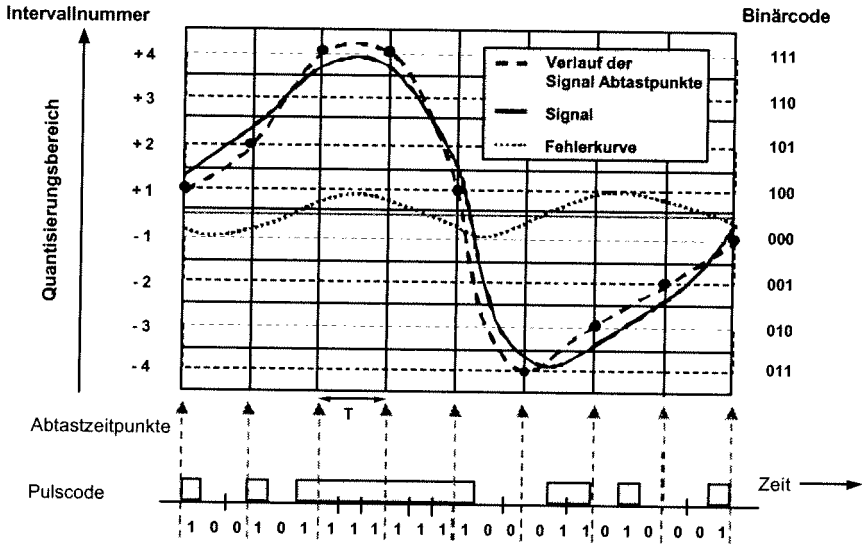


Bild: Prinzip der Pulscodemodulation (PCM)

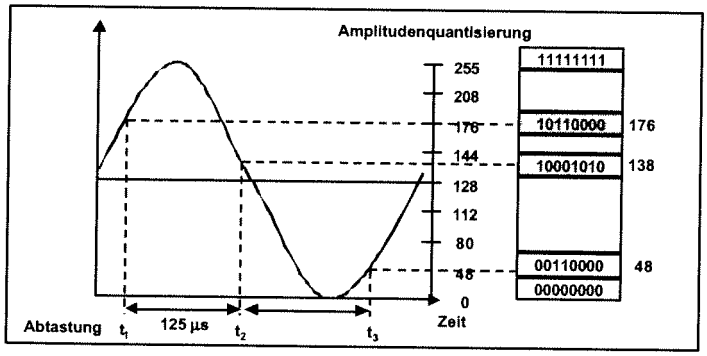


Bild: Logarithmische Quantisierung

Gleichförmige Quantisierung: gleich große Intervalle

- Quantisierungsfehler machen sich bei bei kleinen Signalwerten stärker bemerkbar (Quantisierungsrauschen)
- Kleine Unterschiede werden bei leisen Signalen stärker wahrgenommen als bei lauten

Deshalb:

Kompressor/Expander bei Sender /Empfänger mit logarithmischen Kompressionskennlinien

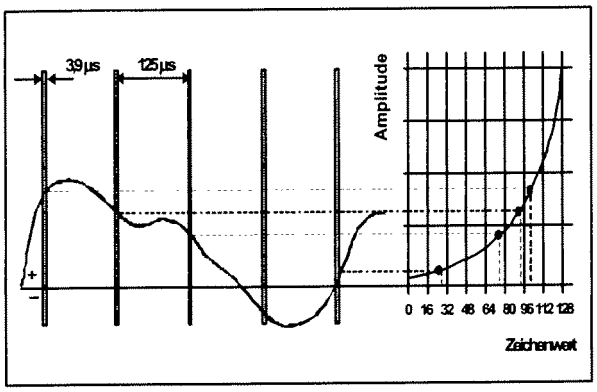
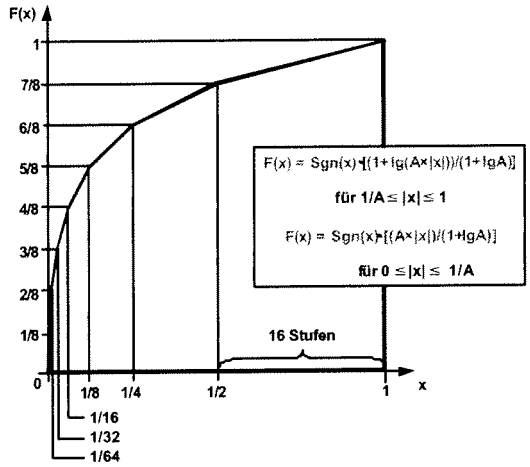
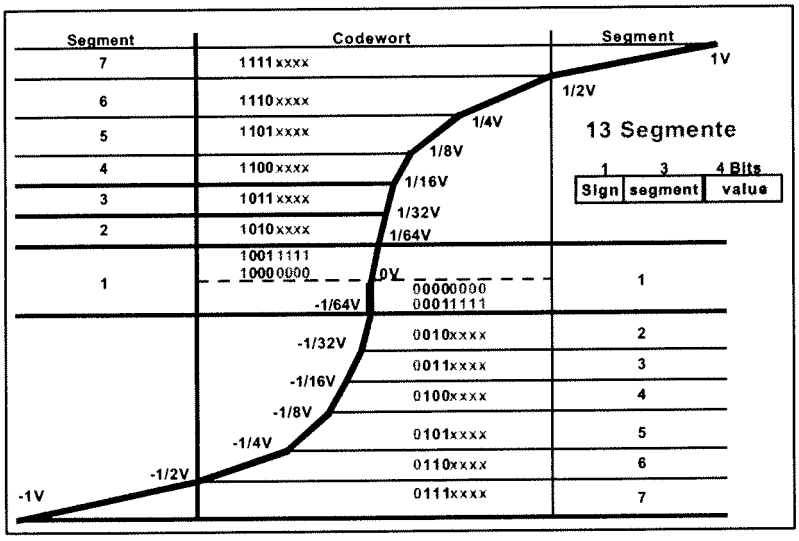


Bild: Kompandierung des Signals bei PCM



X: Eingangssignal, normiert auf die halbe Maximalspannung
F(x): Kompressorausgangsspannung, normiert auf die halbe Maximalspannung

Bild: Positiver Ast der A-Kennlinie



A-Law (Europa)

$$y = \frac{Ax}{1+\log_2(A)}, \quad 0 \le |x| \le \frac{1}{A}$$

$$y = \frac{1+\log_2(Ax)}{1+\log_2(A)}, \quad \frac{1}{A} \le |x| \le 1$$

A = 87,6

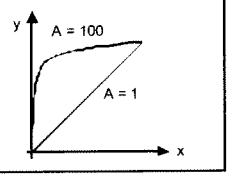
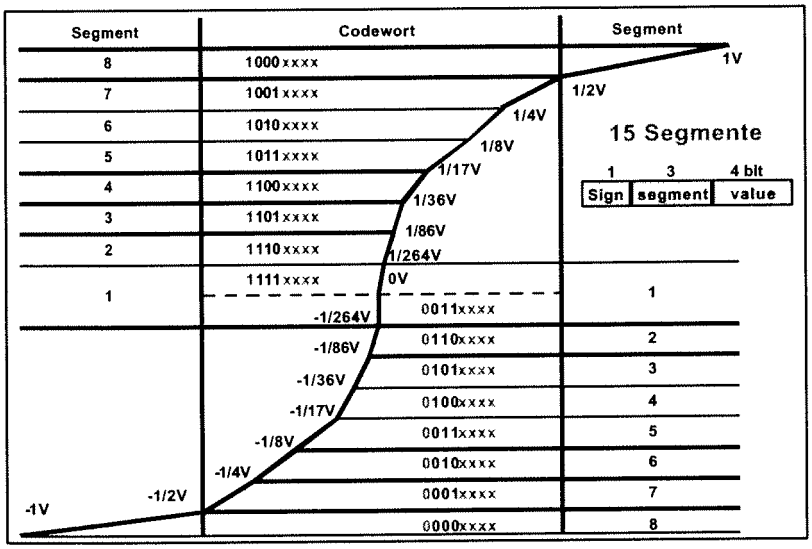


Bild: A- Kennlinie (A-Law) - Europa



µ-Law (USA und Japan)

$$y = \frac{\log_2(1+\mu x)}{\log_2(1+x)}, \quad x \ge 0$$

µ = 255

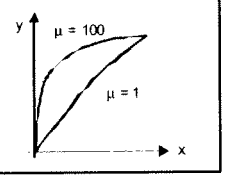


Bild: µ-Kennlinie (µ-Law) - USA, Japan

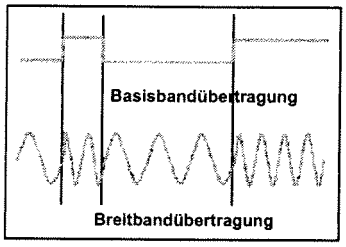
Schritt
- Charakteristisch für zeitdiskrete Signale ist die Existenz eines minimalen Zeitintervalls T_{Min} zwischen aufeinanderfolgenden möglichen Änderungen der Signalkoordinate (Schrittdauer, kurz: Schritt als Signal definierter Dauer)
- **Wichtig:** Digitales Signal mit fester Schrittdauer T (Schritt-Takt)

Isochrones (isochronous) Digitalsignal
- Ein Digitalsignal ist isochron, wenn seine Kennzeitpunkte, d.h. die Zeitpunkte des Übergangs von einem Signalelement zum nächsten, in einem festen Zeitraster liegen

Anisochrones (anisochronous) Digitalsignal:
- Ein nicht-isochrones Digitalsignal

Schrittgeschwindigkeit
- bei isochronen Digitalsignalen: Kehrwert der Schrittdauer: 1/T
- Einheit: baud = 1/s

Bild: Digitale Signalübertragung



- **Basisbandübertragung**
  - direkte Übertragung des rechteckförmigen Quellensignal (z.B. Strom / kein Strom)
- Eigenschaften der Codes
  - Bittaktrückgewinnung
  - Vermeiden von Gleichstromanteilen
  - Codierung mehrerer Zeichen
  - Resynchronisation durch Rahmenbildung
- **Breitbandübertragung**
  - Modulation

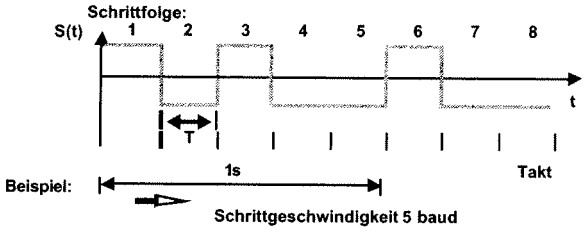
Bild: Digitale Signale zur Datenübertragung

Schrittgeschwindigkeit (Baudrate)
- Zahl der Signalparameter-Zustandswechsel
- Einheit: baud (1/s) (nach Jean Marc Baudot)
- entspricht bei isochronem Takt der Taktfrequenz
- auch als *Baudrate* bezeichnet

Übertragungsgeschwindigkeit (Bitrate)
- Anzahl der übertragbaren Bitstellen pro Zeiteinheit
- Einheit: bit/s

Schrittgeschwindigkeit = Übertragungsgeschwindigkeit
- Nur für binäre Signale, bei denen jeder Schritt als Signalelement genau ein Bit als Codeelement darstellt

Bild: Übertragungsgeschwindigkeit versus Schrittgeschwindigkeit



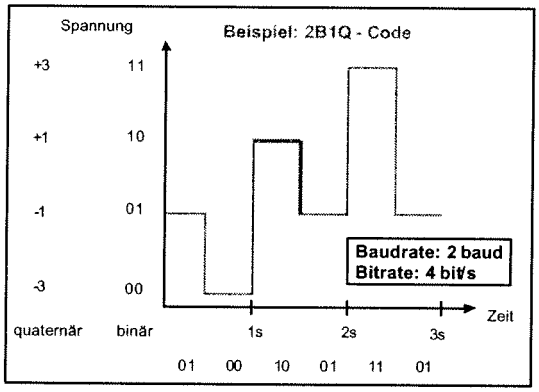


Bild: Beispiel einer Baudrate (Symbolrate)

Zweiwertiges Digitalsignal (Binärsignal)
- Digitales Signal mit nur zwei Werten des Signalparameters

(Digitales Signal, bei dem die Signalelemente binär sind)

Mehrwertiges (mehrstufiges) Digitalsignal
- Die (diskrete) Signalkoordinate kann mehr als zwei Werte annehmen;

Beispiel: DIBIT = zwei Bit pro Koordinatenwert (quaternäres Signalelement)
- Die Anzahl n der diskreten Werte (Kennwerte, Stufen), die ein Signalelement annehmen kann, wird wie folgt gekennzeichnet:

n = 2 binär (binary)
n = 3 ternär (ternary)
n = 4 quaternär (quarternary)
...
n = 8 oktonär (octonary)
n = 10 denär (denary)

Bild: Zwei- und mehrwertige Digitalsignale

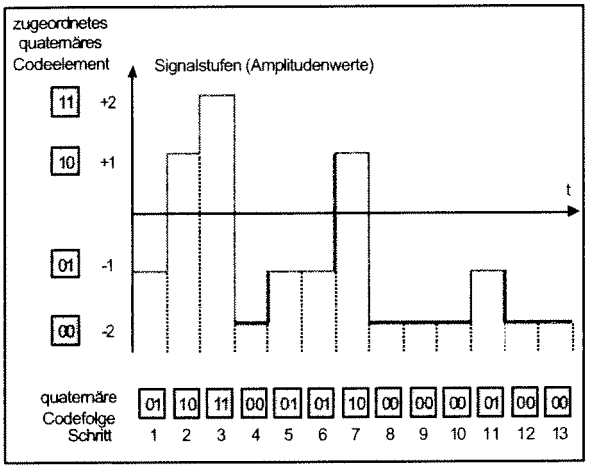


Bild: Mehrwertiges Digitalsignal

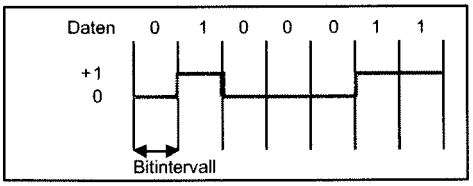
- **Binäre Leitungscodes**
  Symbolwerte werden durch Signalwert bestimmt
- **Biphase Leitungscodes**
  Symbolwerte werden durch Phasensprünge codiert
- **Ternäre Leitungscodes**
  Die beiden Symbolwerte 0 und 1 werden in drei Codiersymbole (-1, 0, +1) abgebildet
- **Blockcodes**
  m Informationsbits werden als Block zusammengefasst und zu einem neuen Block der Länge n codiert (4B/5B, 5B/6B, ...)
- **Faltungscodes**
  - Codebits werden nicht blockweise, sondern kontinuierlich erzeugt
  - Das Codegedächtnis m gibt an, wie viele Informationsbits ein Codebit beeinflussen
  - Coderate r = k / n : pro Takt werden aus k Informationsbits n > k Codebits erzeugt(typische Coderaten 1/3 bis 7/8)

Bild: Unterteilung der Leitungscodes

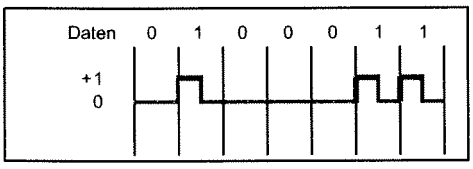
Wichtige Eigenschaften eines Leitungscodes

- **Taktrückgewinnung**
  - Den Signalwerten können Zeichenwerte und Takt entnommen werden
  - Die Taktrückgewinnung ist erforderlich, wenn keine separate Taktleitung zur Verfügung steht
  - Taktgehalt eines Codes sollte möglichst unabhängig vom Inhalt der übertragenen Daten sein
- **Gleichstromanteil**
  - Auf manchen Übertragungsstrecken darf wegen der angeschlossenen Geräte kein Gleichstrom auftreten
  - Kann meist nicht absolut, sondern nur im statistischen Mittel erfüllt werden
- **Fehlererkennung**
  - Signalfehler sollten auf Signalebene erkannt werden
- **Übertragungsreichweite**
  - Hängt mit der Betriebsdämpfung zusammen. Hohe Frequenzen werden stärker gedämpft als niedrige
- **Anzahl gemeinsam codierter Zeichen**
  - In einem Signalwert kann mehr als ein Zeichenwert codiert werden
- **Resynchronisation**
  - Wird meist durch Rahmenbildung ermöglicht

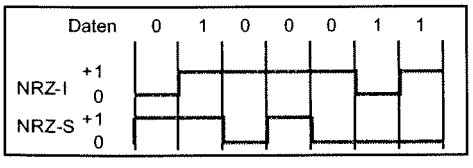
Bild: Leitungscodierung digitaler Signale



Non-Return to Zero (NRZ)
1 = hoher Pegel
0 = niedriger Pegel



Return to Zero (RZ)
1 = Signalübergang am Intervallanfang und Rücksetzung in der Mitte des Bit-Intervalls
0 = kein Signalübergang



Non-Return to Zero Inverse (NRZ-I)
1 = Signalübergang zu Intervallanfang
0 = kein Signalübergang

Non-Return to Zero Space (NRZ-S)
1 = kein Signalübergang
0 = Signalübergang zu Intervallanfang

Bild: Leitungscodierung: NRZ (Non-Return to Zero) – RZ (Return to Zero)

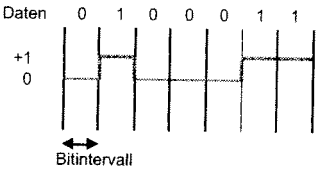
Binärer Code

Kennzeichen
- fester Pegel während eines Bitintervalls
- Signalübergänge (Signalwechsel) erfolgen an den Intervallgrenzen

Non-Return to Zero
"1" hoher Pegel
"0" niedriger Pegel

Eigenschaften
- sehr einfach zu implementieren
- NRZ ist Standard innerhalb von Digitalgeräten (Rechnern, usw.)
- Entspricht Einfach- oder Doppelstromverfahren bei der Telegrafie
- Gleichstromkomponente kann hoch sein
- eignet sich nicht zur Taktrückgewinnung

Bild: NRZ: Non-Return to Zero



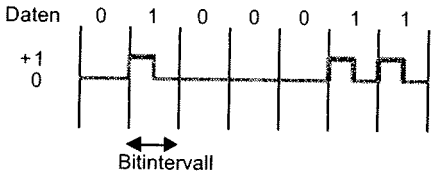
Der **NRZ-Code** *(Non-Return to Zero)* verwendet als Signalelement eine Spannung von (beispielsweise) 0 V für eine logische 0 und (beispielsweise) +5 V für eine logische 1. Beide Signalemente weisen für die Symboldauer, die hier der Bitdauer entspricht, konstante Werte auf.

Binärer Code

Einfacher Ansatz: "1" wird als high-Signal dargestellt; "0" als low-Signal
- Zwei Klassen solcher Codes, um Bitfolgen zu codieren
  - RZ (Return to Zero)
  - NRZ (Non-Return to Zero)

Return to Zero
- Gekennzeichnet durch einen Rechteckimpuls in der 1. Hälfte des Bitintervalls für das Datenelement "1"
- Danach Rückkehr in Grundzustand (Zero)
- Baudrate (Schrittgeschwindigkeit) ist im Extremfall (Folge von "1") doppelt so hoch wie Bitrate
- Bei Null-Folge keine Taktrückgewinnung möglich
- Gleichstromanteil kann hoch werden

Bild: RZ: Return-to-Zero



Beim **RZ-Code** *(Return to Zero)* ist das Signalelement für eine logische 1 eines Pulses (+5 V für die erste Hälfte der Symboldauer, 0 V für die zweite Hälfte).

Es wird nicht der absolute Signalwert in der Zuordnungsvorschrift verwendet, sondern der Signalwert in Abhängigkeit von der Polarität des vorhergehenden Signalelements codiert

- Biphase Code
- Vorteil: Unter Einfluss von Störungen sind Signalwechsel leichter zu erkennen als Signalpegel, die mit einer Schwelle verglichen werden müssen

NRZ-I (Inverse)
- Übergang in den entgegengesetzten Signalwert zur Darstellung einer übertragenen "1"
- kein Wechsel bei "0"
- hoher Gleichstromanteil möglich
- Taktrückgewinnung nicht immer gegeben

NRZ-S (Space)
- Wie NRZ-I, aber Signalwechsel bei übertragener "0"

Bild: Differentielle Codierung

Non-Return to Zero (NRZ)
1 = hoher Pegel
0 = niedriger Pegel

Non-Return to Zero Inverse (NRZ-I)
1 = Signalübergang zu Intervallanfang
0 = kein Signalübergang

Non-Return to Zero Space (NRZ-S)
1 = kein Signalübergang
0 = Signalübergang zu Intervallanfang

Return to Zero (RZ)
1 = Signalübergang am Intervallanfang und Rücksetzung in der Mitte des Bit-Intervalls
0 = kein Signalübergang

Bild: Zusammenfassung der NRZ und RZ Codes

Manchester Code

Signalelemente des Manchester-Codes, die bipolare Spannungspegel U+ und U- sowie eine Flanke zur Bitmitte (deshalb auch als Biphase-Code bezeichnet) aufweisen.

Die Signalelemente J und K entsprechen nicht dieser Definition und werden deshalb als **Codeverletzungen** (code violation) bezeichnet. Diese werden für besonders wichtige Kennzeichnungen eingesetzt, z. B. Rahmenanfang oder –ende.

Die Manchester-Codierung setzt für jedes zu codierende Bit das entsprechende Signalelement ein. Dabei können sich weitere Flanken zwischen aufeinander folgenden Signalelementen ergeben.

Biphase Code

Mindestens ein Signalwechsel pro Bitintervall; Maximal zwei Signalwechsel pro Bit
- 1 = Signalübergang vom hohen Pegel zum niedrigen Pegel in der Intervallmitte
- 0 = Signalübergang vom niedrigen Pegel zum hohen Pegel in der Intervallmitte
- Erzeugbar über XOR -Verknüpfung von NRZ-codierten Daten und dem Takt
  Hilfswechsel erforderlich (erhöht Baudrate)

Vorteile

- Leichte Taktrückgewinnung, da stets mindestens ein Signalwechsel pro Bitintervall
- Keine Gleichstromkomponente
- Fehlererkennung auf Signalebene: Fehlen eines erwarteten Übergangs erkennbar (Verwendung: Ethernet)

Nachteile

Verdoppelt die Rate von Signalwechseln auf der Leitung (Baudrate steigt)
- im schlimmsten Fall ist Bitrate = 50% Baudrate, (d.h. Baudrate größer als Bitrate)
- Baudrate kann auch kleiner als Bitrate sein
- Übertragung von vier unterschiedlichen Signalen

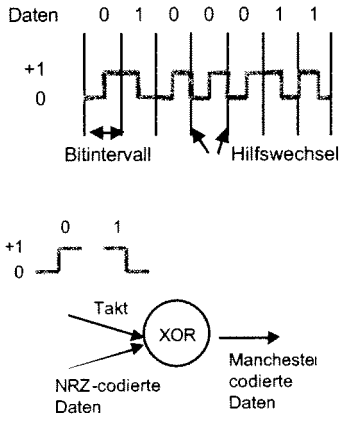
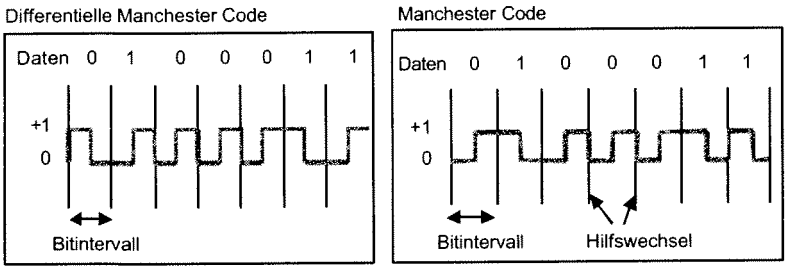


Bild: Manchester Code



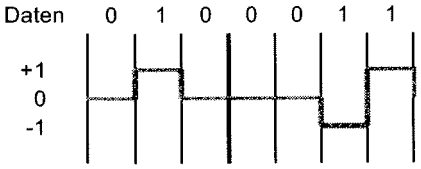
Beim differenziellen Manchester-Code hängt die Auswahl eines Signalelements vom vorhergehenden Signalelement wie folgt ab: für eine logische 0 muss zum Symbolanfang eine Flanke (Übergang 0 zu 1 oder umgekehrt) entstehen, bei einer logischen 1 darf hingegen keine Flanke auftreten.

Biphase Code

Signalwechsel in der Mitte jedes Bitintervalls
Signalwechsel am Anfang eines Bitintervalls nur, wenn "0" codiert wird
- Ausgabesignal von Startlevel abhängig
- Polaritätsunabhängig

Diese Art der Codierung wird beispielsweise im lokalen Netz Token Ring eingesetzt

Bild: Differentieller Manchester Code



Beim **AMI-Code** *(Alternate Mark Inversion)* wird als Symbol für eine logische 1 abwechselnd ein konstanter Wert von +5 V bzw. -5 V verwendet.

Bild: AMI-Code (Alternate Mark Inversion)

Ternärer Code

Leitungscodierung mit mehr als zwei Signalwerten
- keine Gleichstromkomponente
  - Problem: lange "0"-Folgen
  - Lösung: Zwei aufeinanderfolgende "0"en werden durch eine "0" und eine umgekehrte "1" codiert
- einfache Taktrückgewinnung

Beispiel: AMI-Codierung (Alternate Mark Inversion)
- AMI-NRZ: Darstellung von "1" abwechselnd durch positiven oder negativen Impuls in der 1. Hälfte des Bitintervalls
- AMI-RZ: in der Mitte von einer 1-Codierung wird auf den Null-Wert gewechselt

Bild: AMI-Code (Alternate Mark Inversion)

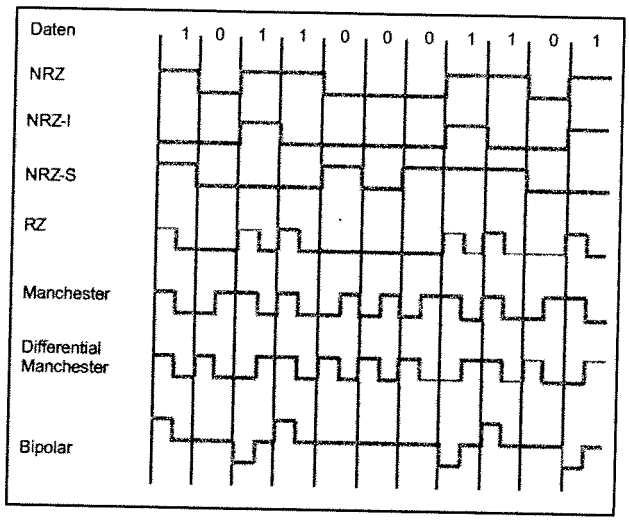


Bild: Leitungscodes

4-Bit Daten	5-Bit Code
0000	11110
0001	01001
0010	10100
0011	10101
0100	01010
0101	01011
0110	01110
0111	01111
1000	10010
1001	10011
1010	10110
1011	10111
1100	11010
1101	11011
1110	11100
1111	11101

- Einfügen zusätzlicher Bits, um "0" bzw. "1"- Folgen zu vermeiden
- 4 Bit Daten werden in 5 Bit Code codiert
  - nicht mehr als eine führende "0"
  - nicht mehr als zwei abschließende "0"
- Übertragung mit NRZ-I
- 80% Effizienz

Bild: Blockcode: 4B/5B-Code

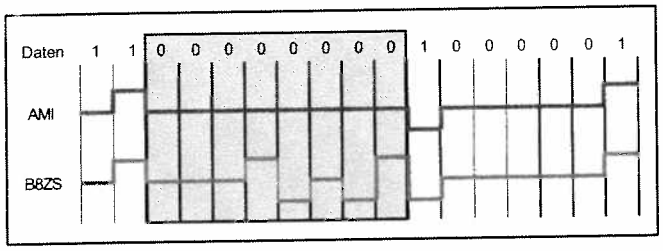
Der 4B5B-Code ist ein Beispiel eines (m-zu-n)-Codes. Dabei werden 16 verschiedene Bitkombinationen auf 32 Codewörter abgebildet. Die Hälfte der 32 Codewörter kann demnach für die Codierung zusätzlicher Informationen genutzt werden, die entsprechenden Codewörter können als Codeverletzungen betrachtet werden. Die Codewörter werden so gewählt, dass nie mehr als zwei Nullen nacheinander auftreten. Zusätzlich wird eine NRZI-Codierung (Non-Return to Zero Invert) eingesetzt. Diese codiert eine Null mit demselben Spannungspegel wie das vorhergehende Bit, bei einer Eins wird der Spannungspegel invertiert. Insgesamt erhält man ein Leitungssignal mit zahlreichen Übergängen (gute Taktregenerierung) und einer gegenüber der NRZ-Codierung nur um 25 % höheren Bandbreite. Weitere Codes (8B10B, 8B6T).

Biphase-Codes werden in lokalen Netzen bis zu einer Datenrate von ca. 10 Mbit/s eingesetzt, nicht aber für Weitverkehrsnetze

Zielsetzung
- Sequenzen von Bits, die über eine längere Zeit keine Signalwechsel erzeugen, werden durch Füllsequenzen ersetzt, um die Synchronisation aufrecht zu erhalten
- Füllsequenz muss vom Empfänger erkannt und durch die Originalsequenz ersetzt werden
- Die Länge der Füllsequenz entspricht derjenigen der Originalsequenz

Beispiele
- B8ZS: Bipolar with 8-zeros substitution (häufig in Nordamerika verwendet)
- HDB3: High-density bipolar with 3 zeros (häufig in Europa und Japan eingesetzt)

Bild: Verwürfelung (Scrambling)

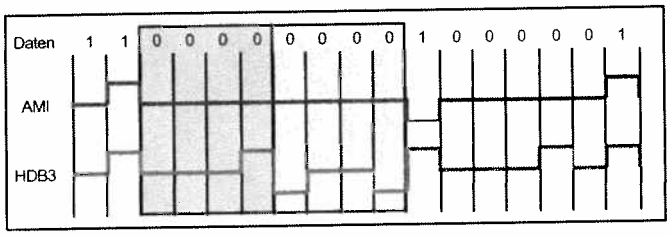


Basiert auf AMI
- Bei AMI können lange Nullfolgen zum Synchronisationsverlust führen

Auftreten von 8 Nullen in Folge
- Letzter vorangegangener Puls positiv: 8 Nullen werden als 000+-0-+ codiert
- Letzter vorangegangener Puls negativ: 8 Nullen werden als 000-+0+- codiert

Führt zu zwei Coderegelverletzungen innerhalb eines Wortes

Bild: B8ZS: Bipolar with 8-Zeros Substitution



Basiert auf AMI
- Bei AMI können lange Nullfolgen zum Synchronisationsverlust führen

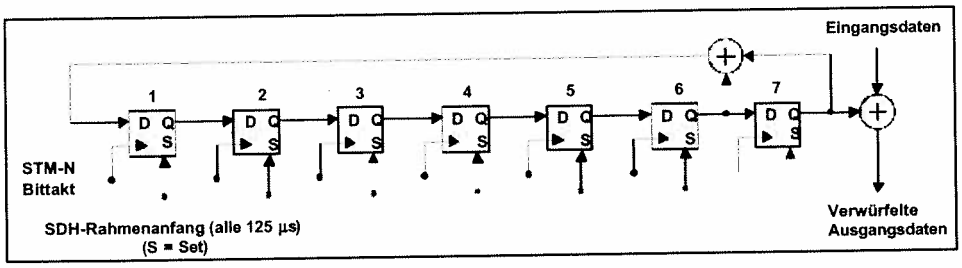
- Auftreten von 4 Nullen in Folge

Ersetzungen — Anzahl von Pulsen seit letzter Ersetzung

Letzter Puls	Gerade	Ungerade
Negativ	000-	+00+
Positiv	000+	-00-

Bild: HDB3: High-Density Bipolar with 3 Zeros

Ein Scrambler und Descrambler dienen der Taktrückgewinnung. Es ist wichtig, dass der im Empfänger erzeugte Takt dem Sendetakt genau entspricht. Die Taktrückgewinnung wird durch eine quasi zufällige Bitfolge wesentlich erleichtert. Deshalb setzt man im Sendeteil einen Scrambler (Verwürfler) ein. Er erzeugt aus der zu sendenden Bitfolge nach einer Operation A eine Pseudozufallsfolge. Dabei muss auf der Empfangsseite durch einen kompatiblen Descrambler (Entwürfler) nach einer Umkehroperation A' die ursprüngliche Bitfolge wiederhergestellt werden. Die Scrambler-Operation A wird in Modem-Standards festgelegt. Ein Scrambler und Descrambler besteht aus einem mehrstufigen Schieberegister mit entsprechenden Rückkopplungen. Der Scrambler verwürfelt die einzelnen Bits in der zu sendenden Folge, so dass lange Sequenzen von Nullen oder Einsen unterdrückt werden. Dadurch kann der Empfänger sicherer den Takt aus dem Empfangssignal ableiten.



- Polynom: $1 + x^6 + x^7$
- Anfangswert am Anfang jedes SDH-Rahmens = 1111111
- Entwürfler gleich (Verwürfelte Eingangsdaten → Ausgangsdaten)
- Verwürfler (Scrambler); Entwürfler (Descrambler)

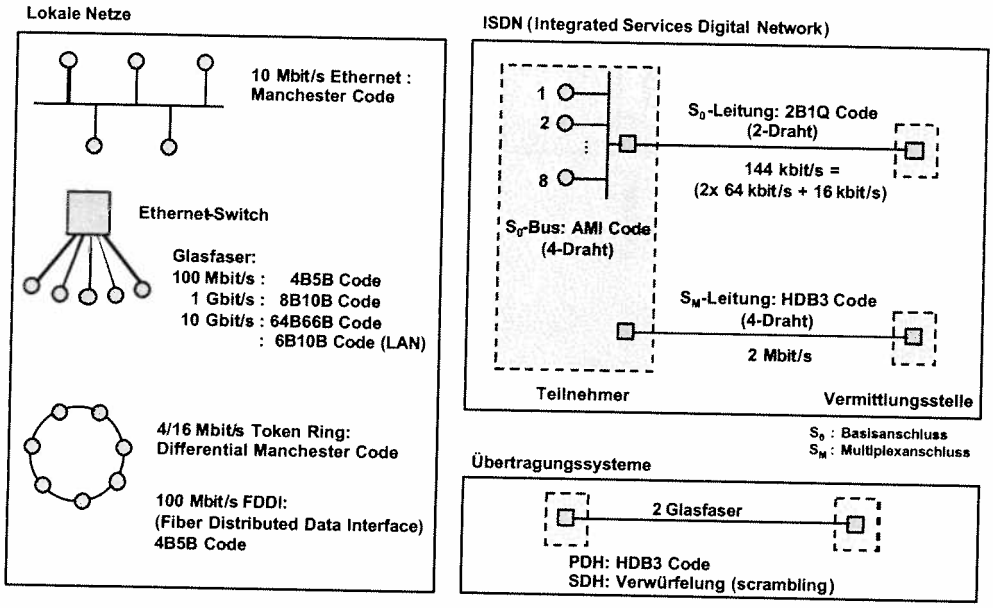
Bitraten: STM-1 = 155 Mbit/s
STM-4 = 622 Mbit/s
STM-16 = 2,5 Gbit/s
STM-64 = 10 Gbit/s

STM : Synchronous Transfer Module

⊕ Modulo 2 Addition oder XOR (exclusive OR): 1 + 1 = 0 1 + 0 = 1
0 + 0 = 0 0 + 1 = 1

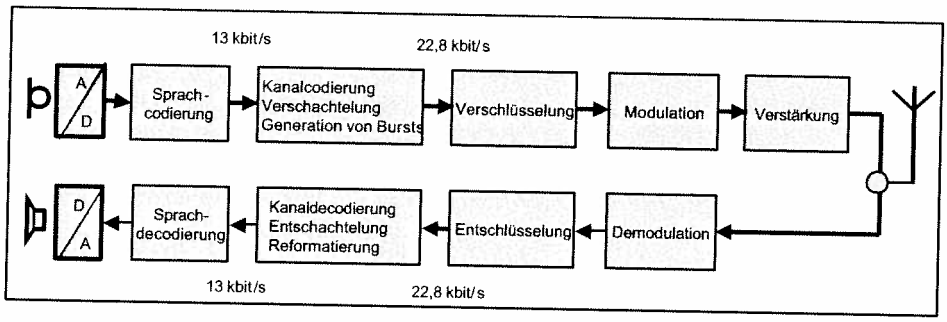
Bild: Synchroner SDH-Verwürfler (Scrambler)

Beim synchronen SDH-Scrambler werden die Eingangsdaten mit den Registerdaten aufgrund einer XOR-Verknüpfung verwürfelt. Alle 125 µs (Anfang des SDH-Rahmens) wird der Schieberegister mit lauter Einser initialisiert. Das Verfahren am Sender und am Empfänger ist gleich.



Das Bild zeigt die Leitungscodes für einige Netzsysteme.

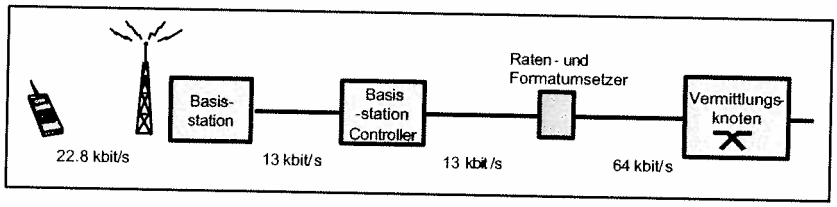
Bild: Verwendung der Leitungscodes



In GSM wird eine spezielle Sprachcodierung verwendet. Sie unterdrückt Gesprächspausen und komprimiert die Sprachinformation. Nach dieser Quellencodierung wird zur Übertragung über den schlechten Funkkanal Zusatzinformation hinzugefügt.

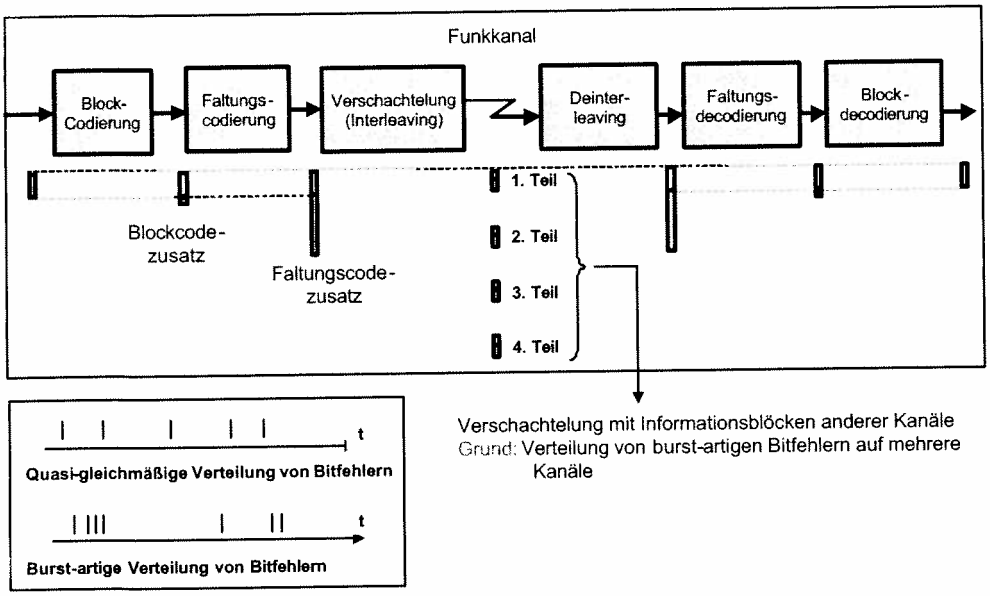
Bild: GSM-Codierung im Mobilgerät

Die Kanalcodierung besteht auf drei Stufen: Blockcodierung, Faltungscodierung und Bitverschachtelung. Eine zusätzliche Verschlüsselung ist für die Abhörsicherheit erforderlich. Die Modulationsstufe verschiebt das digitalcodierte Basissignal auf einen der GSM-Trägerfrequenzen. Für Daten entfällt die Quellencodierung. Auf der Funkschnittstelle ist die GSM-Bitrate 22,8 kbit/s (inklusive 9,8 kbit/s Kanalcodierung).



Zwischen Basisstation und einem sogenannten TRAU (Transcoding and Rate Adaptation Unit) gilt die GSM-Grundrate von 13 kbit/s, die auf die in Sprachnetzen übliche Kanalrate von 64 kbit/s umgesetzt werden muss. Gleichzeitig muss die GSM-Codierung auf PCM (A-law oder μ-law) umcodiert werden.

Bild: GSM-Bitraten



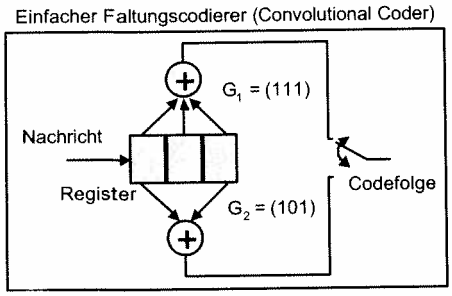
Das Bild illustriert die Zunahme der Zusatzinformation sowie die Verschachtelung in Informationsblöcken (transmission burst), damit büschelartig auftretende Bitfehler über mehrere Sprach- oder Datenverbindungen verteilt werden.

Bild: Codierungsstufen über GSM-Funkkanal

Faltungscodes

Faltungscodes (convolutional codes) erzeugen aus den Informationsbits die Codebits nicht blockweise, sondern gleitend, wie bei einer Faltungsoperation (convolution), so z. B. für ein neues Informationsbit zwei neue Codebits. Statt der Blocklänge ist hier das Codegedächtnis M bzw. die Einflusslänge maßgebend. Letztere gibt an, von wievielen Informationsbits ein Codebit beeinflusst wird. Werden pro Takt aus K Informationsbits N > K Codebits erzeugt, so spricht man von der Coderate R = K/N.

Die Anzahl K ist üblicherweise klein (1 bis 7) und Coderaten von 1/3 bis 7/8 sind typisch. Die Codebits werden im allgemeinen von (M + 1) K Informationsbits erzeugt.



Coderate r = ½ (1 Bit 2 Bits)
Registertiefe K = 3
Eingangsbits per Takt k = 1
Verknüpfungsregel 1: G_1 = (111)
Verknüpfungsregel 2: G_2 = (101)

Einlaufende Bitstrom ...00101
Startwert (000): Codefolge 11,10,00,10,11
Startwert (100): Codefolge 01,01,00,10,11

Registeranfangswert: 000

Takt	Register	Codewort
Start	000	00
1	100	11
2	010	10
3	101	00
4	010	10
5	001	11

Registeranfangswert: 100

Takt	Register	Codewort
Start	100	11
1	110	01
2	011	01
3	101	00
4	010	10
5	001	11

Das Bild zeigt einen einfachen Faltungscodierer. Die Registertiefe K ist 3. Bei jedem Takt wird ein neues Bit im Register aufgenommen und das älteste Bit vernichtet. Bei jedem Takt werden auch zwei Verknüpfungen G_1(111) und G_2(101) durchgeführt. Bei Verknüpfungsregel 1 werden alle drei Bits XOR des Registers verknüpft. Bei Verknüpfungsregel 2 werden Bits 1 und 3 XOR verknüpft. Bei jedem Takt werden dadurch zwei Codebits erzeugt. Das Bild zeigt ein Beispiel für einen bestimmten Bitstrom am Eingang. Dabei werden zwei Registeranfangwerte betrachtet: Anfangswert 000 und Anfangswert 100.

Bild: Faltungscodierung

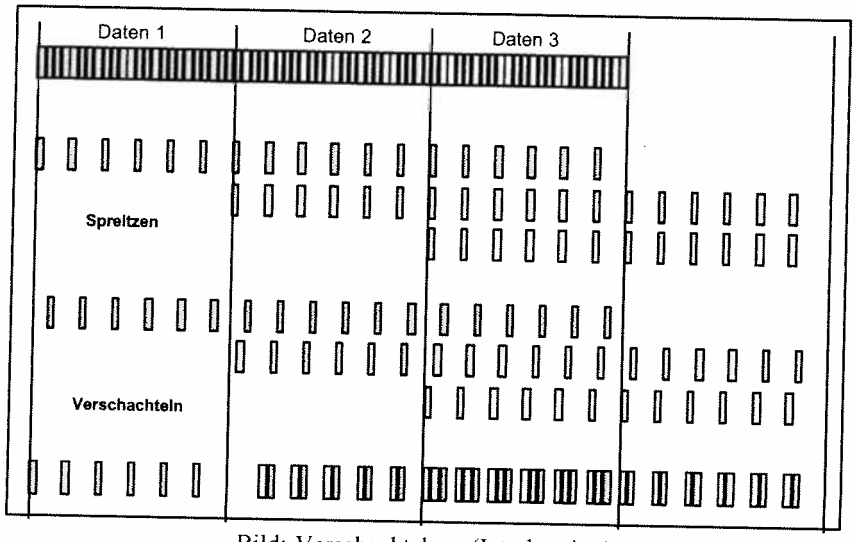
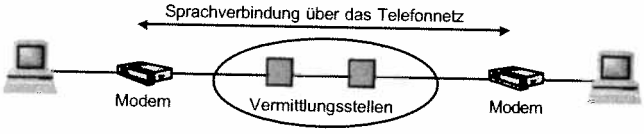


Bild: Verschachtelung (Interleaving)

Das illustriert die Verschachtelung von Informationsblöcken durch Aufspreizen mit zeitlichen Verzögerungen, einer Zusatzverzögerung und Überlagerung. Beim Empfänger ist die Umkehrvorgang notwendig.

Datenmodems



- **Datenübertragung über das analoge Telefonnetz**
  Telefonnetz überträgt Frequenzen zwischen 300 Hz und 3400 Hz
- **Modulation**
  - Änderung von Signalparametern (Amplitude, Frequenz, Phase) eines Trägersignals durch ein modulierendes Signal
  - Wandlung digitaler in analoge Signale
- **Demodulation**
  - Rückgewinnung des modulierenden Signals
  - Wandlung analoger in digitale Signale

Bild: Analoge Übertragung digitaler Daten

Der Begriff Modem ist ein Kunstwort aus Modulation und Demodulation. Diese zwei Begriffe repräsentieren die wichtigsten Eigenschaften. Ein Modem sorgt dafür, dass die von einem Rechner (häufig von einem PC) ankommenden digitalen Datensignale für die Übertragung über eine analoge Leitung oder über ein analoges Fernsprechnetz in analoge Datensignale umgewandelt werden. Dieser Vorgang wird als Modulation bezeichnet. Sie beruht auf den Veränderungen eines Trägersignals durch das digitale Datensignal und wird an der Sendeseite im Modulator durchgeführt. Umgekehrt erfolgt am Ziel die Umwandlung der analogen Datensignale in digitale Datensignale. Dies nennt man Demodulation, und sie wird im Demodulator realisiert.

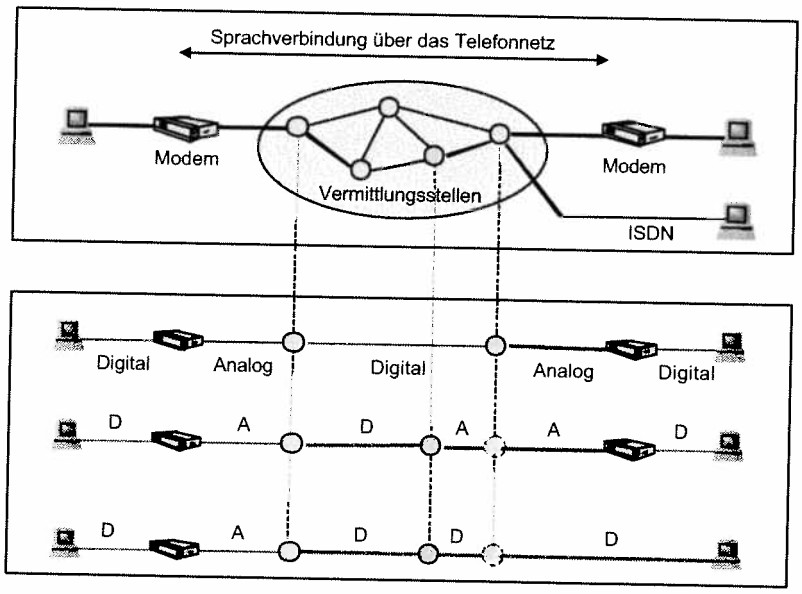


Bild: Analoge Übertragung von digitalen Signalen

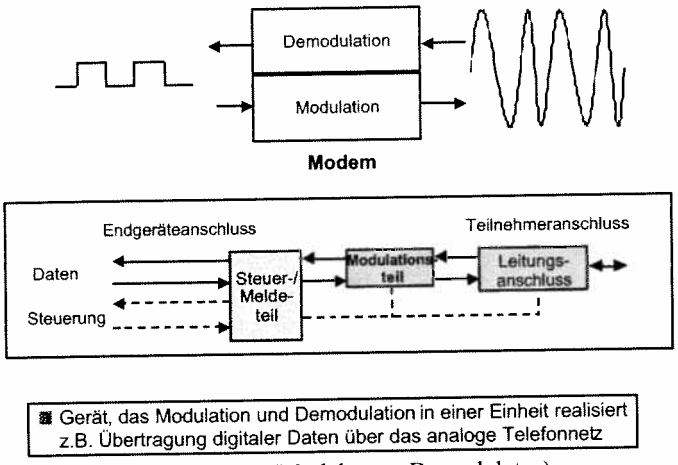


Bild: Modem (Modelator - Demodulator)

In jedem Modern sind zwei Gruppen von Komponenten zu unterscheiden, die folgende Teile bilden:

- Sendeteil: Hierzu gehören folgende Funktionsmodule: Scrambler, Codierer, Modulator und Ausgangsfilter.
- Empfangsteil: Zu diesem Teil gehören: Eingangsfilter, Entzerrer, Demodulator, Decodierer und Descrambler.

Zusätzlich muss ein Taktgeber vorhanden sein, der die erforderlichen Taktsignale erzeug. Als Schnittstelle DTE/DCE wird in diesem Fall oft die Schnittstelle V.24 eingesetzt.

Eine Steigerung der Übertragungsrate bei gleichzeitiger Verbesserung der Übertragungsqualität ist in den high-speed (HS) Modems durch die zusätzliche Umcodierung nach dem Verwürfeln im Scrambler der zu sendenden Daten realisiert. Insbesondere in Modems nach den ITU-T-Standards V.32, V.32bis und V.34 wird die sogenannte Trellis-Codierung eingesetzt. Diese Codierung ist durch die zugefügte Redundanz gekennzeichnet, die eine Fehlererkennung und -korrektur ermöglicht.

Die umcodierte Bitfolge wird weiter im Modulator in analoge Signale umgewandelt. Im Ausgangsfilter werden die irrelevanten Frequenzanteile des analogen Datensignals ausgefiltert. Der Ausgangsverstärker übernimmt die Anpassung der Sendeleistung an die Leitungsanforderungen.

Die empfangenen analogen Datensignale werden nach entsprechender Verstärkung dem Entzerrer zugefügt. Mit dem Entzerrer werden die Signalverzerrungen (Signalverletzungen) beseitigt, die während der Übertragung entstanden sind. Eine genaue Entzerrung bieten erst adaptive (selbstanpassende) Entzerrer. Solche Entzerrer werden vor allem in HS-Modems eingesetzt. Die analogen Signale werden nach der Entzerrung im Demodulator in eine digitale Bitfolge umgewandelt. Diese Bitfolge wird im Decodierer in eine binäre Bitfolge umcodiert, aus der im Descrambler die Daten zurückgewonnen werden.

Da es bei Modems verschiedene Bitraten gibt, wurden ITU-T-Standards - sogenannte V-Standards - definiert, damit Modems unterschiedlicher Hersteller miteinander kommunizieren können. Bei der Datenübertragung über Modem müssen beide Seiten den selben Modem-Standard unterstützen.

Modudulation

Informationstragende elektrische Signale sind in der Regel Basisbandsignale (Tiefpasssignale), die einen Frequenzbereich von 0 bis f_{max}, belegen. In LANs werden die Basisbandsignale direkt übertragen. Für die Nutzung von Multiplex-Verfahren und bei der drahtlosen Übertragung muss jedoch der Frequenzbereich nach höheren Frequenzen verschoben werden. Dazu wird die Modulation genutzt. Das Nutzsignal wird auf einen Träger (carrier) aufmoduliert und liegt dann als so genanntes Breitbandsignal (auch Bandpasssignal) in einem Frequenzbereich zwischen f_{min} und f_{max} vor. Dabei unterscheidet man:

- Analoge Modulation: Der Träger ist eine sinusförmige Schwingung.
- Digitale Modulation: Der Träger ist ein Puls (eine periodische Folge von Impulsen einer bestimmten Form, deshalb auch die Bezeichnung Pulsmodulation.

Analoge Modulation

Die allgemeine Form einer modulierten Sinusschwingung lautet: $am(t) = (1 + a) \sin(2\pi ft + \varphi)$

Dabei ist am(t) der Augenblickswert der Amplitude des modulierten Signals (hier dimensionslos angegeben), (1+a) die Amplitude f die Frequenz und (p die Phase des Trägers. Die Größen a, f und φ können durch das aufzumodulierende Nutzsignal verändert werden.

Entsprechend ergeben sich die analogen Modulationsarten:

- AM, Amplitudenmodulation (Amplitude Modulation): a wird moduliert,
- FM, Frequenzmodulation (Frequency Modulation): f wird moduliert
- PM, Phasenmodulation (Phase Modulation): φ wird moduliert.

Die Verfahren unterscheiden sich bezüglich des Aufwandes für Modulation und Demodulation (Rückgewinnung des Nutzsignals aus dem modulierten Signal), der für das modulierte Signal erforderlichen Bandbreite und Störsicherheit der Übertragung. Die analogen Modulationsverfahren können in Kombination eingesetzt werden, was bei Modems, xDSL und bei der Funkübertragung häufig genutzt wird.

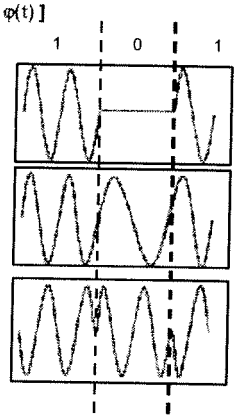
Digitale Modulation

Digitale Modulationsverfahren verwenden als Träger einen Puls (Pulsfolge). Ein Puls ist eine periodische Folge von Impulsen einer bestimmten Amplitude A, Frequenz f = 1/T und Impulsdauer D.

Die wichtigsten digitalen Modulationsverfahren sind:

- **PAM (Pulsamplitudenmodulation):** Für jeden Impuls ist die Amplitude A proportional zum augenblicklichen Wert des Nutzsignals.
- **PFM (Pulsfrequenzmodulation):** Die augenblickliche Frequenz f = 1/T der Impulsfolge ist proportional zum Augenblickswert des Nutzsignals.
- **PPM (Pulsphasenmodulation):** Die Phase eines Impulses (die Abweichung seines Startzeitpunktes vom Startzeitpunkt im unmodulierten Fall) ist proportional zum Augenblickswert des Nutzsignals. Die Frequenz der Pulsfolge ist konstant.
- **PDM (Pulsdauermodulation):** Die Dauer D eines Impulses ist proportional zum Augenblickswert des Nutzsignals, Die Frequenz der Pulsfolge ist konstant.
- **PCM (Pulscodemodulation):** Hier werden binäre Impulsfolgen als Zahlenwerte interpretiert, die den Nutzsignalwert repräsentieren.
- **DPCM (Differenzielle PCM) und DM (Deltamodulation)** unterscheiden sich von der PCM dadurch, dass nur Differenzen zwischen aufeinander folgenden Signalwerten übertragen werden. DPCM und DM können als Verfahren zur Quellencodierung betrachtet werden, die bei Signalen mit langsam veränderlichen Signalwerten eine erhebliche Redundanzminderung bewirken.

Modulationssignal: Sinusschwingung: $S(t) = A(t) \sin [2\pi f(t) + \varphi(t)]$
Informationssignal: digitale Bitfolge



- **Amplitudenmodulation (AM)**
  - technisch einfach, benötigt wenig Bandbreite, störanfällig
  - Beispiel: Kurzwellenfunk, optische Übertragung
- **Frequenzmodulation (FM)**
  - größere Bandbreite
  - verändert die Frequenz des Trägersignals
  - Beispiel: Hörfunkübertragung
- **Phasenmodulation (PM)**
  - verändert Phase der Sinus-Schwingung
  - Arten
    - phasenkohärent: Vergleich mit Referenzsignal
    - differenziell: Sprung gegenüber letzter Phase (z.B. 90°/270°)
  - robust
  - Beispiele: Richtfunk, Mobilfunk, Modems, xDSL
- **Kombination von Amplituden- und Phasenmodulation**

Andere Bezeichnung: **Umtastung (Shift Keying)**

Bild: Modulation

Modulationsprinzipien

Im allgemeinen besteht die Modulation in der Veränderung von Parametern einer analogen Schwingung, die als Datenträgersignal dient, durch die zu sendenden Daten. Als Signalparameter einer Sinusschwingung kommen die Amplitude, die Frequenz und die Phase in Betracht. Die einfachste Form der Modulation beruht auf der Veränderung nur eines Parameters, so dass man von Amplituden-, Frequenz- oder Phasenmodulation spricht.

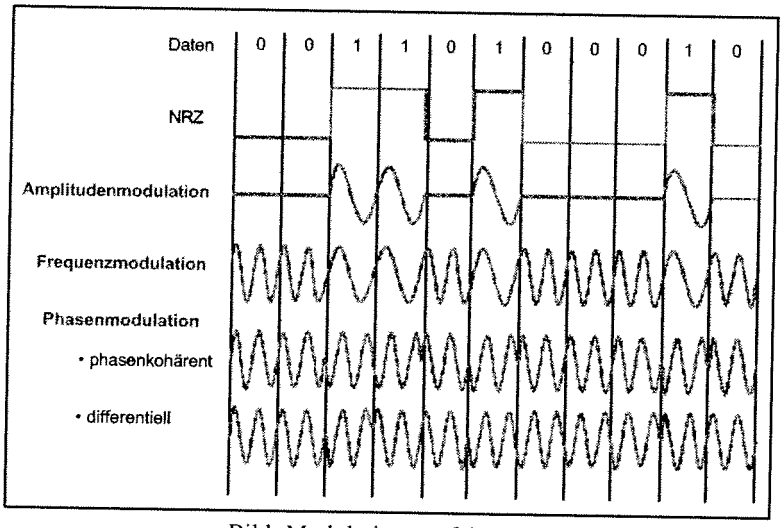


Bild: Modulationsverfahren

Bei der Amplitudenmodulation (AM) wird die Amplitude eines analogen Datenträgers (z. B. Sinusschwingung) entsprechend dem Verlauf von Daten verändert. Eine AM mit einem binären Datensignal besteht in der einfachsten Form aus dem Ein- und Ausschalten einer Trägerschwingung. Reine Amplitudenmodulation hat keine Bedeutung in der Praxis.

Bei der Frequenzmodulation (FM) werden die zu übertragenden Daten durch die Frequenzänderung der Trägerschwingung dargestellt. Die Schwingung mit der höheren Frequenz entspricht der binären "0". Die Frequenzmodulation ermöglicht nur die Übertragungsgeschwindigkeiten bis 1.2 kbit/s und wird in Modems nach V.21 und V.23 eingesetzt.

Bei der Phasenmodulation (PM) wird die Phase einer Trägerschwingung in Abhängigkeit vom zu übertragenden Bitstrom verändert. Zur Wiedergewinnung von Daten an der Empfangsseite muss ein Phasenvergleich der Phase des empfangenen

Datensignals mit einer Bezugsphase durchgeführt werden. Das es aufwendig ist, die Phasendemodulation zu realisieren, verwendet man in der Praxis die Phasendifferenzmodulation, die kurz als DPSK (Differential Phase Shift Keying) bezeichnet wird. Der Vorteil der DPSK liegt in der einfachen Art der Demodulation.

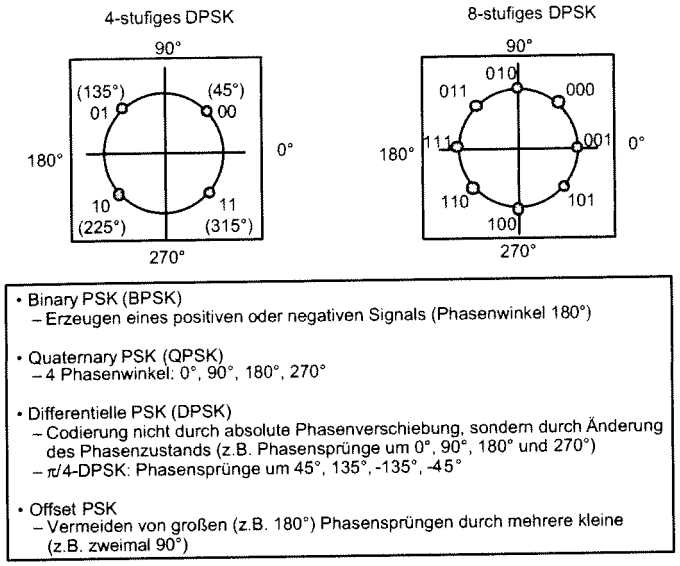


Bild: Phase Shift Keying (PSK)

In Modems für die Übertragungsgeschwindigkeiten 1.2, 2.4 und 4.8 kbit/s wird mehrstufige DPSK eingesetzt, so dass der ankommende binäre Datenstrom umcodiert werden muss. Diese Umcodierung besteht bei der 4-stufigen DPSK darin, dass jeweils zwei Bits zu einem Dibit zusammengefasst werden. Den einzelnen Dibit Zuständen werden entsprechende Phasensprünge zugeordnet. Bei der 8-stufigen DPSK werden jeweils drei Bits zu einem Tribit zusammengefasst und den einzelnen Tribit-Zuständen werden entsprechende Phasensprünge zugeordnet.
Im allgemeinen besteht eine mehrstufige Modulation darin, dass die zu übertragenden Bits zu den (Daten-) Symbolen zusammengefasst und den einzelnen Symbolen entsprechende Trägersignale zugeordnet werden. Die Anzahl der Symbole pro Sekunde stellt die Symbolrate (Symbol Rate) dar, die auch als Schrittgeschwindigkeit bezeichnet wird.

Der Hauptvorteil aller mehrstufigen Modulationsarten beruht darauf, dass die Übertragungsrate auf der Leitung als Symbolrate nur ein Teil der Übertragungsgeschwindigkeit ist. Bei der 4stufigen bzw. 8stufigen DPSK geht die Schrittgeschwindigkeit auf die Hälfte bzw. auf ein Drittel der Übertragungsgeschwindigkeit zurück.

Die zu sendenden Symbole (als Gruppen von Bits) bei einer mehrstufigen Modulation können in dem Signalraum in Form eines Signalzustanddiagramms dargestellt werden. Das Signalzustanddiagramm nach ITU-T Empfehlung V.26 (sog. Alternative A) für die 4-stufige DPSK. Es ist hier zu bemerken, dass die einzelnen Symbole (Dibits) als Punkte gleichmäßig verteilt sind. Dadurch sind die Abstände zwischen den benachbarten Punkten möglichst groß und somit lassen sich Fehlentscheidungen vermeiden.

Da alle Punkte auf einem Kreis liegen, haben die zu sendenden Trägersignale für alle Symbole die gleiche Amplitude. Der Modulationsvorgang bei der 4-stufigen DPSK läuft wie folgt ab:

- Wird 00 gesendet, so erfolgt der Phasensprung um 45°.
- Wird 01 gesendet, so erfolgt der Phasensprung um 135° usw. Jeder Phasensprung bezieht sich auf die vorherige Phasenlage. Eine absolute Bezugsphase ist nicht erforderlich.

Das Signalzustanddiagramm nach ITU-T-Empfehlung V.27 für die 8-stufige DPSK ist ebenfalls gezeigt. Aus diesem Diagramm kann die Zuordnung der Phasensprünge von Trägersignalen für die einzelnen Symbole (Tribits) abgelesen werden.

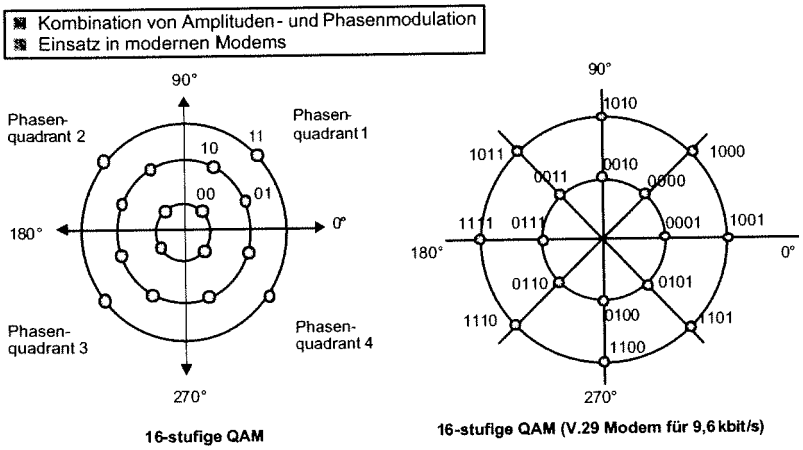
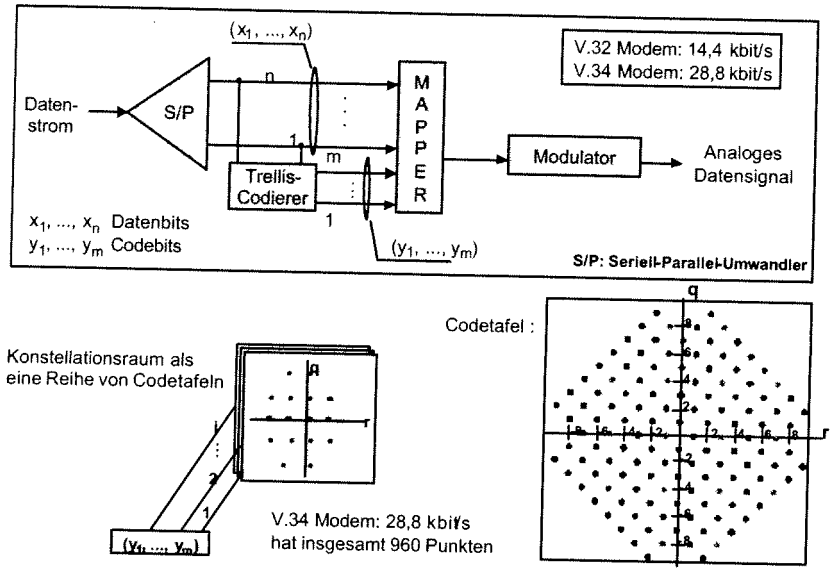


Bild: Quadratur-Amplituden-Modulation (QAM)

Bei den mehrstufigen DPSK-Verfahren sind die Punkte in den Zustandsdiagrammen auf einem Kreis verteilt. Dies bedeutet, dass die Trägersignale für alle Symbole die gleiche Amplitude haben. Eine weitere Erhöhung von Modulationsstufen kann durch die Veränderungen der Amplitude von Trägersignalen erfolgen. Dies führt zur sogenannten Quadraturamplitudenmodulation (QAM: Quadrature Amplitude Modulation). Unter der QAM ist im allgemeinen eine kombinierte Amplituden- und Phasendifferenzmodulation zu sehen.

Bei der QAM werden mehrere Amplitudenstufen der Trägersignale für die zu übertragenden Symbole verwendet. Bei der QAM nach V.29 in den Modems mit der Bitrate 9.6 kbit/s werden jeweils vier Bits zu einem Symbol (Punkt) zusammengefasst. Das Bild zeigt die Verteilung dieser Symbole im Signalzustandsdiagramm. Ein Signalzustandsdiagramm wird bei der QAM auch als Konstellationsgitter bezeichnet.



Die QAM wird in Modems verwendet, in denen die Übertragungsgeschwindigkeiten 7.2 und 9.6 kbit/s unterstützt werden. Eine weitere Steigerung der Übertragungsgeschwindigkeit bei gleichzeitiger Verbesserung der Übertragungsqualität ist durch die sogenannte Trellis-Codierung (in Deutsch: Gitter-Codierung) zu erreichen. Diese Codierung wird in Modems mit der QAM eingesetzt. Dadurch lassen sich die Übertragungsgeschwindigkeiten 14.4 und 28.8 kbit/s erreichen. Die Modems mit diesen Übertragungsgeschwindigkeiten werden auch als High Speed Modems (kurz HS-Modems) bezeichnet.

Bild: Hochgeschwindigkeitsmodem

In HS-Modems wird die QAM mit der Trellis-Codierung verwendet. Auf diese Codierung beziehen sich die Modem-Standards V.32, V.32bis und V.34.

Die zu sendenden Bits werden nach der Seriell/Parallel-Wandlung zu den Bitgruppen $(x_1, ..., x_n)$ zusammengefasst und an einen Mapper weitergeleitet. Die Bitgruppen werden als Symbole (Punkte) im Konstellationsgitter dargestellt. Der Mapper hat die Aufgabe, das zu sendende Symbol einem Punkt im Konstellationsgitter optimal anzuordnen. Die Konstellation besteht z. B. beim Modems nach V.34 aus einem Gitter mit insgesamt 960 Punkten. Eine so große Anzahl von Punkten wird auf eine Reihe von Tafeln verteilt. Die einzelnen Tafeln werden durch die Codewörter am Ausgang des Trellis-Codierers ausgewählt.

Die Verteilung der zu sendenden Symbole auf mehrere Tafeln ermöglicht die Vergrößerung der Abstände zwischen den benachbarten Symbolen auf den einzelnen Tafeln. Dies führt zu Vermeidung der Fehlentscheidungen an der Empfangsseite. Dieses Prinzip hat nur dann Vorteile, wenn die Nummer der Tafel (d. h. Codewort am Ausgang des Trellis-Codierers) fehlerfrei ist. Dies bedeutet, dass die Tafelnummern besonders zuverlässig übertragen werden müssen.

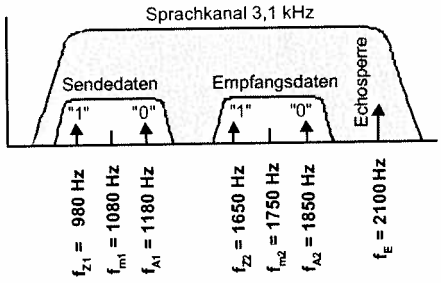
Im Trellis-Codierer wird sendeseitig eine Redundanz zugefügt, die eine Fehlererkennung und -korrektur ermöglicht. Diese Redundanz ist von den zuvor verarbeiteten Signalen (d. h. von der Vorgeschichte) abhängig. Die Vorgeschichte wird an der Empfangsseite ebenfalls berücksichtigt. Hierfür wird ein sogenannter Viterbi-Decoder verwendet, in dem mit Hilfe des Viterbi-Algorithmus die Vorgeschichte ermittelt wird. Der Decodierungsvorgang beruht darauf, dass alle möglichen Signalabläufe zurückverfolgt werden und der wahrscheinlichste Signalverlauf als der richtige ausgewählt wird. Mit diesem Verfahren lassen sich einzelne Bitfehler mit großer Wahrscheinlichkeit korrigieren. Bei den Gruppenbitfehlern funktioniert dieses Verfahren nicht immer sicher.

Standard	Modulations-verfahren	Anwendung
V.21	2 PSK	Duplexmodem mit 300 bit/s für Wahlleitungen
V.22	4 PSK	Duplexmodem mit 600 oder 1200 bit/s für Wahlleitungen
V.22bis	16 QAM	Duplexmodem mit 1200 oder 2400 bit/s für Wahlleitungen
V.32	32 QAM	Duplexmodem mit 4800 oder 9600 bit/s für Wahlleitungen
V.32bis	128 QAM	Duplexmodem bis 14400 bit/s für Wahlleitungen
V.34	960 QAM	Duplexmodem bis 33600 bit/s für Wahl- und Mietleitungen
V.90	128 PAM	Asymmetrisches Duplexmodem bis 56000 bit/s downstream und 33600 bit/s upstream
V.92	128 PAM	Erweiterung von V.90 mit diversen Zusatzmerkmalen sowie PCM-Übertragung

Bild: Datenmodems

- **MOD**ulator - **DEM**odulator
  - Modulation: Digitales Signal in analoges Signal
  - Demodulation: Analoges Signal in digitales Signal
- **Begrenzung der Übertragungskapazität durch Bandbreitenbeschränkung**
  - Sprachband: 300-3400 kHz
- **Begrenzung durch Signal/Rausch Verhältnis (SNR)**
  - SNR typisch 30-35 dB
  - max. 30-35 kbit/s

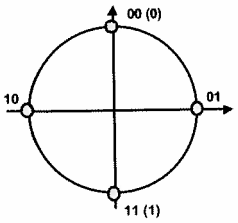
Bild: Modemübertragung



- Modulationsverfahren: 2-PSK
- Nutzung des Telefonkanals bis 300 bit/s, Vollduplex-Betrieb

Bild: Datenmodem: V.21

V.22

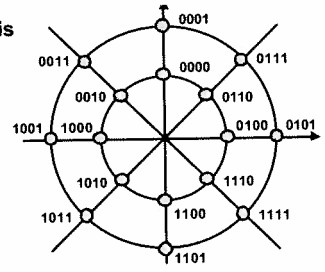


Modulation:
Phase Shift Keying (4-PSK)

Datenrate 1,2 kbit/s (600 Baud, 2 Bit)

Vollduplex
- Upstream: 1200 Hz
- Downstream: 2400 Hz

V.22bis



Modulation:
Quadrature-Amplitude Modulation (16-QAM)

Datenrate 2,4 kbit/s (600 Baud, 4 Bit)

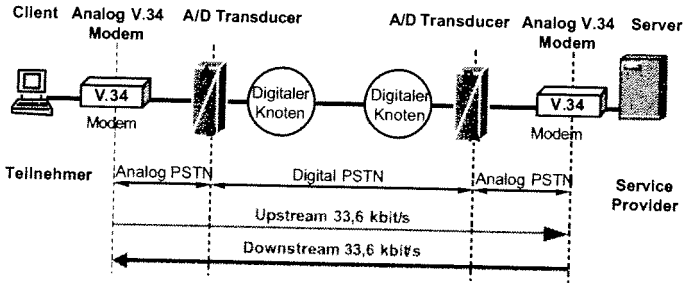
Vollduplex
- Upstream: 1200 Hz
- Downstream: 2400 Hz

Bild: Datenmodems: V.22 und V.22bis

V.32
- Modulation QAM
- Datenrate 9,6 kbit/s (2400 Baud, 5 Bit - 1 Redundanzbit)
- Up/Downstream: 1800 Hz
- Echokompensation

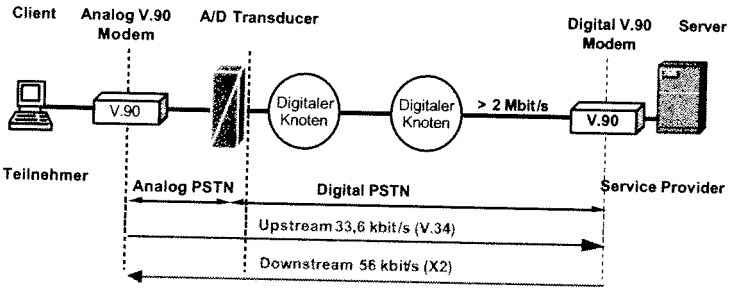
V.32bis
- Modulation QAM
- Datenrate 14,4 kbit/s (2400 Baud, 7 Bit - 1 Redundanzbit)
- Up/Downstream: 1800 Hz
- Echokompensation

Bild: Datenmodems: V.32 und V.32bis



- Modulation QAM
- Datenrate 33,6 kbit/s (2400-3200 Baud)
  - max. 35 kbit/s durch Quantisierungsrauschen des A/D-Wandlers
- Datensicherung und Datenkompression V.42
  - Kompressionsfaktor max. 4

Bild: Datenmodem: V.34



- Weniger Rauschen in Downstream Richtung durch optimale A/D-Wandlung (PCM) in modernen Vermittlungsstellen
- Nichtlineare A/D Wandlung (A-Law, μ-Law)
  - nur 7 Bit (56 kbit/s) von 8 Bit (64 kbit/s) können genutzt werden
- Ende-zu-Ende nur eine A/D-Wandlung möglich - Upstream V.34

Bild: Datenmodem: V.90

- **PCM Upstream**
  - max. 48 kbit/s
- **Modem-On-Hold**
  - Call Waiting Service ermöglicht das Anhalten der Modemverbinung um eingehende Anrufe zu beantworten.
- **Quick Connect**
  - Modem speichert Leitungscharakteristik und ermöglicht so einen schnelleren Verbindungsaufbau (<10 Sekunden).
- **V.44-Kompression**
  - V.42bis wird durch V.44 abgelöst. V.44 kann die Daten um rund 25% besser komprimieren (bis max 300 kbit/s).
- **V.59-Protokoll**
  - minimiert Störungen beim Datenaustausch

Bild: Datenmodem: V.92

xDSL (Digital Substriber Line)

Dies ist eine Technologie, die im allgemeinen. ungenutzte Frequenzbereiche von Kupferadern für Datenübertragung verwendet Verschiedene Varianten wie ADSL, SDSL oder VDSL werden zusammenfassend als xDSL bezeichnet. Die Entwicklungsanfänge gehen auf das Jahr 1987 zurück.

	Datenraten Downstream - Upstream	Entfernung km	Modulation	Bandbreite
VDSL	25 Mbit/s – 1,6 Mbit/s	0.9	QAM (DMT)	~30 MHz
ADSL	8 Mbit/s - 1 Mbit/s	5.5	DMT/CAP	~1 MHz
HDSL	1,5 Mbit/s – 1,5 Mbit/s	4.6	2B1Q/CAP	~240 kHz
SDSL	784 kbit/s - 784 kbit/s	6.9	2B1Q/CAP	~240 kHz
IDSL	144 kbit/s - 144 kbit/s	5.5	2B1Q (4B3T)	~80 (120) kHz

DSL: Digital Subscriber Line
VDSL: Very High Bit Rate DSL
ADSL: Asymmetric DSL
HDSL: High Bit Rate DSL
SDSL: Symmetric DSL
IDSL: ISDN-DSL
QAM: Quadrature Amplitude Modulation
DMT: Discrete Multi-Tone Modulation
CAP: Carrierless Amplitude/Phase Modulation

Bild: xDSL Technologien

Das erste DSL-Verfahren wurde entwickelt, um Video-on-Demand und interaktives Fernsehen über Kupferkabel übertragen zu können. Als klar wurde, dass eine flächendeckende Glasfaserverkabelung an alle denkbaren Standorte (Consumer-Market) nicht möglich war (Preis), und es zudem die Liberalisierung des Telekommunikationsmarktes begann, wurde die DSL-Idee ab 1996 neu belebt.

- **ADSL:**
  - meist verbreitetste DSL-Lösung
  - unterschiedliche Up- und Downstream-Geschwindigkeiten
    - Downstream bis zu 8 Mbit/s
    - Upstream bis zu 0,8 Mbit/s
  - parrallele Übertragung von Daten und Sprache über eine Kupferdoppelader
  - gutes Verhältnis zwischen Bandbreite und überbrückbarer Entfernung
  - Adaptives Modulations-Verfahren, welches sich dynamisch an die Leitungsqualität anpaßt (DMT, CAP)
- **Standards**
  - ITU-T G.992.1
  - ANSI T1.413-1998

Bild: ADSL (Asymmetric Digital Substriber Line)

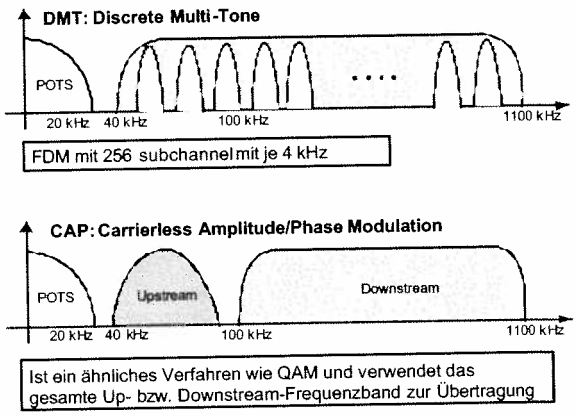


Bild: ADSL-Modulationsverfahren

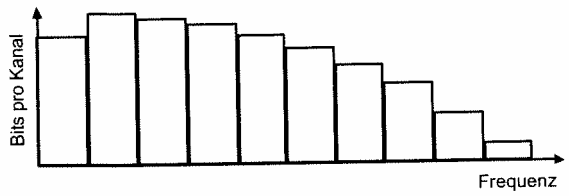


Bild: Discrete Multi-Tone Modulation (DMT)

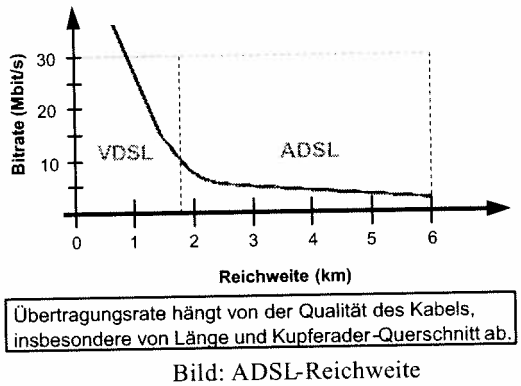


Bild: ADSL-Reichweite

Teil 1.6 Grundlagen: Übertragung

Version: Feb. 2004

- Klassifizierung und Kenngrößen von Übertragungsmedien
- Kupferkabel, Koaxialkabel und Glasfaser
- Richtfunkstrecke und Satellitenstrecke
- Anschlusstechnik: Kupfer, Koax, Glasfaser, Funk (Eigenschaften und Bitraten)
- Parallele vs. Serielle Übertragung, Basisband vs. Breitband Übertragung
- Bit- und Byteorientierte Übertragung
- Synchrone und asynchrone Übertragung
- Bit-, Byte- und Rahmen-Synchronisation
- Raum-, Frequenz-, Wellenlänge- ,Zeit- und Codemultiplex
- Raum-, Frequenz-, Wellenlänge- und Zeitduplex
- Simplex-, Halbduplex- und Vollduplex-Übertragung

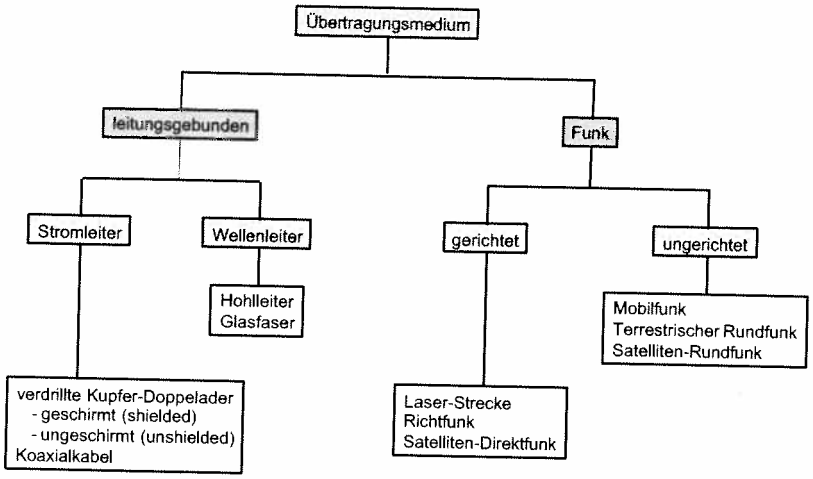


Bild: Klassifizierung von Übertragungsmedia

Übertragungsmedien

Für Datennetze können verschiedene Übertragungsmedien genutzt werden. Abhängig von den physikalischen Eigenschaften eines Mediums ergeben sich für die Anwendung verschiedene Vor- und Nachteile. In der Praxis werden bei leitungsgebundenen Übertragungsmedien für kurze Strecken (bis ca. 100 m) Kabel mit verdrillten Kupfer-Doppeladern und für längere Strecken Glasfaserkabel bevorzugt. Der zunehmende Einsatz von Funkübertragung (Freiraum-Übertragung) ist in vielen Anwendungen zu beobachten (drahtlose LANs, Bluetooth, drahtlose Netzzugänge).

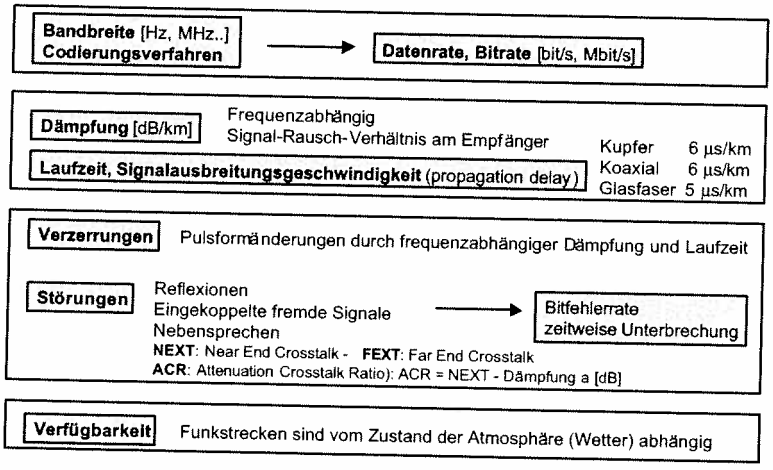
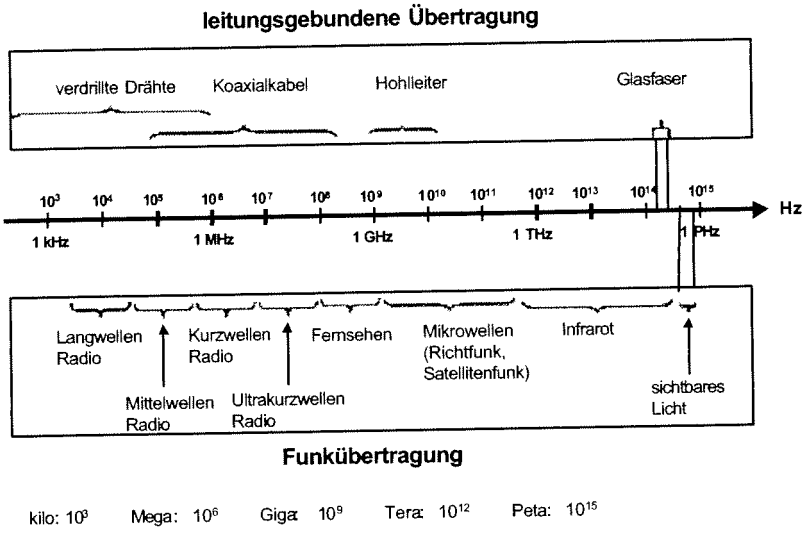


Bild: Kenngrößen von Übertragungsmedia

Übertragungsmedien werden durch einige wichtige Kenngrößen beschrieben:

- **Bandbreite:** Bei höherer Bandbreite (in Hz, MHz) des Übertragungsmediums lässt sich eine höhere Datenrate (Bitrate, gemessen in bit/s, Mbit/s) erreichen. Der genaue Zusammenhang zwischen Bandbreite und Datenrate hängt wesentlich vom gewählten Codierungsverfahren ab.
- **Dämpfung:** Bei geringer Dämpfung lassen sich längere Distanzen überbrücken. Die Dämpfung ist sehr stark von der übertragenen Frequenz abhängig. Geringe Dämpfung ergibt auch ein höheres Signal-Rausch-Verhältnis, das zu einer niedrigeren Bitfehlerrate führt und/ oder den Einsatz einfacherer Empfänger erlaubt.
- **Laufzeit (Signalausbreitungsgeschwindigkeit, propagation delay):** Die Signalausbreitungsgeschwindigkeit liegt in der Größenordnung der Lichtgeschwindigkeit. Der genaue Wert ist vom Aufbau des Übertragungsmediums und von der Frequenz (Wellenlänge) abhängig.
- **Verzerrungen:** Digitale Signale werden als Impulse einer bestimmten Form (zeitlicher Verlauf der Spannung) gesendet. Infolge frequenzabhängiger Dämpfung und Laufzeit wird die Form der Impulse verzerrt. Die verzerrten Impulse überlagern sich zusätzlich. Damit eine fehlerfreie Signalrekonstruktion (Wiedererkennung des gesendeten Impulses) möglich ist, dürfen die Verzerrungen ein bestimmtes Maß nicht überschreiten.

- **Störungen:** Neben Rauschen, das aus physikalischen Gründen unvermeidlich ist, entstehen Störungen durch Reflexionen und eingekoppelte fremde Signale. Das Nebensprechen bei Kupferkabeln muss durch eine geeignete Auslegung der Übertragungsstrecken berücksichtigt werden. Einwirkungen durch systemfremde Störungen können zu einer erhöhten Bitfehlerrate oder zur zeitweisen Unterbrechung der Kommunikation führen. Derartige Probleme werden im Gebiet der EMV (Elektromagnetische Verträglichkeit, EMC: Electromagnetic Compatibility) behandelt.
- **Verfügbarkeit:** Übertragungsstrecken können vorübergehend oder permanent ausfallen. Funkstrecken sind vom Zustand der Atmosphäre (Wetter) abhängig, was bei der Planung berücksichtigt werden muss. Ausfälle müssen durch das Netzmanagement erkannt und behandelt werden.



VLF (very low frequency), Längstwelle	3 – 30 kHz
LF (low frequency), Langwelle	30 – 300 kHz
MF (medium frequency), Mittelwelle	300 – 3000 kHz
HF (high frequency), Kurzwelle	3 – 30 MHz
VHF (very high Frequency)	30 – 300 MHz
UHF (ultra high frequency)	300 – 3000 MHz
SHF (super high frequency)	3 – 30 GHz
EHF (extremely high frequency)	30 – 300 GHz

Telefonsignal	300 – 3400 Hz
Audiosignal	15 – 20 000 Hz
TV-Bildsignal	0 – 5 MHz
TV-Farbinformation	0 – 2,5 MHz
HDTV	0 – 27 MHz

Bild Frequenzbänder

kilo: 10^3 Mega: 10^6 Giga: 10^9 Tera: 10^{12} Peta: 10^{15}

Bild: Elektromagnetisches Spektrum

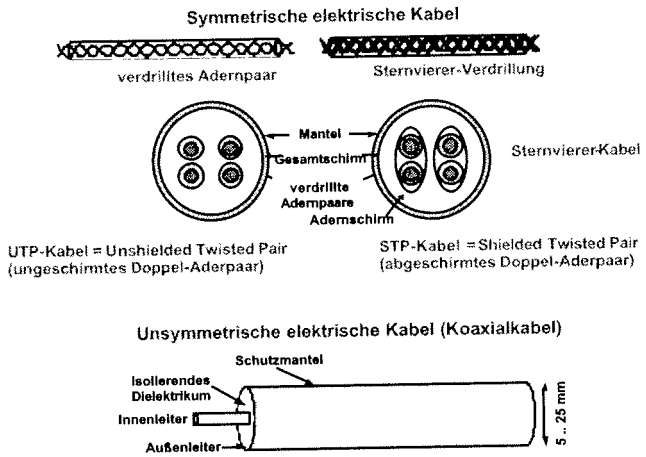


Bild: Elektrische Kabel

Metallische Leiter

Metallische Leiter werden in Form von verdrillten Kupfer-Doppeladern und von Koaxialkabeln eingesetzt. Mehrere Kupfer-Doppeladern fasst man in der Regel zu einem Kabel zusammen.

Kupferkabel sind aus mehreren **Doppeladern** aufgebaut. Bei Kabeln des Typs UTP (Unshielded Twisted Pair) und STP (Shielded Twisted Pair) ist jede Doppelader für sich verdrillt, bei STP zusätzlich abgeschirmt. Das gesamte Kabel kann zusätzlich abgeschirmt sein, was durch die Bezeichnung **S/STP** bzw. **S/UTP** (das erste S steht für Screened) ausgedrückt wird. Für die Zwecke der strukturierten Verkabelung wurden in Normenwerken Kabelklassen definiert.

Zusätzlich zu den allgemein gültigen Kenngrößen sind hier weitere Größen von Bedeutung:

- **Wellenwiderstand:** Der Wellenwiderstand Z eines Kabels ist eine charakteristische Größe, die durch Geometrie und Material des Kabelaufbaus bestimmt wird. Ein Kabel muss beidseitig mit seinem Wellenwiderstand abgeschlossen sein, damit keine Reflexionen entstehen, die die Datenübertragung stören bzw. verhindern würden.
- **Nahnebensprechen** (NEXT: Near End Crosstalk): Dieses entsteht durch elektromagnetische Kopplungen zwischen Adernpaaren in einem Kabel. Das Nahnebensprechen ist besonders störend, da ein Empfänger beim Empfang eines schwachen Signals zusätzlich das (relativ starke) Nebensprechen eines benachbarten Senders empfängt. Gemessen in dB.
- **Fernnebensprechen** (FEXT: Far End Crosstalk, auch FECT): Nebensprechen, das von einem Sender am entfernten Ende der Übertragungsstrecke eingekoppelt wird. FEXT ist in der Regel schwach gegenüber NEXT.
- **Verhältnis von Dämpfung zu Übersprechen** (ACR: Attenuation Crosstalk Ratio): ACR wird berechnet als Differenz zwischen NEXT und der Dämpfung a, die beide in dB gemessen werden. Ein höherer Wert von ACR bedeutet, dass das Nahnebensprechen gegenüber dem empfangenen Nutzsignal schwächer wird und somit die Übertragungssicherheit steigt.

Koaxialkabel

Das Koaxialkabel gehört zu den unsymmetrischen Kupferleitern. Es besitzt einen zylindrischen Innenleiter, der von einem als Hohlleiter ausgebildeten Außenleiter umgeben ist. Die Verwendung zusätzlicher Außenleiter dieser Art ermöglicht eine weiter Erhöhung der Unempfindlichkeit gegenüber Fremdeinkopplungen. Die Formgebung des Außenleiters ermöglicht die Ausnutzung hoher Frequenzen bis in den Bereich Megahertz innerhalb des Koaxialkabels. Der zentrale Innenleiter des Kabels besteht somit aus Kupfer mit einem Durchmesser von 5-10 mm, einer Isolierschicht, einem rohrförmigen Außenleiter und einer Außenisolierung. Der Außenleiter stellt gleichzeitig eine Abschirmung dar. Als Dielektrikum zwischen Innen- und Außenleiter kommen verschiedene Materialien wie PVC oder Polyäthylen in Frage.

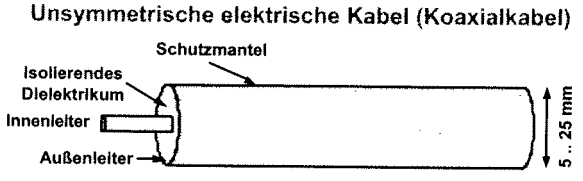


Bild: Koaxialkabel

Die Durchmesser der Innen- und Außenleiter werden je nach Anwendungsfall dimensioniert. Höhere Frequenzen erfordern einen größeren Durchmesser. Eine wichtige Größe des Koaxialkabels ist dabei der Wellenwiderstand. Er muss zur Vermeidung von Reflexionen an den Widerstandsbelag des Kabels angepasst werden.

Übliche Einsatzgebiete und Werte für den Wellenwiderstand sind:

- **Ethernet mit 50 Ohm:** 10Base5 (Yellow Cable) und 10Base2 (RG-58U),
- **Breitbandübertragungssysteme mit 75 Ohm:** Kabelmodems (RG-59).

Die Vorteile dieses Kabeltyps liegen in seiner preiswerten Verfügbarkeit und seiner einfachen Anschlusstechnik. Allerdings nimmt die Verwendung des Koaxialkabels zur Datenübertragung trotz der guten übertragungstechnischen Eigenschaften weiter ab. Im LAN wird dieser Kabeltyp durch die symmetrischen Kupferleiter abgelöst, während im MAN und WAN die Glasfaser eingesetzt wird. Das liegt hauptsächlich an den Nachteilen der begrenzten übertragungstechnischen Möglichkeiten und der relativ schwierigen Verlegbarkeit und Handhabung.

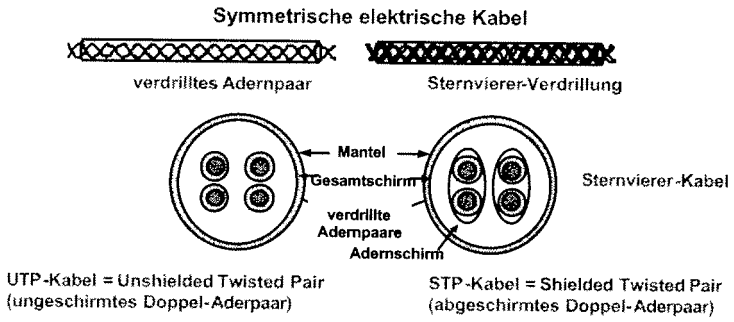


Bild: Doppel-Aderpaar (Twisted-Pair)

Twisted-Pair-Verkabelung

Twisted Pair (TP) ist die generelle Bezeichnung für Kupferkabel mit einem oder mehreren verdrillten Leitungspaaren. Fast alle Dienste benötigen zur Signalübertragung zwei Paare, d.h. vier Adern, wobei ein Paar zum Senden und das andere für den Datenempfang vorgesehen ist.

Um Störungen der Signale auf den Leitungspaaren zu verhindern, sind die Adern symmetrisch gegeneinander verdrillt. Dadurch neutralisieren sich die elektromagnetischen Kräfte, die von den stromführenden Adern ausgehen, weitgehend.

Zusätzlich wird das Kabel mit einem metallischen Schirm umgeben, der starke Störungen kompensieren kann. Dieser Schirm besteht meistens aus einer Folie oder Drahtgeflecht. Ein weiterer Effekt ist die Abschirmung nach außen, so dass neben besserer EMV-Werte auch die Abhörsicherheit erhöht wird. Der Grad der Verdrillung wird durch die Drillzahl pro Längeneinheit angegeben.

TP gehört heute zu den üblichsten Verkabelungen im Bereich lokaler Netze, da es sich um ein sehr kostengünstiges und einfaches Übertragungsmedium handelt. Unterschieden wird TP in der Art der Abschirmung. Während Unshielded Twisted Pair (UTP) nur mit einer Gesamtschirmung ausgestattet ist, sieht Shielded Twisted Pair (STP) eine zusätzliche Abschirmung eines jeden Adernpaares vor. Zusätzlich sind unterschiedliche Wellenwiderstände von 100, 120 bis 150 Ohm vorhanden. Deshalb sind sehr unterschiedliche Kombinationen und Varianten im Einsatz.

- **STP 150 Ohm:** Paarweise geschirmtes Kabel mit einem Gesamtschirm aus Metallgeflecht.
- **STP 100 Ohm:** Aufbau wie STP 150 Ohm, jedoch geringere Impedanz.
- **S/UTP 100 Ohm:** Keine Schirmung für die einzelnen Adernpaare, wobei aber eine Gesamtschirmung aus Metallfolie und/oder Metallgeflecht besteht.
- **UTP 100 Ohm:** Kabel ohne jede Schirmung der Adernpaare.

Die Standardisierung der Ethernet-Verkabelung beinhaltet folgende Punkte:

- Topologie der Verkabelung,
- Spezifikation der Kabel und der Anschlusstechnik,
- Leistungsfähigkeit der Übertragungsstrecke,
- Prüfverfahren.

Die Übertragungsraten stiegen in den letzten Jahren immer weiter stetig an, wodurch die Qualität der Kupferleitungen ebenfalls nachziehen musste. Bandbreiten von 155 Mbit/s und 2,5 Gbit/s (ATM: OC-3, OC-12 und OC-48) und 1 Gbit/s (Gigabit-Ethernet) müssen transportiert werden. Es wurden nach Kategorie 5 weitere Kupferleitungen spezifiziert. Dabei entstand auch der Entwurf für Kategorie-6-Kabel. Es handelt sich hierbei um die Spezifikation von 300 bis 600-MHz-Kupferleitungen, die auch zukünftigen Anforderungen gewachsen sein wollen. Dieser Entwurf sieht deutlich verschärfte Anforderungen an das Nahnebensprechen vor.

Der Grund hierfür ist darin zu sehen, dass eine wesentliche Verbesserung des ACR-Wertes eines Kabels nicht durch Verringerung der Leitungsdämpfung, sondern vielmehr durch eine bessere Kanaltrennung in Form einer Paarabschirmung zu erreichen ist. ACR (Attenuation Crosstalk Ratio, Verhältnis von Dämpfung zu Übersprechen). Die Mindestforderung des neuen Standards ist ein ACR-Wert von 10 dB bei 600 MHz sein, mit der sich Datenraten bis 622 Mbit/s sicher übertragen lassen. Dabei wird eine Dämpfung von 20 dB auf 100 m und ein Nahnebensprechen von 40 dB bei 100 MHz auftreten.

Die Angaben für Kabel und Anschlusstechniken beziehen sich auf vorgegebene Kategorien, erweitert um entsprechende Werte für die gesamte Übertragungsstrecke (Link). Weiterhin sind Anwendungsklassen definiert worden. Diese entsprechen den Eigenschaften eines kompletten Netzsystems bezüglich Universalität, Stecker und Verlegevorschriften.

Anwendungsklassen	Eigenschaften	Anwendung
Klasse A	bis 100 kHz	Niederfrequenz, Sprach- und Datenverbindungen, Telefondienste
Klasse B	bis 1 MHz	Telefondienste, Datenverbindungen (mittlere Datenraten)
Klasse C	bis 16 MHz	Datenverbindungen (hohe mittlere Datenrate)
Klasse D	bis 100 MHz	Datenverbindungen (hohe Datenrate)
Klasse E	bis 200 MHz	Datenverbindungen (sehr hohe Datenrate)
Klasse F	bis 600 MHz	Datenverbindungen (extrem hohe Datenrate)

Bild: Anwenderklassen von Übertragungsmedien

Die Beziehung der Anwendungsklassen zu den Übertragungsmedien ist festgelegt. Dabei sollte die Toleranz der Vernetzung von Komponenten nicht überbeansprucht werden.

Werden die Werte beispielsweise bei Kategorie 5 und Anwendungsklasse D nur knapp erfüllt, so besteht keine Garantie dafür, dass die Installation über 100 m einwandfrei funktioniert. Dies liegt an der mangelnden Festlegung von Leistungsreserven.

Kabelkategorie	Anwendung
Keine Standardisierung	Kabel für analoge Sprachübertragung Kabel für Datenübertragung mit 64 kbit/s
Keine Standardisierung	Kabel für Datenübertragung bis 4 Mbit/s über mittlere Entfernungen Netze: Token-Ring, Token-Bus, ISDN
Kategorie 3	UTP/STP-Kabel für Datenübertragung bis 16 Mbit/s. Ethernet 10Base-T bis 100 m
Kategorie 4	UTP/STP-Kabel für Datenübertragung bis 20 Mbit/s über größere Entfernungen.
Kategorie 5	UTP/STP-Kabel für Datenübertragung bis 100 Mbit/s. Durch Codierung auch höhere Datenraten. Netze: FDDI, Fast-Ethernet, ATM.
Kategorie 6	UTP-Kabel für Datenübertragung bis 200 Mbit/s. Netze: High-Speed Token-Ring (100 Mbit/s), ATM.
Kategorie 7	UTP-Kabel für Datenübertragung bis 600 Mbit/s. Netze: Gigabit-Ethernet, Fibre Channel, ATM.

Bild: Kabelkategorien

Qualitätsverschlechterung durch

- Alterung von Werkstoffen,
- Fehlanpassung von Komponenten,
- Temperaturschwankungen,
- Installationseffekte,
- Störquellen oder
- Längenüberschreitungen (elektrisch und physikalisch)

Deshalb ist es ratsam, höherwertige Kabel mit besseren Qualitätsparametern zu verlegen, um Performance-Engpässen vorzubeugen.

Um dies besser einschätzen zu können, gibt es zur einfachen Qualitätsbestimmung von Netzkabeln ebenfalls die Grenzwerte für den Wellenwiderstand, die Dämpfung und das Nahnebensprechen (NEXT). Die Norm beschränkt sich dabei ausschließlich auf die Tertiärverkabelung (Wiring Closet). Das Ziel ist, die Sicherstellung neutraler Dienstanforderungen. Dabei finden insbesondere die Eigenheiten des amerikanischen Marktes Berücksichtigung. Für die vier grundsätzlichen Kabelarten, die zwischen Endgeräten und Etagenverteiler verwendet werden können, sind sechs Anwendungsklassen definiert worden. Dabei ist wichtig, dass alle Komponenten des Verkabelungssystems die Ansprüche der Anwendungsklasse erfüllen. Zum System gehören neben dem Kabel auch Wanddosen, Patchkabel, Steckverbindungen und Verteilerschränke.

Kabeltyp	Anwendungs-klasse	Frequenz	Wellenwider-stand [Ω]	Dämpfung [dB/km]	NEXT [dB]
Kategorie 1	Klasse A Level 1		-	-	-
Kategorie 2	Klasse B Level 2	1 MHz	84 - 113	2,4	-
Kategorie 3	Klasse C Level 3	10 MHz 16 MHz	100/15 100/15	< 9 < 12	26 23
Kategorie 4	Level 4	10 MHz 16 MHz 20 MHz	100/15 100/15 100/15	< 6,6 < 8,1 < 9,3	> 40 > 40 > 40
Kategorie 6	Klasse D Level 5	10 MHz 16 MHz 20 MHz 100 MHz	100/15 100/15 100/15 100/15	< 6 < 7,5 < 8,4 < 20	> 42 > 41 > 41 > 32
Kategorie 5	Klasse D+ Level 5	10 MHz 16 MHz 100 MHz	100/15 100/15 100/15	< 7,5 < 9,4 < 23,2	> 39 > 36 > 24
Kategorie 6	Klasse E Level 6	10 MHz 16 MHz 100 MHz 200 MHz	100/15 100/15 100/15 100/15	< 6,0 < 8,0 < 20,0 < 30,0	> 66 > 63 > 47 > 42

Bild: Wellenwiderstand und NEXT für TP-Kabel

Ein Problem bildet ein einheitlicher Wellenwiderstand für alle LAN-Technologien.

IEEE 802.3 für Ethernet 10Base-T schreibt 100 für UTP, IEEE 802.5 für Token Ring 150 für STP bei 16 Mbit/s und das Telefonkabel einen Wert von 100 vor. Für Token Ring entsteht damit der Druck, eine Definition für 100er-Kabel liefern zu müssen.

Aufgrund der gewonnenen Erkenntnisse entstanden schnell strengere Bewertungsmaßstäbe, die bereits in Klasse D+ und E berücksichtigt wurden. Die Klasse D+ ist bis 100 MHz spezifiziert, umfasst aber eine Reserve für Installation und Alterung der Komponenten und weist einen um 10 dB höheren SNR-Wert auf. Klasse E unterstützt Anwendungen bis 200 MHz, so dass auch Bereiche von ATM abgedeckt sind. Klasse F geht bis zu 600 MHz.

Link Performance

Neben der genauen Einhaltung der Vorschriften für die Verkabelung besteht noch die Möglichkeit, ein Netz anhand der Link Performance aufzubauen. Diese legt fest, welche Eigenschaften für eine Punkt-zu-Punkt-Verbindung gelten, damit der Standard eingehalten wird. Für den Horizontalbereich ist die Strecke von der Netzsteckdose am Arbeitsplatz bis zur Geräteanschlussseite des Patchfeldes standardisiert. Dabei werden nur die passiven Komponenten berücksichtigt. Zusätzlich besteht die Möglichkeit, durch die Anforderungen an das ACR, das Verkabelungssystem mit niederer Dämpfung und Nahnebensprechen einzusetzen. Der große Vorteil der Link Performance ist es, jede Verkabelung auf ihre Konformität bezüglich des Standards überprüfen zu können. Dadurch lassen sich auch nicht spezifizierte Kabel und Leitungen verwenden, die aber trotzdem den Vorschriften entsprechen müssen.

Elektromagnetische Verträglichkeit (EMV)

Ein weiteres Problem im Rahmen der Verkabelung stellt die Elektromagnetische Verträglichkeit (EMV) dar. In der Theorie sorgt man durch die Verdrillung der Twisted Pair Kabel dafür, dass sich die EMV-Wirkung der einzelnen Adern gegenseitig aufhebt. Allerdings können jedoch Störungen in der Symmetrie der Verdrillung in der Praxis dazu führen, dass die Schutzanforderungen nicht mehr eingehalten werden können. Insgesamt sind die Vorschriften für den Bereich EMV noch sehr unterschiedlich. Grundlage für die EMV-Sicherheit gilt die zulässige Störfeldstärke im Frequenzbereich 0,15 bis 1000 MHz. Bei einer Überschreitung muss eine durchgängige Schirmung der Kommunikationsanlage vorgenommen werden. Zusätzlich ist noch die Immissionsfestigkeit für Verkabelungssysteme definiert worden. Durch die immer höheren Frequenzen sind die Normen allerdings immer schwerer einzuhalten. Ein Ausweg besteht nur in der Verwendung gut geschirmter Kabel.

Zusammenfassend kann man Twisted Pair (TP) für das lokale Netz bewerten und die Punkte auf unterschiedliche Bereiche ausdehnen. Dabei sollte auf mechanische, übertragungstechnische und wirtschaftliche Aspekte Wert gelegt werden. Die mechanischen Vorteile liegen dabei auf der Hand. TP ist flexibel und handlich, wodurch eine einfache Verlegung ermöglicht wird sowie ein leichtes Anbringen von Steckern. TP beinhaltet aber auch Nachteile bezüglich der mechanischen Eigenschaften. Neben relativ großen, schweren Kabeln, die man nicht platzsparend einsetzen kann, lassen sich auch die Patchfelder relativ ineffizient nutzen.

Die Nachteile hinsichtlich der Übertragungstechnik wiegen aber wesentlich schwerer. Neben der geringen Bandbreite ist auch hohe Signaldämpfung und somit Leistungsverluste durch schlechte Leitfähigkeit einzuplanen. Weiterhin kann es eine aktive und passive Beeinflussung der Übertragung durch elektromagnetische Störungen geben.

Die wirtschaftlichen Vorteile liegen aber auf der Hand. Zum einen sind die geringen Kosten des Kabels entscheidend. Auch die Investitionssicherheit ist bezüglich der vorhandenen LAN-Technologien gegeben, da im Grunde alle Technologien TP unterstützen. Allerdings lässt sich das nur nach heutigen Maßstäben messen, da zukünftigen Technologien aufgrund des physikalischen Aufbaus Grenzen gesetzt sind.

Neben diesen Aspekten sind aber auch noch andere Faktoren von Bedeutung. So besteht in einigen europäischen Ländern und in den USA eine große Präferenz für UTP-Kabel aufgrund ihrer weiten Verbreitung und ihrer bisherigen Nutzung als Telefonkabel. Ihre Verwendung auch für die Vernetzung senkt die Installations- und Investitionskosten in die Infrastruktur beträchtlich, weshalb auch weiter mit UTP gerechnet werden muss. Allerdings ist bei Neuverkabelung dringend von dieser Leitungsart abzuraten.

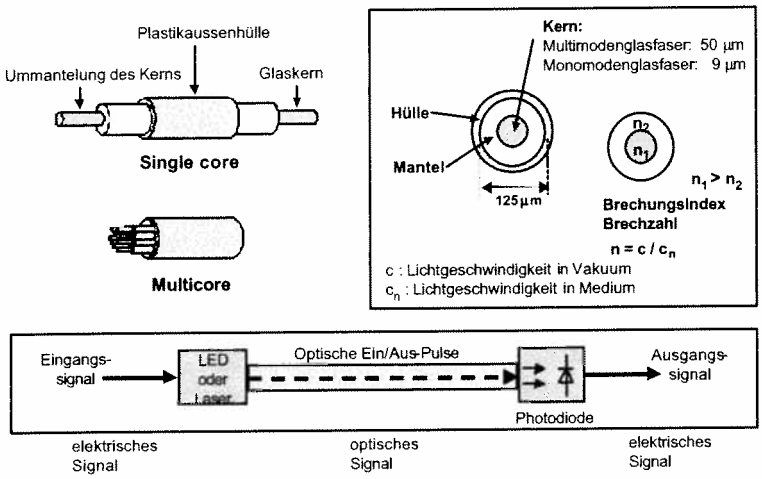
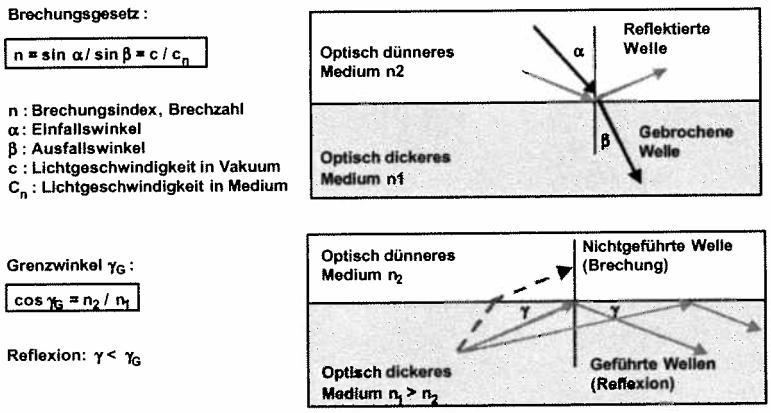


Bild: Glasfaser und optische Übertragung

Glasfaser (Optische Wellenleiter, optische Faser, optical fiber) dienen zum Transport von Lichtstrahlen, die mit den zu übertragenden Daten moduliert sind. Eine Faser besteht aus einem Kern (core) und einem Mantel (cladding). Der Brechungsindex des Mantels ist niedriger als der des Kerns. Dadurch wird Licht, das in den Kein eingestrahlt wird, durch Totalreflexion am Übergang Kern-zu-Mantel im Kern gehalten und breitet sich zickzackförmig im Kern aus. Die Faser wird durch eine weitere Hülle mechanisch geschützt.

Als Werkstoffe können Glas oder Kunststoff verwendet werden. Für Anwendungen in der Kommunikationstechnik wird Glas bevorzugt. Es bietet eine geringere Dämpfung als Kunststoff, ist jedoch teurer.



Elektrische Signale werden durch elektrooptische Sender (LED Light Emitting Diode oder Laserdiode) in optische Signale gewandelt. Nach der Übertragung auf der Glasfaser findet beim Empfänger eine Optoelektronische Wandlung (Fotodiode) statt.

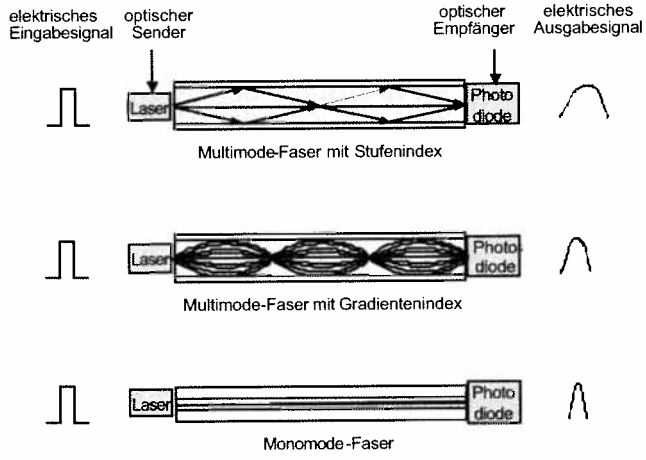
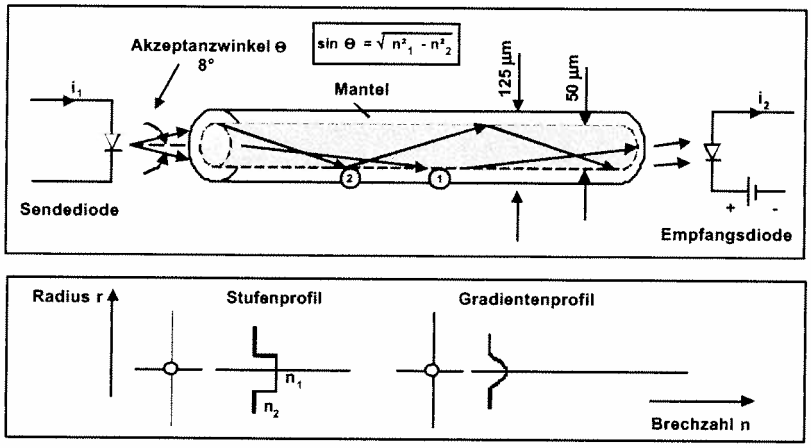


Bild: Glasfaser-Typen

Multimode-Faser: In der Faser können sich mehrere Moden ausbreiten. Die Pfadlängen und damit die Laufzeiten sind dabei unterschiedlich. Diese so genannte Modendispersion führt zur Verzerrung der gesendeten Lichtimpulse und begrenzt dadurch das Bandbreite-Länge-Produkt (Produkt aus Übertragungsdistanz und nutzbarer Bandbreite. Multimode-Fasern können als Stufenindex-Faser oder als Gradientenindex-Faser realisiert werden. Mit der Stufenindex-Faser wird ein Bandbreite-Länge-Produkt der Größenordnung 10 (Mbit/s) x km erreicht, bei der Gradientenindex-Faser sind es ca. 4 (Gbit/s) x km.

Monomode-Faser: Durch die Verwendung eines sehr kleinen Kerndurchmessers (wenige µm) kann erreicht werden, dass nur ein Mode existieren kann. Dadurch entfällt die Modendispersion. Es zeigt sich aber, dass nun die Materialdispersion eine Grenze darstellt. Mit einem Bandbreite-Länge-Produkt der Größenordnung 250 (Gbit/s) - km liegt dieses jedoch um Größenordnungen höher als bei Multimode-Fasern.



Das Bild illustriert die Ein- und Auskopplung sowie die Strahlenausbreitung im Glasfaserkern einer Multimode-Glasfaser. Bei der Einkopplung spielt die Akzeptanzwinkel eine wichtige Rolle: Maximale Einkopplungswinkel. Bei Multimode-Glasfaser wird heute nur noch das Gradientenprofil für die Brechzahl (Brechungsindex) verwendet.

Bild: Multimode Glasfaser

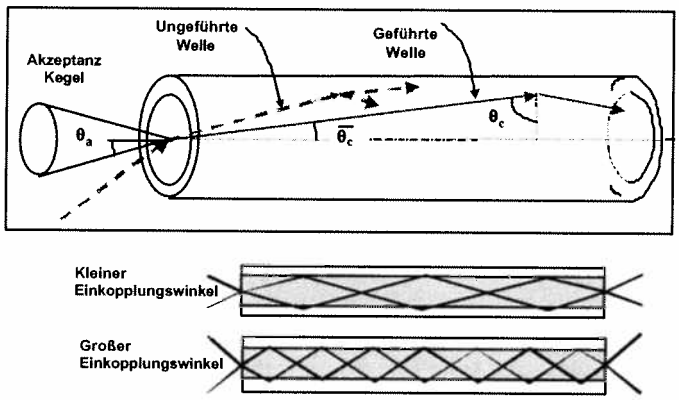
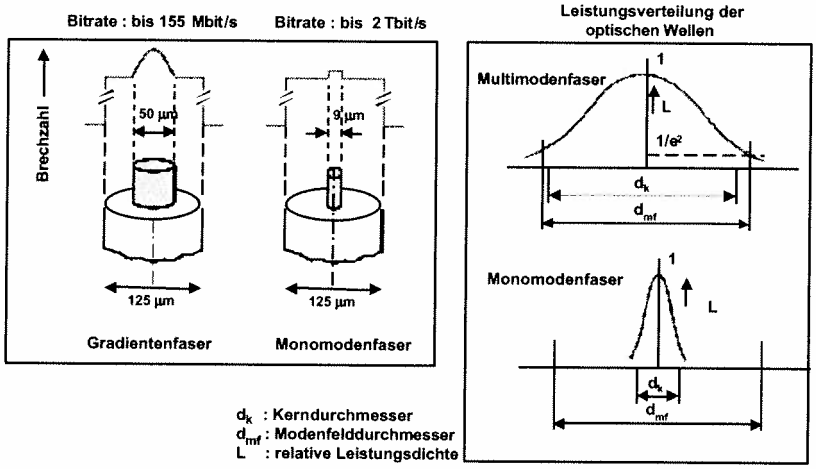


Bild: Akzeptanzwinkel Θ



Das Bild zeigt die Diameterunterschiede zwischen beiden Fasertypen.
Multimode: 50 µm
Singlemode: 9 µm

Die Glasfaser selbst hat den gleichen Diameter: 125 µm.
Darüber kommt den Schutzmantel.

Bild: Multimode und singlemode Glasfaserabmessungen

Bei 850 nm Wellenlänge werden Multimode-Fasern zusammen mit **LEDs** als Sender verwendet. Die erreichbaren Distanzen sind entsprechend gering. Bei 1,3 µm und 1,55 µm kommen Monomode-Fasern mit (den gegenüber LED wesentlich teureren) **Laserdioden** zum Einsatz. WDM (Wavelength Division Multiplexing) wird bei Glasfasern eingesetzt, um mehrere Datenströme über eine Faser zu übertragen.
Die Dämpfung drückt den Leitungsverlust des Signals auf dem Übertragungsmedium aus. Dabei lässt sich die Dämpfung eines Lichtsignals in folgende Unterpunkte aufteilen, die den Betrieb der Glasfaser beeinflussen:

- Materialdämpfung,
- Installationsdämpfung,
- Dämpfung in Abhängigkeit von der Wellenlänge.

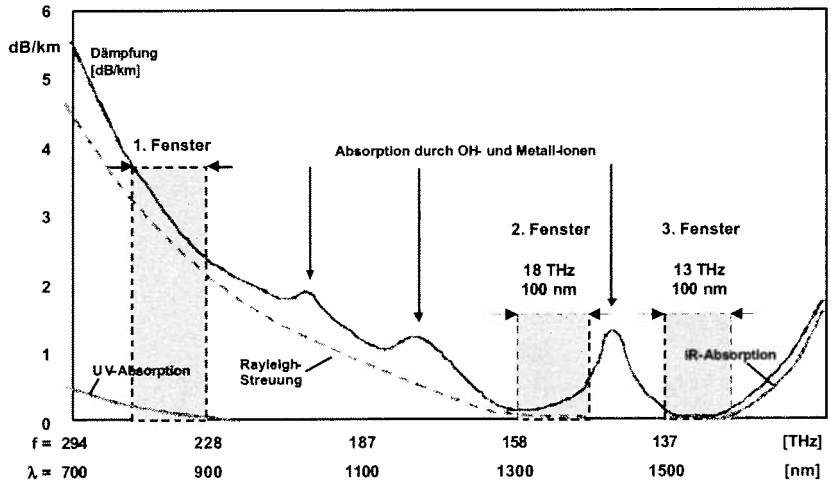


Bild: Dämpfungsverlauf von Glasfasern

Die genutzten optischen Wellenlängen ergeben sich aus dem typischen Verlauf der Dämpfung in Abhängigkeit von der Wellenlänge:

- Ein **erstes optisches Fenster** findet man bei einer Wellenlänge um 850 nm. Die erreichbare Dämpfung liegt bei 2 dB/km.
  Grund: billige optische LED-Komponenten.
- Bei einer Wellenlänge von 1,3 µm gibt es ein **zweites optisches Fenster** mit geringerer Dämpfung mit 0,35 dB/km.
  Grund: Dispersionsminimum.
- Bei 1,55 µm existiert ein **drittes optisches Fenster** mit 0,2 dB/km.
  Grund: Minimale Dämpfung.

Eigenschaft	Multimode Stufenglasfaser	Multimode Gradientenglasfaser	Monomode Glasfaser
Brandbreite	200 Mbit/s bei 850 nm 200 Mbit/s bei 1300 nm	400-800 Mbit/s bei 850 nm 1 Gbit/s bei 1300 nm	800 Mbit/s bei 850 nm 10 Gbit/s bei 1300 nm 10 Gbit/s bei 1550 nm
Dämpfung	uni- / bidirektional	bidirektional	unidirektional
Reichweite	1 - 2 km	2 - 4 km	60 -80 km
Numerische Apertur	0,29	0,2	0,0..

Bild: Eigenschaften von Glasfasern

Die Materialdämpfung findet aufgrund von Fehlerstellen in der Glasfaser statt, die durch Verunreinigungen des Glaskerns, Luftblasen oder Risse entstehen können. Durch Installationsfehler, wie die Nichteinhaltung der Biegeradien, schlechtes Spleißen oder Kleben, schlecht poliertes Faserende, Achsversatz, Fehlwinkel oder Verkippung der Glasfaser, wird das Signal geschwächt. Die Länge einer Glasfaser, mit der Anzahl der Verbindungen, verursacht noch eine zusätzliche Dämpfung.

Während Spleißverbindungen im Mittel eine Dämpfung von nur 0,1 dB besitzen, kommt man durch Kleben oder Verschmelzen bereits auf Werte von 0,5 bis 0,8 dB. Die Dämpfung allgemeinen ist natürlich abhängig von der Wellenlänge des Lichts. Bei zunehmender Wellenlänge nimmt die Dämpfung durch Streuverluste ab. Bestimmte in den Glasfasern enthaltende Moleküle absorbieren das Lichtsignal bei bestimmter Wellenlänge unterschiedlich stark. Deshalb hat man sich für Übertragungsfenster bei 850, 1300 und 1550 nm entschieden, bei denen die Dämpfung lokale Minima annimmt.

Eigenschaft	Multimode Stufenglasfaser	Multimode Gradientenglasfaser	Monomode Glasfaser
Brandbreite	200 Mbit/s bei 850 nm 200 Mbit/s bei 1300 nm	400-800 Mbit/s bei 850 nm 1 Gbit/s bei 1300 nm	800 Mbit/s bei 850 nm 10 Gbit/s bei 1300 nm 10 Gbit/s bei 1550 nm
Dämpfung	uni- / bidirektional	bidirektional	unidirektional
Reichweite	1 - 2 km	2 - 4 km	60 -80 km
Numerische Apertur	0,29	0,2	0,0..

Bild: Eigenschaften von Glasfasern

Wenn man der Glasfasertechnik einer Bewertung unterziehen möchte, so ist eine Unterteilung in mechanische, übertragungstechnische und wirtschaftliche Bereiche sinnvoll. Die mechanischen Vorteile sind die dünnen und leichten Glasfasern, die man sehr platzsparend verlegen kann. Dies macht sich besonders beim Management von Patchfeldern bemerkbar. Zusätzlich sind die Kabel sehr flexibel und handlich, wodurch die Verlegung stark vereinfacht wird.

Nachteilig ist das aufwendige Anbringen von Steckern sowie der Spleißvorgang. Dieser wird aber durch neue Klebe- und Stecktechniken immer weiter vereinfacht.

Die übertragungstechnischen Vorteile lassen sich wie folgt auflisten. Ihnen stehen bislang keine Nachteile gegenüber:

- Hohe Übertragungsbandbreite bei gleichzeitig hoher Signaldichte bis in den Terahertzbereich,
- Niedrige Signaldämpfung und damit geringer Leistungsverlust des Lichts entlang des Kabels,
- Unempfindlich gegenüber elektromagnetischen Störungen,
- Kein Aussenden von elektromagnetischen Feldern,
- Galvanische Entkopplung zwischen Sender und Empfänger, wodurch keine Gefahr durch Blitzschlag droht,
- Hohe Abhörsicherheit.

Die wirtschaftlichen Vorteile sind die geringen Kosten eines virtuellen Kanals. Auch die Investitionssicherheit spielt eine entscheidende Rolle. Inzwischen unterstützen alle LAN-Technologien Glasfaser als Übertragungsmedium. Nachteilig ist der höhere Investitionsbedarf durch die anfallenden Adapter zwischen Glasfaser und Endgerät. Zusätzlich ist die Konfektionierung der Glasfaser immer noch relativ aufwendig. Schwierige Fehlersuche und aufwendige Bestimmung des Dämpfungsbudgets kommen zu den wirtschaftlichen Nachteilen noch hinzu.

Inzwischen kommt die Entwicklung einer polymeroptischen Faser (POF) mit hoher Übertragungsbandbreite und schneller Leuchtdiode (LED) als günstiges optisches Übertragungsmedium zu den Lichtwellenleitern noch hinzu. Die Plastikfaser genügt dabei bereits heute den Anforderungen von LAN-Spezifikationen wie zum Beispiel Fast-Ethernet.

Die Optimierung verfügbarer LEDs und die Entwicklung neuer Komponenten machen es möglich, Netzstandards über POF zu nutzen. Anwendungen von LEDs verschiedener Wellenlänge ermöglichen außerdem die gleichzeitige Ausnutzung mehrerer unabhängiger logische Netze auf einer einzelnen Faser als Bitübertragungsschicht mit unterschiedlichen Übertragungsraten. Dabei können bereits Sender/Empfängermodule weite Distanzen überbrücken, da die Strahlaufspaltung ohne Koppler ermöglicht wird. Dämpfungsarme Gradienten-Index-Fasern könnten 2,5 Gbit/s über 300 in Entfernung zukünftig leisten.

Bisher erhältliche 650-nm-AlGaInP-LEDs nutzen bereits ein Minimum in der Faserdämpfung (150 dB/km) für die Übertragung bis zu 155 Mbit/s aus. Neue 500-nm-AlGaS-LEDs ermöglichen hingegen ohne aufwendige Beschaltung Bandbreiten bis zu 50 Mbit/s nahe dem Dämpfungsminimum von 520 nm (80 dB/km). Zusammen erlauben beide LEDs eine unabhängige und gleichzeitige Datenübertragung über eine Faser mit dem WDM-Verfahren unter Beibehaltung der vollen Bandbreite für beide Richtungen. Das Übersprechen des Senders auf seinem eigenen Empfänger wird durch einen Farbfilter unterdrückt. Der Einsatz bidirektionaler WDM-Strecken stellt somit eine preisgünstige Alternative gegenüber der Duplexverkabelung für die Datenkommunikation in einem typischen LAN für kurze bis mittlere Strecken unter 100 m dar.

Medium	Verdrillte Kupferadern	Koaxialkabel, Basisband	Koaxialkabel, Breitband	Lichtwellenleiter
Übertragungsart	analog, digital	digital	analog, digital	digital
Betriebsart	uni- / bidirektional	bidirektional	unidirektional	unidirektional
Datenrate	100 Mbit/s	bis 60 Mbit/s	bis 600 Mbit/s	bis 10 Gbit/s
Bitfehlerrate	10^{-5}	10^{-7} bis 10^{-8}	10^{-8} bis 10^{-9}	< 10^{-11}
Abhörsicherheit	gering	*)	*)	hoch
Störempfindlichkeit	groß	**)	**)	sehr gering
Verlegbarkeit	sehr gut	gut	gut, mit Sorgfalt	schwierig
Kosten	gering	hoch	hoch	relativ hoch

*) gute Abschirmung möglich, Kabel jedoch leicht anzapfbar
**) durch elektromagnetische Felder möglich

Bild: Leitungsgebundene Übertragungsmedien

Zusammenfassung der Verkabelungen
Die wesentlichen Eigenschaften der im LAN-Bereich gebräuchlichen Kabeltypen sind in der Tabelle zusammengefasst. Um die Leistungsfähigkeit der Verkabelung bewerten zu können, ist die Berechnung des Dämpfungsbudgets zu empfehlen. Dieses ist die Summe der Grunddämpfung der Kabel und der Dämpfungswerte aller Verbindungen. Sie stellt somit die theoretische Grundlage der Leistungseinschätzung eines Netzes dar.

Die Differenz aus der beim Endgerät ankommenden Leistung und der minimalen Empfängerempfindlichkeit ergibt dann die Leistungsreserve. Hieraus wird ersichtlich, dass Twisted-Pair-Verkabelung immer mehr von der Glasfaser verdrängt wird. Zum Desktop ist TP allerdings eine auch weiterhin ausreichende Alternative, weshalb auch hier weitere Wachstumsraten zu verzeichnen sind.

Weiter sinkende Preise im LWL-Bereich und die geringere Anzahl aktiver Komponenten im Vergleich zu TP machen die Glasfaser bereits heute konkurrenzfähig im Campus- und Gebäudebereich. Zukünftig wird durch die Weiterentwicklung der Hochgeschwindigkeitsnetze auch die Anforderung LWL-to-the-Desktop hinzukommen. Eventuell würde Kupfer dann bei Neuverkabelung nicht mehr in dem Maße berücksichtigt werden , wie das bisher der Fall war. Im Backbone tritt dieser Umstand heute bereits auf. Neue Spezifikationen wie Kategorie 6 und 7 versuchen den noch immer hohen Bedarf an Kupferleitungen, gerade nach höheren Frequenzbereichen, zu erfüllen. Die Standardisierung ist allerdings noch nicht abgeschlossen und könnte auch zu spät kommen, da die Kosten für Lichtwellenleiter weiter fallen werden.

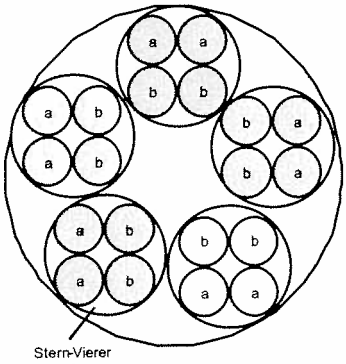


Bild: Kabelaufbau mit 8 Doppeladerpaare

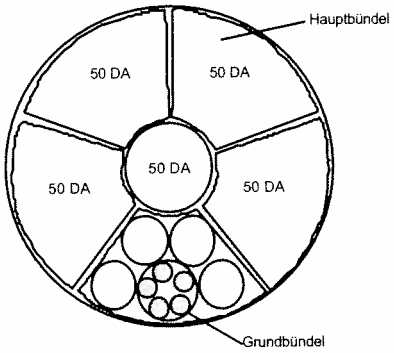


Bild: Kabelaufbau mit 300 Doppeladerpaaren

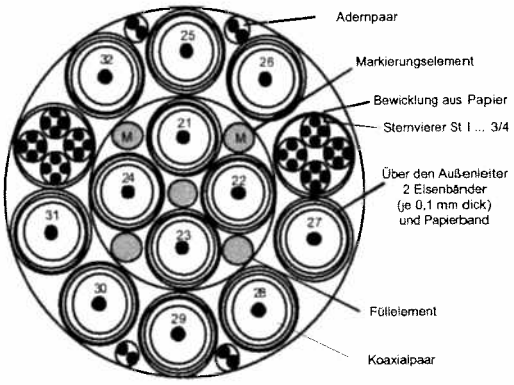


Bild: Kupferkoaxialkabel

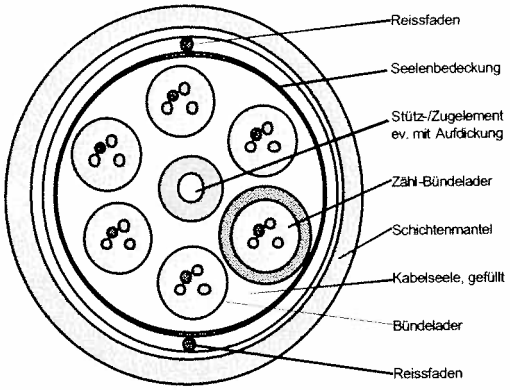


Bild: Glasfaserkabel mit 24 Fasern

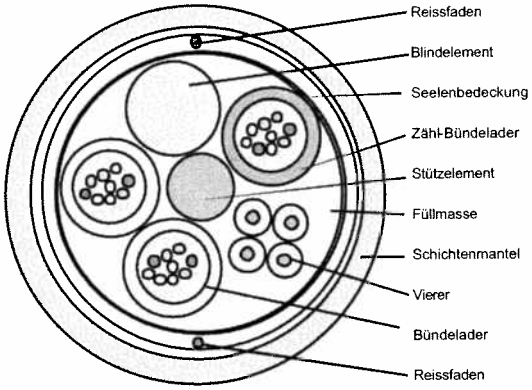


Bild: Glasfaserkabel mit 30 Fasern

Funkverbindungen

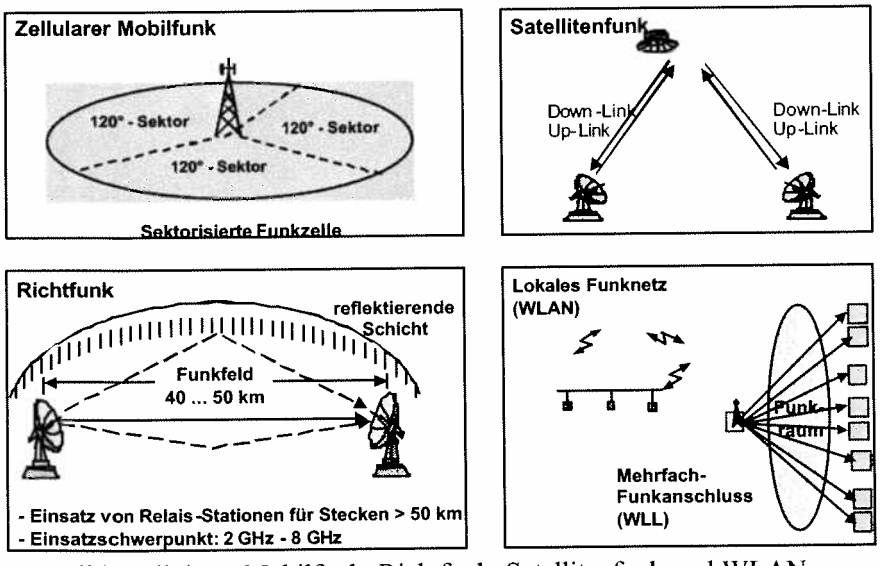


Bild: Zellularer Mobilfunk, Richtfunk, Satellitenfunk und WLANs

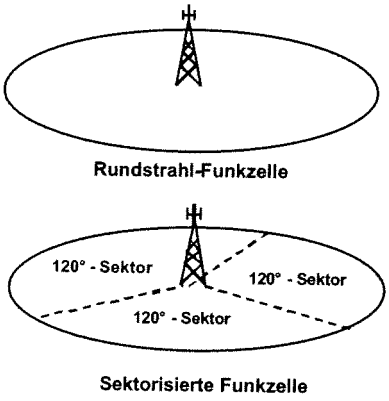
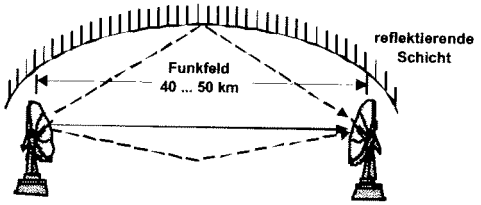


Bild: Mobilfunkzelle

Funkübertragung mit ungerichteter Ausbreitung

Die Ausbreitung elektromagnetischer Wellen im freien Raum ermöglicht eine leitungsungebundene Informationsübertragung. Bei relativ niedrigen Frequenzen strahlt eine Antenne isotrop, d. h. gleichmäßig in alle Richtungen. Damit kann ein Sender auf einer bestimmten Frequenz alle Empfänger erreichen, die auf derselben Frequenz empfangen und deren Distanz zum Sender hinreichend klein ist.

Diese Broadcast-Eigenschaft hat den Nachteil, dass auf einer Frequenz nur ein Sender zu einem Zeitpunkt senden darf. Eine Halbduplex-Verbindung zwischen zwei Kommunikationspartnern ist so ebenfalls möglich. Falls eine Vollduplex-Verbindung erforderlich ist, werden zwei Frequenzen benötigt. Bei der Funkübertragung sind Frequenzen immer knapp. Ein Ausweg ist die Bildung von Funkzellen durch geringe Sendeleistungen und eine Basisstation pro Funkzelle. Damit wird eine Wiederverwendung von Frequenzen möglich. Bei sorgfältiger Planung kann die Ebene durch Funkzellen mit nur sieben verschiedenen Frequenzen überdeckt werden.



- Einsatz von Relais-Stationen für Stecken > 50 km
- Einsatzschwerpunkt: 2 GHz - 8 GHz

Bild: Richtfunkstrecke

Funkübertragung mit gerichteter Ausbreitung

Elektromagnetische Wellen können mit geeigneten Antennen gerichtet abgestrahlt und empfangen werden. Dazu muss die Antennenstruktur größer sein als die verwendete Wellenlänge. Insbesondere für Mikrowellen (Frequenzen von ca. 1 GHz bis ca. 20 GHz, entsprechende Wellenlängen von 30 cm bis ca. 1 cm) ist die Abstrahlung mit sehr kleinen Öffnungswinkeln machbar. Entsprechende Punkt-zu-Punkt-Verbindungen werden im terrestrischen (erdgebundenen) Richtfunk und bei der Satellitenübertragung (extraterrestrischer Richtfunk eingesetzt. Trotz relativ geringer Sendeleistung können erhebliche Distanzen überbrückt werden. Dabei ist eine Bandbreite verfügbar, die auch eine rasche Übertragung digitaler Daten zulässt.

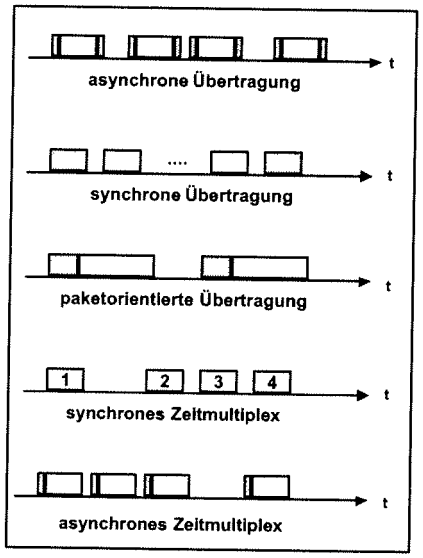


Bild: Übertragungsverfahren

Synchronisation bei bitserieller Übertragung

- **Asynchrone Übertragung**
  - Übertragung eines Datenblocks kann zu jedem Zeitpunkt erfolgen
  - Anfang und Ende müssen vom Sender speziell markiert werden
    - Start/Stop-Verfahren
    - Präambel mit 0/1-Folge
  - Sender und Empfängertakt können voneinander abweichen dadurch beschränkte Datenrate und Rahmengröße
- **Synchrone Übertragung**
  - Übertragung der Daten nur zu festen Zeitpunkten
  - Permanente Synchronisation auch wenn keine Nutzdaten gesendet werden
    - gemeinsames Taktsignal
    - Leitungscodes mit Bittaktrückgewinnung (eventuell mit Verwürfeln (Scrambling) der Daten)

Bild: Bitsynchronisation

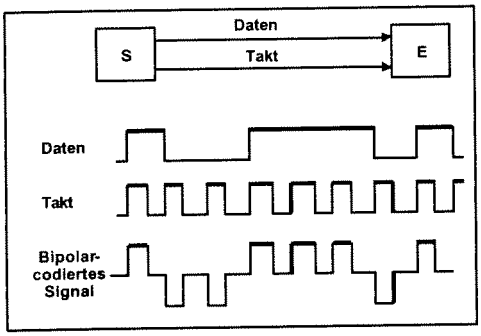


Bild: Synchrone Übertragung mit Taktleitung

Taktsynchrone Übertragung

Bei der synchronen Übertragung arbeiten Sender und Empfänger taktsynchron. Diese Synchronität kann entweder durch Mitführen des sendeseitigen Taktsignals in einer eigenen Taktleitung oder durch Taktrückgewinnung aus dem Empfangssignal erreicht werden.

In Kommunikationsnetzen wird aus technischen Gründen (zu große Entfernung, unterschiedliche Laufzeit auf Takt- und Datenleitung) und aus Kostengründen meist die zweite Methode angewandt. Dazu ist auf der Empfangsseite eine Taktrückgewinnungseinrichtung erforderlich, z.B. auf der Basis eines Phasenregelkreises (Phase Lock Loop). Das empfangene Signal wird mit dem rückgewonnenen Taktsignal abgetastet.

Wenn die Taktsignale von Sender und Empfänger nominell gleich sind und nur eine geringe zeitliche Schwankung aufwesen, kann die Anpassung der beiden Bitraten durch Stopfen erreicht werden.

Asynchrone Übertragung

Sehr häufig verwenden Sender und Empfänger Taktsignale, die voneinander unabhängig sind. Wenn die Asynchronität bestimmte Grenzen nicht überschreitet, kann mit dem Verfahren der empfangsseitigen Überabtastung das übertragene Signal fehlerfrei detektiert werden. Für die weitverbreitete asynchrone Übertragung von Zeichen im ASCII, hier mit 7 Schritten, davon 1 Start- und 1 Stop-Bit). Jedes Zeichen Z_i wird in nahezu beliebigem Abstand zum vorhergehenden gesendet (zeichenasynchron), d.h., der zeitliche Abstand zwischen zwei Zeichen Z_i und Z_{i+1} ist fast beliebig groß. Innerhalb des Zeichens ist der Schrittakt näherungsweise konstant.

Empfangseitig steht ein unabhängiges Taktsignal zur Verfügung, dessen Rate das m-fache des Nennwerts des Takts beträgt, mit dem die empfangenen Zeichen gesendet wurden. Ein typischer Wert von m ist 16. Mit Hilfe dieses hochratigen Empfangstakts wird das ankommende Signal jeweils möglichst in der Mitte eines Bitschritts abgetastet, also dort, wo das sogenannten Auge des Emp fangssignals in der Regel am weitesten geöffnet ist.

Zeichen- bzw. Symbolsynchronisierung

Bei einer Asynchronität hinsichtlich des Zeichenflusses (oder Symbolflusses) ist eine Synchronisierung des Empfängers auf Zeichen bzw. Symbolgrenzen erforderlich, damit diese richtig erkannt werden.

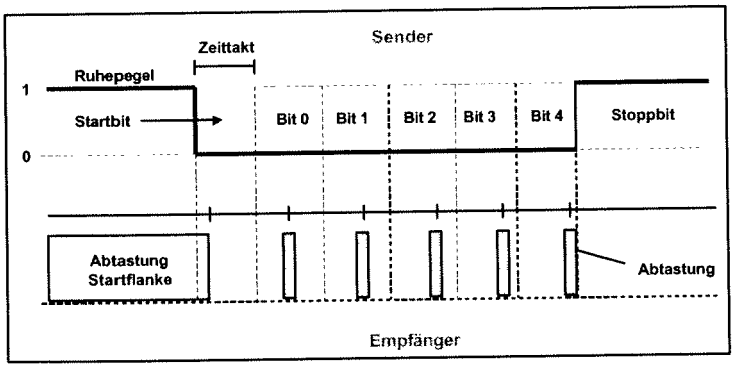


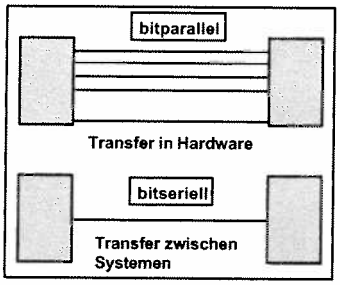
Bild: Asynchrone Übertragung

Synchronisierung des Empfängers auf Zeichen bzw. Symbolgrenzen.

Dies kann wie folgt erfolgen:

- durch Start-Stop-Bits;
- durch Erkennung bestimmter eindeutiger Bitfolgen (Kennungen, Flags);
- durch periodisches Übertragen spezieller Sync-Symbole;
- durch Korrelation, z.B. mittels mitgeführter CRC-Prüfzeichen;
- durch spezielle Codierungen (z.B. definierte Codeverletzungen).

Der Ausfall der Synchronität muss möglichst schnell erkannt werden. Daher ist im synchronisierten Zustand eine fortlaufende Prüfung des Synchronzustands und - im Falle des Außertrittfallens - ein schneller Übergang in den Zustand Wiedersynchronisieren erforderlich.



Speicherung oder Pufferung in
Bytes (8 Bits) oder Worte (16, 32, 64 Bits)

Bild: Informationsdarstellung und -transfer

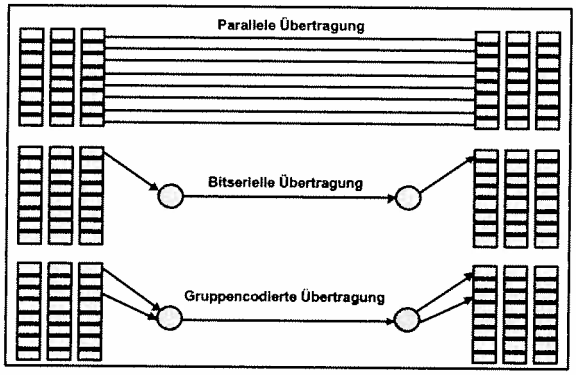


Bild: Übertragungsweisen

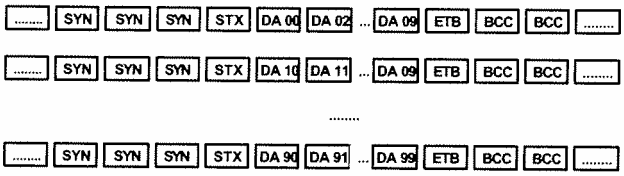


Bild: Übertragungsblöcke

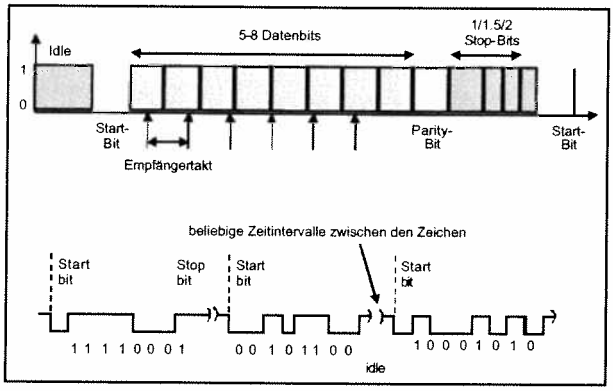


Bild: Start-Stopp-Verfahren

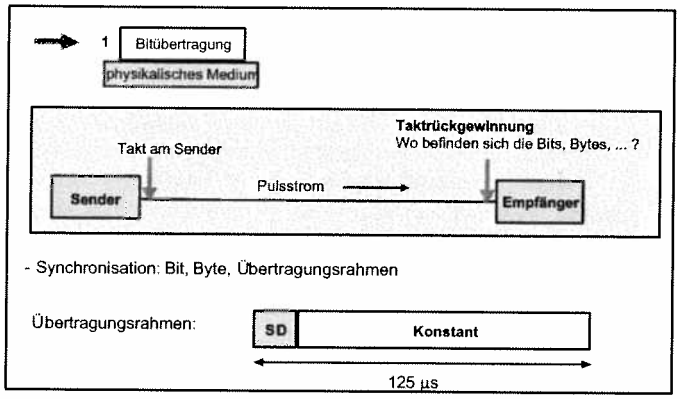


Bild: Synchronisation auf Hardware-Ebene

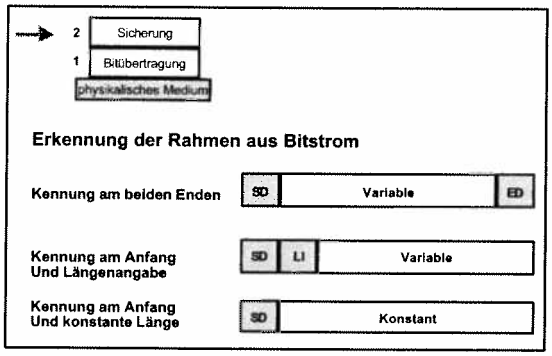
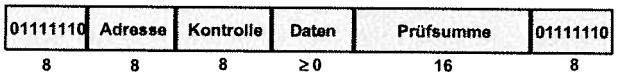


Bild: Synchronisation auf Software-Ebene



- Bitorientiert
- Bit Stuffing: 111111 ⇒ 1111101
  - Sender fügt außer bei den Flags nach jeder fünften ‚1' eine ‚0' ein.
  - Empfänger löscht die nach fünf ‚1' vorkommende ‚0'.

Bild: Bitorientierte Protokolle

- DLE (data link escape)
  - zeigt Steuerzeichen an
- Steuerzeichen
  - zeigen Anfang und Ende eines Datenpakets an
  - STX (start of text)
  - ETX (end of text)
- Character Stuffing

Bild: Zeichenorientierte Protokolle

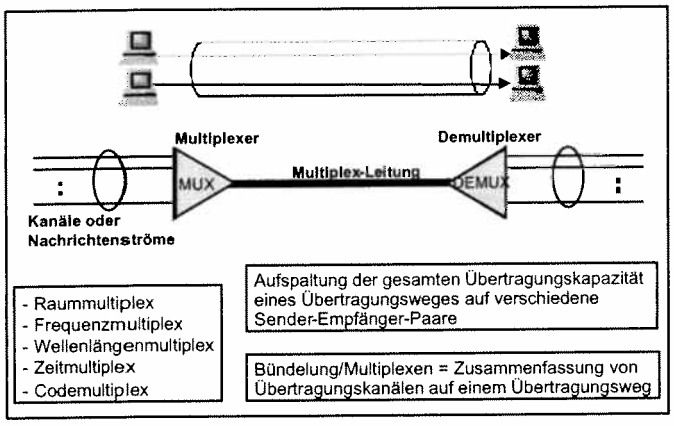


Bild: Multiplexverfahren

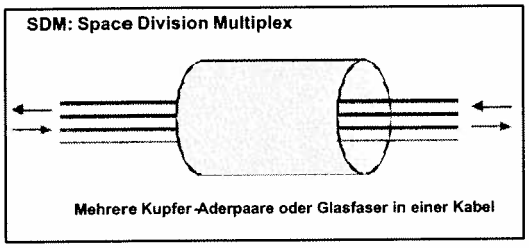


Bild: Raummultiplex (Space Division Multiplex)

Raummultiplex
Beim Raummultiplex werden den Signalen räumlich verschiedene Übertragungswege zur Verfügung gestellt.
Für n Signale werden n Leitungen verwendet. Das klassische Telefonnetz verwendet Raummultiplex mit Hilfe der Leitungsvermittlung. Dabei wird jeder Kommunikationsbeziehung (Telefongespräch) für ihre Dauer eine durchgeschaltete Leitung exklusiv zur Verfügung gestellt.

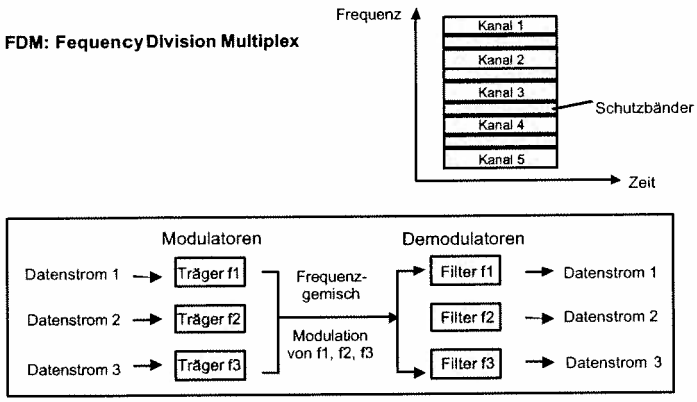


Bild: Frequenzmultiplex (Frequency Division Multiplex)

Frequenzmultiplex
Frequenzmultiplex wird realisiert, indem die einzelnen Signale auf Träger unterschiedlicher Frequenz aufmoduliert werden. Dabei ist eine geeignete Modulationsart zu wählen. Die (lineare) Summe aller Signale wird auf den Übertragungskanal gegeben. Beim Empfänger werden die einzelnen Signale durch Demodulation mit der jeweils richtigen Trägerfrequenz wiedergewonnen.

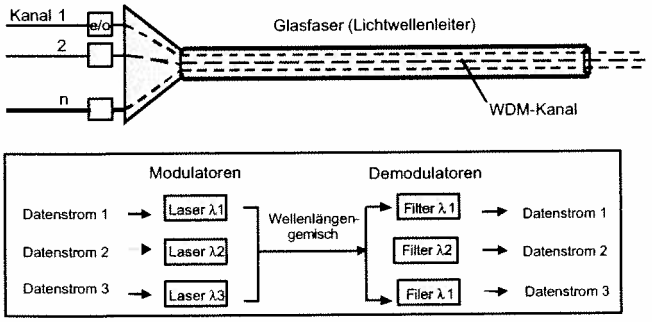


Bild: Wellenlängenmultiplex (Wavelength Division Multiplex)

Wellenlängenmultiplex
Wellenlängenmultiplex ist im Prinzip dasselbe wie Frequenzmultiplex. Bei optischen Fasern spricht man jedoch von Wellenlängenmultiplex, wenn verschiedene Signale auf Lichtwellen mit verschiedener Wellenlänge aufmoduliert werden. Wellenlängenmultiplex auf Glasfasern besitzt eine große und zunehmende Bedeutung.

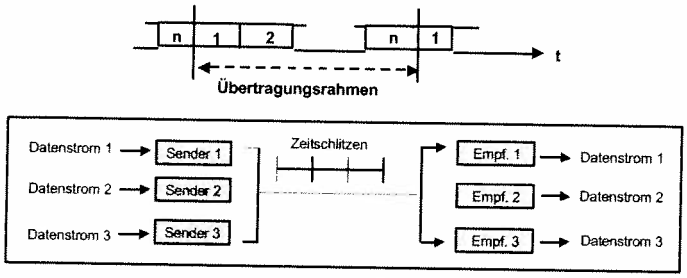


Bild: Zeitmultiplex (Time Division Multiplex)

Zeitmultiplex
Beim Zeitmultiplex wird ein Rahmen (frame) mit einer festgelegten Dauer definiert. Dieser wird in Zeitschlitze (time slot) unterteilt, die den einzelnen Signalen zugeordnet werden. Die Realisierung erfolgt durch (konzeptionell einfache) digitale Schaltungen. Wenn n Signale der Bandbreite B im Zeitmultiplex übertragen werden sollen, ist ein Übertragungskanal der Bandbreite n x B erforderlich, da die einzelnen Signale zeitlich komprimiert werden müssen.

Beim synchronen Zeitmultiplex (STDM, STM) muss der Beginn eines Rahmens jeweils durch ein Rahmenzeichen (framing code) gekennzeichnet werden. Da jedes Signal dieselbe Anzahl Bits erhält, kann ein bestimmtes Signal durch Abzählen der Bits lokalisiert werden. Ein Nachteil des synchronen Zeitmultiplex liegt darin, dass ein Kanal seinen Zeitschlitz auch dann behält, wenn gerade nichts gesendet wird.

Beim asynchronen Zeitmultiplex (ATDM, ATM, auch statistischer Zeitmultiplex) erhalten in einem Rahmen nur diejenigen Signale einen Zeitschlitz, für die tatsächlich etwas übertragen werden muss. Dadurch kann die verfügbare Übertragungskapazität im statistischen Mittel besser ausgenutzt werden. Die Zuordnung von Signal und Zeitschlitz muss jedoch mit übertragen werden, wodurch die Datenmenge zunimmt.

STM (Synchronous Transfer Mode, auch STDM): geringer Qverhead, jedes Signal erhält dieselbe Bandbreite, Zuordnung durch Abzählen.

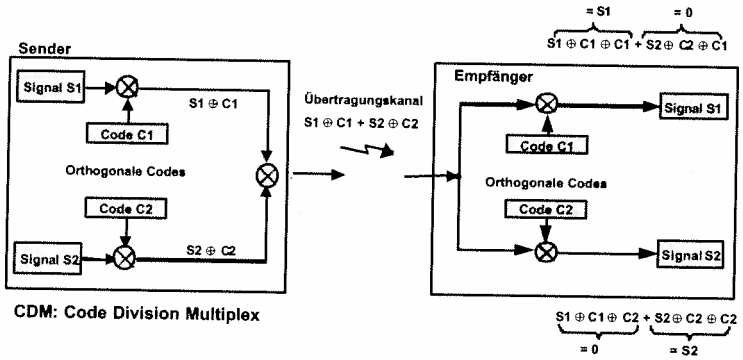


Bild: Codemultiplex (Code Division Multiplex)

Codemultiplex ordnet jedem der zu übertragenden Signale einen eigenen Code zu. Alle Signale können über ein gemeinsames Medium (gleicher Raum, gleiche Frequenz- und Zeitlage) übertragen werden. Der Empfänger kann ein bestimmtes Signal eindeutig decodieren, wenn er dessen Code kennt.

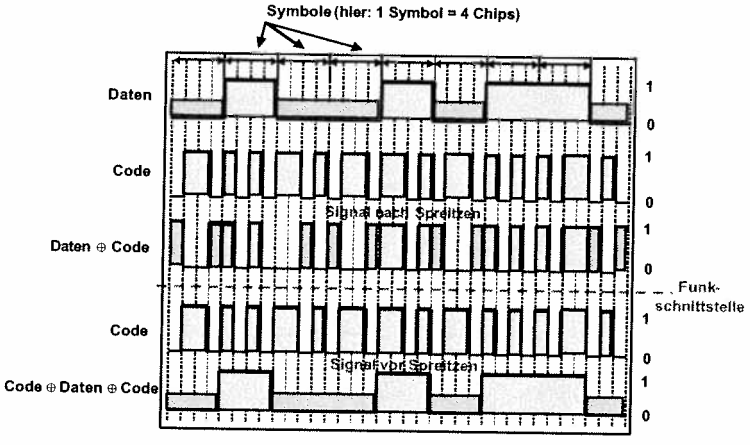
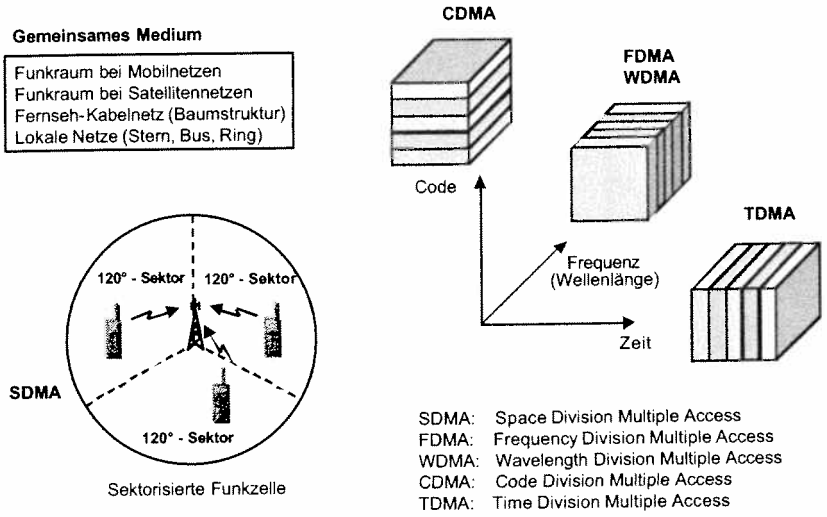
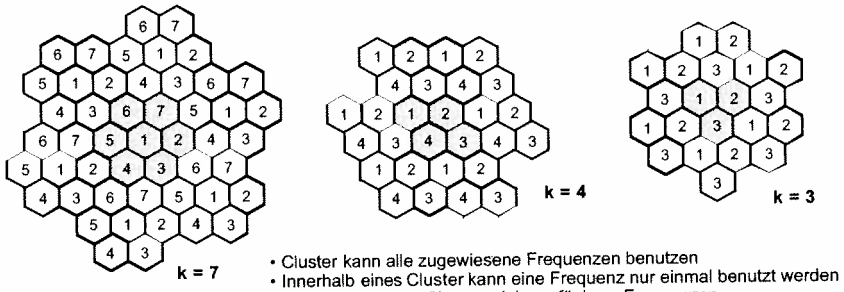


Bild: Bit – Symbol - Chip



Bei Freiraum-Übertragung wird ein gemeinsames Medium *(shared medium)* verwendet, das einen Raummultiplex-Betrieb verhindert (außer bei gerichteter Ausbreitung). Jedoch kann die Reichweite der gesendeten Signale durch die Sendeleistung in Relation zur Empfänger-Empfindlichkeit gesteuert werden. Somit kann dieselbe Frequenz außerhalb bestimmter Entfernungen wieder verwendet werden, ohne dass die Signale sich gegenseitig stören.

Bild: Mehrfachzugriff auf gemeinsames Medium



Clustergröße $k = i^2 + i \cdot j + j$ $\quad i,j = 0,1,2,3,\ldots \; i \geq j$

Nächste Zelle mit gleicher Frequenz:
i Zellen in einer Richtung, danach Drehung um 60° gegen den Uhrzeigersinn und j Zellen in gleicher Richtung

i	1	1	2	2	3	2	3	4
j	0	1	0	1	0	2	1	0
k	1	3	4	7	9	12	13	16

Bild: Zellorganisation in GSM-Netzen

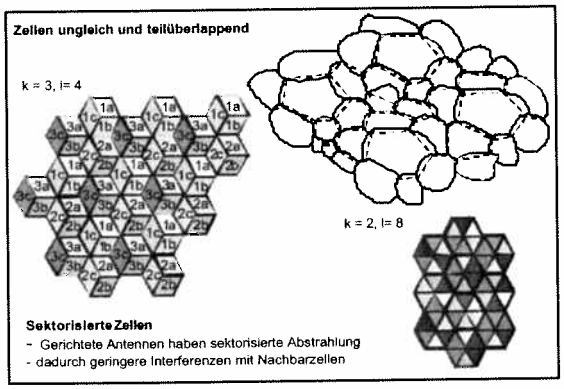


Bild: Zellstrukturen

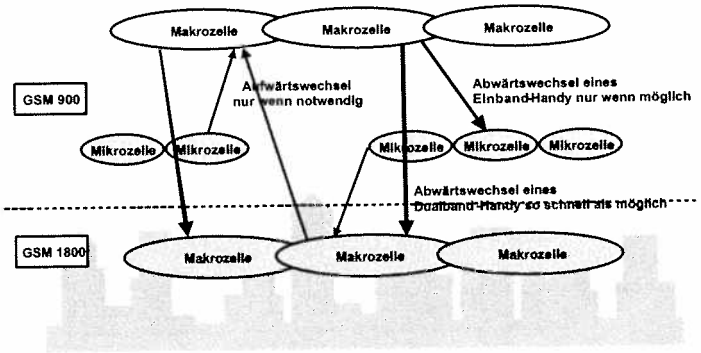


Bild: Hierarchische Zellstruktur

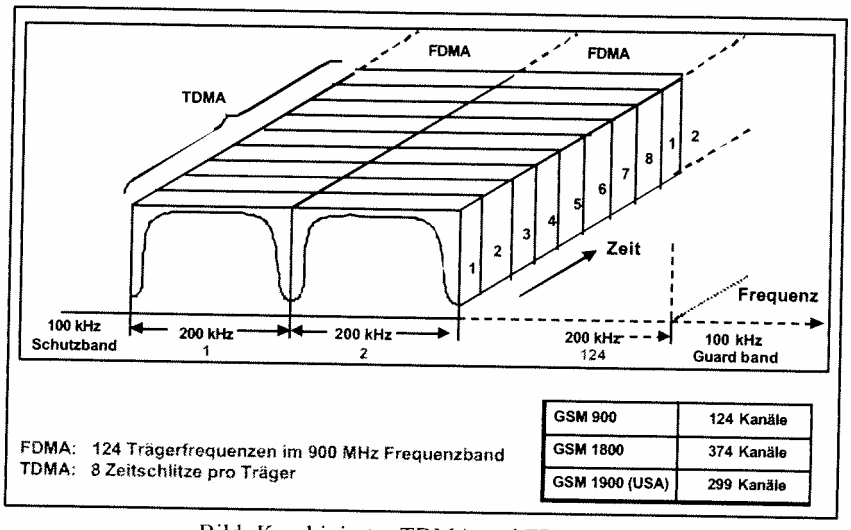


Bild: Kombinierter TDMA und FDMA bei GSM

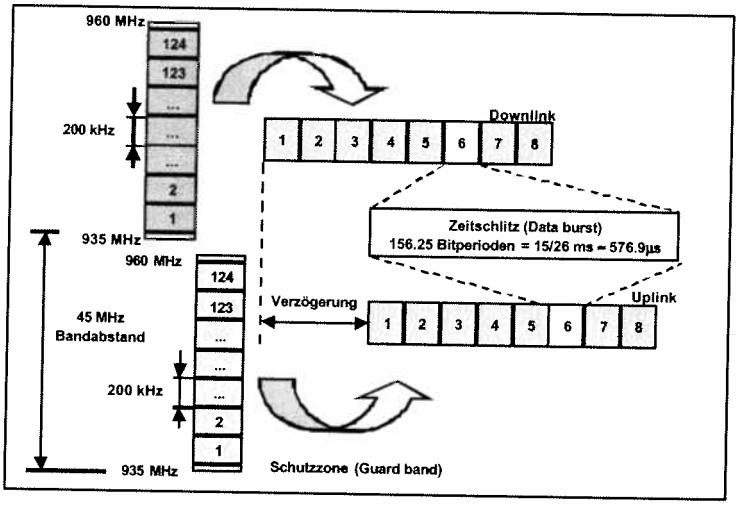


Bild: GSM: Trägerfrequenzen und TDMA-Rahmen

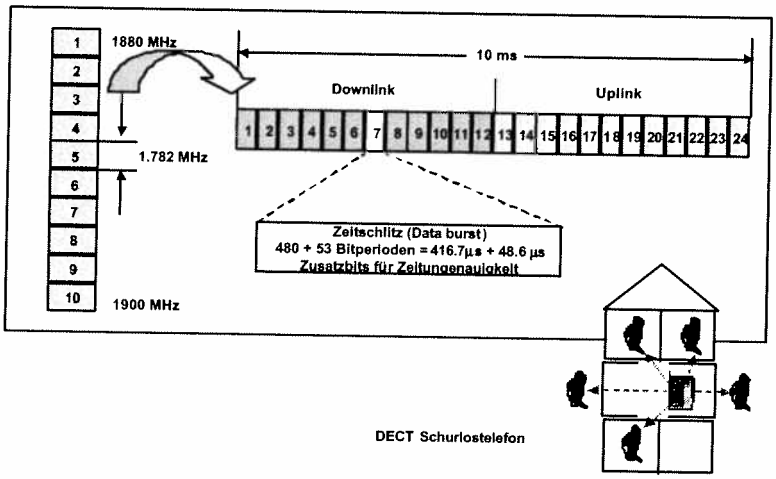


Bild: DECT: Digital Enhanded Cordless Telephone

Das DECT-System wählt dynamisch einen der 10 Trägerfrequenzen und einen freien Slot im Rahmen mit 24 Slots auf diesem Träger. Dabei gibt es eine feste Beziehung zwischen der Slotposition auf dem Downlink und der auf dem Uplink. (Erste 12 Slots down, zweite 12 Slots up).

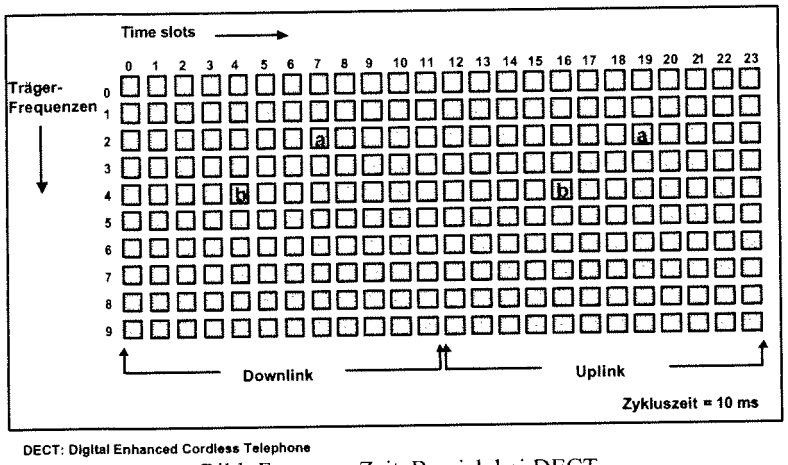


Bild: Frequenz-Zeit-Bereich bei DECT

Das Bild zeigt den Frequenz-Zeit-Bereich bei DECT.

Verbindung a (Slot 7 und Slot 19), Verbindung b (Slot 4 und Slot 16).

Es handelt sich um TDD (Time Division Duplex).

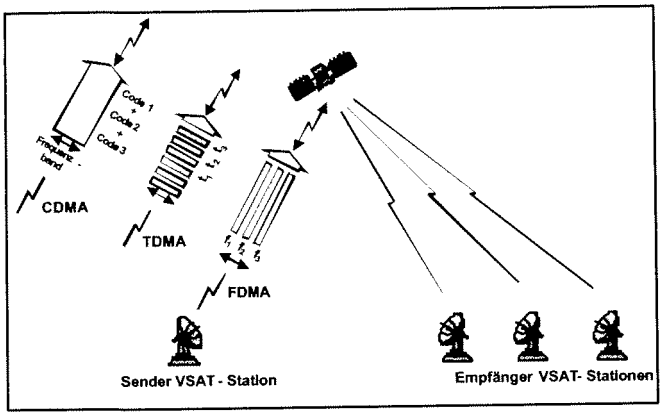


Bild: Satellitenzugriffsverfahren

Auch bei Satellitenzugriff gibt es die Mutiplexzugriffsverfahren FDMA, TDMA und CDMA.

Beispiel: Satellitenzugriff mit VSAT-Stationen (VSAT, Very Small Aperture Terminals).

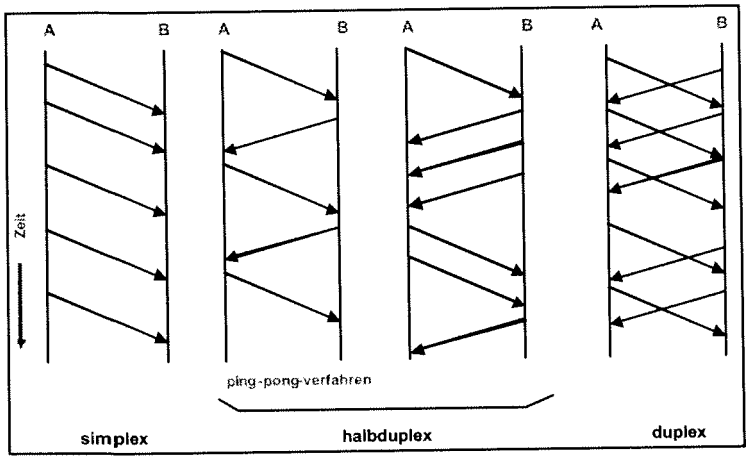


Bild: Betriebsarten der Übertragung

Uni- und bidirektionale Übertragung

Eine unidirektionale Übertragung von A nach B lässt in der Gegenrichtung (B nach A) keine Kommunikation zu. Fast immer ist eine bidirektionale Übertragung gewünscht, bei der beide Übertragungsrichtungen nutzbar sind.

Eine Teilstrecke kann um- oder bidirektional genutzt werden. Der Begriff **Simplex** bezeichnet eine unidirektionale Übertragung, **Duplex** eine bidirektionale Übertragung. Im **Halbduplex-Betrieb** werden die beiden Übertragungsrichtungen abwechselnd genutzt, im **Vollduplex-Betrieb** gleichzeitig.

- Raumduplex
- Frequenzduplex
- Wellenlängenduplex
- Zeitduplex
- Codeduplex

- Leitungen
- Mobilfunk
- Satellitenfunk

Bild: Duplex-Verfahren

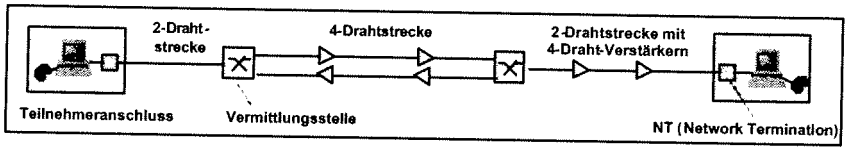
Simplex- und Duplex-Übertragungsverfahren

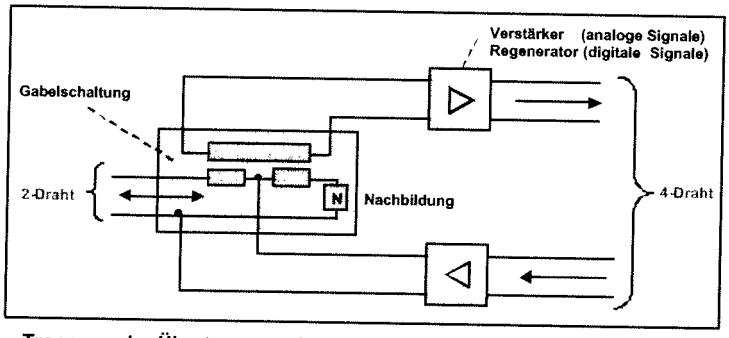
Bei einem Übertragungssystem lassen sich hinsichtlich der Gleichzeitigkeit der Übertragung mehrere Betriebsarten unterscheiden:

- Simplexbetrieb
- Halbduplexbetrieb
- Duplex- bzw. Vollduplexbetrieb

Bei der **Simplexübertragung** werden Nachrichten nur in einer Richtung gesendet. Die Übermittlung mehrerer Nachrichten kann zeitlich überlappend erfolgen. Beim **Halbduplex-Betrieb** ist eine Übertragung in beiden Richtungen möglich, allerdings nicht gleichzeitig, sondern wahlweise in Hin- oder Rückrichtung, z. B. alternierend, nach dem Prinzip der Wechselsprechanlage. Im Unterschied zum **Vollduplexbetrieb** vereinfacht sich insbesondere bei Zweidrahtsystemen das Übertragungssystem erheblich, da eine Störung des Empfangskanals, z. B. durch Echos eigener Sendesignale, nicht auftreten kann. Der Halbduplexbetrieb bedeutet eine Einschränkung der Kommunikationsfähigkeit.

Für einen uneingeschränkten bidirektionalen Betrieb wird ein Kanal im Vollduplex betrieben. Dabei kann gleichzeitig gesendet und empfangen werden. Um bei der Übertragung über Zweidrahtleitungen Störungen der Empfangssignale zu minimieren, können z. B. Echokompensationsverfahren verwendet werden.





Trennung der Übertragungsrichtungen durch einen Gabelschaltung

Bild: 2-Draht und 4-Draht-Übertragungsstrecken

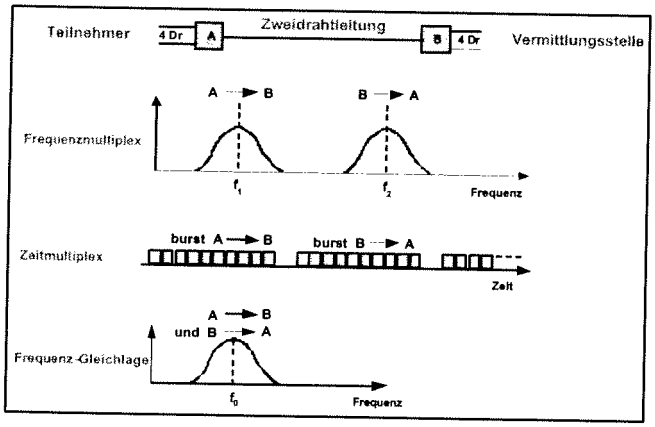


Bild: Vollduplexverkehr auf Zweidrahtle itungen

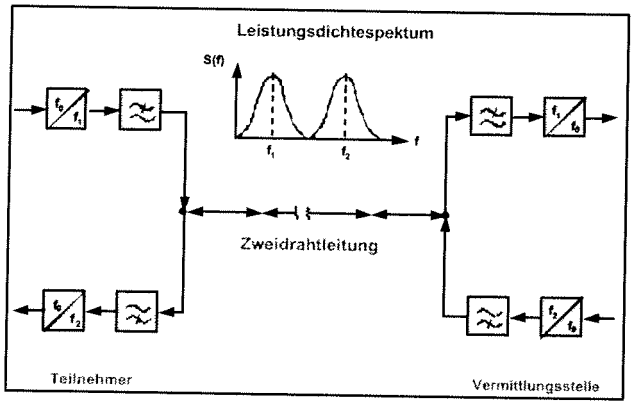


Bild: Zweidraht-Frequenzmultiplex

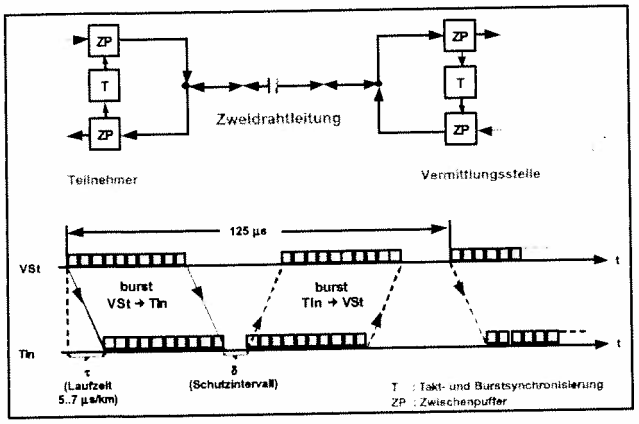


Bild: Zweidraht-Zeitmultplex

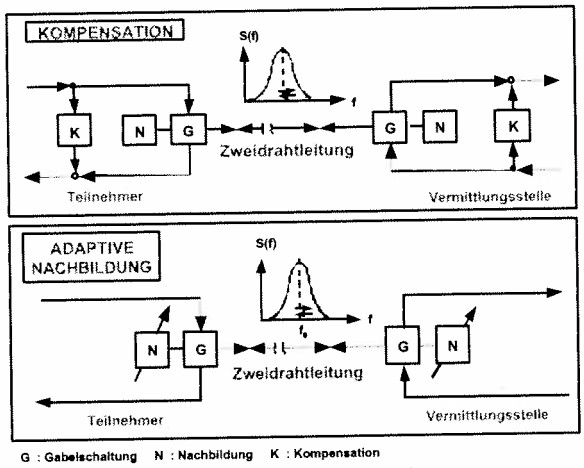


Bild: Bild: Zweidraht-Frequenz-Gleichlage

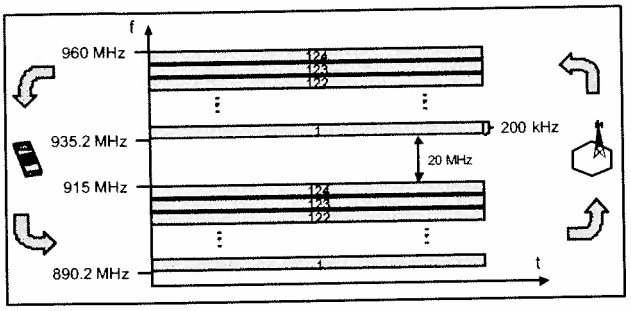


Bild: FDD/FDMA bei GSM

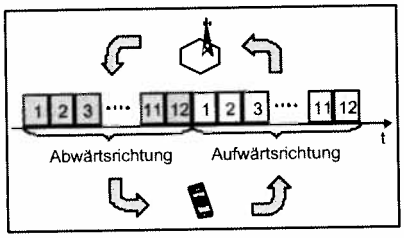


Bild: TDD/TDM bei DECT

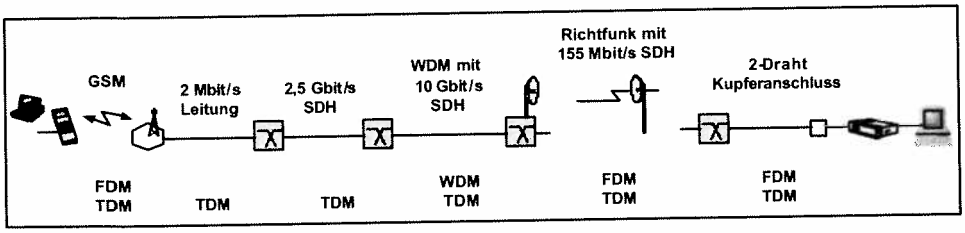


Bild: Multiplexverfahren einer Verbindung

1.7 Grundlagen: Vermittlung

Version: Feb. 2004

Inhalt

- Durchschalte-, Nachrichten-, Paket-, Datagramm-, Rahmen- und Zellvermittlung
- Raum-, Zeit- und Wellenlängenvermittlung
- Synchrone und asynchrone Koppelnetze
- Struktur von Vermittlungsknoten und Router

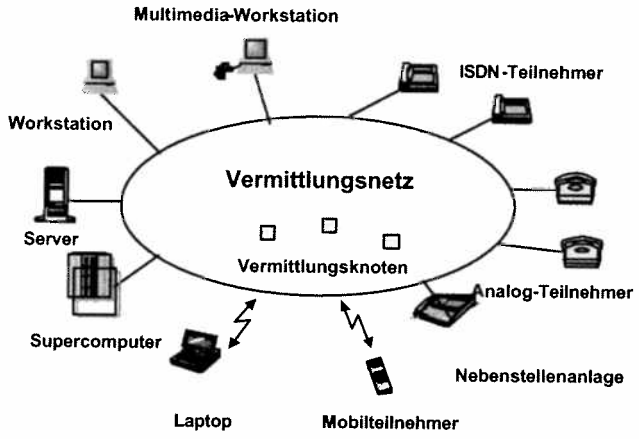


Bild: Vermittlungsaufgabe

Ein Vermittlungsnetz hat die Aufgabe, eine temporäre Verbindung zwischen zwei Teilnehmern herzustellen, wobei der rufende Teilnehmer A dem Vermittlungsnetz die Zielinformation des gerufenen Teilnehmers B mitteilt. Dabei können die an der Verbindung beteiligten Teilnehmer an dieselbe Vermittlungsknoten oder an verschiedene Knoten des Netzes angeschlossen sein.

Teilnehmer können Menschen oder Maschinen sein. Die Anbindung an das Netz ist drahtgebunden (wired) oder drahtlos (wireless). Die Endsysteme am Netz sind analoge Telefone und digitale Geräte.

Zur Vermittlung stehen zwei Prinzipien zur Verfügung: Durchschalte- und Paketvermittlung. Bei der Paketvermittlung gibt es diverse Formen.

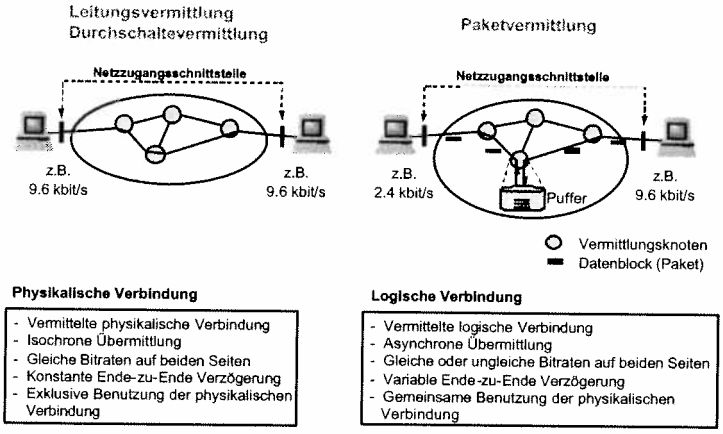


Bild: Vermittlungsprinzipien

Bei Durchschaltevermittlung wird immer eine physikalische Verbindung aufgebaut. Beide Datenendgeräte müssen mit der gleichen Datenrate (z. B. 9.6 kbit/s) operieren.

Bei Paketvermittlung kann eine virtuelle oder logische Verbindung notwendig sein (verbindungsorientierter Betrieb) oder Pakete können ohne vorherigen Verbindungsaufbau geschickt werden (verbindungsloser Betrieb). Datenendgeräte auf beiden Seiten können mit verschiedenen Bitraten arbeiten, weil im Paketvermittlungsnetz zwischengepuffert werden kann.

Fünf Unterschiede zwischen einer physikalischen und einer logischer Verbindung sind im Bild zusammengestellt.

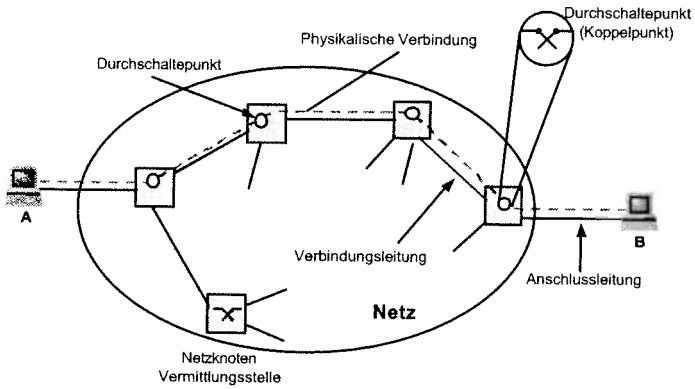


Bild: Leitungs- oder Durchschaltevermittlung

Durchschaltevermittlung
(Leitungsvermittlung; Circuit Switching, CS)

Dies ist ein verbindungsorientiertes Vermittlungsverfahren, bei dem ein durchgehender physikalischer Übermittlungskanal zur ausschließlichen Nutzung zur Verfügung gestellt wird. Dieser durchgehende Kanal entsteht durch Verknüpfen mehrerer aufeinanderfolgender Übermittlungsabschnitte, die über Koppelpunkte miteinanderverbunden werden.

Die Übermittlungsabschnitte sind funk- oder leitungsgebunden und abschnittsweise wird Raum-, Frequenz-, Wellenlängen- Zeitmultiplex- oder Codemultiplex verwendet werden.

Das Merkmal eines physikalischen Übermittlungskanal ist seine streng periodische Verfügbarkeit, um eine bestimmte Bitmenge isochronon von Netznoten zu Netzknoten bis zum Endgerät des Ziels zu transportieren. Bei einem Sprachkanal werden genau alle 125 µs acht Bit transportiert.

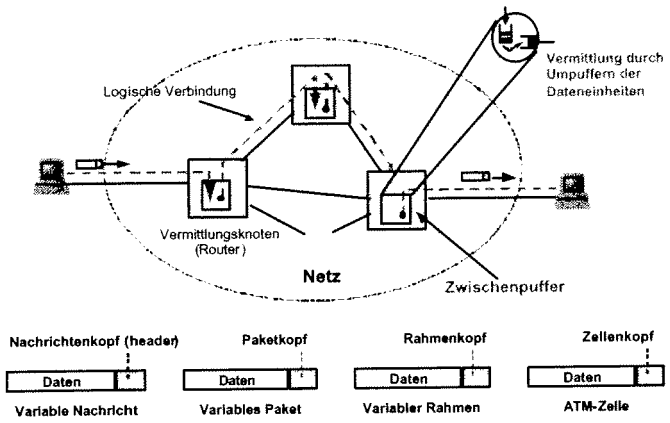


Bild: Sendungs-, Paket-, Rahmen- und Zellenvermittlung

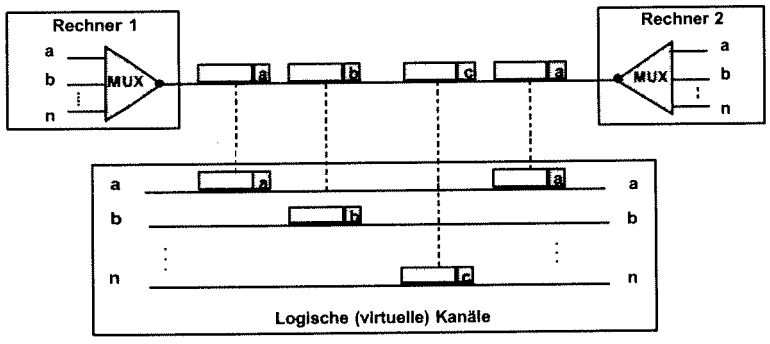
Bei der Paketvermittlung (Packet Switching, PS) gibt es verschiedene Formen. Man unterscheidet zwischen:

- Sendungsvermittlung (message switching, auch: Nachrichtenvermittlung),
- Paketvermittlung (packet switching),
- Datagrammvermittlung (datagram switching),
- Rahmenvermittlung (frame switching),
- Zellenvermittlung (cell switching, ATM switching).

Die einzelnen Datenblöcke werden über Vermittlungsknoten (bzw. Router im Internet) durch Zwischenpufferung und aufgrund von der mitgeführten Adressinformation zum Ziel geleitet.

Wie im obigen Bild angegeben, haben die Datenblöcke je nach Verfahren andere Bezeichnungen. Die Datenblöcke bestehen immer aus Benutzerinformation (Nutzdaten, payload) und Zusatzinformation (Datenblock-Kopf, header). Nur bei ATM (Asynchronous Transfer Mode) haben payload (48 Byte) und header (5 Byte) eine konstante Länge.

Die Zieladressinformation ist entweder voll im header vorhanden (verbindungsloser Betrieb) oder die Adressierung ist abschnittsweise organisiert (verbindungsorientierter Betrieb, d.h. es existiert eine logische oder virtuelle Verbindung zwischen den Endsystemen).



MUX: Multiplexerfunktion

Bild: Virtuelle (logische) Kanäle in der Paketvermittlung

Logische oder virtuelle Verbindung
Bei einer logischen Verbindung wird beim Verbindungsaufbau lediglich ein Weg durch das Netz festgelegt, entlang dessen einzelne Datenblöcke (Pakete, Rahmen, Zellen) abschnittsweise übertragen werden. Die übertragungs- und vermittlungstechnischen Betriebsmittel (Kanäle, Puffer, Koppelelemente) werden dynamisch (d.h. nach Bedarf) zugeteilt und müssen mit anderen Verbindungen geteilt werden (dynamisches time sharing). Konflikte bei gleichzeitigem Bedarf der gleiche Netzressource (z.B. Übertragungsleitung oder Koppelnetz innerhalb eines Vermittlungsknotens bzw. Router) werden durch Zwischenpufferung gelöst.

Virtuelle Verbindungen werden mit dem Paketvermittlungsverfahren realisiert, indem die Kanalabschnitte in logische oder virtuelle Kanäle unterteilt werden und die virtuelle Verbindung als Kettung von logischen Kanälen repräsentiert wird. Bei der Vermittlung der Pakete werden über die logische Kanalnummer, welche jeweils im Paketkopf mitgeführt wird, der physikalische Ausgangskanal und die logische Kanalnummer auf dem physikalischen Ausgangskanal über den Verbindungstabelle ausgelesen, aufgrund deren die Vermittlung erfolgt.

Verbindungslose Kommunikation: Für nur sporadische Kommunikation mit geringem Datenvolumen wird aus Zeit- und Aufwandsgründen keine Verbindung aufgebaut. Grundlage für die verbindungslose Kommunikation ist das Paketvermittlungsverfahren, indem einzelne Datenblöcke von Quellensystem zum Zielsystem befördert werden. Verbindungslose Kommunikation ist stets erforderlich als Mechanismus für den Verbindungsaufbau bei verbindungsorientierter Kommunikation.

Datagramm-Betrieb: Hier werden einzelne Datenblöcke (Pakete) durch das Netz übermittelt. Besteht die Sendung aus mehreren Paketen, übernimmt das Netz keine Garantie über die Richtigkeit der Reihenfolge oder die Integrität der Sendung bei Verlust eines Paketes.

Quittiertes Datagramm: Die verbindungslose Kommunikation kann erweitert werden, indem das Zielsystem für jedes empfangene Paket eine Quittung an das Quellensystem zurücksendet.

Verbindungsmerkmale (Connection Attributes)
Die einzelnen Verbindungstypen können durch weitere Merkmale (Attributes) näher beschrieben werden. Einige wichtige Merkmale sind in der nachfolgenden Tabelle aufgeführt

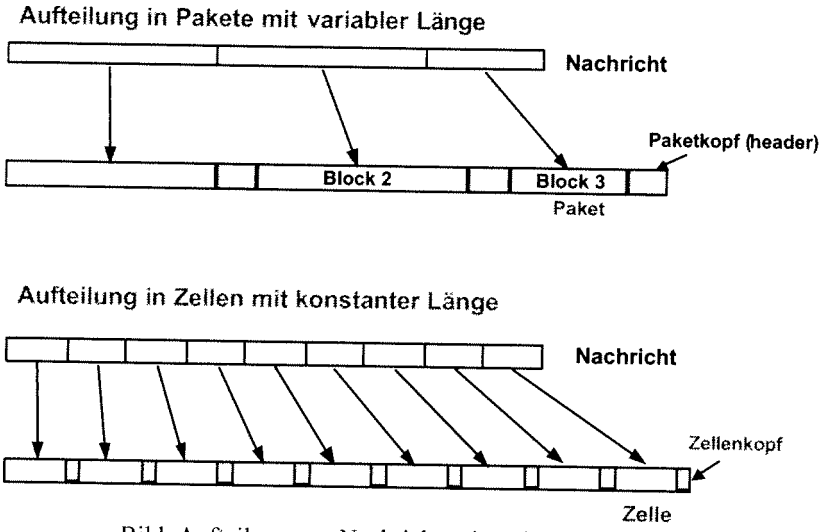


Bild: Aufteilung von Nachrichten in Pakete oder Zellen

Aufteilung von Paketen (Segmentieren, Fragmentieren)
Datendateien oder Nachrichten, deren Länge die maximale Übermittlungseinheit überschreiten, müssen in kleinere Dateneinheiten aufgeteilt werden. Dabei sind zwei Vermittlungsverfahren zu berücksichtigen:

1) Aufteilung in variable Pakete
- Jeder Datenblock erhält ein Paketkopf.
- Erste Datenblöcke mit maximaler Länge.
- Letzter Datenblock enthält den Rest der Daten und ist meistens kleiner.

2) Aufteilung in konstante Zellen (ATM)
- Jeder Datenblock erhält ein Zellenkopf.
- Alle Datenblöcke haben eine konstante Länge von 53 Byte (Header: 5 Byte).

Sendungsvermittlung
- Übermittlungsblock enthält die gesamte Nachricht; es findet somit keine Zerstückelung statt; der gesamter Datenblock wird übermittelt.
- Da der ganze Datenblock in jedem Vermittlungsknoten zwischengepuffert werden muss, bevor er weitergeleitet werden kann, entstehen lange Gesamtübertragungszeiten.
- Das Verfahren benötigt einen großen Pufferbedarf.
  Nur geeignet für zeitunkritischen Massendatentransport.
- In der Regel wird einen verbindungsloser Betrieb verwendet.

Paketvermittlung (Packet Switching, PS)
- Nachrichtenblöcke begrenzter Länge.
- Aufteilung/Zusammenführung in beiden Endknoten .
- günstige Pufferorganisation.
- kurze Übertragungszeiten .
- geeignet für Burst-Betrieb (interaktive Betriebsweise) .
- verbindungsorientierter Betrieb (Virtuelle Verbindung).
- oder verbindungsloser Betrieb (Datagramm).

Rahmenvermittlung (Frame Relay, FR)
- Die Vermittlung findet auf Schicht 2 statt und ist dadurch effizienter und schneller.
- gleiche Eigenschaften wie die Paketvermittlung.
- verbindungsorientierter Betrieb (Virtuelle Verbindung).

Merkmal	Möglichkeiten
Vermittlungsprinzip	- Durchschaltevermittlung (CS) - Sendungsvermittlung - Paketvermittlung (PS) - Rahmenvermittlung (FR) - Zellenvermittlung (ATM)
Nutzinformations-übertragung	- analog - digital transparent - digital nichttransparent (Redundanzminderung) - kontinuierlich (stromförmig) - diskontinuierlich (paketiert)
Übertragungsrate	- konstante Bitrate - variable Bitrate - Paketrate
Verbindungsaufbau	- festgeschaltet - wählvermittelt
Verbindungs-konfiguration	- Punkt-zu-Punkt-Verbindung - Punkt-zu-Mehrpunkt-Verbindung - Mehrpunkt-Verbindung

Zellvermittlung (Asynchronous Transfer Mode, ATM)
- Nachrichtenblöcke konstanter Länge (53 Byte).
- Aufteilung/Zusammenführung in beiden Endknoten.
- günstige Pufferorganisation.
- Sehr kurze Übertragungszeiten.
- geeignet für Burst-Betrieb (interaktive Betriebsweise).
- Geeignet für Echtzeit-Betrieb (Sprache, Video, Multimedia)
- verbindungsorientierter Betrieb (Virtuelle Verbindung).

Vermittlungsverfahren und Verkehrslenkung

Unter Vermittlung wird das wahlweise Herstellen von Verbindungen (bei verbindungsorientierter Kommunikation) und das Übermitteln von Informationen zwischen wechselnden Anschlusspunkten oder Benutzern verstanden. Zur Vermittlung gehören insbesondere die Steuerung des Verbindungsauf- und -abbaus, die Bereitstellung (Reservierung) oder Belegung übertragungstechnischer und vermittlungstechnischer Betriebsmittel (Kanäle, Koppeleinrichtungen, Puffer) einschließlich der zugehörigen Steuerungsalgorithmen und Steuerungstabellen.

Zu beachten ist, dass es zwei Arten von Ende-zu-Ende Verbindungen gibt:

1) Die physikalische Verbindung bei der Durchschaltevermittlung (Leitungsvermittlung).
2) Die logische Verbindung bei den diversen paketvermittlenden Verfahren. Hierbei handelt es sich um einen verbindungsorientierter Betrieb.

In beiden Fällen besteht die Kommunikation aus einer Aufbau-, Informationsaustauch- und Abbauphase.

Analog zu den unterschiedlichen Verbindungskonzepten existieren unterschiedliche Vermittlungsverfahren. Für die netzweite Einrichtung von Verbindungen bzw. die netzweite Übermittlung von Dateneinheiten (Paketen) ist ein Datenweg durch das Netz auszuwählen; die zugehörige Funktion ist die Verkehrslenkung.

Beides, Verkehrslenkung (routing) und Vermittlung (switching) sind typische Funktionen der Schicht 3 des ISO-Basisreferenzmodells, welche aufgrund der Nummerierung bzw. Adressierung des Zielteilnehmers durchgeführt werden.

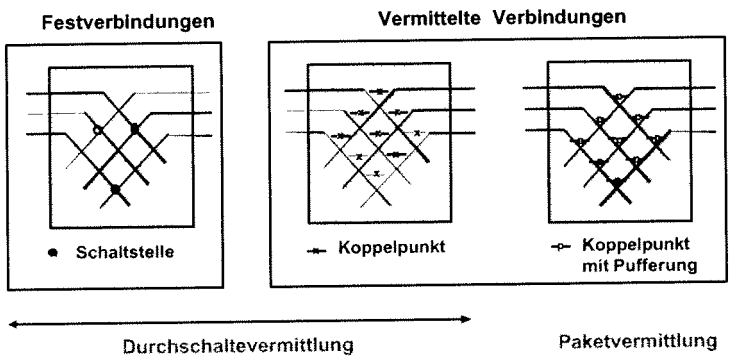
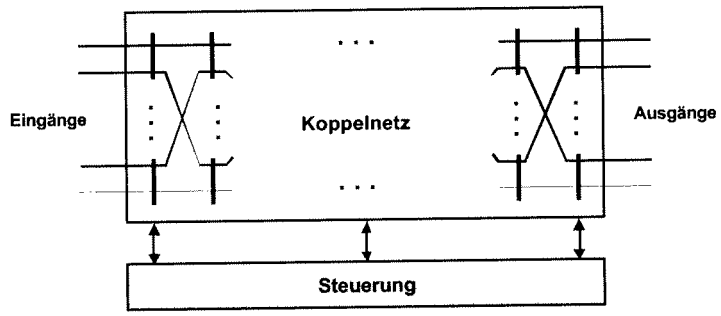


Bild: Vermittlungsfunktion in Netzknoten

Verbindungen sind entweder fest durchgeschaltet (manuell oder durch Netzmanagement) oder sie werden nach dem momentanen Bedarf automatisch vermittelt. Bei der Durchschaltevermittlung (Telefonie) werden die elektronischen Koppelpunkte in einem konstanten Zeittakt durchgeschaltet. Die Durchschalte-Information steht in einer Tabelle. Dieselbe Verbindung (Kanal) steht alle 125 µs zur Verfügung. Bei Paketvermittlung gibt es keine periodische Durchschaltung und eine Pufferung an den Koppelpunkten können hier Paketkollisionen weitgehend vermeiden.



Einstufiges Koppelnetz: viele Koppelpunkte notwendig (Anzahl Eingänge x Anzahl Ausgänge)
Mehrstufiges Koppelnetz: Reduktion der Koppelpunkte je nach interne Verbindungsstruktur

Externe Blockierung: Zielausgang ist belegt
Interne Blockierung: Ziel Ausgang ist frei, aber kein Weg durch Koppelnetz ist verfügbar

Bild: Mehrstufige Koppelnetzstruktur

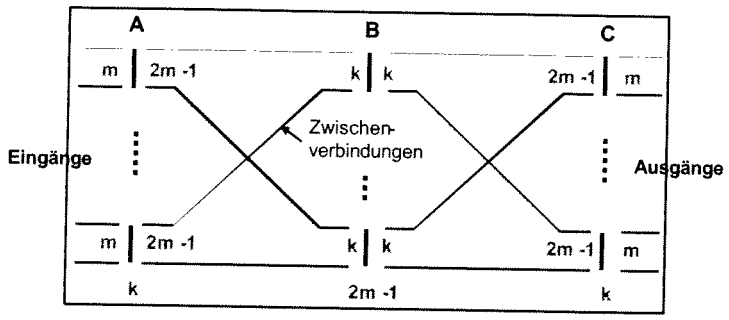
Der Koppelpunktaufwand eines Koppelmatrizes steigt quadratisch mit der Anzahl der Anschlüsse. Dies führt bei größeren Anschlusszahlen zu sehr hohem Aufwand. Ein **einstufiges Koppelnetz** besteht aus einer einzigen Koppelmatrix.

Der Aufwand lässt sich reduzieren, wenn man die Zahl der an einer Koppelmatrix angeschlossenen Anschlüsse gering hält und die einzelnen Anschlusskoppelmatrizen mit einander verbindet. Damit entsteht ein **mehrstufiges Koppelnetz**.

Bei Koppelnetzen unterscheidet man zwei Arten von Blockierungen:

1) Bei einer **externen Blockierung** ist der Zielausgang bereits belegt und somit kann keine Verbindung aufgebaut werden.

2) Bei einer **internen Blockierung** ist der Zielausgang frei, aber im mehrstufigen Koppelnetz verhindern bereits belegt Zwischenverbindungen den Verbindungsaufbau.



Blockierungsfreies Koppelnetz:

Anzahl Ein- bzw. Ausgänge	k × m
Anzahl Zwischenverbindungen pro Stufe	(2m-1) × k
Anzahl Ein- bzw. Ausgangsmatrizen	k
Anzahl Zwischenstufenmatrizen	2m-1
Ein- bzw. Ausgangskoppelmatrix	m × (2m-1)
Zwischenstufenkoppelmatrix	k × k

Einstufiger Koppelmatrix mit m Eingängen und n Ausgängen

Bild: Dreistufiges Koppelnetz nach Clos: Strukturparameter

Das kann nach einem Vorschlag von C. Clos aus dem Jahr 1953 auf folgende Weise geschehen.

Das Koppelnetz wird in drei Koppelstufen A, B und C unterteilt. Koppelstufen A und C bestehen jede aus k Koppelmatrizen. An Koppelstufe A sind Benutzer einer ersten Kategorie und an Koppelstufe B die Benutzer einer zweiten Kategorie angeschlossen. Koppelmatrix A hat m Eingänge und 2m-1 Ausgänge. Für Stufe C gilt das Umgekehrte. In der Mitte ist eine Koppelstufe mit 2m-1 Koppelmatrizen mit k Eingängen und k Ausgängen angeordnet. Die Struktur der Zwischenverbindungen ist sehr regelmäßig: von jedem Koppelmatrix A bzw. C führt nur eine einzige Zwischenleitung zu jedem Koppelmatrix B. Aus dieser Regelmäßigkeit ergeben sich auch die korrespondierenden Werte in B- und A/C-Stufen.

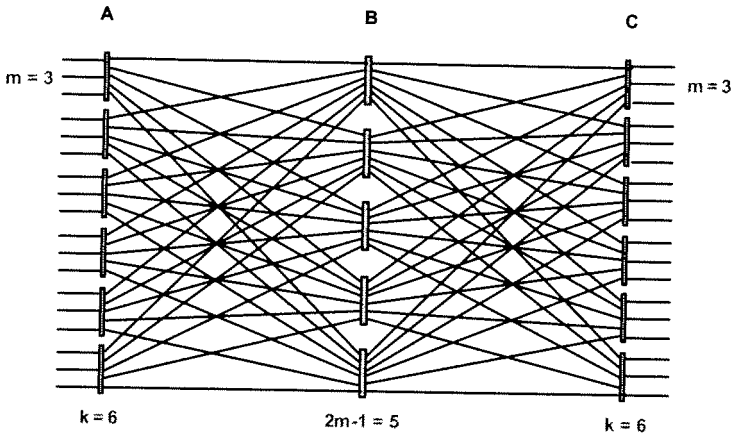
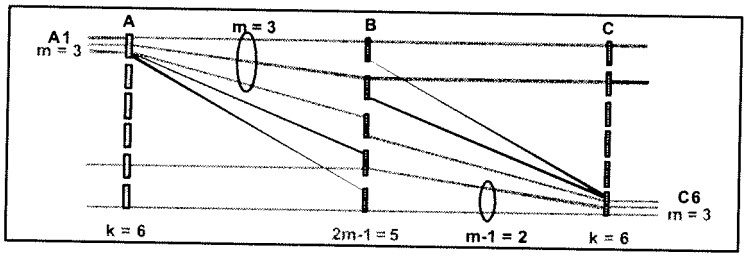


Bild: Dreistufiges Koppelnetz nach Clos: Zwischenverbindungen

Im Bild nebenan sind alle Zwischenverbindungen gezeichnet. Im nachfolgenden Bild wird die Funktionsweise an einem Zahlenbeispiel mit m=3 dargestellt, wobei 18 Anschlüsse auf k=6 Koppelmatrizen A/C verteilt werden. Es soll sichergestellt sein, dass auch unter ungünstigen Verhältnissen noch Verbindungen aufgebaut werden können, d.h. dass das Koppelnetz blockierungsfrei arbeitet. Ein ungünstiger Fall liegt z. B. vor, wenn vom Koppelmatrix A1 (links oben) eine Verbindung zum Koppelmatrix C6 (rechts unten) aufgebaut werden soll, wobei in jedem dieser beiden Koppelvielfache schon zwei Verbindungen zu anderen Koppelmatrizen bestehen.



Bedingung für ein blockierungsfreies Koppelnetz:

- Es soll immer ein Weg von einem freien Eingang zu einem freien Ausgang vorhanden sein.
- Betrachtet wird eine Verbindung über Eingangsmatrix A1 und Ausgangsmatrix C6.
- Bei m Eingängen pro Koppelmatrix A müssen jeweils m Zwischenkoppelmatrizen B mit einer freien Zwischenverbindung zum Ausgangsmatrix C des Zielausgangs erreichbar sein.
- Diese m Zwischenverbindungen zwischen Stufen B und C können nur garantiert frei sein, falls es zusätzlich m -1 weitere Zwischenkoppelmatrizen B für m-1 Verbindungen über den betrachteten Ausgangsmatrix gibt.

Bild: Dreistufiges Koppelnetz nach Clos: Beweisführung

Im Koppelmatrix A1 sind dadurch schon die Zwischenleitungen 1 und 2 belegt, währen Zwischenleitung 4 und 5 zwar noch frei sind, jedoch auf belegte Zwischenleitungen 4 und 5 zwischen den Koppelstufen B und C treffen. Für die Zwischenleitungen am Koppelmatrix C6 gilt das gleiche sinngemäß. Die letztmögliche hinzukommende Verbindung muss aber noch einen durchgehenden freien Weg über zwei Zwischenleitungen zwischen A- und B-Stufe sowie zwischen B- und GStufe finden, hier also über Koppelmatrix B3.

Wenn m-1 Zwischenleitungen eines Koppelmatrizes A und m-1 Zwischenleitungen eines Koppelmatrizes C bereits belegt sind, muss für die letztmögliche Verbindung noch ein zusätzlicher Weg bestehen. Die Zahl der notwendigen Koppelmatrizen B beträgt also 2(m-1)+1=2m-1.

Dieses Prinzip lässt sich fortsetzen, wenn man jeden Koppelmatrix B wiederum in eine Anordnung nach Clos auflöst. Die prinzipielle Anordnung und der dafür notwendige Koppelpunktaufwand ist in der Tabelle angegeben.

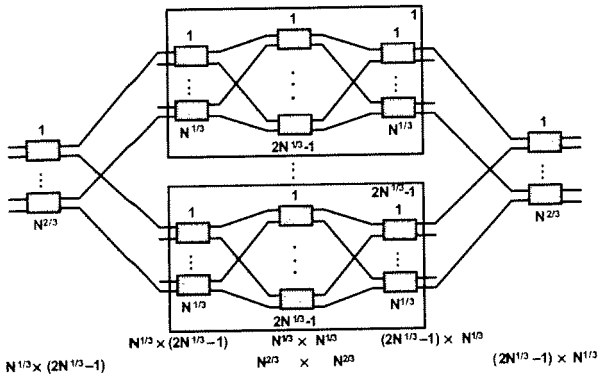


Bild: Fünfstufiges Koppelnetz nach Clos

Anzahl Koppelpunkte in mehrstufigen Koppelnetzen nach Clos

Anzahl Ein- bzw. Ausgänge N	Stufenzahl s = 1	s = 3	s = 5	s = 7	s = 9
100	10 000	5 700	6 092	7 386	9 121
200	40 000	16 370	16 017	18 898	23 219
500	250 000	65 582	56 685	64 165	78 058
1 000	1 000 000	186 737	146 300	159 904	192 571
2 000	4 000 000	530 656	375 651	395 340	470 292
5 000	25 000 000	2 106 320	1 298 858	1 295 294	1 511 331
10 000	100 000 000	5 970 000	3 308 487	3 159 700	3 625 165

Bild: Anzahl Koppelpunkte in mehrstufigen Koppelnetzen nach Clos

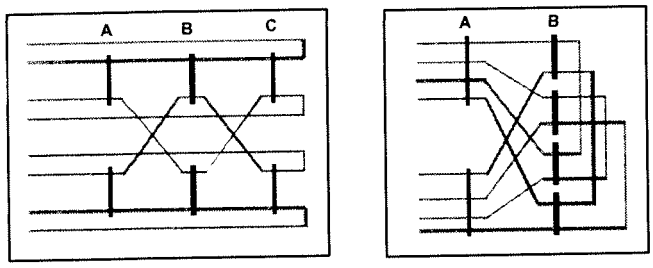


Bild: Einseitige Koppelnetze

Damit alle Anschlusse für Endgeräte sich an einer Seite befinden, verwendet man entweder die Faltgruppierung, wo die Ausgänge des Koppelnetzes durch eine Verdrahtung zurückgeführt werden, oder die Umkehrgruppierung, wo die Verbindung zweimal durch das Koppelnetz gehen muss. Im letzteren Fall sind weniger Koppelstufen notwendig.

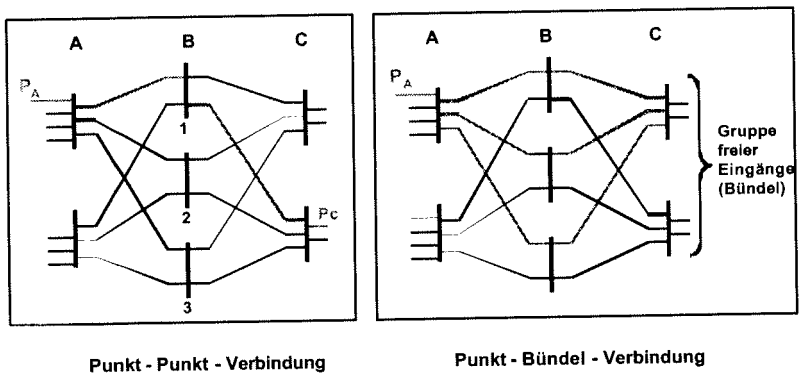


Bild: Verbindungsarten in Koppelnetzen

Wird der Eingang de Expansionsstufe A belegt, der einen ganz bestimmten Ausgang am Koppelmatrix C erreichen will, so handelt es sich um eine **Punkt-Punkt-Verbindung**. Im Gegensatz dazu steht die **Punkt-Bündel-Verbindung**, die bei der Bündelwahl anzutreffen ist. Die Punkt-Bündel-Verbindung ist deshalb dadurch gekennzeichnet, dass von einem Punkt aus mehrere Ausgänge in freier Wahl abgesucht werden, die letztlich alle in dieselbe Richtung, also zum selben Ziel, führen.

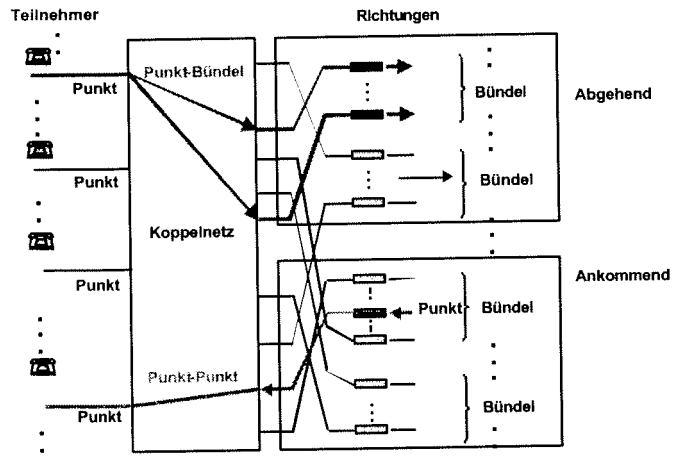


Bild: Aufgaben der Wegsuche

Die Wahrscheinlichkeit innerer Blockierung in ein und demselben Koppelnetz ist also davon abhängig, ob eine Punkt-Punkt-Verbindung oder eine Punkt-Bündel-Verbindung aufgebaut werden soll. Bei einer Punkt-Bündel-Verbindung ist die Wahrscheinlichkeit, durch das Koppelnetz zu gelangen, größer als bei einer Punkt-Punkt-Verbindung, da dem Verbindungspfad mehr Möglichkeiten zur Auswahl stehen.

Punkt-zu-Punkt:
- Endgerät zum Endgerät.
- Eingangsleitung zum Endgerät.

Punkt-zu-Mehrpunkt (Bündel):
- Endgerät zur Ausgangsleitung.
- Endgerät zur Gruppe gleicher Vermittllungseinrichtungen.

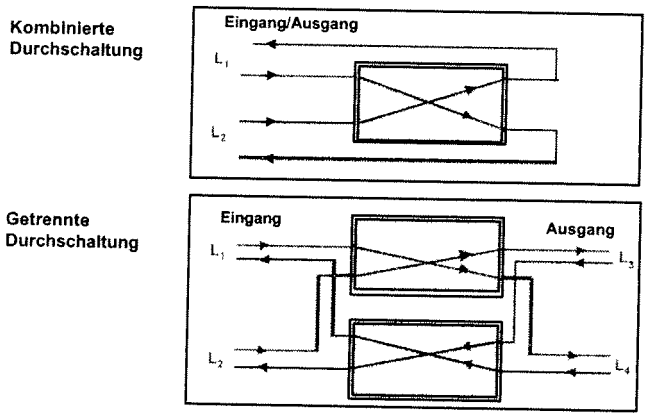


Bild: Vierdrahtdurchschaltung

Für die Realisierung der gleichzeitigen Durchschaltung von zwei Kommunikationsrichtungen gibt es verschiedene Lösungsansätze: die Duplexfähigkeit kann entweder dadurch erreicht werden, dass die ankommenden Kommunikationsrichtungen der Multiplexübertragungssysteme an die eine Seite, die abgehenden Kommunikationsrichtungen an die andere Seite der Koppeleinrichtung angeschlossen werden (Combined Switching Mode, Kombinierte Vierdrahtdurchschaltung).

Im Gegensatz dazu kann für jede Kommunikationsrichtung eine eigene Koppeleinrichtung vorgesehen werden, die allerdings beide gemeinsamen gesteuert werden können (Separated Switching Mode, getrennte Vierdrahtdurchschaltung).

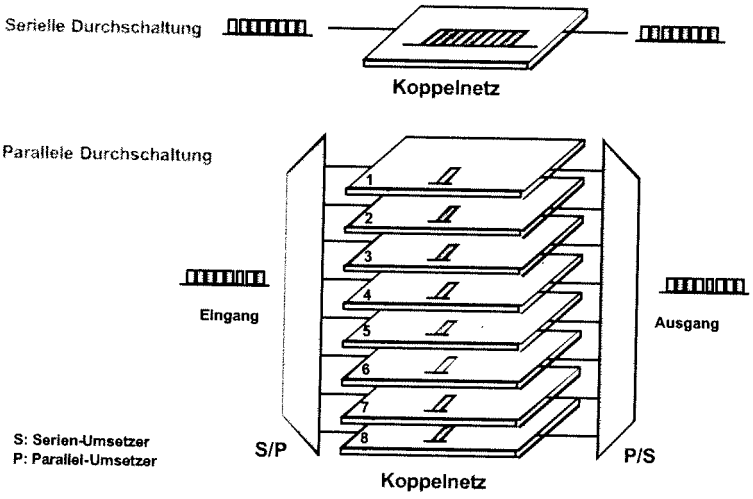


Bild: Serielle/parallele Durchschaltung

Weitere Durchschaltevarianten bei digitalen Koppelnetzen sind z. B. serielle und parallele Durchschaltung. Bei serieller Durchschaltung werden alle acht Bit jedes Oktetts nacheinander über das Koppelnetz oder über Teile davon durchgeschaltet, bei paralleler Durchschaltung werden sie dagegen gleichzeitig über acht parallele Ebenen vermittelt. Alle Ebenen können von denselben Steuerungseinrichtungen bedient werden. Auch Modifizierungen wie Durchschaltung von Halboktetts oder Durchschaltung von Doppeloktetts sind möglich. Der Vorteil der Paralleldurchschaltung liegt – bei erhöhtem Durchschalteaufwand - in der z.B. achtfach höheren Arbeitsgeschwindigkeit. Damit lässt sich ein einfaches Prinzip wie das Kombinationsvielfach auch für größere Koppelanordnungen anwenden

In der Festnetz-Telefonie werden Pulscodemodulierte Signale (PCM-Signale) in der Vermittlungstechnik seit der 80er Jahren erfolgreich angewendet. Im Vergleich mit der analogen Raumvielfach-Vermittlungstechnik konnte mit der digitalen Vermittlung die Koppelpunktkosten deutlich gesenkt werden. Heute werden hochintegrierte Koppelmatrix-Chips verwendet.

Die Durchschaltung in einer PCM-Vermittlungsstelle geschieht so, dass die PCM-Signale der einzelnen Sprach- oder Datenwege, die zeitlich verschachtelt übertragen werden, auch direkt im Zeitvielfach vermittelt werden. An das Koppelnetz einer PCM-Vermittlungsstelle werden also nur mehr Multiplexleitungen angeschlossen. In den folgenden Bilder erkennt man den Unterschied zwischen einem reinen Raumvielfach-Koppelnetz und einem digitalen Koppelnetz. Während bei analogen Vermittlungsstellen die ankommenden Verbindungen nur die Raumlage wechseln konnten, erfolgt die Vermittlung bei digitalen Vermittlungsstellen durch Auswahl sowohl einer Raum- als auch einer Zeitlage.

Raummultiplex
(Space Division Multiplex, SDM)

Koppelpunkt:
Analog: Metallischer Kontakt, 2 .. 8 – adrig
Digital: Elektronischer Schalter
Optisch: Optischer Schalter

Koppelmatrix:
Matrix aus m_1 x m_2 Koppelpunkten
m_1: Eingangsleitungen (-bündel)
m_2: Ausgangsleitungen (-bündel)

Verbindung: Leitung x_1 ankommend mit Leitung x_2 abgehend durch Schließen des Koppelpunktes (x_1, x_2)

Steuerung: Die Steuerung erfolgt beim Verbindungsaufbau (Festlegung des/der Koppelpunkte).

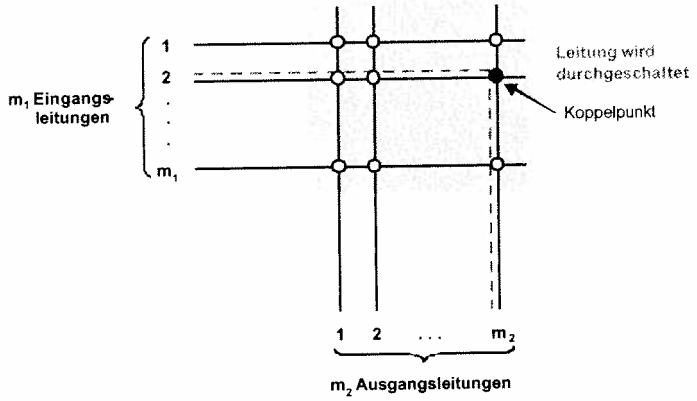


Bild: Raumvermittlung

Raum- und Zeitmultiplex
(Space and Time Division Multiplex, STDM)

Koppelpunkt: Periodisch gesteuerter elektronischer Schalter für digitale Signale (PCM)
n: Multiplexgrad (z.B. 32 Zeitlagen oder Zeitschlitze)

Koppelmatrix:
Matrix aus m_1 x m_2 STDM-Koppelpunkten
m_1: Anzahl ankommender Highways
m_2: Anzahl abgehender Highways

Vermittlung: (Highway x_1, Kanal y_1) mit (Highway x_2, Kanal y_1) durch periodisches Schließen des STDM-Koppelpunktes (x_1, x_2) zur Zeitlage y_1.

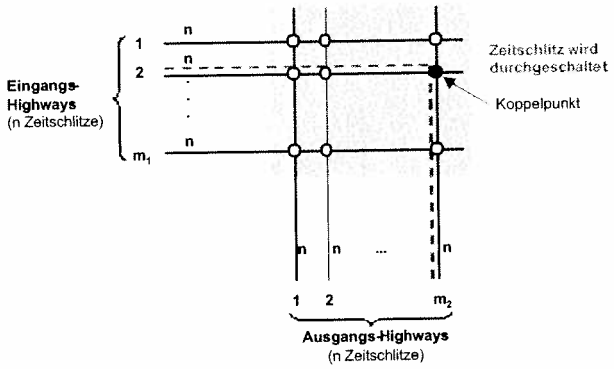


Bild: Raum- und Zeitvermittlung

Die Funktionsweise einer Kombinationsstufe ist im nebenstehenden Bild nochmals verdeutlicht. Betrachtet wird eine Übertragungsrahmenstruktur mit nur vier Zeitlagen. Bei reinem Zeitmultiplex kann nur die Zeitlage gewechselt werden. Dazu muss ein ganze Übertragungsrahmen stetig für die Rahmendauer zwischengepuffert werden können und ausgangsseitig die einzelne Zeitlagen wahlweise ausgelesen werden können. Bei reinem Raummultiplex kann auf einen anderen Ausgang gewechselt werden. Bei der Kombination beider Mechanismen hat jeder Eingang einen Zeitstufepuffer und alle Eingänge können während der Zeit einer Zeitlage mit einem der Ausgänge durchgeschaltet werden.

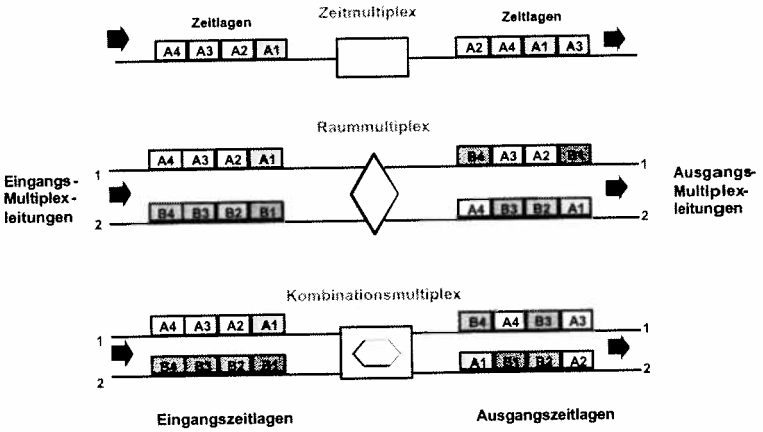


Bild: Koppelnetzelemente

Für die Steuerung einer Raumstufe wird für jede der m_1 Eingänge ein Eintrag im Steuerspeicher zum Schalten eines Ausgangskoppelpunktes de Koppelpunktreihe des betrachteten Eingangs benötigt. Ein Eintrag besteht aus ld m_2 Bit (bei 4 Ausgängen sind dies 2 Bits, bei 16 Ausgängen sind 4 Bits notwendig)

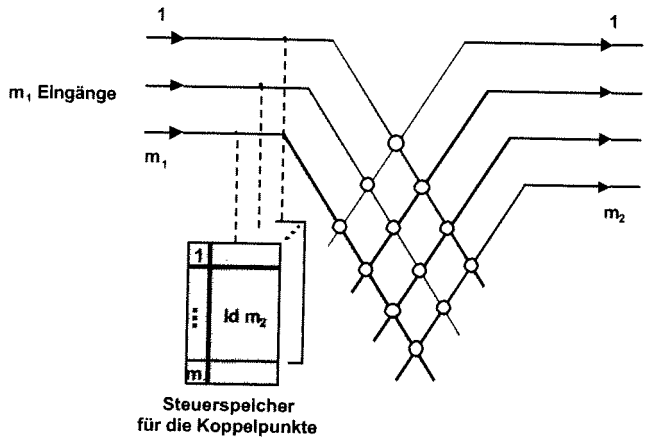


Bild: Raumvermittlungssteuerung

Eine Zeitvermittlungsstufe mit n Zeitlagen mit je x Bits erfordert einen Vermittlungspuffer mit n Einträgen von jeweils x Bits.

Es werden zuerst alle Zeitlagen einer Übertragungsrahmen zyklisch zwischengepuffert und anschließend tabellengesteuert ausgelesen.

Zur Steuerung des Auslesevorgangs enthält der Steuerspeicher n Einträge mit jeweils ld n Bits.

Damit ein kontinuierliche Strom von Übertragungsrahmen auf dieser Weise vermittelt werden kann, werden zwei Puffer, die abwechselnd eingeschrieben und ausgelesen werden, verwendet.

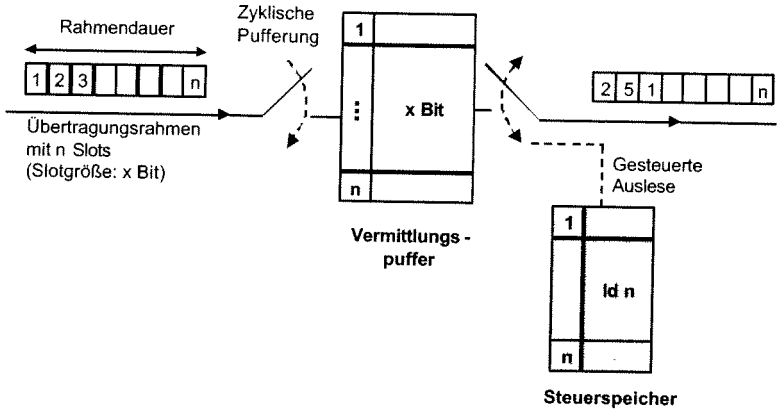


Bild: Zeitvermittlungssteuerung

Zur Realisierung einer Kombinationsstufe mit m Eingängen und m Ausgängen werden zuerst alle Zeitlagen der Eingänge verschachtelt (gemultiplext). Dadurch sind auf der Zwischenleitung zum Vermittlungspuffers n x m Zeitlagen vorhanden. Man erhöht hier die Taktrate der Zwischenleitungselektronik und/oder man verwendet parallele Zwischenleitungen falls der Taktrate nicht weiter erhöht werden kann.

Für den Vermittlungspuffer und den Steuerspeicher ist nun die Zeitlagenzahl n x m maßgebend.

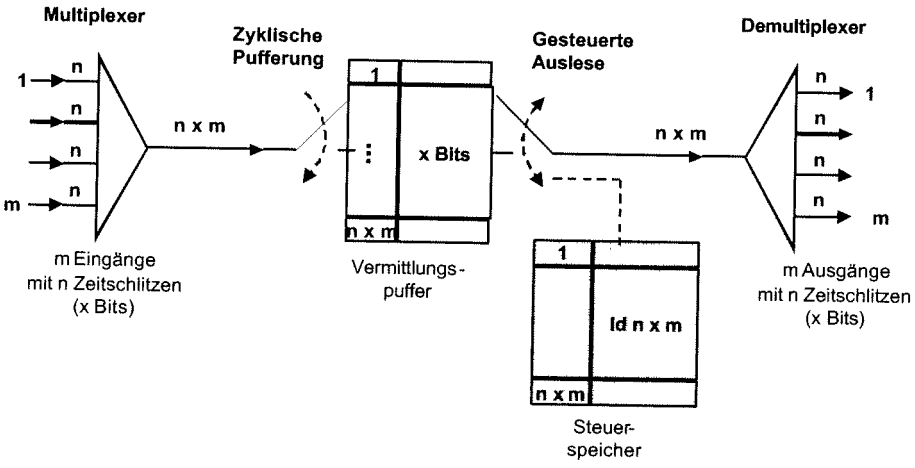


Bild: Steuerung bei Raum- und Zeitvermittlung

Synchrones Zeitmultiplex (Durchschaltevermittlung)

Als Zeitstufe für die Durchschaltevermittlung ist der Betriebsweise voll synchron, wobei der Vermittlungspuffer auch gesteuert eingeschrieben und zyklisch ausgelesen werden kann.

Pufferworte: 1 Zeitlage

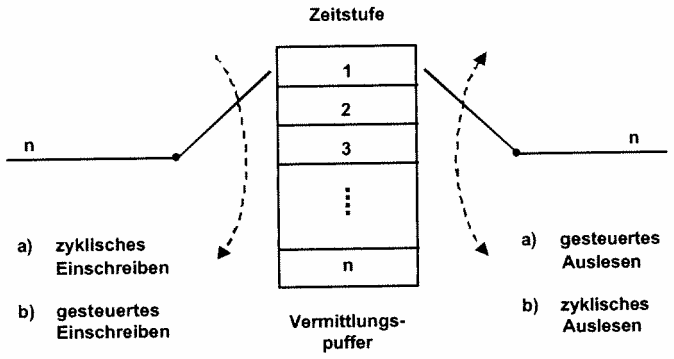


Bild: Synchrones Zeitmultiplex

Synchrone und asynchrone Vermittlung

Für den asynchronen Betrieb mit Paketvermittlung ist eine kurze Zwischenpufferung am Eingang und Ausgang erforderlich zur Geschwindigkeitsanpassung und kurzzeitige Konfliktauflösung. Der statische Multiplexer am Eingang multiplext alle eintreffenden Pakete (Zellen) und schreibt sie nacheinander in den Vermittlungspuffer.

Ausgangsseitig werden dann die gepufferten Pakete (Zellen) ausgelesen und auf die entsprechende Ausgänge verteilt (demultiplext).

Pufferworte: 1 Paket (1 Zelle)
Bottleneck: Pufferbandbreite

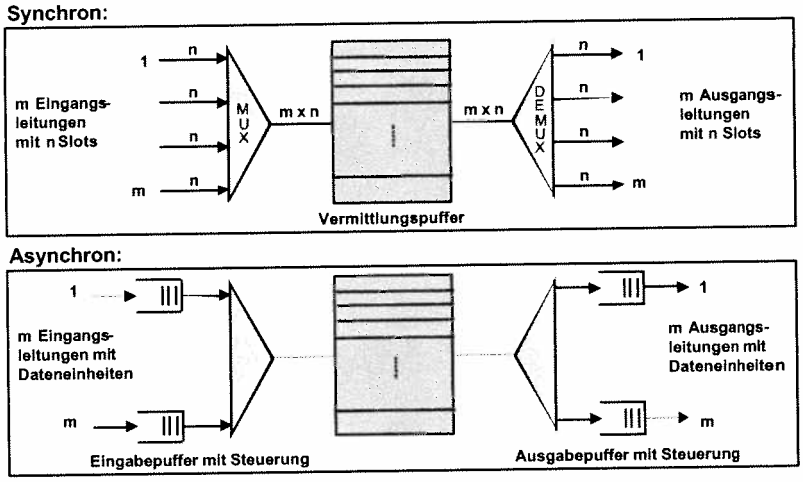


Bild: Synchrone und asynchrone Vermittlung

Asynchrone Koppelnetze basieren auf einer getakteten Struktur. Dies bedeutet, intern werden Datenblöcke konstanter Länge vermittelt. Dazu werden Pakete mit variabler Länge am Eingang zerlegt. Die Zerlegung fängt mit dem Header an und danach folgt den Payloadteil. Im Bild ist die Richtungsdarstellung gezeichnet worden. Zur Lenkung fängt jeder Datenblock mit einer internen Zusatzinformation an, so dass die einzelnen Datenblöcke sich selbständig durch das Koppelnetz lenken können. Am Ausgang werden alle Datenblöcke gesammelt und das Paket wieder zusammengesetzt. Je nach Koppelnetz kann die Reihefolge der Datenblöcke sich ändern und muss sortiert werden. Bei ATM-Zellen ist lediglich die interne Zusatzinformation notwendig.

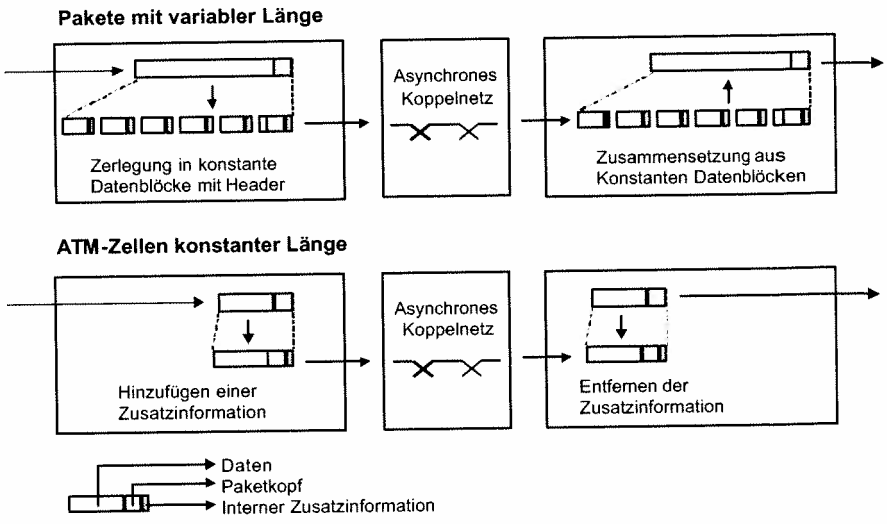


Bild: Asynchrone Vermittlung

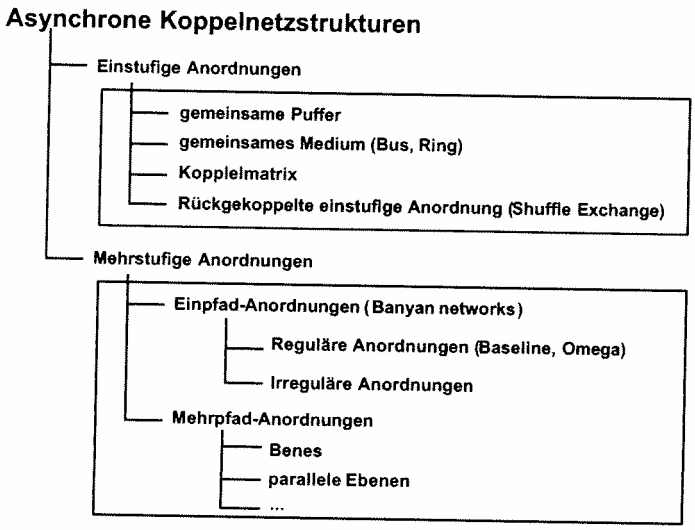


Bild: Strukturen von asynchronen Koppelnetzen

Asynchrone Koppelnetze bilden den Kern aller Paketvermittlungsknoten, ATM-Knoten, Ethernet Switches und Router. Die Klassifizierung der asynchrone Koppelnetze erfolgt nach unterschiedlichen Kriterien:

- Koppelnetzstruktur.
- Anzahl der Vermittlungsstufen.
- Zwischenleitungsführung.
- Struktur der Koppelnetz-Elemente.
- Pufferung.
- Pufferung am Eingang oder Ausgang.
- Pufferung im Innern der Koppelanordnung.
- Konfliktauflösung (Rückstau, Überholen, ...).

Unterschieden wird zuerst mal nach einstufige oder mehrstufige Anordnung. Bei einstufigen Koppelnetzen gibt es den einfachen Schaltmatrix, ein gemeinsames Medium (Bus, Ring) und die einstufige Anordnung mit Rückkopplungen bis den gewünschten erreicht wird. Bei mehrstufigen Anordnungen unterscheidet man Einpfad- und Mehrpfad-Anordnungen. Bei letzteren führen mehrere Pfade zum Zielausgang. Bei den Einpfad-Koppelnetze (Banyan-Koppelnetze) sind zwischen regulären und irregulären Strukturen.

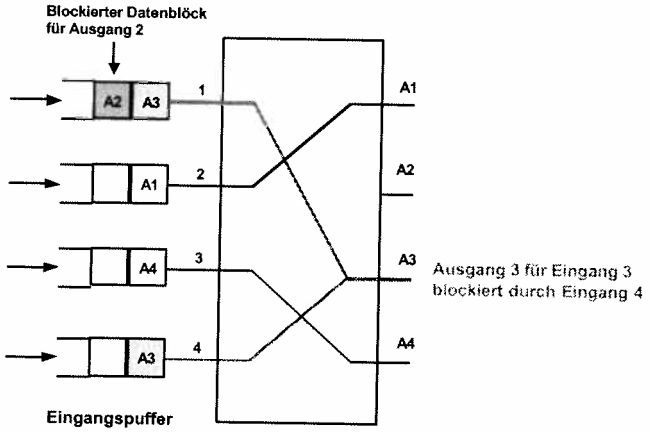


Bild: Head-of-the-Line Blockierung

Head-of-the-Line (HOL) Blockierung

Ein wichtiger Grund für eine verkehrsabhängige Leistungseinbusse von Vermittlungsknoten, Switches und Routern ist die HOL-Blockierung. Dies passiert, wenn

- Pakete von mehreren Eingängen für den selben Ausgang bestimmt sind.
- der gewünschte Ausgang durch eine temporäre Überlastung nicht zum Übertragung zur Verfügung steht.

Im Bild sind die Datenblöcke am Eingänge 1 für Ausgang A3 durch Datenblöcke von Eingang 4 zum selben Ausgang A3 blockiert. Dadurch ist am Eingang 1 auch der Datenblock für Ausgang A2 blockiert.

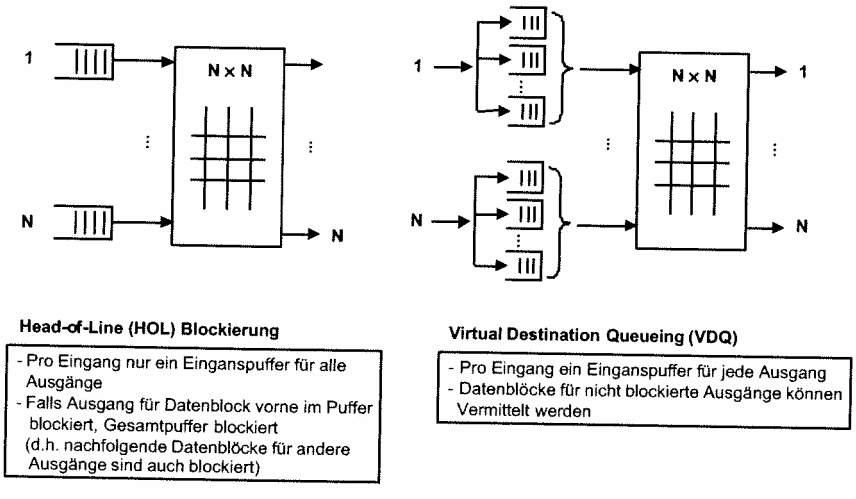


Bild: Vermeidung der Head-of-the-Line (HOL) Blockierung

Virtual Destination Queueing (VDQ)

HOL Blockierung kann vermieden werden, wenn am jeden Eingang die Pakete in einen Puffer für jeden Ausgang eingereiht werden.

Als einzige Möglichkeit zur Erweiterung der Crossbar mit Ausgangspuffer-Architektur ergibt sich logischerweise die Integration von mehreren parallelen Eingangspuffern. Die empfangenen Pakete werden über einen internen Mechanismus in jeweils einen Puffer des Ports gepuffert. Über eine zusätzliche Kontrollogik würde der Switch die einzelnen Datenpakete zur Übermittlung über die Cross-Matrix priorisieren.

Diese Architektur würde zwar unter Performance-Gesichtspunkten das Maximum leisten, wäre jedoch aufgrund der Komplexität der Hardware und der Software zu teuer in der Entwicklung. Dies würde bedeuten, dass Produkte, die auf dieser Architektur basieren würden, nicht im Markt konkurrenzfähig sind.

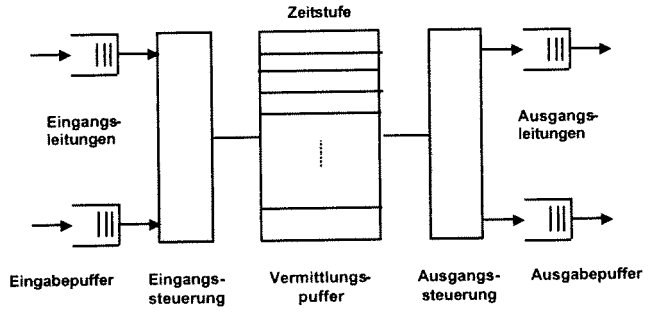


Bild: Gemeinsame Puffer

Bei Verwendung einer zentralen Puffer werden Pakete aus den Eingabepuffern von der Eingangssteuerung eingeschrieben und von der Ausgangssteuerung ausgelesen und anschließend zu den Zielausgabepuffern geleitet.

Gemeinsames Medium mit getakteter Struktur

Koppelanordnungen beschränkter Größe können auf dem Prinzip eines gemeinsamen Mediums (shared media) aufgebaut werden, und zwar sowohl für synchrones Zeitmultiplex (Durchschaltevermittlung) als auch für asynchrones Zeitmultiplex (Paket-, Zellenvermittlung). Je nach Ausdehnung des gemeinsamen Mediums handelt es sich um eine zentral gesteuerte Vermittlung oder um eine verteilte Vermittlung in Form eines lokalen Netzes (Local Area Network, LAN) als Bus oder senr selten als Ring.

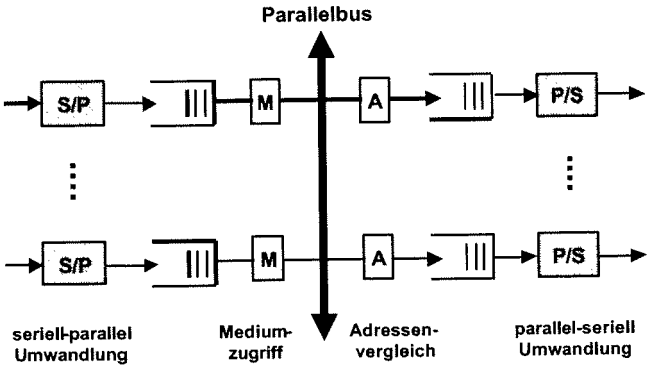


Bild: Gemeinsames Medium (Shared Medium)

Gemeinsam ist für Beide, dass die beschränkte Kapazität des gemeinsamen Mediums über ein **Vielfachzugriffsverfahren** verwaltet bzw. zugeteilt werden muss. Die getaktete bus- oder ringbasierte Technik ermöglicht eine **variable** Zuordnung und damit gleichzeitig auch die Möglichkeit, Kapazitäten in variabler, bedarfsangepasster Weise bereitzustellen. Neben reinen Bus- oder Ringsystemen können zur Kapazitätssteigerung auch Doppelbus- oder Doppelringsysteme eingesetzt werden. Das Vermittlungsprinzip basiert auf der Zuteilung periodischer Zeitschlitze (Zeitkanal bei Durchschaltevermittlung) bzw. aperiodischer Zeitschlitze für die Dauer einer Paket- oder Zellenübertragung (Paketvermittlung).

Busvergabe über Medienzugriffsprotokolle (Vielfachzugriffsverfahren)

- zentral: zyklisch (Polling), FIFO-Arbitrierung,
- dezentral: ALOHA, CSMA, CSMA/CD, Token-Bus, ...
- Vermittlung durch Adressenvergleich und kopieren im Falle des positiven Vergleiches Paketadresse-Stationsadresse

Getakteter Ring (Slotted Ring) mit fester Zuteilung der Zeitschlitze

- Erzeugung der Zeitschlitzstruktur durch Ring-Master
- Synchrone Zuordnung des (der) Zeitschlitze beim Verbindungsaufbau durch Ring-Master
- Übertragung in Hinrichtung in festgelegtem Zeitschlitz bei Port A
- Entnahme bei Port B
- Bei Vollduplexbetrieb kann derselbe Zeitschlitz für die Rückrichtung benutzt werden

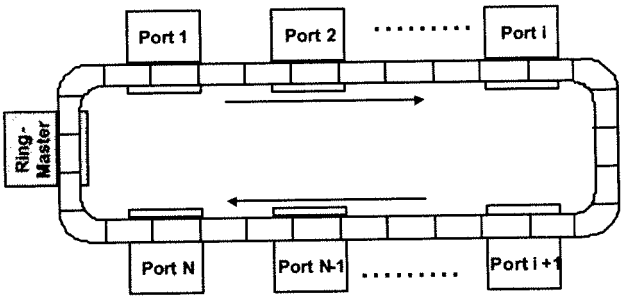


Bild: Getakteter Ring mit Master
(Synchrones Zeitmultiplex)

Getakteter Ring (Slotted Ring) mit dem ATMR-Zugriffsmechanismus

Die Medienzugriffskontrolle nach dem Prinzip des ATM-Rings basiert auf einem verteilt arbeitenden Quotenverfahren und einem Reset-Mechanismus. Das Quotenverfahren übernimmt die Steuerung des quotierten Zugriffs der einzelnen Ports. Jede Port darf pro Zyklus maxi mal die durch die Quote vorgegebene Kapazität des Mediums belegen. Läuft die Quote aus, so wird ein Port inaktiv. Der letzte noch aktive Port initiiert nach Ablauf seiner eigenen Quote einen Reset, mit dem die anderen Ports aktiviert und deren Quoten erneuert werden (Reset-Mechanismus). Der Zeitraum zwischen zwei aufeinanderfolgenden Resets wird als Reset-Periode bezeichnet. Die Dauer dieser Periode ist abhängig sowohl von der Größe der Quote für jeden Port als auch von der aktuellen Lastverteilung auf dem Ring. Dieses Verfahren ist geeignet für mittelgroße Vermittlungsknoten, Switches und Router mit 50 bis 500 Ports und sehr dynamische Verkehrsflüsse. Für viele Ports und hoher Verkehrsdynamik kann ein gegenläufiger Doppelring eingesetzt werden. Die Zugriffkontrolle läuft auf beiden Ringen unabhängig ab.

Getakteter Ring (Slotted Ring) mit Zugriffsmechanismus

- Erzeugung der Zeitschlitzstruktur durch momentanen Master in einem der Ports
- Asynchrone Zuordnung der Zeitschlitze nach einem fairen Zugriffsmechanismus (z.B. ATMR-Mechanismus)

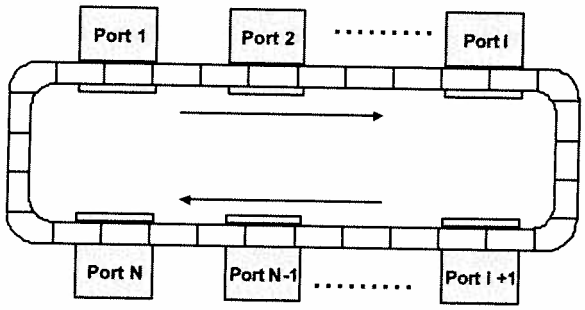


Bild: Getakteter Ring mit Zugriffsmechanismus (Asynchrones Zeitmultiplex)

Der Reset-Mechanismus

Das Ende des aktuellen Protokollzyklus kann mit einem verteilten Kontrollmechanismus wie folgt erkannt werden. Jeder noch aktive Port schreibt seine Adresse als sogenannte busy-Adresse in jeden passierenden Zeitschlitz. Inaktive Ports lassen die Zeitschlitze dagegen unverändert. Empfängt ein Port einen Zeitschlitz mit der eigenen busy-Adresse, erkennt er, dass alle anderen Ports zu dem Zeitpunkt, zu dem der Zeitschlitz sie passiert hat, inaktiv waren. Dieser Port sendet dann, sobald er selbst inaktiv wird, eine Reset-Meldung aus und geht in den sogenannten Hunting-Zustand über. Auch an Ports, die zwischenzeitlich durch die Ankunft neuer sendebereiter Daten wieder aktiv geworden sind, wird mit der Ankunft der Reset-Meldung die Quote neu initialisiert, womit diese Ports einen gewissen Kapazitätsverlust hinnehmen müssen. Andererseits kann es wegen der nicht vernachlässigbaren Ringlatenz auch vorkommen, dass mehrere Ports nahezu gleichzeitig das Ende des Protokollzyklus erkennen und ein Reset-Meldung generieren. Dieser Konflikt wird dadurch gelöst, dass ein Port im Hunting-Zustand ein bei ihr ankommende Reset-Meldung, unabhängig davon, ob es das von ihm gesendet ist, vom Ring entfernt und den Hunting-Zustand wieder verlässt.

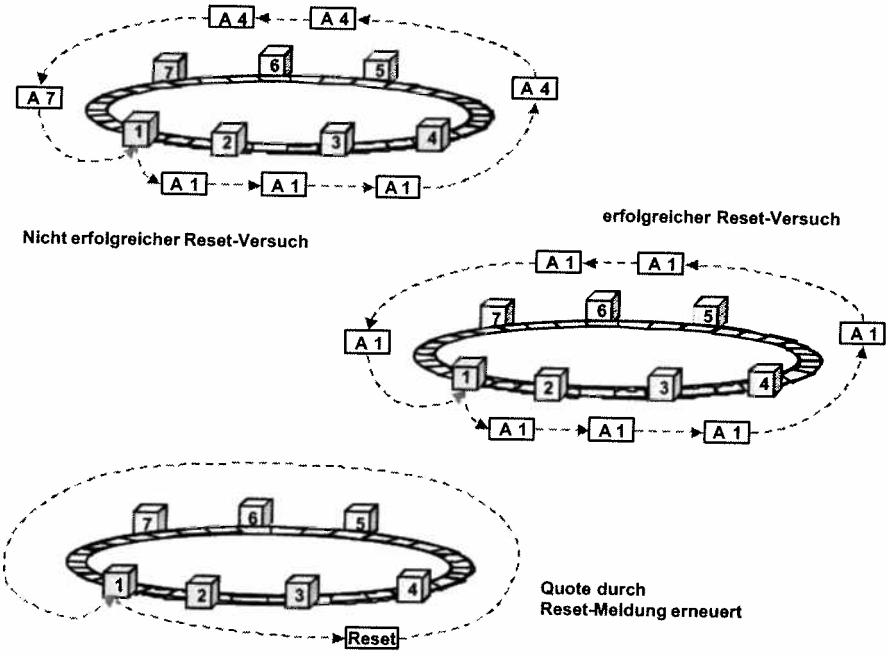


Bild: Reset Mechanismus

Dualbussystem (Slotted Bus)

- Erzeugung der Pulsrahmenstruktur auf Bus A (B) durch Slotgenerator A (B).
- Feste Reservierung von n Zeitkanälen je Port in Senderichtung bzw. variable Zuteilung einer beliebigen Anzahl von Zeitschlitzen je Port.
- Verbindungsauf-/abbau über speziellen Steuerkanal (nicht gezeigt), dabei Festlegung des benutzten Zeitschlitzes (oder mehrerer Zeitschlitze).
- Eintrag des Abtastwertes in festgelegtem Zeitschlitz beim Sender und Entnahme des Abtastwertes beim Empfänger
- Übertragung in Hin- und Rückrichtung über getrennte Busse auf (z. B.) gleichnamigen Zeitlagen.

Verkehrseinschränkung im Falle k < N.z, wobei k die Anzahl der Zeitlagen/Pulsrahmen, N die Anzahl der Ports und z die maximale Anzahl von Verbindungen pro Port.

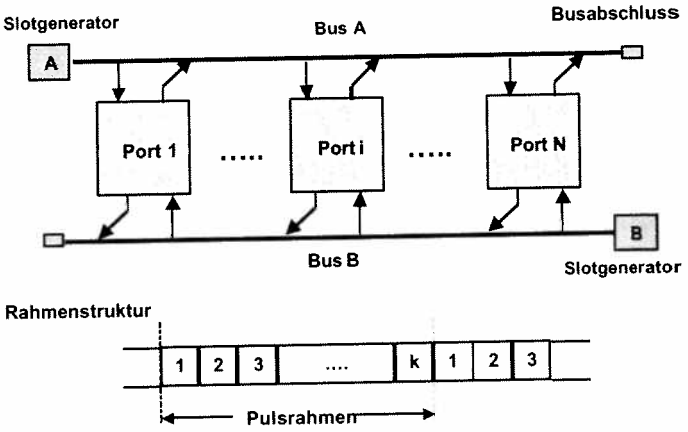


Bild: Dualbussystem (Slotted Bus)

In den meistens Vermittlungseinrichtungen werden Koppelnetze eingesetzt. Hier gibt es je nach Anzahl Ports eine Vielzahl von Möglichkeiten.

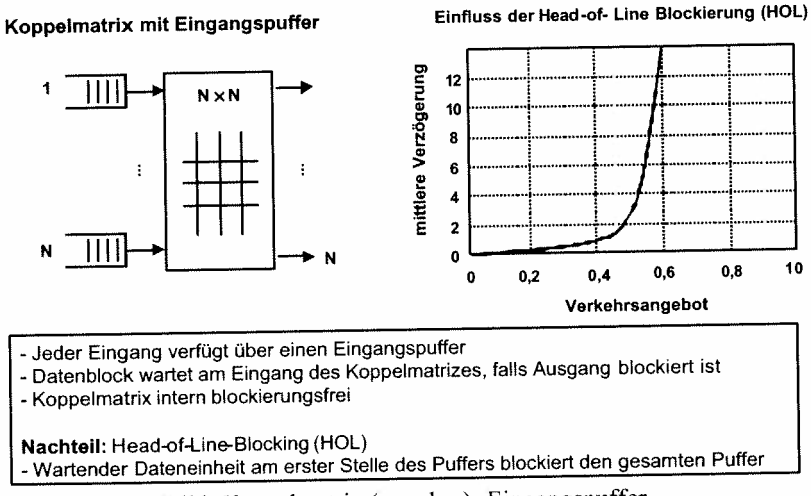


Bild: Koppelmatrix (crossbar): Eingangspuffer

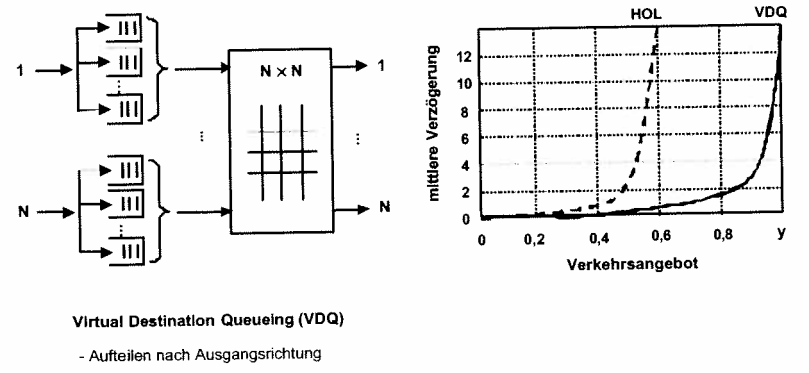


Bild: Koppelmatrix (crossbar): mehrere Eingangspuffer

Crossbar Switch mit Eingangspuffern

Bei dieser Architektur werden alle Ports des Switches über eine Koppelmatrix miteinander verbunden. Wird ein Datenblock von einem der Ports auf die Koppelmatrix gesendet, so ist der gesamte Koppelnetz oder ein Teil des Koppelnetzes belegt. Dadurch könnten während der Datenübertragung des Datenblockes keine weiteren Datenblöcke mehr von anderen Ports übermittelt werden und gehen verloren. Um dies zu vermeiden, wurde jeder Eingangsport mit Zwischenpuffern versehen. Wird auf der Koppelmatrix bereits ein Datenblock übermittelt, so werden alle neuen Datenblöcke in den Eingangspuffern zwischengelagert, bis der Koppelmatrix für die Übermittlung des nächsten Datenblockes frei wird.

Bei gering ausgelasteten Netzen werden durch den Koppelmatrix mit Inputpuffer-Architektur eine relativ geringe Verzögerungszeit zwischen den einzelnen Datenblöcken erzielt. Bei steigender Last jedoch steigt die Verzögerungszeit extrem an. Dies wird durch die Head-of-the-Line Blockierung verursacht. Die obere Grenze des Arbeitsbereichs liegt etwa bei 58 %. Steigt die Last weiter an, so erhöht sich die Datenverzögerung erheblich. Diese Leistungseinbusse kann durch Virtual Destination Queueing eliminiert werden.

Vorteile eines Crossbar mit Inputpuffer-Architektur

- relativ geringer Hardware-Aufwand
- kostengünstig
- leicht zu modifizieren
- ideal für den Einsatz in Workgroups mit einer geringen Last
- ideale Architektur für Boadcast und Multicast

Nachteile eines Crossbar mit Inputpuffer-Architektur

- ab einer Durchsatzrate von 58 % kommt es zu hohen Verzögerungen
- zum Anschluss von Segmenten nicht geeignet
- kann nicht im Voll-Duplex-Betrieb verwendet werden
- schwer skalierbar

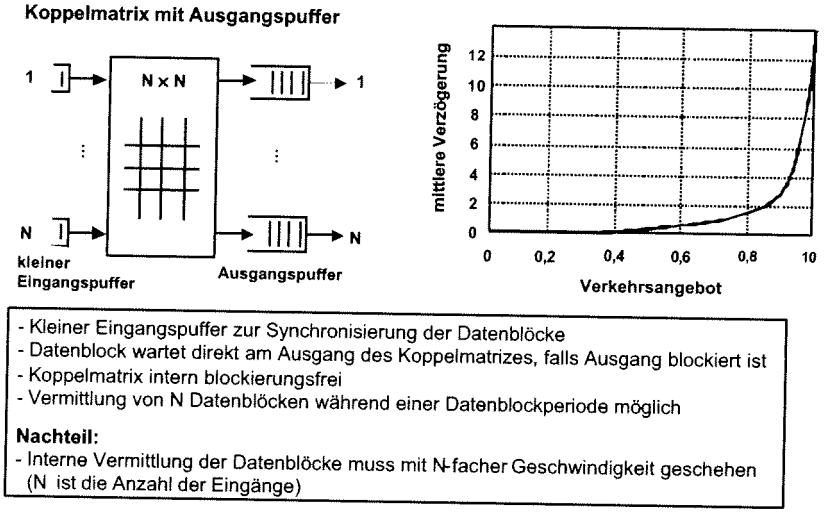


Bild: Koppelmatrix (crossbar): Ausgangspuffer

Crossbar Switch mit Ausgangspuffern

Bei dieser Architektur findet keine Eingangspufferung statt. Lediglich eine kleine Eingangspuffer zur Geschwindigkeitsanpassung ist notwendig. Da die Datenblöcke sofort vermittelt werden, kommt es bei Ausgangspufferung nicht zur HOL-Blockierung. Die Architektur verlangt jedoch, dass mit einem sehr schnellen Koppelmatrix dafür gesorgt wird, dass alle ohne Verzögerung übermittelt werden können. Erst im Ausgangpuffer werden die Datenblöcke für die weitere Übertragung auf den Ausgangsport zwischengelagert. Dies setzt voraus, dass die Ausgangspuffer relativ groß (mehrere MByte) sind und die Zugriffsmechanismen auf diesen Puffer optimiert wird.

Nur durch das direkte Zusammenspiel des Koppelnetzes mit dem optimierten Ausgangspuffer ist eine große Effektivität des Switches zu garantieren. Der große Vorteil dieser Architektur liegt darin, das auch bei steigender Netzlast und bei steigender Portzahl die Verzögerung zwischen den einzelnen Datenblöcke gleich bleibt. Die Effektivität des Switches kann in der Praxis annähernd das Durchsatzoptimum von 99,xx% erreichen.

Vorteile der Ausgangspuffer-Architektur

- leicht zu modifizieren
- ideal für Workgroups und zentralen Applikationen
- gleichbleibende Verzögerungszeiten bis zu einer Durchsatzrate von annähernd 100%
- kann auch im Voll-Duplex-Betrieb verwendet werden
- ideale Architektur für Broadcast und Multicast
- leicht skalierbar

Nachteile der Ausgangspuffer-Architektur

- relativ komplexer Hardware-Aufbau
- durch den komplexen Hardware-Aufbau steigen die Kosten
- großer Output-Puffer und ein optimiertes Puffer-Management notwendig

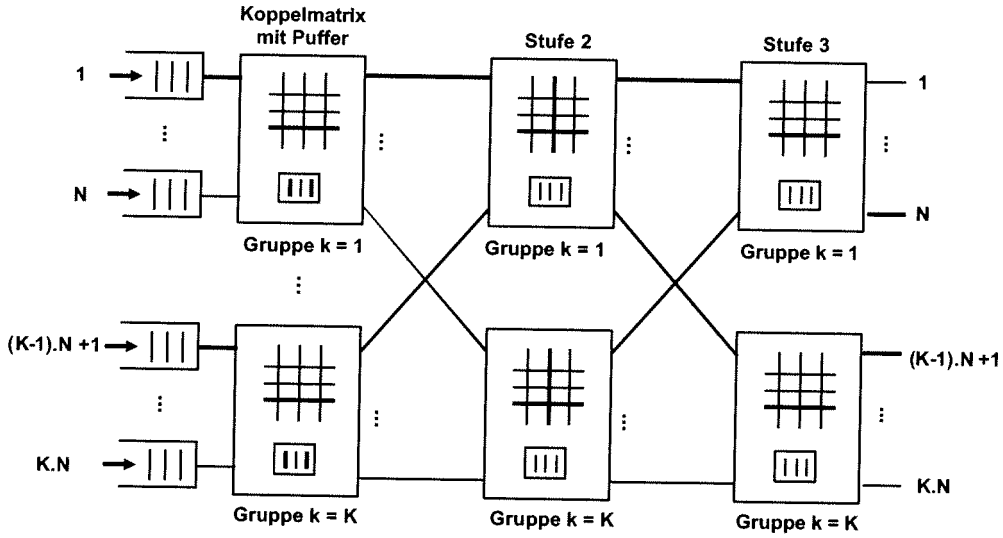


Bild: Mehrstufiges Koppelnetz mit Puffer in jedem Koppelmatrix

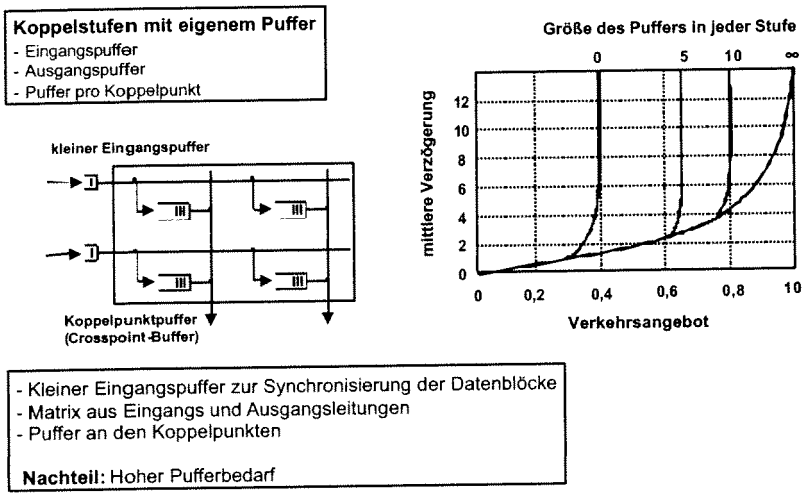


Bild: Mehrstufiges Koppelnetz: verteilter Puffer

Mehrere Koppelstufen

Bei dieser Architektur stehen einem Port oder einer Gruppe von Ports eine Reihe von Eingangspuffern mit einem separaten Koppelmatrix zur Verfügung. Wird ein Datenblock an einem Port empfangen, so wird dessen Zieladresse ermittelt. Anschließend wird der Datenblock mit Hilfe des Koppelnetzes an den Zielport weitertransportiert. Befindet sich der Empfänger an einem Port des lokalen Koppelmatrix, wird das Datenpaket direkt an den Zielport übermittelt. Befindet sich der Empfänger jedoch an einem anderen Koppelmatrix, so müssen die Datenblöcke im nächsten Schritt an das Ziel-Koppelmatrix weitergeleitet werden. Die Pufferung in den einzelnen Stufen kann verschieden organisiert werden: Eingangspuffer, Ausgangspuffer, kombiniert oder auch Puffer pro Koppelpunkt.

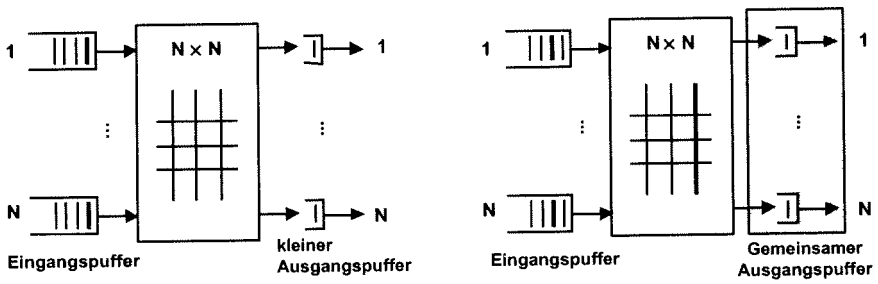
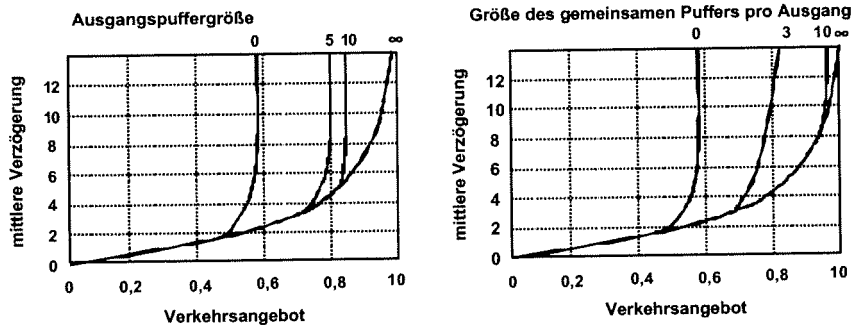


Bild: getrennte oder gemeinsame Ausgangspuffer

Koppelmatrix mit Eingangs- und kleinen Ausgangspuffern

Bei der Eingangspuffer-Architektur kann der Durchsatz eines Koppelnetzes durch die Verwendung von kleinen Ausgangspuffern wesentlich gesteigert werden.
Die einzelnen parallelen Ausgangspuffer können auch durch einen gemeinsamen Ausgangspuffer-Pool ersetzt werden.



Kleinerer Pufferbedarf bei gemeinsamem Ausgangspuffer

Grund: Ausgänge mit niedrigeren Auslastung können Ausgänge mit hohem Last mit Pufferplatz aushelfen

Nachteil: Ein blockierter Ausgang kann mit ihren gepufferten Datenblöcken den Datenfluss zu den anderen Ausgängen beeinträchtigen

Durch den gemeinsamen Ausgangspuffer wird der Effekt des Head-of-the-Line Blockierens nur minimal reduziert. Bei steigendem Datenverkehr und bei der Zunahme von Stationen erhöhen sich die Verzögerungszeiten in beiden Fällen drastisch.

Ein gemeinsamer Ausgangspuffer reduziert den Pufferbedarf am Ausgang.

Grund: Ausgänge mit niedrigeren Auslastung können Ausgänge mit hohem Last mit Pufferplatz aushelfen

Nachteil: Ein blockierter Ausgang kann mit ihren gepufferten Datenblöcken den Datenfluss zu den anderen Ausgängen beeinträchtigen

Rückgekoppelte Einstufige Anordnung (Shuffle Exchange)

- eine einstufige Vermittlungsanordnung aus elementaren Koppelelementen (z. B. 2 x 2) mit Zwischenpuffern
- eine spezielle Zwischenleitungsanordnung, durch welche die Eingänge auf die Koppelelement-Eingänge aufgeteilt werden (Permutation)
- Rückkopplung für mehrmaliges Durchlaufen eines Datenblocks durch die einstufige Koppelanordnung

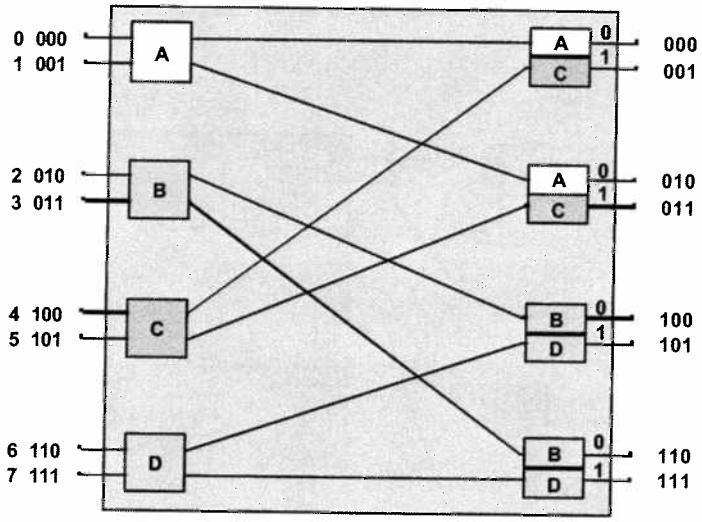


Bild: 8 x 8 Shuffle Koppelnetzstufe

- 2 x 2 - Koppelelemente
- Durchschaltung des Datenblockes von einem Eingang zum oberen (unteren) Ausgang; je nach Wegeinformation 0 (1)
- duale Codierung der Eingänge (Ausgänge); 0 ... 7 durch 000 ... 111
- Vermittlung entsprechend der mitgeführten Zieladresse (Ausgang) durch 3-maliges Durchlaufen der einstufigen Anordnung
- es existiert genau ein Pfad zwischen jedem Paar Eingang-Ausgang
- eine kürzere Durchlaufzeit ist möglich, wenn der Ausgang schon vorher erreicht wird (dann ist aber die Auswertung der ganzen Information erforderlich)

Beispiel:

Datenblocktransfer von Eingang E6 auf Ausgang A3
Der Routing Code ist (011)
1. Durchlauf (0): von E 6 auf A 4
2. Durchlauf (1): von E 4 auf A1
3. Durchlauf (1): E 1 auf A 3

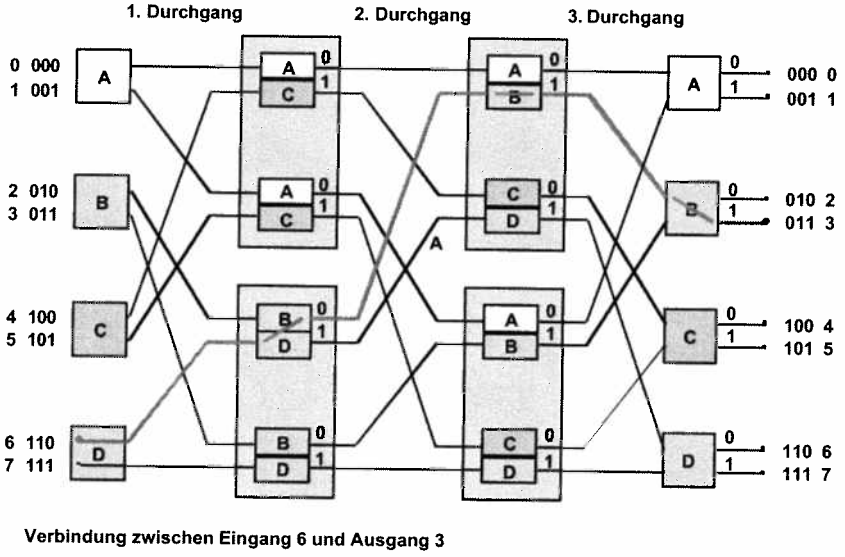


Bild: Binäre Vermittlung (Räumliche Darstellung von 3 Durchläufen im einstufigen Shuffle Koppelnetzstufe

Räumliche Darstellung der zeitlich nacheinander erfolgenden Durchschaltungen:

- Beispiel-Verbindung zwischen Eingang 6 und Ausgang 3
- Merkmal: Anwendung des Codebaum-Prinzips von jedem Eingang aus

Mehrstufige Anordnungen

a) Einpfad-Anordnungen

- Mehrstufige Anordnung mit einer Zwischenleitungsführung wie bei Shuffle Exchange Netzen
- Gleiches Schema der Durchschaltung räumlich wie bei der Shuffle Exchange zeitlich
- Rekursiver Aufbau der Struktur eines N-stufigen Netzes aus zwei (N-1)-stufigen Netzen durch Vorschalten einer weiteren Stufe mit kanonischer Zwischenleitungsführung
- Erweiterbarkeit entsprechend des Ausbaubedarfs
- Bei der Omega-Stuktur verwendet man zwei Shuffles in Serie.
- Der Baseline-Struktur verwendet eine Shuffle-Stufe und anschließend eine Auskreuzungsstufe.

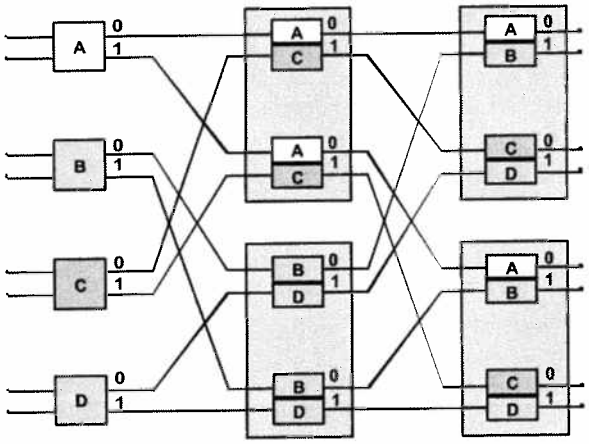


Bild: Omega-Koppelnetze

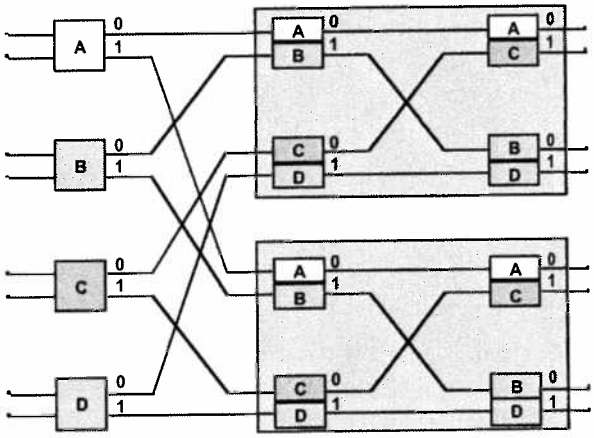


Bild: Baseline Koppelnetze

b) Mehrpfad-Anordnungen

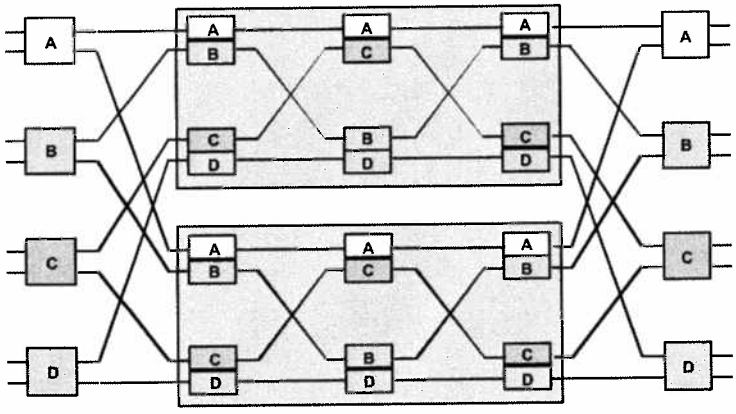


Bild: Benes- Koppelnetze

- rekursive Definition der Struktur mit N Eingängen und N Ausgängen durch Vor- und Nachschalten von je einer weiteren Stufe zu zwei Benes-Netzen mit je N/2 Eingängen bzw. Ausgängen und kanonischer Zwischenleitungsführung
- Koppelnetz ist nur bedingt blockierungsfrei, d.h. es kann durch Umordnung bestehender Verbindungen Blockierungsfreiheit erzielt werden.

Prinzip der rekursiven Definition der Struktur von Benes-Netzen:

- Aufbau aus 2 x 2 –Koppelelementen für Koppelnetze mit N Eingängen und N Ausgängen durch N/2 Koppelelemente je Stufe und 2 ld (N-1) Stufen.

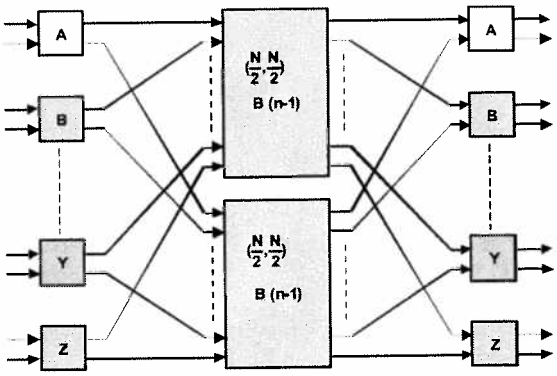


Bild: Struktur von Benes-Netzen

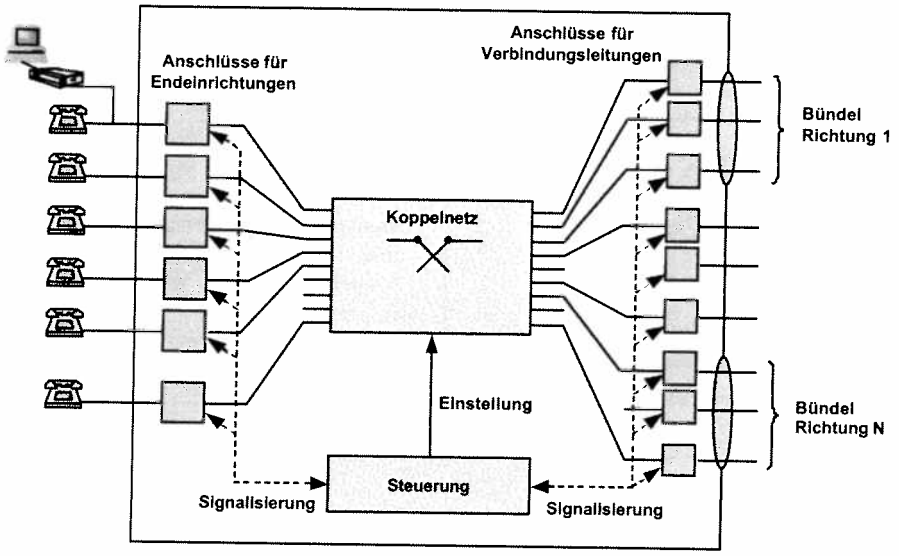


Bild: Teilnehmer-Vermittlungsknoten

Eine Vermittlungsknoten besteht im allgemeinem aus

- Teilnehmeranschlussmodulen,
- Leitungsanschlussmodulen,
- Koppelnetz,
- Steuerung.

Durch die Signalisierung zwischen den Anschlussmodulen und der Steuerung werden die Verbindungen im Koppelnetz durchgeschaltet.

Alle Glasfaser zu und von einem Nachbar-Vermittlungsknoten werden als Leitungsbündel bezeichnet. Diese Glasfaser liegen in einem oder mehreren Übertragungskabeln..

Datenverbindungen mit Modems werden über die 64 kbit/s Sprachekanäle des synchronen Koppelnetzes geführt. Internetverbindungen werden in den Teilnehmeranschlussmodulen ausgeschieden und über asynchrone Koppelnetze geleitet.

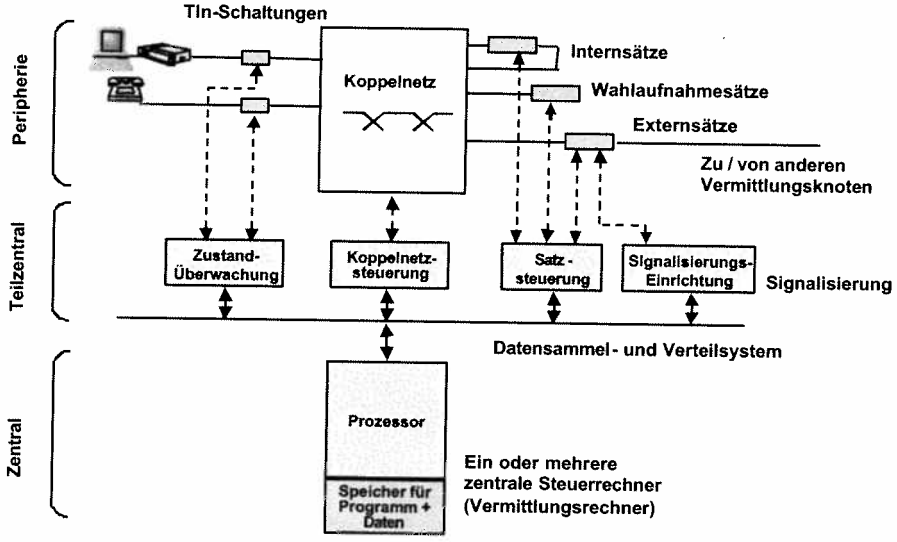
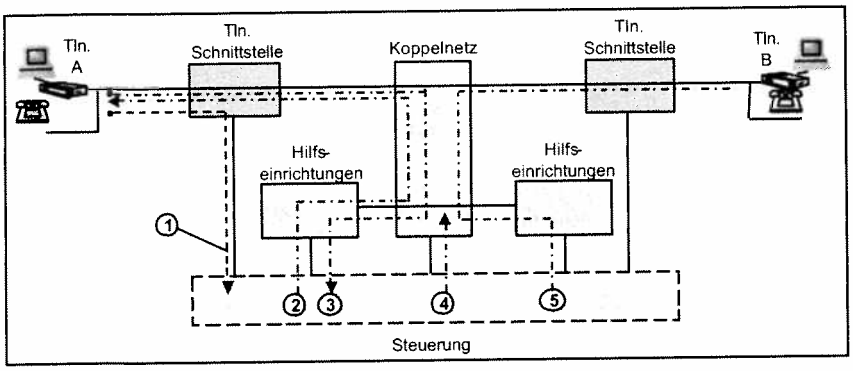


Bild: Grundstruktur von Vermittlungsknoten

Periphere Ebene
Sie enthält das Koppelnetz und die peripheren Einheiten. Teilnehmer sind über Teilnehmereinheiten (TS) an das Koppelnetz angeschlossen. Intern/Extern Sätze übernehmen während einer Verbindung die Speisung und Überwachung der Teilnehmer-Verbindung. Der Wahlaufnahmesatz dient zum Erkennen und Aufnehmen der Wählziffern.

Teilzentrale Ebene
Hier sind Steuerungsbaugruppen angesiedelt. Die Baugruppen können für die Teilnehmer-Sätze (Anrufidentifizierung und Zustandsüberwachung) oder für das Koppelnetz (Koppelnetzsteuerung) oder für die Intern-, Extern-, Wahlaufnahmesätze (Einheitsteuerung) zuständig sein. Ebenfalls in dieser Ebene angesiedelt sind Einrichtungen zur Signalisierung mit anderen Vermittlungsstellen.

Zentrale Ebene
Sie umfasst den bzw. die Vermittlungsrechner, bestehend aus Prozessor und Speicher für Software und Daten.



① Feststellung des Verbindungswunsches und Identifizierung des A-Teilnehmers
② Wahlaufforderung
③ Empfang und Auswertung der Wählinformation
④ Wegesuche; Einstellen des Koppelnetzes für Verbindung A – B
⑤ Anschalten das Ruftons zum B-Teilnehmer

Bild: Verbindungsaufbau

Eine erfolgreiche Verbindung besteht prinzipiell aus drei Phasen: der Verbindungsaufbauphase, der Gesprächsphase und der Auslösungsphase. Die Steuerung sowie die Vermittlungseinrichtungen werden während der Verbindungsaufbauphase am intensivsten beansprucht. Am Beispiel des Aufbaus einer internen Verbindung, d.h. beide Teilnehmer sind an dieselbe Vermittlungsstelle angeschlossen, werden einige Grundaufgaben eines Vermittlungssystems in 5 Steuerungsschritten dargestellt.

Steuerungsprinzipien und Architektur

Klassifizierung der strukturellen Merkmale sowie Organisationsprinzipien der Steuerung:

Steuerung	konzentriert - verteilt
Hardware-Struktur	zentral – dezentral - teilzentral
Software -Struktur	nicht-modular - modular

Man findet in einem System mit zentraler Struktur häufig das konzentrierte Steuerungsprinzip, während das in modernen Vermittlungssystemen oft angewendete Prinzip der verteilten Steuerung eine dezentrale bzw. gemischt zentral/dezentrale Systemstruktur voraussetzt.

Zentrale Struktur mit konzentrierter Steuerung

Bei dieser Steuerung konzentrieren sich alle vermittlungstechnischen Funktionen in einer Steuerungseinheit, die aus einem oder mehreren gleichartigen Rechnern besteht. In dieser zentralen Steuerungseinheit befinden sich alle Programme, die für die Verbindungssteuerung benötigt werden, sowie die Zustandsspeicherung des gesamten Systems, d.h. ein komplettes Abbild der aktuellen Zustände von Teilnehmern, Verbindungsleitungen, dem Koppelnetz und der systemeigenen peripheren Einrichtungen.

Diese Steuerungsart erfordert eine große Speicher- und Rechenkapazität sowie eine hohe Zuverlässigkeit des Steuerrechners, welcher aus Sicherheitsgründen in der Regel gedoppelt wird. Die Leistungsfähigkeit des Systems wird durch die Kapazität der Steuereinheit bestimmt, die für eine Überlast-Betrachtung den Engpass des Systems bildet. Die zentrale Steuereinheit muss in der Regel für den Endausbau des Vermittlungssystems dimensioniert werden. Die zentrale Systemstruktur verursacht, bedingt durch die Konzentration der gesamten Intelligenz des Systems, einen intensiven Steuerdatentransport zwischen der peripheren Ebene und der zentralen Steuereinheit. Diese Aufgabe erfordert einen leistungsfähigen Ein/Ausgabe-mechanismus für vermittlungs-technische Signale und Befehle.

Das Bild zeigt eine übliche Realisierung des Steuerdatentransfers, indem alle Steuersignale durch ein Bussystem von der Peripherie zur Steuerung und umgekehrt transportiert werden.

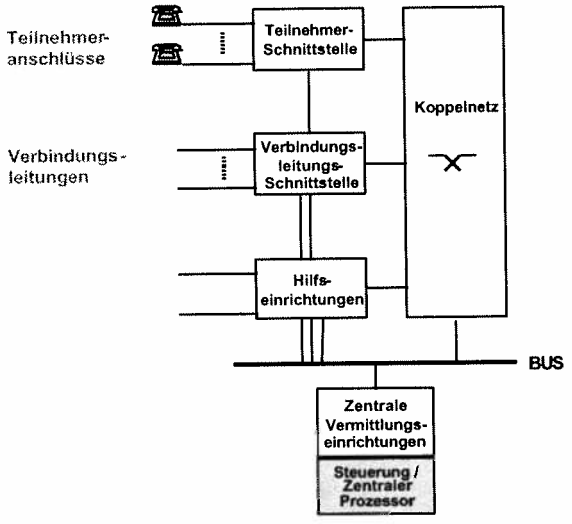


Bild: Zentraler Vermittlungsknoten

Dezentrale Struktur mit verteilter Steuerung

Die technologischen Fortschritte, insbesondere die Entwicklung von Mikrorechnern und schnellen Speichern in der Hardware und die Verfügbarkeit von Entwicklungs- und Beschreibungsmethoden in der Software, ermöglichen eine wirtschaftliche Verlagerung der Intelligenz in die periphere Systemebene. Die Systemfunktionen werden auf mehrere Steuereinheiten verteilt, wobei jede Steuereinheit (Rechner) ausschließlich für ein Modul zuständig ist, z. B. Teilnehmer- oder Verbindungsleitungsschnittstelle, usw.

Die Module können wegen ihrer autonomen Steuerung beim Ausbau der Vermittlungsstelle nach Bedarf hinzugefugt werden. Dadurch werden die Realisierung und die Anpassung verschiedener neuer Dienste oder Signalisierungssysteme erleichtert. Bei der Erweiterung eines Teilsystems wird der Normalbetrieb des vorhandenen Systems nicht wesentlich beeinflusst. Überdies bietet die verteilte Steuerung eine erhöhte Ausfallsicherheit und eine verringerte Wirkbreite von Störungen. Man findet bei der dezentralen Systemstruktur häufig eine Mischung zwischen Funktions- und Lastteilungsprinzipien. Die Vermittlungsfunktionen werden je nach Aufgabe auf die dezentralen Module verteilt (Funktionsteilung). Einige wichtige Vermittlungsfunktionen (z. B. Verbindungssteuerung) werden von mehreren Steuereinheiten übernommen, die nach dem Lastteilungsprinzip operieren.

Da die dezentralen Steuereinheiten autonome Datenbereiche besitzen und keine Steuereinheit das gesamte Abbild der Systemperipherie in seinem Speicherbereich enthält, muss eine funktionsfähige Interprozessorkommunikation für den Datenaustausch gewährleistet werden.

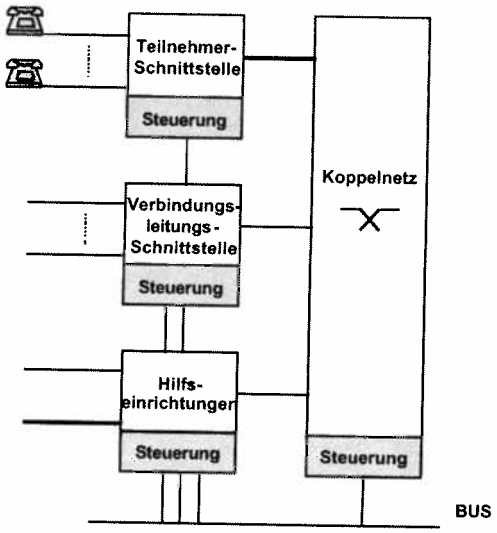


Bild: Dezentraler Vermittlungsknoten

Gemischt zentral/dezentrale Struktur mit verteilter Steuerung

Diese Struktur findet Anwendung in den meisten rechnergesteuerten Vermittlungssystemen. Ein Teil der Systemintelligenz wird hier in die periphere Ebene verlagert. Es handelt sich hierbei um vermittlungstechnische Funktionen, die ohne großen Kommunikationsaufwand mit der zentralen Steuereinheit extern verarbeitet werden können. Beispiele hierfür sind das Abtasten von Teilnehmern und von Verbindungsleitungen, der Ziffernempfang und die Überwachung des Wahlvorganges, die Ablaufsteuerung der Ein/Ausgabe von Steuersignalen.

Eine Variante dieser Systemarchitektur ist eine Systemkonfiguration mit dezentraler Hardware-Struktur, bei der eine hierarchische Steuerungsstruktur realisiert ist. Während einige Steuereinheiten bestimmten Teilnehmergruppen, Verbindungsleitungen oder Hilfseinrichtungen fest zugeordnet sind, übernehmen andere Steuereinheiten bzw. Rechner einer höheren Steuerebene die zentralen Vermittlungsfunktionen (z. B. Signalisierung, Verbindungssteuerung, ...). Abhängig von der Intensität des Steuerdatenverkehrs wird die Kommunikation zwischen den Steuereinheiten organisiert. Sie kann entweder über das Koppelnetz mittels fest zugeordneter bzw. vermittelter Kanäle erfolgen oder, wie in Bild dargestellt, mit einem Bussystem realisiert werden.

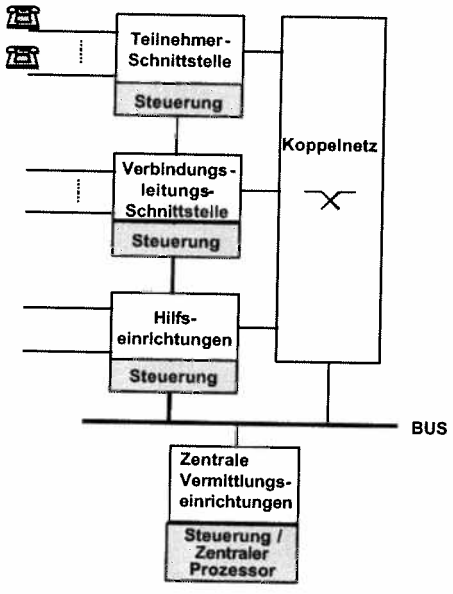


Bild: Teilzentraler Vermittlungsknoten

Interprozessor- und Interprozess-Kommunikation
Aufgrund der Aufteilung von Vermittlungsfunktionen in autonome Module, die sowohl in der Software als auch in der Hardware moderner Vermittlungssysteme realisiert wird, erhöht sich der Steuerungsaufwand für den Austausch von vermittlungstechnischen Signalen zwischen Steuereinheiten und zwischen autonomen Software-Modulen innerhalb einer Steuereinheit.

Hardware-Modularisierung und Interprozessor-Kommunikation
In Vermittlungssystemen mit dezentraler oder gemischt zentral/dezentraler Struktur, in denen die Systemintelligenz in mehrere Steuerungseinheiten bzw. Rechner aufgeteilt wird, gewinnt die Interprozessor-Kommunikation eine zentrale Bedeutung bei der Beurteilung der Leistungsfähigkeit des Systems.

Autonomes Bussystem
Der Steuerdatenaustausch erfolgt hier über einen Steuerdatenbus, auf den von allen Steuerungseinheiten gemäß eines Protokolls zugegriffen werden kann. Während bei der dezentralen Struktur mit verteilter Steuerung i.a. alle angeschlossenen Hardware-Module den Steuerdatenbus gleichberechtigt aktivieren können, wird bei der gemischt zentral/dezentralen Struktur der Bus häufig von einer zentralisierten Bus-Steuereinheit aus gesteuert (z. B. dem Ein/Ausgabe-Steuerwerk), die den Ablauf des Steuerdatenaustausches zwischen der zentralen Steuerungseinheit und den peripheren Rechnern kontrolliert.

Koppelnetz
Der Steuerdatenaustausch zwischen Steuerungseinheiten geschieht hier über festgeschaltete oder aufgebaute Wege im Koppelnetz. Dieses Prinzip wird bei den dezentralen Strukturen oft angewendet. Abhängig von der Rate der auszutauschenden vermittlungstechnischen Steuerdaten bzw. der Signale zwischen zwei Steuereinheiten werden Wege entweder semipermanent zugeteilt oder nach Bedarf über das Koppelnetz aufgebaut

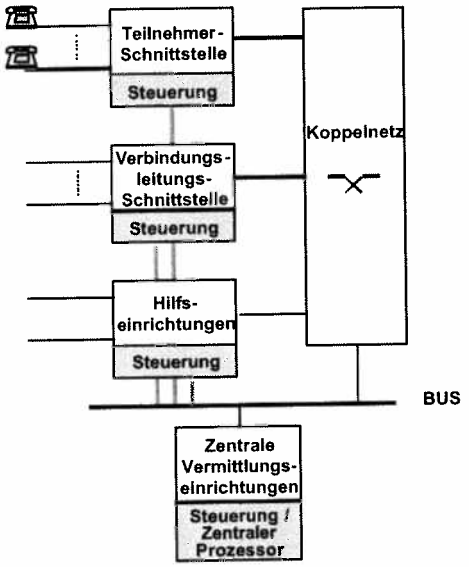


Bild: Interne Kommunikation via Bussystem

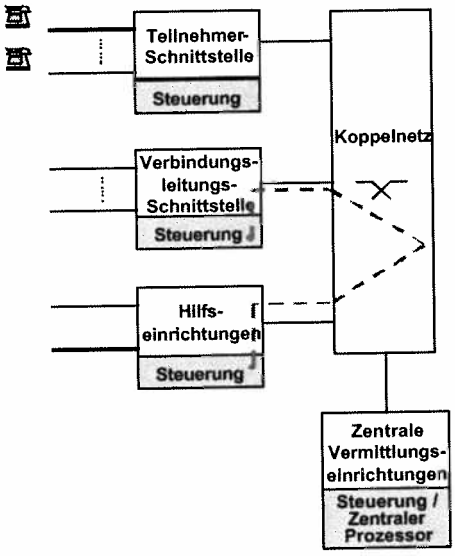


Bild: Interne Kommunikation via Koppelnetz

Für einen sinnvollen Einsatz der Vermittlungsrechner benötigt man mehrere solche teilzentrale Geräte, die nacheinander vom Rechner bedient werden. Sie sind heute vielfach über ein dupliziertes Bussystem, den Zentralbus, mit den Rechnern der Zentralsteuerung verbunden. Da Geräte im teilzentralen Bereich für eine Vielzahl peripherer Steuermaßnahmen verantwortlich sind, ergeben Ausfälle dieser Einrichtungen Störungen mit relativ großer Wirkungsbreite. Es ist daher notwendig, auch auf dieser Ebene Ersatzschaltestrategien anzuwenden.

	n + 1 Redundanz	**Duplizierung**	
Voraussetzungen	Busstruktur an Ein- und Ausgang mehrere gleiche nicht spezialisierte Geräte	keine	
		Feste Zuordnung	Konfigurationsverschränkung
		zum Zentralbus	zwischen teilzentralen Geräten und Zentralbus

Die Programme, die aus der Universalsteuerung eine speziell auf die Aufgaben zugeschnittene Einheit bilden, können bei Bedarf über das zentrale Bussystem geladen werden

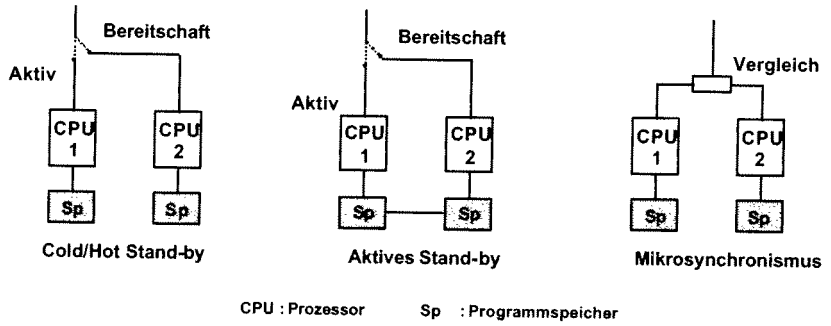


Bild: Erhöhung der Betriebsverfügbarkeit

Um die von Vermittlungssystemen geforderte hohe Verfügbarkeit zu erreichen (**ca. 99.9992% oder 2h Totalausfall in 30 Jahren**), sind besondere Maßnahmen zu treffen.

Sicherheitserhöhende Strukturen und Betriebsweisen

Es sind sogenannte Ausfalleinheiten zu definieren, die im Fehlerfalle von Wartungspersonal ausgetauscht werden. Diese Einheiten dürfen dann nur unwesentliche Aufgaben wahrnehmen oder nur für eine geringe Zahl von Teilnehmern zuständig sein. (z.B. bestimmte Speicherbereiche).

Für alle anderen Einheiten der zentralen Ebene müssen für den Fehlerfall im System Reserveeinheiten vorhanden sein. Hierbei wird unterschieden zwischen der Duplizierung und der n+1 Redundanz. Bei der Duplizierung steht für jedes Gerät ein Reservegerät zur Verfügung. Bei der n+1 Redundanz ist für eine Reihe gleichartiger Geräte (bei Prozessoren mit mindestens der gleichen Hardware) eine Reserveeinheit vorhanden.

Für beide Betriebsarten können die folgenden Ersatzschaltestrategien angewendet werden.

Cold Standby

Der Bereitschaftsrechner (Reserverechner) ist nicht in Betrieb und wird dann ein- und angeschaltet, wenn ein Fehler des online Rechners auftritt. Sein Speicher muss dann aktualisiert werden, was einen hohen Zeitaufwand erfordert. Die Fehlererkennung muss aufgrund von zusätzlicher Hardware und mit Hilfe von Fehlererkennungs- und Prüfprogrammen im aktiven Rechner erfolgen.

Hot Standby

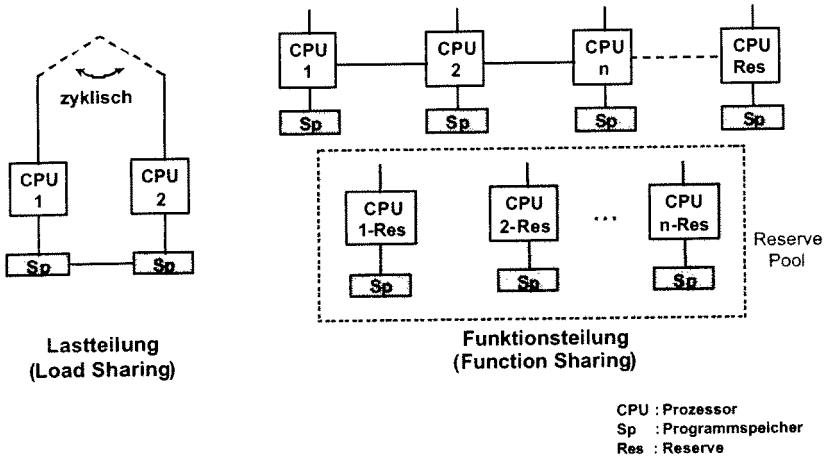
Der wesentliche Unterschied zu cold standby ist, dass der Bereitschaftsrechner in Betrieb ist. Es werden entweder keine Programme bearbeitet, oder aber Prüfprogramme, welche die Bereitschaft zur Übernahme des Vermittlungsbetriebs anzeigen, sog. Selbstdiagnoseprogramme. Bevor im Ersatzschaltefall der Betrieb durch den standby Rechner übernommen werden kann, muss ebenfalls der Speicherinhalt aktualisiert werden.

Active Standby

Eine Weiterentwicklung des hot standby ist die Betriebsart active standby. Hierbei ist der standby Rechner über das Speicherleitsystem mit dem aktiven Rechner verbunden. Der aktive Rechner schreibt in beide Speicher aktuelle Daten ein, so dass im Umschaltefall das Aktualisieren des Speichers entfallen kann. Es ist sowohl die Möglichkeit zur Selbstdiagnose als auch zur gegenseitigen Überprüfung der beiden Rechner möglich.

Mikrosynchronismus

In diesem Fall sind beide Rechner in Betrieb. Beide Rechner haben denselben Speicherinhalt, der deshalb immer aktuell ist. Beide Rechner bearbeiten dieselben Eingabeinformationen, aber nur ein Rechner gibt Steuerbefehle an die peripheren Einheiten ab. Die von beiden Rechnern generierten Ausgabeinformationen werden in einer hochzuverlässigen Logik verglichen, die bei unterschiedlichen Ausgabeinformationen der beiden Rechner Prüfprogramme in den einzelnen Rechnern anstößt. Mit Hilfe dieser Programme muss nun der fehlerhafte Rechner ermittelt werden



Hierbei werden zwei oder mehr aktive Steuerrechner eingesetzt.
Eingesetzt werden dabei im wesentlichen die Betriebsweisen

- call sharing (auch load sharing genannt).
- function sharing.

Bild: Leistungssteigernde Betriebsweisen

Call sharing (Load sharing, Lastteilung)

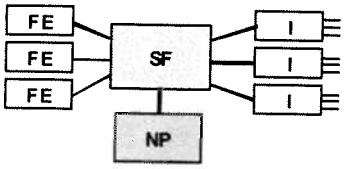
Es ist jedem Rechner möglich, von allen angeschlossenen Teilnehmer bzw. Leitungen Vermittlungswünsche zu empfangen, dieselben zu bearbeiten und alle Geräte der Peripherie mit Steuerbefehlen zu versorgen.
Das System wird so ausgelegt, dass bei der Verwendung von z. B. zwei Rechnern jeder der beiden Rechner in der Lage ist, im Fehlerfall alle Verbindungswünsche zu bearbeiten. Die Fehlererkennung muss im Rechner durch Selbstprüfung erfolgen. Im Normalfall werden die anfallenden Verbindungswünsche zwischen den Rechnern aufgeteilt. Hierbei ergibt sich dann z.B. eine Leistungsfähigkeit von ca. 160 % bezogen auf den Fehlerfall (nur 1 Rechner aktiv). Die Rechner müssen sich dann gegenseitig informieren, welchen Verbindungswunsch sie bearbeiten (z.B. 40 % der Kapazität). Ein Verbindungswunsch wird von dem Rechner, der ihn einmal angenommen hat, vollständig bearbeitet. Diese Betriebsweise wird auch als load sharing bezeichnet.

Function sharing (Funktionsteilung)

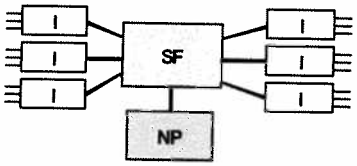
Jeder Rechner einer Mehrrechnerkonfiguration bearbeitet nur eine bestimmte Aufgabe innerhalb eines Verbindungsaufbaus, z.B. Ziffernauswertung, Wegesuche, Signalisierung, usw. Ein Verbindungsaufbau wird nacheinander oder gleichzeitig von verschiedenen Rechnern bearbeitet. Ist die Hardware dieser Vermittlungsrechner unterschiedlich, muss auch für jeden Typ eine Reserveeinheit bereitgestellt werden, dabei kann dann wieder cold/hot/active standby angewendet werden.
Bei diesem Verfahren kann eine Leistungssteigerung durch Parallelarbeit, aber auch durch die Möglichkeit des Einsatzes spezieller aufgabenorientierter Prozessoren erfolgen.

Struktur von Routern

Router mit getrennten Routing-Tabelle Prozessoren



Router mit Routing-Tabellen in den Anschlussmodulen



FE : Forward Engine
SF : Swiching Function
NP : Network Processor
I : Interface

Bild: Router-Aufbau

Im allgemeinen gibt es drei Arten von Router-Strukturen:

- Router mit eigenen Routing Prozessoren (forward engines, FE), welche die Weiterleitung der Pakete auf Grund von Routing-Tabellen ermitteln.
- Router, welche die Routingfunktion direkt in den Anschlussmodulen (Interfaces) erledigen können.
- Router, welche die Routintabelle hierarchisch zwischen den beiden Arten von Modulen aufgeteilt haben.

Die Vermittlung geschieht mit einem asynchronem Koppelnetz. Alle übergeordnete Funktionen wie Aktualisierung der Routing-Tabellen wird in einer zentralisierten Recheneinheit (network processor, NP) abgewickelt.

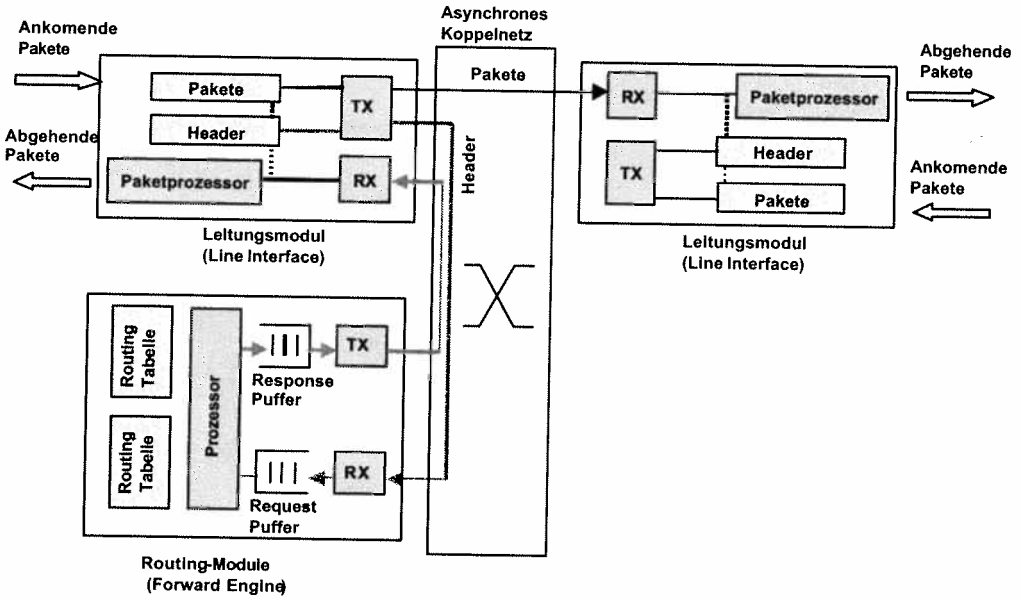


Bild: Verarbeitung von Paketen in einem Router

Die Verarbeitung von Paketen mit Routing-Prozessoren läuft wie folgt ab. Ankommende Pakete werden im Anschlussmodul zwischengepuffert und deren Header wird via dem Koppelnetz an einen Routing-Prozessor weitergeleitet. Sobald der richtigen Ausgangsport ermittelt ist, wird diese Information zurück gemeldet und kann das dazugehörende Paket, auch wieder via das Koppelnetz, zum Ausgangsmodul transportiert werden.

1.8 Grundlagen: Schichtenmodelle und Protokolle

Version: Feb. 2004

- OSI Referenzmodell
- Erweiterte Referenzmodelle
- Protokollinstanzen und -dienste
- Dienstelemente
- Protokollmechanismen

Das ISO/OSI-Modell ist als **Referenzmodell** weltweit akzeptiert. Es hilft bei der Einordnung, der Diskussion und dem Verständnis von Kommunikationssystemen. Die Anzahl von sieben Schichten hat sich im Lauf der Entwicklung so ergeben. Manchmal wird kritisiert, dass die Zahl der Schichten zu groß und der Ablauf unnötig kompliziert sei. Es gibt deshalb Modelle, die mit weniger Schichten auskommen. Ferner wird bei der Implementierung der Protokolle und Dienste die starre Schichteneinteilung teilweise ignoriert, um den Implementierungsaufwand gering zu halten und eine brauchbare Leistung (gemessen am erreichten Durchsatz für Anwendungsdaten) zu gewährleisten. Das TCP/IP-Modell fasst zum Beispiel die beiden unteren Schichten 1 und 2 sowie die Schichten 5 - 7 zusammen. Damit werden insgesamt 4 Schichten unterschieden. Der TCP/IP-Protokollstapel ist jedoch schon älter als das OSI-Modell. Manchmal werden auch Unterschichten eingeführt, wie zum Beispiel bei lokalen Netzen (LANs), wo Schicht 2 auch den Schichten 2a, Medium Access Control (MAC) und Schicht 2b, Logical Link Control (LLC) besteht. Um mehrere Übertragungsmedien (d.h. verschiedene Arten von Kupfer- und Koaxialleitungen sowie verschiedenen Glasfasern) nutzen zu können, wird heute auch die Bitübertragungsschicht in zwei Subschichten aufgeteilt und zwar in einen gemeinsamen Teil und in einen mediumabhängigen Teil.

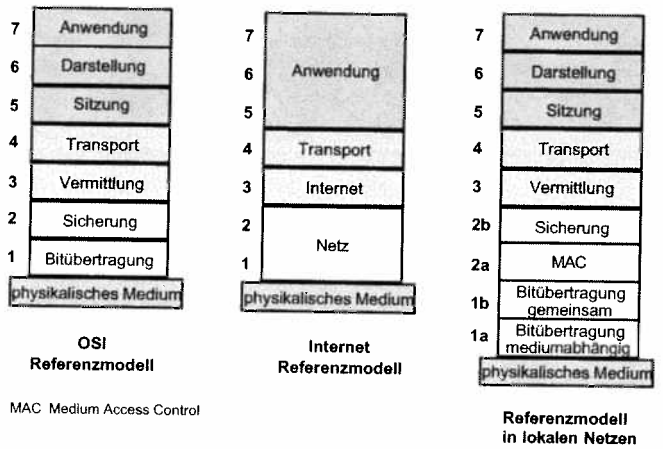


Bild: Protokoll-Referenzmodelle

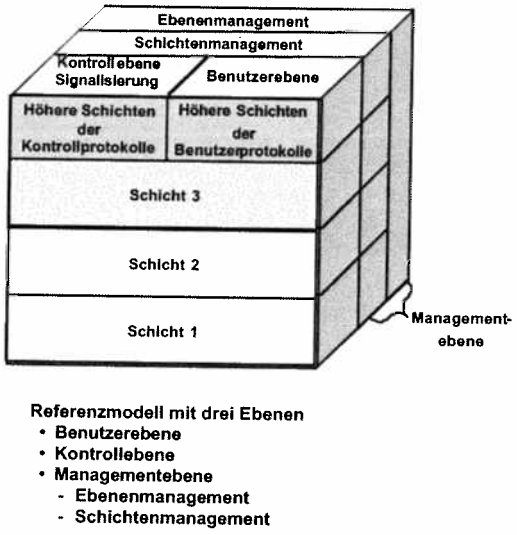


Bild: Protokoll-Stapel mit Schichten und Ebenen

Die Aufgaben eines Protokolls innerhalb einer Schicht n hängen von der betreffenden Schicht ab.
In vielen Fällen sind dies:

- Auf- und Abbau von Verbindungen der Schicht n,
- Übertragung von Schicht-n Datenblöken,
- Reihenfolgeeinhaltung der übertragenen Dateneinheiten,
- Flusskontrolle zur Anpassung der sendenden Instanz an die empfangende Instanz,
- Fehlererkennung (z. B. fehlende Dateneinheiten),
- Fehlerbehebung (z. B. durch wiederholte Übertragung),
- Quittierung von richtig empfangenen Dateneinheiten,
- Zeitüberwachung zur Erkennung und Behebung von Verklemmungszuständen (deadlock),
- Kommunikation mit den benachbarten Schichten (n-1) bzw. (n+1) über das Adjacent Layer Protokoll (Dienstprotokoll).

Schicht 1

1) Mechanisch 2) Elektrisch
3) Funktional 4) Prozedural

Schicht 2

1) Auf- und Abbau der Schicht-2 Verbindung
2) Übertragung von Schicht-2 Datenblöcken
3) Rahmensynchronisation
4) Reihenfolgeerhaltung
5) Flusskontrolle
6) Fehlersicherung

Schicht 3

1) Auf- und Abbau der Schicht-3 Verbindung
2) Übertragung von Schicht-3 Datenblöcken
3) Wegelenkung (routing)
4) Reihenfolgeerhaltung
5) Flusskontrolle, Überlastabwehr
6) Fehlersicherung

Schicht 4

1) Auf- und Abbau der Schicht-4 Verbindung
2) Übertragung von Schicht-4 Datenblöcken
3) Reihenfolgeerhaltung
4) Flusskontrolle
5) Fehlersicherung

Schicht 5

1) Auf- und Abbau der Schicht-5 Verbindung
2) Übertragung von Schicht-5 Datenblöcken
3) Dialog-Management
4) Synchronisation mehrerer Datenflüsse
5) Flusskontrolle
6) Fehlerbehandlung

Schicht 6

1) Auf- und Abbau der Schicht-6 Verbindung
2) Übertragung von Schicht-6 Datenblöcken
3) Anpassungen von Formatierung, Codierung und Komprimierung von Daten

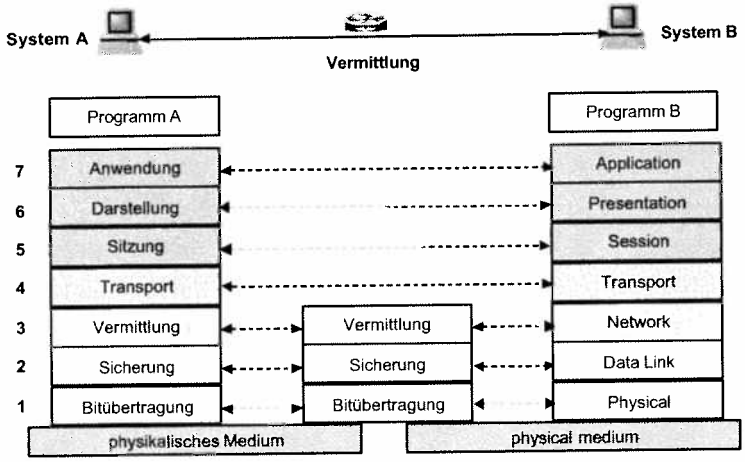
Schicht 7

1) Auf- und Abbau der Schicht-7 Verbindung
2) Übertragung von Schicht-7 Datenblöcken
3) Identifizierung der gewünschten Kommunikationspartner
4) Authentisierung der Kommunikationspartner
5) Feststellung der momentanen Verfügbarkeit der Partner
6) Festlegung der Verantwortlichkeit bei Fehlerbehebung
7) Feststellung von eventuellen Einschränkungen bezüglich der Syntax
8) Einigung auf ein Verfahren zur Ressourcenaufteilung
9) Aushandlung der akzeptablen Dienstqualität
10) Synchronisation kooperierender Anwendungen

Spezielle Schichtaufgaben:

Schicht 2:
Rahmensynchronis ation.
Schicht 3:
Wegelenkung (Routing), Überlastabwehr
Schicht 4:
-
Schicht 5:
Dialogmanagement, Synchronisation von Flüssen.
Schicht 6:
Anpassungen (Formatierung, Codierung, Komprimierung)
Schicht 7:
Authentisierung der Partner-anwendung, Aushandlung verschiedener Kommunikationsparameter.

Bild: Aufgaben der sieben OSI-Schichten.

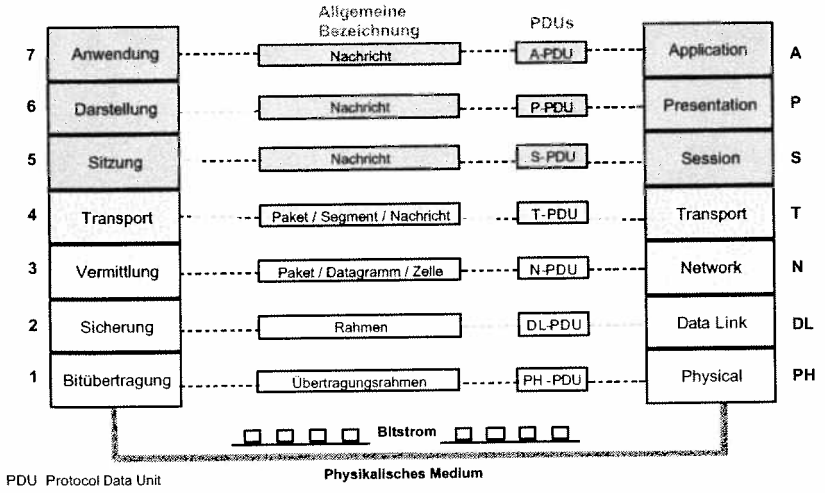


Das Basisreferenzmodell ist ein allgemeines Architektur-Modell für die Kommunikation zwischen Systemen auf der Basis digital codierter Daten (einschließlich Text, Sprache und Bild). Das Referenzmodell definiert, welche Funktionen in welchem Zusammenhang in einer Kommunikation auftreten und stellt damit den Rahmen für die Erarbeitung von Normen auf, die nötig sind, um das Normungsziel - Offene Kommunikationssysteme (OSI: **O**pen **S**ystems **I**nterconnection) - zu erreichen.

Es beruht auf drei Konzepten:

- Strukturierung,
- Dienste,
- Protokolle.

Bild: OSI-Referenzmodell über Zwischensystemen



Je nach Protokollschicht werden die Dateneinheiten (Data Unit, DU) verschieden bezeichnet. Generisch werden Protocol Data Units (PDU) zwischen Partner-Protokollschichten der beiden Endsysteme ausgetauscht, zum Beispiel T-PDU auf der Transport-Schicht.

Bezeichnungen für die Dateneinheiten:

- Daten (data)
- Nachricht (message)
- Paket (packet)
- Segment (segment)
- Datagramm (datagram)
- Zelle (cell)
- Rahmen (frame)
- Übertragungsrahmen (transmission frame).

Bild: Übermittlungs- und Übertragungseinheiten

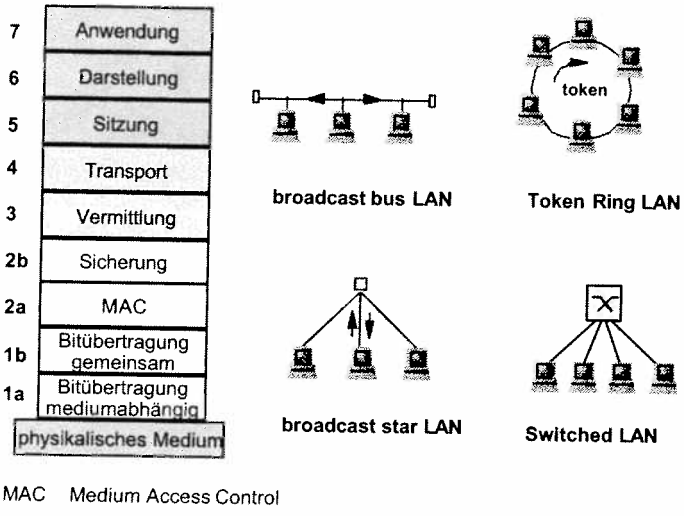


Bild: Referenzmodell in lokalen Netzen

Bei Netzen mit einem gemeinsamen Medium wie bei traditionellen lokalen Netzen (LAN, Local Area Networks) wird die Schicht 2 weiter aufgeteilt in eine Mediumzugriffsschicht 2a und die eigentliche Sicherungsschicht. Ein Mediumzugriffmechanism (MAC, Medium Access Control) ist in allen Systemen mit einem gemeinsamen Medium erforderlich:

- Lokale Netze (LAN),
- Lokale Funknetze (WLAN, Wireless LAN),
- Mobilfunk (Sternstruktur durch Basisstation),
- Satellitenfunk (Sternstruktur durch Satellit),
- Mehrfach-Funkanschluss (WLL, Wireless Local Loop, Sternstruktur durch Funkkopfstation)
- Kabelnetze (Baumstruktur mit Kabelkopfstation),
- Passive optische Netze (PON, Passive Optical Network, Stern- oder Baumstruktur mit Glasfaserkopfstation)

Ferner werden in heutigen Protokollspezifikationen die Bitübertragungsschicht aufgeteilt in einen gemeinsamen und einen mediumabhängigen Teil.

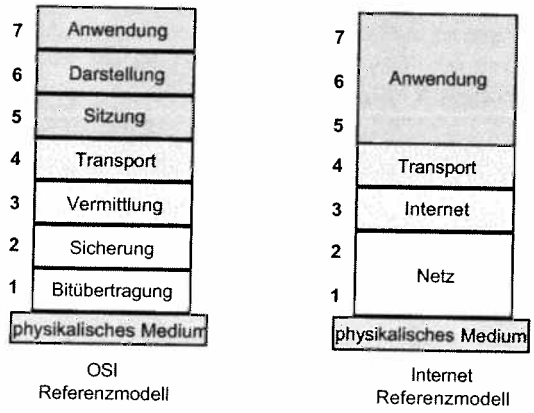


Bild: OSI- und Internet Referenzmodelle

Die technische Entwicklung hat eine Erweiterung des prinzipiellen Siebenschichten-Modells erforderlich gemacht durch Einführung von

- Leerschichten für Null-Funktionalitäten in bestimmten Anwendungsfällen,
- Subschichten für eine feinere Unterteilung der Funktionalität wie z. B.
  in Schicht 1 bei ATM-Netzen
  in Schicht 2 bei LAN/MAN-Netzen
  in Schicht 3 bei LAN/MAN-Netzen
  in Schicht 7 für unterschiedliche Anwendungsklassen.

Das Grundsätzliche Schichtenprinzip bleibt jedoch erhalten.

Netzkopplung (Internetworking)

Ein Internet ist ein Netz, das aus vielen Subnetzen (Teilnetzen) besteht, die untereinander vernetzt sind. Die Verbindung zwischen Subnetzen wird durch Zwischensysteme (intermediate systems) hergestellt. Die in den Subnetzen vorhandenen Systeme werden hingegen als Endsystem (end system) bezeichnet, sie bieten Dienste für die Netznutzer an. Der Begriff Internet ist ein generischer Begriff. Das Internet ist ebenfalls ein Internet, aber eine spezifische Implementierung, die als Kernprotokolle TCP/IP verwendet (Transmission Control Protocol/Internet Protocol).Zu Beginn der Rechnervernetzung wurden häufig zuerst lokale Netze aufgebaut. Diese können nach recht unterschiedlichen Konzepten funktionieren, weshalb sie sich in ihren Eigenschaften erheblich unterscheiden können. Später sollte das Internetworking existierende verschiedenartige Netzinseln miteinander vernetzen. Ziel war es, die Anzahl der erreichbaren Kommunikationspartner zu vergrößern und so den (betriebswirtschaftlichen) Nutzen aus den getätigten Investitionen zu steigern. Ein **Internet** kann als ein virtuelles Netz bezeichnet werden. Obwohl es aus vielen, möglicherweise unterschiedlichen Subnetzen aufgebaut ist, kann jedes Endsystem mit jedem anderen kommunizieren. Das Endsystem bekommt die Abstraktion eines großen, einheitlichen Netzes geboten, das einen einheitlichen Adressraum und einheitliche Protokolle (zumindest auf einigen OSI-Schichten) aufweist. Solche Netze werden mit Routern als Zwischensysteme realisiert.

Als Zwischensysteme werden Repeater, Konverters, Brücken (bridge), Switches, Router und Gateways verwendet.

- Repeater und Konverters arbeiten auf Schicht 1,
- Brücken vermitteln Rahmen auf Schicht 2,
- Switches vermitteln generell Rahmen auf Schicht 2, können dazu aber Information von allen Schichten 2 bis 7 beiziehen.
- Router vermitteln Pakete auf Schicht 3
- Gateways bearbeiten Nachrichten auf Schicht 4, eventuell unter Berücksichtigung von Informationen höherer Schichten.

All diese Kopplungselemente findet man in LANs. In den MANs und WANs werden Switches, Routers und Gateways eingesetzt.LAN (Local Area Network), MAN (Metropolitan Area Network), WAN (Wide Area Network).

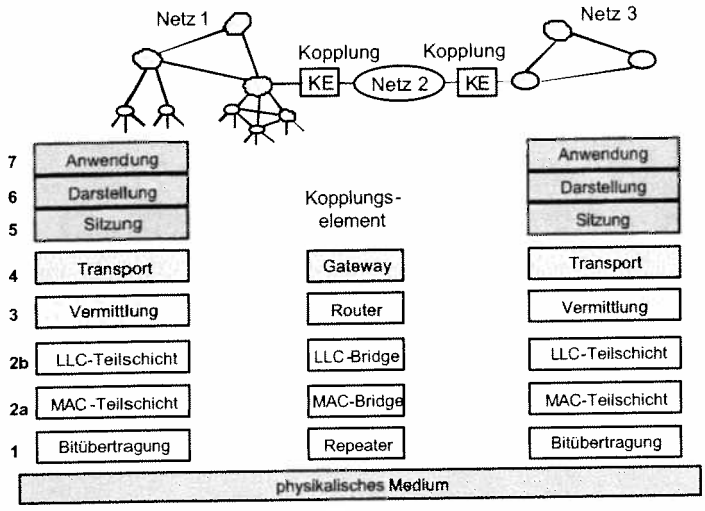


Bild: Gekoppelte Netze

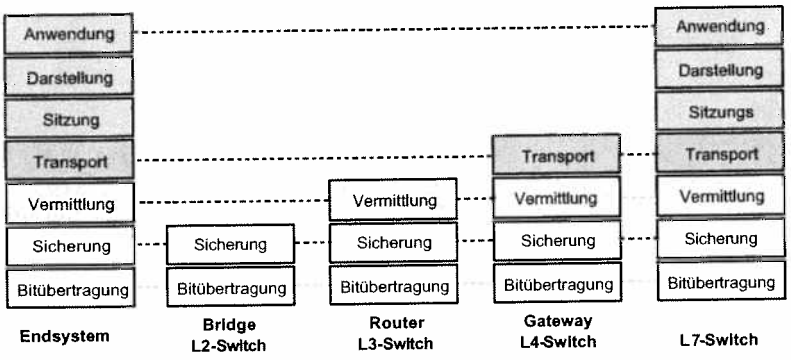
Repeater verbinden Netzsegmente (z. B. Ethernet-Segmente) unmittelbar miteinander. Ein Repeater funktioniert auf der OSI-Schicht 1. Er regeneriert und verstärkt elektrische Signale. Repeater werden zur Vergrößerung der Ausdehnung eines Netzes eingesetzt. Daneben gibt es **Konverters**, die zwei Arten von Übertragungsmedien, beispielsweise Kupfer und Glasfaser, verbinden können.

Brücken (Bridge) verbinden Netzsegmente zu einem Netz. Sie funktionieren auf der OSI-Schicht 2 und trennen die Segmente logisch voneinander. Man unterscheidet zwischen der MAC-Brücke auf Schicht 2a und der LLC-Brücke auf den Schichten 2a und 2b (Logical Link Control).

Eine **MAC-Bridge** filtert sogenannten MAC-Adressen (es werden nur Rahmen weitergegeben, die tatsächlich die Brücke passieren müssen) und passen die Zugriffsmechanismen an, sofern diese auf den zu verbindenden Segmenten unterschiedlich sind (zum Beispiel Ethernet und Token Ring). Brücken sind unabhängig von den höheren Protokollschichten. Sie werden primär zum Verkehrsmanagement eingesetzt, dessen Ziel es ist, lokalen Verkehr auch lokal zu begrenzen.

Eine **LLC-Bridge** sieht zusätzlich eine getrennte Flusskontrolle in den beiden gekoppelten LANs vor. Dies gilt nur, wenn die verbindungsorientierte Kommunikation in den LANs aktiv ist. Normalerweise ist Kommunikation in LANs verbindungslos.

Eine **Remote Bridge** kann zur Kopplung weit entfernter Netzinseln eingesetzt werden. Dabei wird für die große Distanz entweder eine Glasfaserverbindung oder eine schmalbandige Telefon- oder Standleitung eingesetzt. Im ersten Fall reicht eine normale Brücke mit einem Glasfaseranschluss. Im zweiten Fall sind die Brücken an beiden Enden mit einer entsprechenden WAN-Leitungsanschluss ausgerüstet.



L2-Switch: Layer-2 Switch

Bild: Switches mit Unterstützung von verschiedenen Protokollschichten

Switches vermitteln generell Rahmen auf Schicht 2, können dazu aber Information von allen Schichten 2 bis 7 beiziehen.

Man spricht von Layer-2, Layer-3, Layer-4 und Layer-7 Switches.

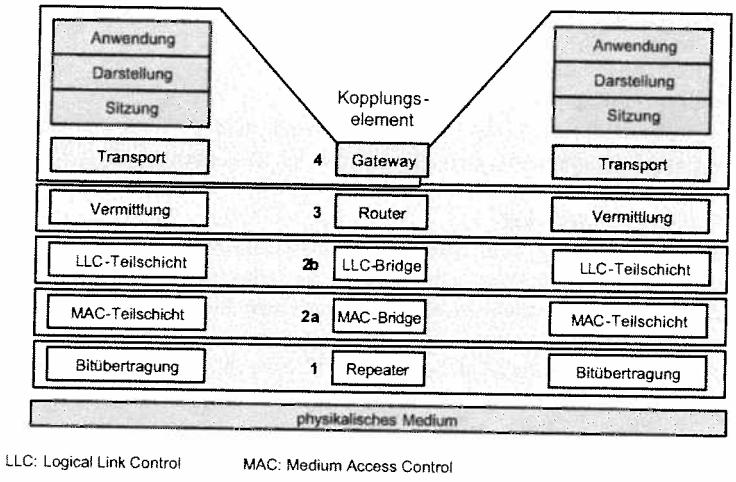


Bild: Netzkopplung: Schichtenmodell

Router verbinden Netze (die dadurch zu Subnetzen werden) zu einem Netz. Sie funktionieren auf der OSI-Schicht 3 und trennen die Subnetze logisch. Router sind vom eingesetzten Netzprotokoll abhängig, sie müssen die Netztopologie kennen. Router werden zum Aufbau von Internets, also zur Vernetzung einzelner Netze (Netzinseln) zu größeren Netzen, eingesetzt.

Gateways verbinden Netze zu einem System. Dies bedeutet sie ermöglichen die Kommunikation zwischen unterschiedlichen Transportprotokollen, eventuell mit Informationen der höheren Schichten auf beiden Endsystemseiten. Gateways funktionieren somit auf Schicht 4, wobei die Übersetzung der beiden Transportprotokollseiten möglicherweise Informationen der höheren Schichten benötigt.

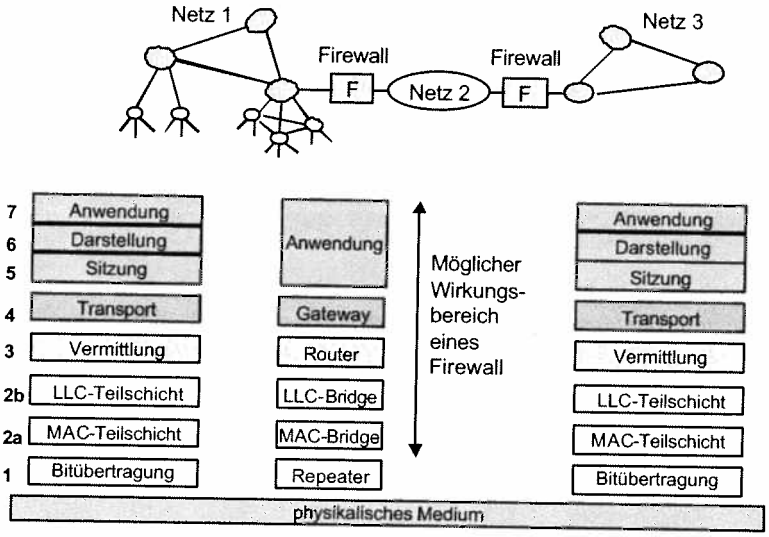


Bild: Möglicher Wirkungsbereich von Firewalls

Firewalls
Zum Schutz von LANs oder Subnetzen werden heute generell Firewalls eingesetzt. Dabei gibt es verschiedene Arten von Firewalls (Brandmauer, Schutzmauer) zu unterscheiden. Die jeweilige Bezeichnung orientiert sich an der höchsten ausgewerteten OSI-Schicht. Ein MAC-filter wertet Rahmen auf Schicht 2 aus. Ein Paketfilter (oder packet filter, screening router) wertet Pakete bis zur Schicht 3 aus. Ein Verbindungs-Gateway (connection-level gateway) wertet primär Nachrichten der Transportschicht (Schicht 4) aus, während ein Anwendungs-Gateway (application-level gateway, proxy) bis zur Schicht 7 eingreift.

Die im OSI-Modell definierten Schichten beziehen sich auf die eigentliche Informationsübertragung. Für bestimmte Aufgaben wird jedoch eine Signalisierung oder Kontrolle (control) benötigt, die an der eigentlichen Informationsübertragung nicht beteiligt ist. Damit ein Datennetz zuverlässig und mit guter Leistung funktioniert, muss es laufend überwacht werden. Aus der Analyse der Messdaten werden Maßnahmen zum Management des Netzes abgeleitet. Diese werden den betroffenen Netzknoten übermittelt und dort ausgeführt. Um diese Aufgaben einzuordnen, sind die Schichten des Schichtenmodells durch orthogonal dazu liegende Ebenen (planes) ergänzt. In der Regel werden drei Ebenen unterschieden, die ihrerseits in Schichten eingeteilt sind.

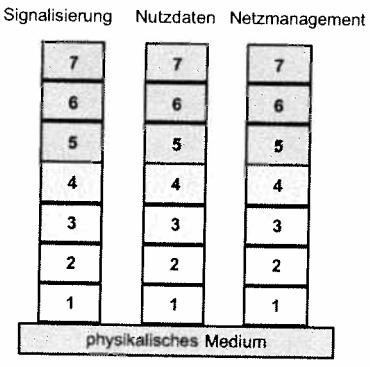


Bild: Referenzmodell-Erweiterung

Prinzip der Protokoll-Ebenen
Das aus der Paketkommunikation entstandene Strukturierungskonzept musste erweitert werden, um z. B. die im getrennten Signalisierungsnetz SS7 (Signaling Network Number 7, Signalisierungsnetz Nummer 7) ablaufende Verbindungs- und Dienststeuerung einzubeziehen. Darüber hinaus gewann das System- und Netzmanagement an Bedeutung, so dass heute das Referenzmodell in drei Ebenen (Planes) aufgeteilt ist, welche nach Kontexten aufgeteilt sind und welche jeweils eine vertikale Schichtung aufweisen.

- Benutzerdaten (User Plane),
- Steuerdaten (Control Plane),
- Managementdaten (Management Plane).

In den verschiedenen Protokoll-Ebenen kann die Anzahl der Protokoll-Schichten unterschiedlich sein.

Die Protokoll-Ebenen beziehen sich teilweise auf unterschiedliche Abschnitte eines Übertragungsweges.

- Protokolle der Benutzerebene steuern die Abläufe zwischen Endknoten.
- Protokolle der Kontrollebene sind primär zwischen einem Endsystem und dem ersten Zwischensystem im Netz wirksam.
- Managementprotokolle werden für die Kommunikation von Managementsystemen mit Zwischensystemen benötigt.

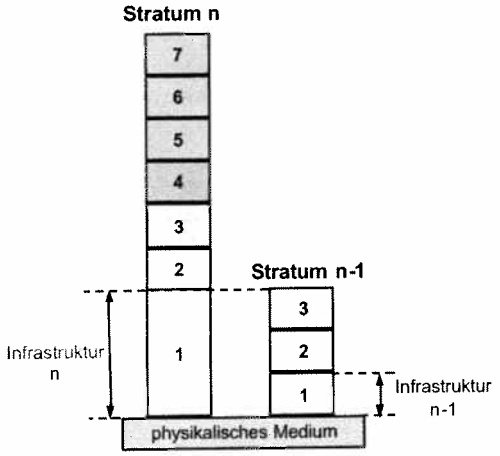


Bild: Referenzmodell-Erweiterung: Stratum

Der Begriff Stratum

Bei Verwendung von heterogenen Netztechnologien können die netzrelevanten Protokollschichten durch sukzessives Ersetzen der Bitübertragungsschicht in einer gemeinsamen Protokollstruktur dargestellt werden. Dies ist das Stratum-Konzept.
Ein wichtiges Beispiel dazu ist TCP/IP über ATM über SDH über Optik

TCP/IP : Transmission Control Protocol / Internet Protocol
ATM : Asynchronous Transfer Mode
SDH : Synchronous Digital Hierarchy

Bemerkung

Beim Ersetzen der Bitübertragungsschicht ist allerdings zu beachten, dass in verschieden Stratumtechnologien nicht der gesamten Bitübertragungsschicht ersetz werden darf. Dies ist dann der Fall, wenn der Bitübertragungsschicht weiter unterteilt ist in einem gemeinsamen Teil und einem Mediumspezifischen Teil. In diesem Fall kann nur der letzte Teil ersetzt werden.

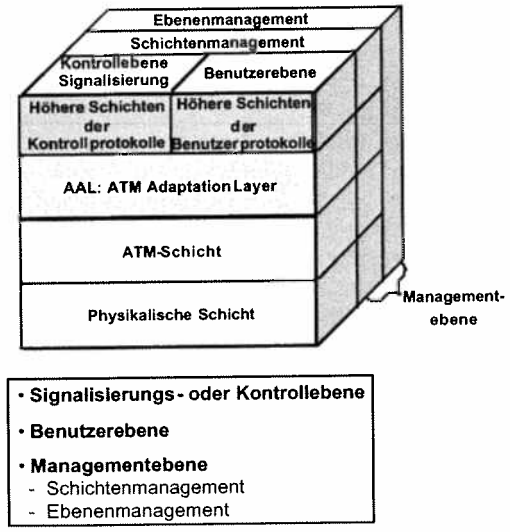


Bild: ATM-Referenzmodell

B-ISDN-Referenzmodell

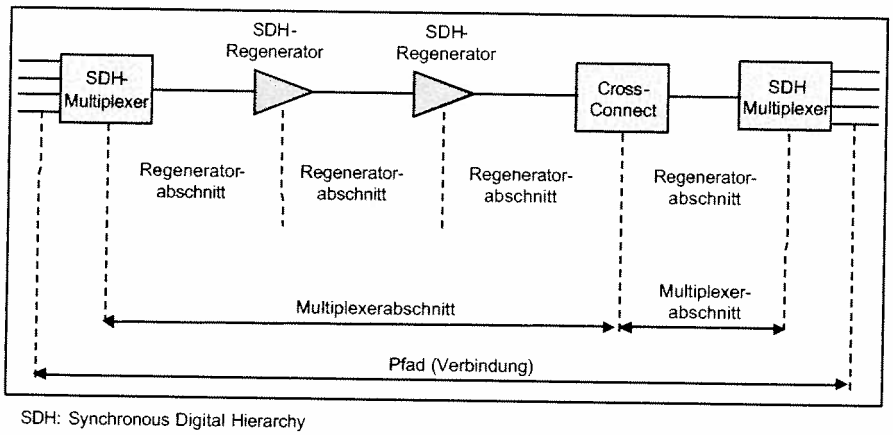
Das Schichtenmodell für B-ISDN (Broadband ISDN) bzw. ATM zeigt eine konkrete Anwendung der Strukturierung in Schichten und Ebenen. Einzelne Schichten sind weiter unterteilt. Die Anwenderebene (userplane) repräsentiert die Funktionen für die Nutzdatenübertragung, die Kontrollebene (control plane) beinhaltet die Signalisierung, die für die hier realisierte verbindungsorientierte Kommunikation erforderlich ist.

Die **Managementebene** (management plane) ist aufgeteilt in:

- **Schichtenmanagement** (layer management) zur Ausführung schichtenspezifischer Managementfunktionen.
- **Ebenenmanagement** (plane management) zur Koordination aller Ebenen.

ATM besteht aus den Schichten:

- ATM Adaptation Layer (AAL), wo die Konvertierung zwischen den Stratumschichten darüber und der ATM-Vermittlungsschicht stattfindet.
- ATM-Schicht, wo die zentrale Aufgabe der Zellenvermittlung stattfindet
- Bitübertragungsschicht mit einem gemeinsamen und einem mediumspezifischen Teil.



SDH: Synchronous Digital Hierarchy

Bild: Netzmanagement einer SDH- Übertragungsstrecke

Netzmanagement der SDH-Übertragungsebene

Zur Überwachung der Übertragungsqualität einer SDH-Strecke sind folgende Abschnitte definiert:

- Regeneratorabschnitt,
- Multiplexabschnitt,
- Verbindungsabschnitt (Pfad).

Ein Abschnitt besteht immer zwischen zwei Netzelementen, d.h. vom Ausgang des einen Systems zum Eingang des nachfolgenden Systems.

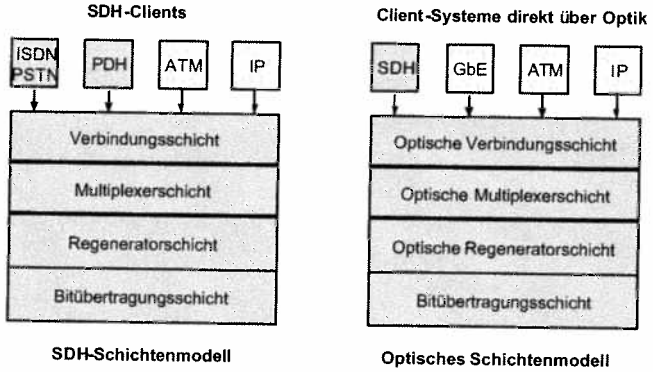
- **Regeneratorabschnitt:** alle Abschnitte zwischen Netzelementen, die das Übertragungssignal regenerieren (Amplitude, Phase (zeitliche Position) und Signalform). Diese sind alle SDH-Netzelemente (Multiplexer Add-Drop-Multiplexer, Cross-Connects und Regeneratoren).
- **Multiplexabschnitt:** alle Abschnitte zwischen Netzelementen, die Signalströmen Multiplexen oder Schalten können. Dies sind die Multiplexer, Add-Drop-Multiplexer und Cross-Connects).
- **Verbindungsabschnitt (Pfad):** alle Ende-zu-Ende Abschnitte zwischen Netzelementen, die sogenannten Client-Systeme zu SDH-Übertragungsströmen mit den standardisierten Bitraten von 155 Mbit/s, 622 Mbit/s, 2,5 Gbit/s, 10 Gbit/s und 40 Gbit/s. Es besteht eine eventuell geschaltete Verbindung (Pfad) zwischen zwei SDH-Clients.

Bemerkung: Wenn Fehler festgestellt werden, dient es nur zur Entscheidung, ob auf eine andere SDH-Übertragungsstrecke umgeschaltet werden muss. Dies ist nicht zu verwechseln mit den Aufgaben der OSI-Protokollschicht 2. Wir befinden uns in einem anderen Stratum.

Netzmanagement der optischen Übertragungsebene

In der optischen Übertragungsebene gilt die gleiche Streckeneinteilung für die Überwachung der optischen Übertragungsqualität. Dabei ist zu beachten, dass die Messungen auf optischen Methoden beruht, die danach als elektrische Ergebnisse vorliegen.

Netzelemente: ADM (Add-Drop-Multiplexer) OADM (Add-Drop-Multiplexer)
DXC (Digital Cross-connnet) OXC (Optical Cross-Connect)



ISDN	Integrated Services Digital Network	IP	Internet Pprotocol
PSTN	Public Switched Telephone Network	ATM	Asynchronous Transfer Mode
PDH	Plesiochronous Digital Hierarchy	GbE	Gigabit Ethernet
SDH	Synchronous Digital Hierarchy		

Bild: Übertragungsschichtenmodell

Das SDH-Schichtenmodell sowie das optische Schichtenmodell für das Netzmanagement haben die gleiche Struktur. Beide Modelle zeigen die Möglichkeiten zur Verbindung von Client-Systemen über eine geschaltete Ende-zu-Ende Übertragungsverbindung.

SDH-Clientsysteme:

- Telefonsysteme PSTN und ISDN,
- PDH Zubringerübertragungsleitungen (E1: 2 Mbit/s, E3: 34 Mbit/s, T1: 1,5 Mbit/s, T3: 45 Mbit/s)
- Verbindungsorientierte ATM-Verbindungen,
- Verbindungslose IP-Paketströme.

Client-systeme direkt über Optik:

- SDH-Übertragungsströme (bisher Normalfall),
- Gibabit-Ethernet-Verbindungen,
- Verbindungsorientierte ATM-Verbindungen,
- Verbindungslose IP-Paketströme.

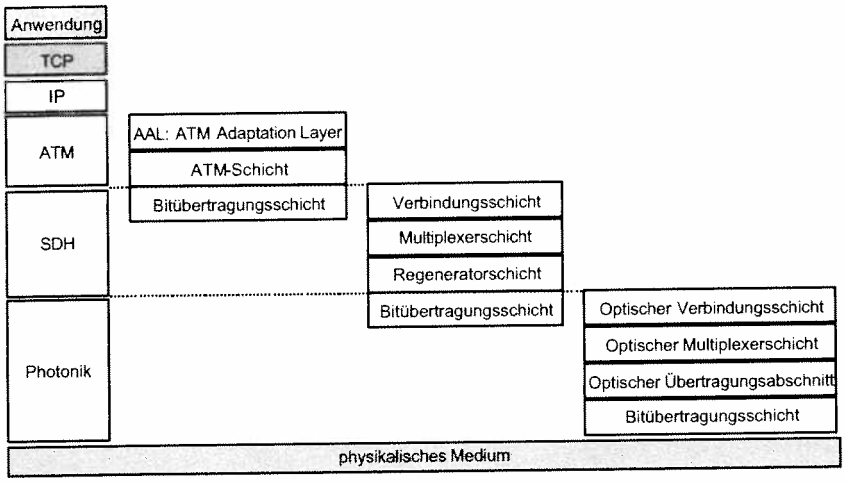


Bild: Stratum-Protokollschichtung

Stratum-Protokollschichtung
Das Bild zeigt ein Beispiel für eine Stratum-Protokollschichtung: TCP/IP über ATM über SDH über Optik

Bemerkung: Falls zum Beispiel ATM nicht verwendet wird ist dieses Stratum auch nicht vorhanden.

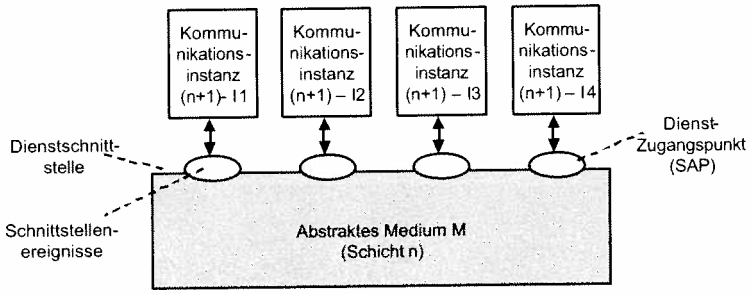


Bild: Dienstbegriff

Ein Dienst ist die Realisierung der Funktionen einer OSI-Schicht n, die mit allen Schichten (n-1) bis 1 als abstraktes Medium betrachtet werden kann. Dieser n-Dienst wird als Diensterbringer bezeichnet, der durch sogenannte Protokoll-Instanzen (entity) über Dienstzugangspunkte (SAP, Service Access Point) den Dienstbenutzern auf Schicht (n+1) zur Verfügung steht (Kommunikationsinstanzen (n+1)). Da mehrere Benutzer diesen n-Dienst beanspruchen können ist eine Adressierung über die Dienstpunkte notwendig. Die Verarbeitung in den verschiedenen Schichten wird im allgemeinen durch nur einen Prozessor ausgeführt, und somit dient ein Dienstpunkt als adressierbaren Pufferbereich, wo Dateneinheiten bis zur Bearbeitung zwischengepuffert werden.

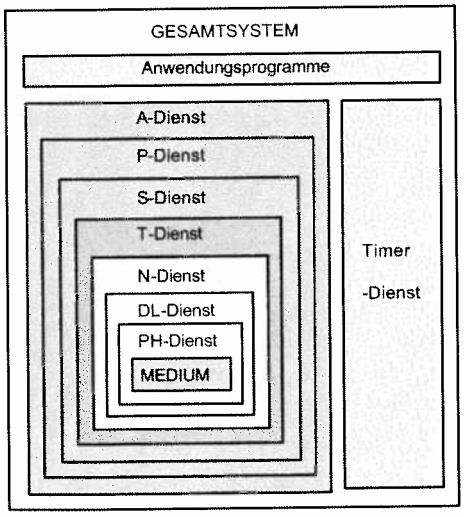
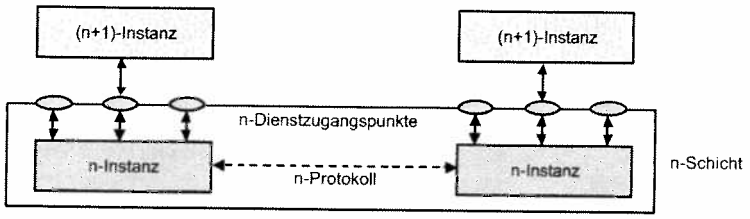


Bild: Hierarchische Dienststruktur

Die hierarchische Dienststruktur ist als Verschachtelung zu sehen. Jeder höherer Dienst kann auf die Gesamtheit der Dienste darunter aufsetzen.

Oberhalb der Kommunikationsprotokolle sind die Anwenderprogramme angesiedelt.

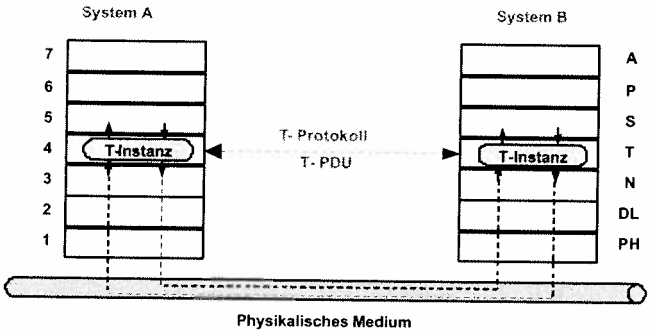
Zur Überwachung des zeitgerechten Ablaufes der Schichtenfunktionen sind viele Zeitzähler (Timer) notwendig. Sie werden im allgemeinen durch einen gemeinsamen Timer-Dienst zur Verfügung gestellt.



- n-Instanz:
  erbringt einen n-Dienst, der von (n+1)-Instanzen über n-Dienstzugangspunkte genutzt werden können
- n-Schicht:
  Abstraktionsebene mit definierten Aufgaben. Sie besteht aus allen n-Instanzen.
- n-Protokoll:
  bestimmt den Ablauf und Regeln zum Datenaustausch zwischen n-Instanzen

Bild: Instanz, Schicht und Protokoll

Im Bild ist die Kommunikation zwischen zwei Partner-Instanzen auf der (n+1)-Schicht unter Verwendung des n-Dienstes dargestellt. Dazu wird dieser n-Dienst über einen n-Dienstzugangspunkt (n-SAP) auf beiden Seiten adressiert, um die entsprechenden n-Instanzen zu identifizieren. Diese n-Instanzen auf beiden Seiten tauschen n-PDUs (Protocol Data Unit) über eine logische Verbindung mit Hilfe des n-Protokolls aus. Für jedes (n+1)-Instanzen-Paar ist auf beiden Seiten einen eigenen n-Dienstpunkt und einen eigenen n-Instanz notwendig. Für jedes (n+1)-Instanzen-Paar existiert auch eine eigene logische Verbindung.

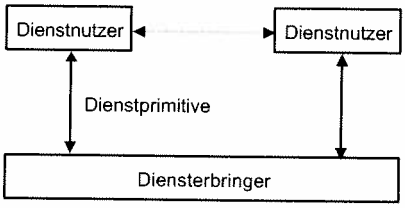


A: Application
P: Presentation
S: Session
T: Transport
N: Network
DL: Data Link
PH: Phyical

PDU: Protocol Data Unit

Bild: Kommunikation innerhalb einer Schicht

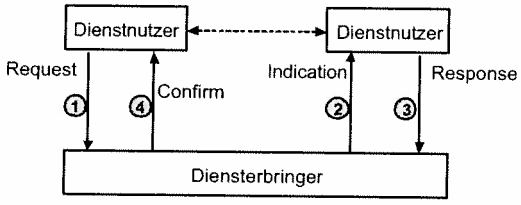
Das Bild zeigt eine logische Verbindung zwischen einem T-Instanzen-Paar in den Endsystemen A und B (Transportschicht). Sie dient als Diensterbringer für ein S-Instanzen-Paar als Dienstnutzer auf der Sitzungsschicht.



Diensterbringer:
z.B. gesamtes Kommunikationssystem, einzelne Schicht

Dienstbenutzer:
z.B. Benutzer, einzelne Schicht

Bild: Dienstnutzer / Diensterbringer



4 Typen von Dienstprimitiven:
- Anforderung (Request)
- Anzeige (Indication)
- Antwort (Response)
- Bestätigung (Confirm)

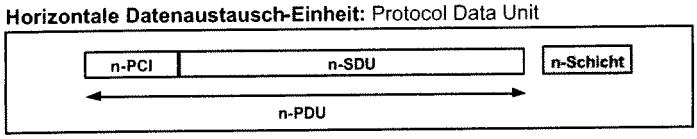
Bild: Austausch von Dienstprimitiven

Dienstprimitive (primitives, Dienstelemente)

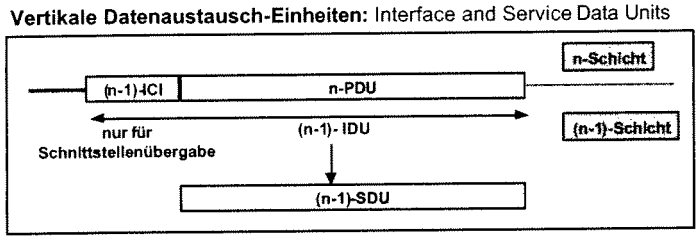
Damit ein Dienst in Anspruch genommen werden kann, müssen sogenannte Dienstprimitve (Dienstelemente) zwischen benachbarten Schichten im selben Protokollstapel (protocol stack) ausgetauscht werden. Dies geschieht immer über einen Dienstzugangspunkt (SAP, Service Access Point).

- Es gibt vier Typen von Dienstprimitiven: Request, Indication, Response und Confirm.
- Unterschieden wird zwischen einem bestätigten Dienst (alle vier Primitive) und einem unbestätigten Dienst (erste zwei Primitive).
- Eine Dienstprimitive wird wie folgt gekennzeichnet: Abkürzung der Schicht – Meldung.Dienstprimitiventyp (z.B. T-connect.request., T-connect.indication, T-connect response, T-connect.confirm).

Horizontale Datenaustausch-Einheit: Protocol Data Unit



Vertikale Datenaustausch-Einheiten: Interface and Service Data Units



SDU : Service Data Unit
PDU : Protocol Data Unit
IDU : Interface Data Unit
PCI : Protocol Control Information
ICI : Interface Control Information

Bild: Horizontaler und vertikaler Datenaustausch

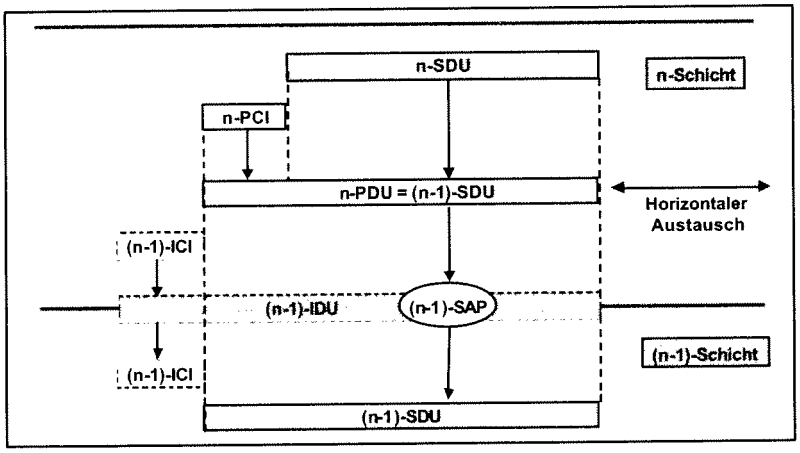
Horizontaler Datenaustausch: PDU

Für den horizontalen Datenaustausch zwischen Partner-Instanzen auf beiden Seiten werden PDUs (Protocol Data Unit) verwendet. Ein n-PDU besteht aus einem Datenteil, der als n-SDU (Service Data Unit) bezeichnet wird und einem Headerteil, der als n-PCI (Protocoll Control Information) bezeichnet wird.

Vertikaler Datenaustausch: SDU, IDU

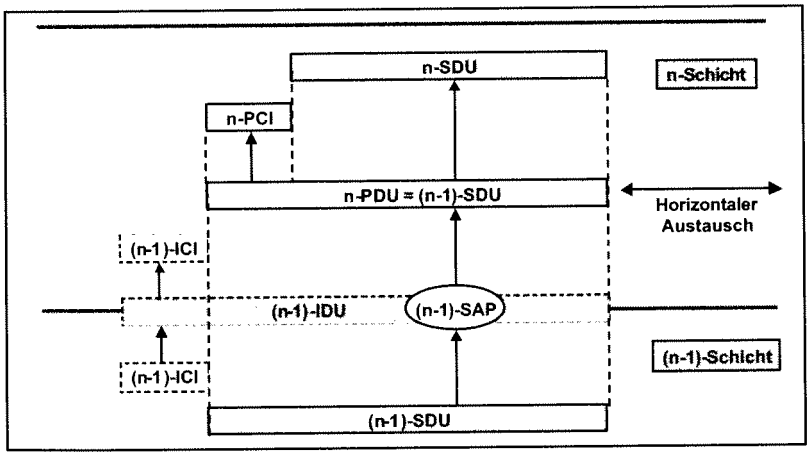
Der vertikale Datenaustausch zwischen Instanzen in benachbarten Schichten desselben Protokollstapels geschieht über SDUs. Da die Schichtübergabe Zusatzinformation benötigt, bildet ein SDU zusammen mit dem ICI (Interface Control Information einen IDU (Interface Data Unit).

Es gilt: (n-1)-SDU = n-PDU



PDU : Protocol Data Unit
PCI : Protocol Control Information
SDU : Service Data Unit
IDU : Interface Data Unit
ICI : Interface Control Information
SAP : Service Access Point

Bild: Schnittstellenübergabe von der n-Schicht zur (n-1)-Schicht



PDU : Protocol Data Unit
PCI : Protocol Control Information
SDU : Service Data Unit
IDU : Interface Data Unit
ICI : Interface Control Information
SAP : Service Access Point

Bild: Schnittstellenübergabe von der (n-1)-Schicht zur n-Schicht

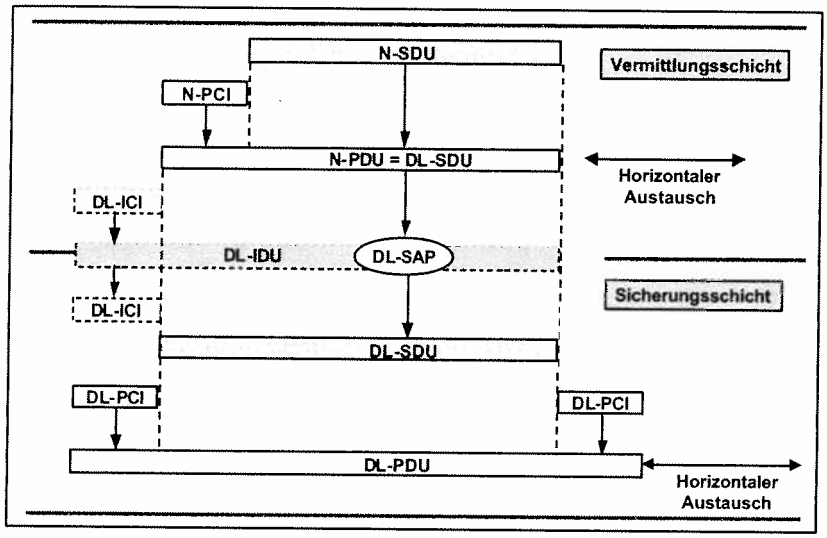


Bild: Schnittstellenübergabe von der Netzschicht zur Sicherungsschicht

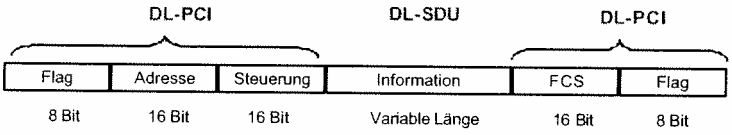
Zu beachten ist, dass aus einem DL-SDU durch Hinzufügen von DL-PCIs auf beiden Seiten einen DL-PDU entsteht.

PDU = Protocol Data Unit
SDU = Service Data Unit
IDU = Interface Data Unit

PCI = Protocoll Control Information
ICI = Interace Control Information

SAP = Service Access Point

Schicht 2: Rahmen-Format



PCI : Protocol Control Information
SDU : Service Data Unit
FCS: Frame Check Sequence

Bild: Beispiel für einen Protocol Data Unit (PDU)

Zu beachten ist, dass aus einem DL-SDU durch Hinzufügen von DL-PCIs auf beiden Seiten einen DL-PDU entsteht.

Services	SAP	Instanz	SDU	PCI	PDU
Application	-	A - Instanz	-	A - PCI	A - PDU
Presentation	P - SAP	P - Instanz	P - SDU	P - PCI	P - PDU
Session	S - SAP	S - Instanz	S - SDU	S - PCI	S - PDU
Transport	T - SAP	T - Instanz	T - SDU	T - PCI	T - PDU
Network	N - SAP	N - Instanz	N - SDU	N - PCI	N - PDU
DataLink	DL - SAP	DL - Instanz	DL - SDU	DL - PCI	DL - PDU
PHysical	PH - SAP	PH - Instanz	PH - SDU	PH - PCI	PH - PDU

SAP: Service Access Point
SDU: Service Data Unit
PDU: Protocol Data Unit
PCI: Protocol Control Information

Bild: Schichtenbezogene Namensgebung

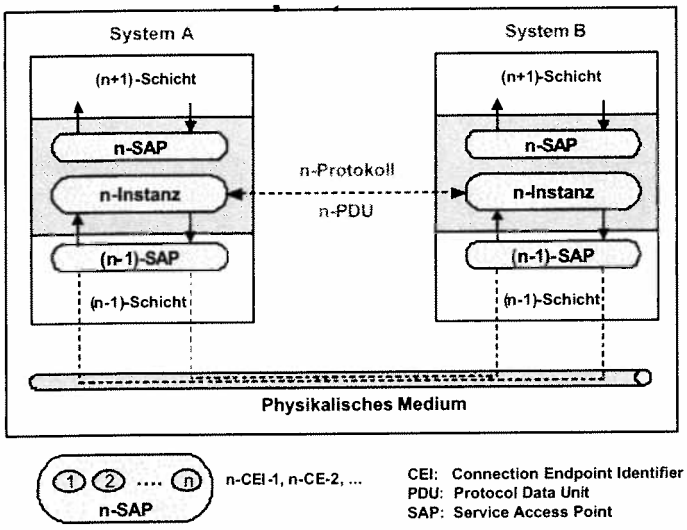


Bild: Logische Verbindungen

Verbindungskonzepte

Zur Unterstützung des Datenaustausches zwischen zwei n-SAPs wird das Konzept einer Verbindung (Connection) eingeführt. Dabei kann die n-Verbindung, die logisch zwei n-SAPs miteinander verknüpft, als Funktion der Schicht n aufgefasst werden, welche ihrerseits auf Funktionen unterer Schichten zurückgreift. Innerhalb eines n-SAP können mehrere Endpunkte von n-Verbindungen liegen, welche jeweils durch Verbindungsendpunkt-Kennungen (Connection Endpoint Identifier, CEI) unterschieden werden.

Verbindungsorientierte Kommunikation

Aufbau einer Verbindung bevor der Informationsaustausch stattfindet

Vorteil: Aushandlung von Kommunikationsparametern möglich:
Fenstergrößen, verwendeter Code, verwendete Fehlerkontrollmechanismen, Sequenznummern,...

Nachteile:
- eigentlicher Datenaustausch verzögert
- Overhead der Verbindungsetablierung und -verwaltung kann höher sein als der eigentliche Datenaustausch (kurze Daten)

Verbindungslose Kommunikation

Informationen werden versendet, ohne vorherigen Aufbau einer Verbindung

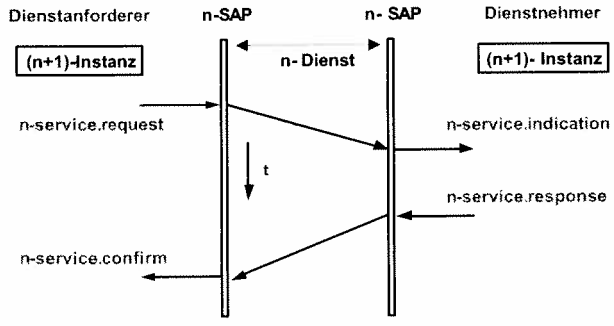
Vortell: schnelle Datenversendung möglich

Nachteil: keine Möglichkeit der Kontrolle, ob der Kommunikationspartner überhaupt empfängt bzw. empfangen kann

Bild: Verbindungsorientierte vs. verbindungslose Kommunikation

Eine **verbindungsorientierte** Kommunikation (Connection-Oriented Mode, CO) wird durch eine Reihe von Funktionen unterstützt. Bevor eine Kommunikation zwischen zwei (n+1)-Instanzen erfolgt, muss erst eine n-Verbindung hergestellt werden (Connection Establishment). Innerhalb einer Verbindung kann der Datenaustausch durch Merkmale wie Folgenummerierung, Reihenfolgesicherung, Fehlererkennung mit automatischer Wiederholung sowie Datenflusssteuerung sehr zuverlässig gestaltet werden. Die Parameter hierzu sind im allgemeinen Gegenstand eines gegenseitigen Abstimmungsprozesses beim Verbindungsaufbau. Sie sind selbst während einer Verbindung noch änderbar. Die Verbindung wird nach Abschluss des Datenaustausches wieder abgebaut (Connection Release).

Der **verbindungslose** Datenaustausch (Connectionless Mode, CL). Ist einfacher. Diese Variante wird insbesondere für lokale Rechnernetze (LANs) interessant, wo die zuverlässige Kurzstreckenübertragung nicht in allen Kommunikationsschichten dieselben Funktionen wie Reihenfolgesicherung, Fehlerbehandlung und Datenflusssteuerung erfordert. Das Konzept ist auch in Weitverkehrsnetzen auf der Basis des Austausches voll adressierter, autonomer Pakete (Datagramm) realisiert worden.



4 Typen von Dienstprimitiven:

- Anforderung (Request)
- Anzeige (Indication)
- Antwort (Response)
- Bestätigung (Confirm)

Bild: Dienstprimitive

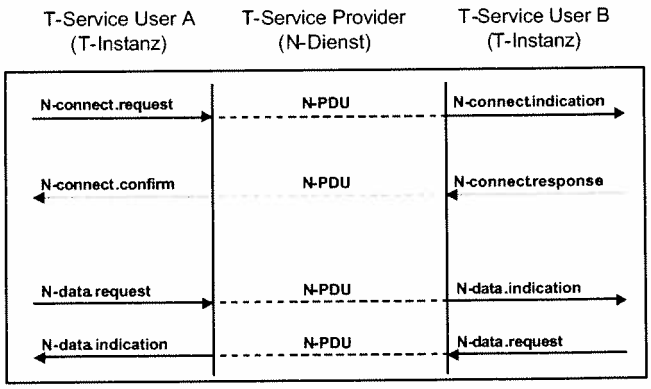


Bild: Dienstprimitive des Netzdienstes angefordert von der Transportschicht

Das Bild zeigt das Beispiel eines Transportverbindungsaufbaus, der von der Schicht 4 (T) initiiert wird und durch den Netzdienst (N) ausgeführt wird. Die übergebenen Parameter beziehen sich in diesem Falle auf die Adressen (Rufnummern) der rufenden und gerufenen Datenendeinrichtungen. Die Optionsdaten können die Anforderung eines beschleunigten Transports, Dienstparameter sowie Benutzerdaten sein. Der Verbindungsaufbau ist ein bestätigter Dienst. Danach erfolgt den Datenaustausch selbst. Dies ist ein unbestätigter Dienst.

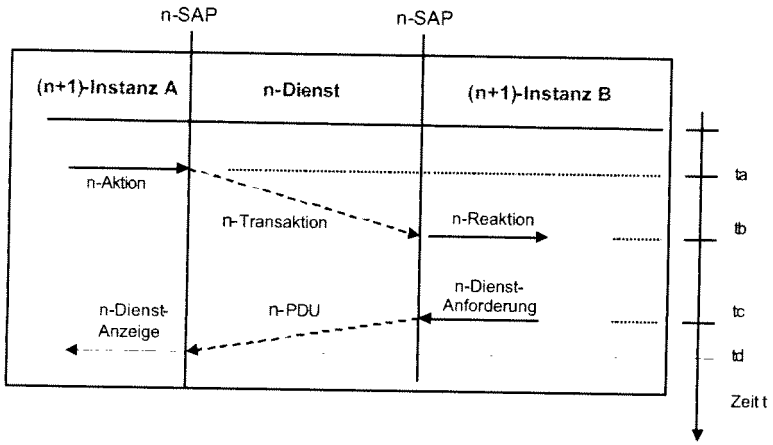


Bild: Zeitfolgediagramm

Die zeitliche Folge von Primitiven, welche zwischen benachbarten Schichten zur Dienst-anforderung benutzt werden, unterliegt im allgemeinen bestimmten Synchronisations-bedingungen. Zusammen mit dem Format der dazu benutzten Steuerdatenblöcke kann dieser Vorgang in Form eines Dienstprotokolls definiert werden. Die einzelnen Dienstprimitiven werden mit einer Parameterliste versehen und in einem Steuerdatenblock übertragen.

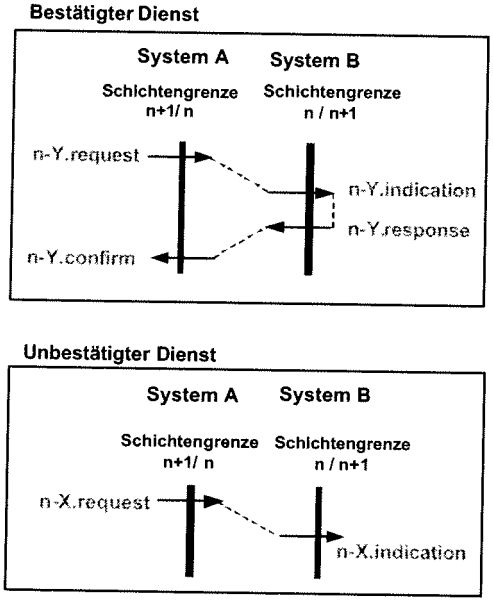


Bild: Kommunikation innerhalb Schicht n

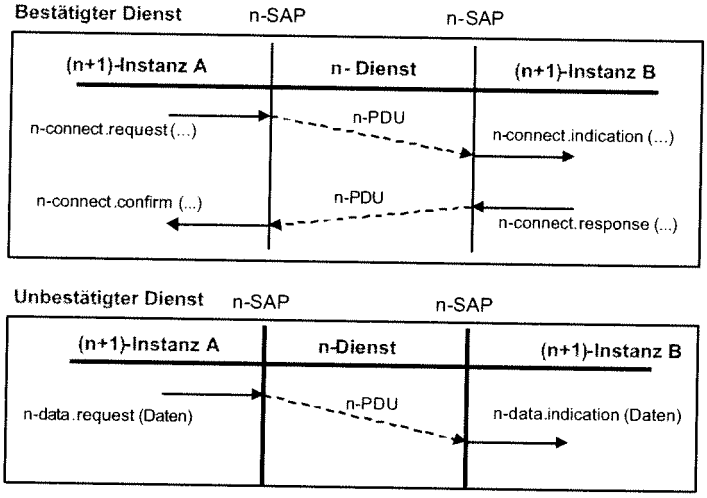


Bild: Kommunikationsabläufe

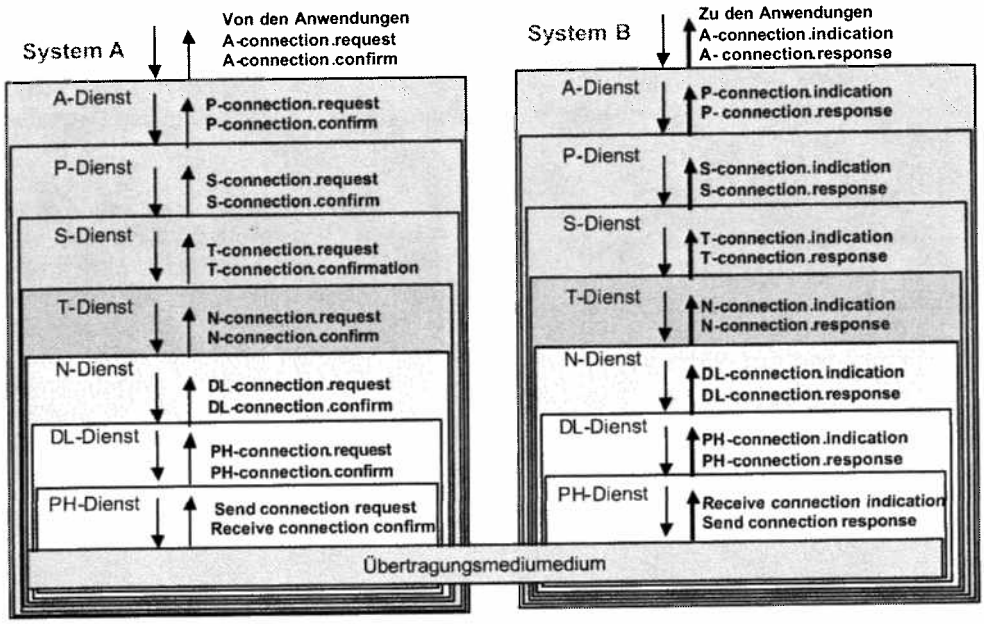


Bild: Verbindungsmanagement

Im Bild ist illustriert wie Dienstprimitive zwischen Protokollschichten ausgetauscht werden, um eine logische Verbindung zwischen zwei Anwendungs-Instanzen aufgebaut werden soll und nur der physikalische Dienst eingerichtet ist.

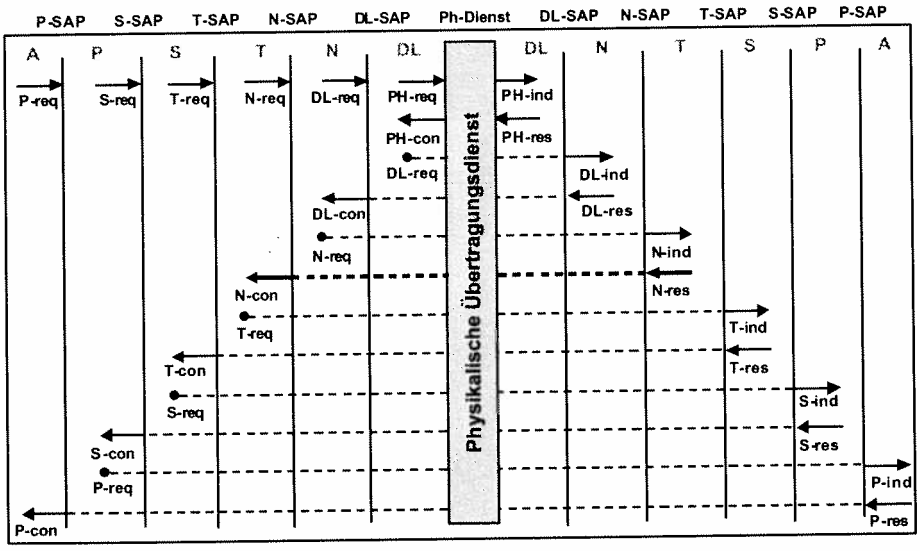


Bild: Zeitlicher Ablauf des Verbindungsaufbaus

Das Bild zeigt den zeitlichen Ablauf beim Aufbau einer logischen Verbindung zwischen zwei A-Instanzen für den Fall, dass nur der physikalische Dienst eingerichtet ist

Requests können nur weiter geleitet werden, wenn der Dienst darunter vorhanden ist.

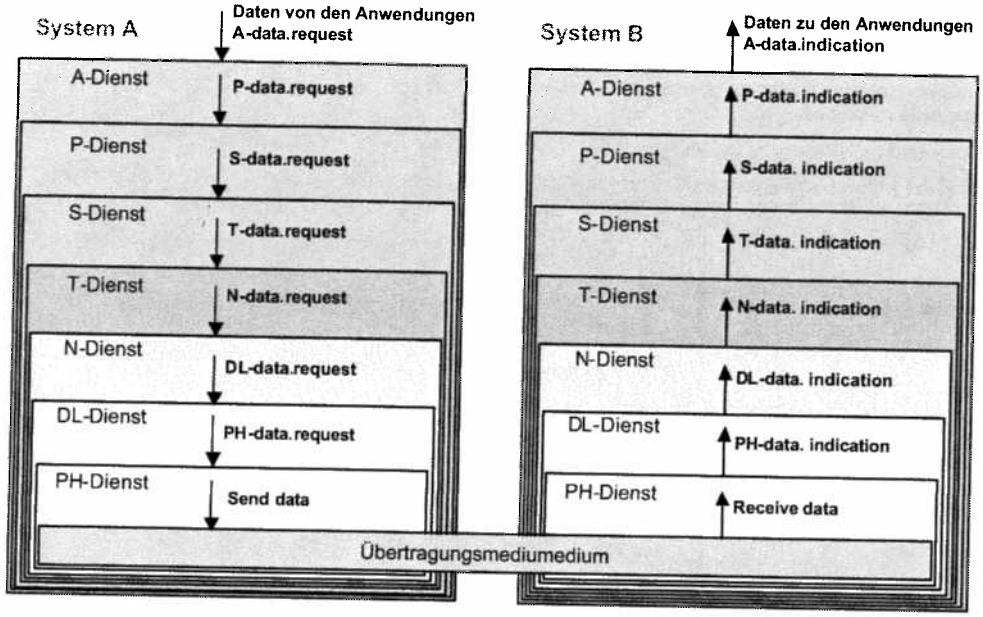


Bild: Datenaustauchprimitive

Das Bild zeigt alle Dienstprimitive, die zwischen den Protokollschichten ausgetauscht, wenn eine Anwendungs-Instanz Daten sendet und die Partner A-Instanz sie empfängt.

Daten zwischen Schichten werden immer unbestätigt ausgetauscht. Die Datenbestätigung geschieht immer zwischen Partnerinstanzen.

Beispiel: (n+1)-Daten, die durch n-Datenprimitive an einen n-Dienst übergeben werden, werden bei einer bestätigten Dienst durch die (n+1)-Instanzen gegenseitig bestätigt.

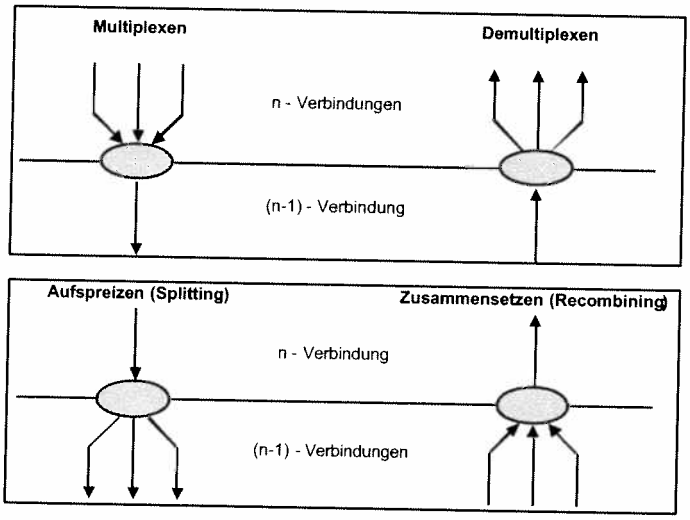
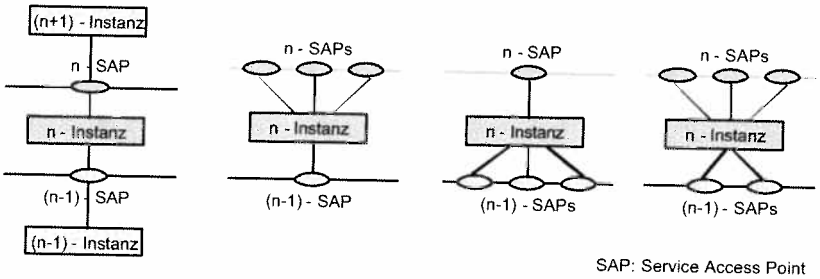


Bild: Verbindungsmanagement

Zur Leistungsanpassung können verschiedenen n-Verbindungen auf einen (n-1)-Verbindung zusammengefasst werden. Dieser Vorgang bezeichnet man als Multiplexen. Die Umkehrung ist Demultiplexing. Die (n-1)-Verbindung benötigt nur eine (n-1)-Instanz auf beiden Seiten. Es handelt sich hier um eine Konzentration.

Umgekehrt können verschiedenen n-Verbindungen auf mehrere (n-1)-Verbindungen verteilt werden. Dieser Vorgang bezeichnet man als Aufspreizen (Splitting). Die Umkehrung ist Zusammensetzen (Recombining). Die (n-1)-Verbindungen benötigt nun auch mehr (n-1)-Instanzen auf beiden Seiten. Es handelt sich hier um eine Expansion.



In Zusammenhang mit Multiplexen und Aufspreizen sind auch mehrere SAP-Kombinationen möglich.

- n-Instanz und (n+1)-Instanz, die über einen n-SAP verbunden sind, befinden sich im gleichen System
- (n+1)-Instanz kann mit mehreren n-SAPs verbunden sein
- n-SAPs können mit einer oder mehreren n-Instanzen verbunden sein
- n-Instanz kann mit mehreren (n+1)-Instanzen über mehrere n-SAPs verbunden sein

Bild: Beziehungen zwischen SAPs und Instanzen

- zu einem gegebenen Zeitpunkt ist ein n-SAP mit genau einer (n+1)-Instanz und genau einer n-Instanz verbunden
- n-SAP kann von einer n-Instanz und/oder einer (n+1)-Instanz getrennt und einer anderen n-Instanz und/oder (n+1)-Instanz zugeordnet werden
- n-SAP wird über seine n-Adresse lokalisiert
- Adresse wird von (n+1)-Instanzen bei der Anforderung einer n-Verbindung benötigt

Bild: Temporäre Beziehungen zwischen SAPs und Instanzen

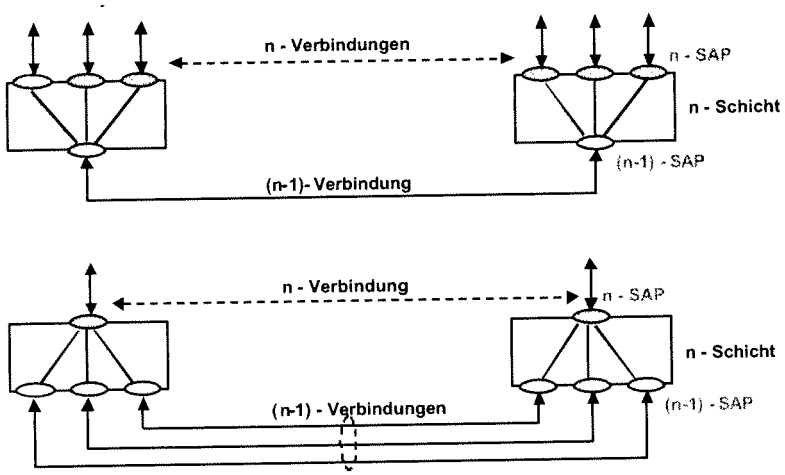


Bild: Multiplexen und Aufspreizen

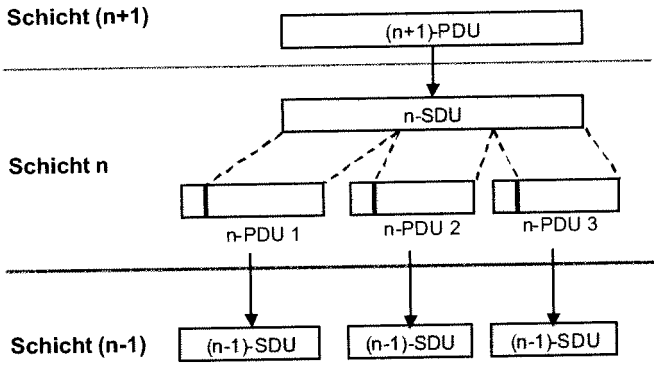


Bild: Aufteilen / Vereinigen

Zur Längenanpassung ist es manchmal notwendig, längere Dateneinheiten aufzuteilen. Dies ist zum Beispiel notwendig, wenn die maximal erlaubte Rahmenlänge der verwendeten Netztechnologie überschritten wird. Diese Einheit wird als MTU (Maximum Transfer Unit) bezeichnet. Jeder Teil des n-SDU erhält die Zusatzinformation PCI (Protocol Control Information). Die Umkehrfunktion ist die Vereinigung.

Beispiele für MTUs sind:

- ATM: 53 Bytes
  (5-Byte Header, 48-Byte Payload),
- Ethernet: 1518 Bytes
  (18-Byte Header, 1500-Byte Payload).

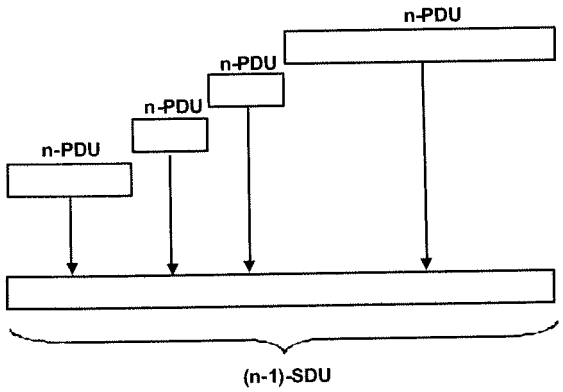


Bild: Verketten / Trennen

Eine Längenanpassung kann auch bedeuten, dass mehrere n-PDUs zu einem einigen (n-1)-SDU zusammengefasst wird. Dieser Vorgang als Verkettung bezeichnet. Der Umkehrvorgang heißt Trennen.

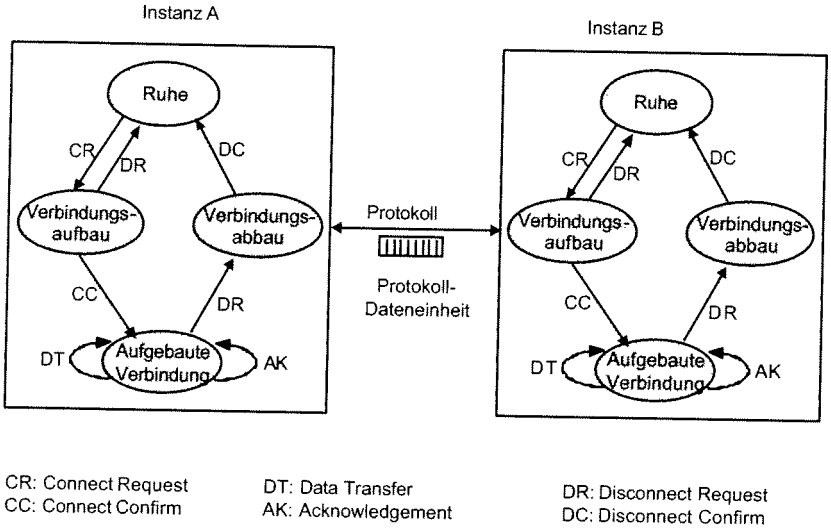


Bild: Kommunikation von Instanz-zu-Instanz

Eine Protokollinstanz ist ein Software-Prozess, der den Ablauf des Protokolls regelt. Zu jeder logischen Verbindung sind zwei Partner-Instanzen notwendig. Sie werden bei Aufbau einer logischen Verbindung generiert und bei Abbau der logischen Verbindung wieder gelöscht. Eine Instanz besteht aus einer Anzahl von Zuständen mit Übergängen dazwischen. Ein Übergang erfolgt durch ein eingehendes Ereignis (event) oder aufgrund einer intern ausgeführten Aktion. Eine Instanz ist somit das Gedächtnis des Protokollzustandes. Jede Instanz besteht im wesentlichen aus Zustandsdaten und einem Programmpointer (Zustand), der angibt welcher Aktion zuletzt ausgeführt wurde.

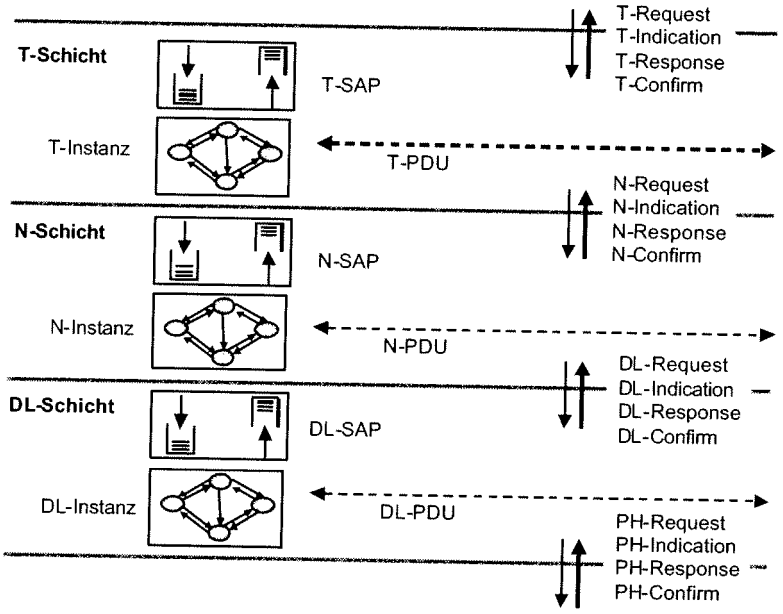


Bild: Peer-to-Peer und Schichten Kommunikation

Das Bild illustriert nochmals die Bezeichnungen des horizontalen und vertikalen Austausches von Dateneinheiten und die Lage der Dienstzugangspunkte (SAP).

Die Primitive haben immer die Bezeichnung des beanspruchten Dienstes.

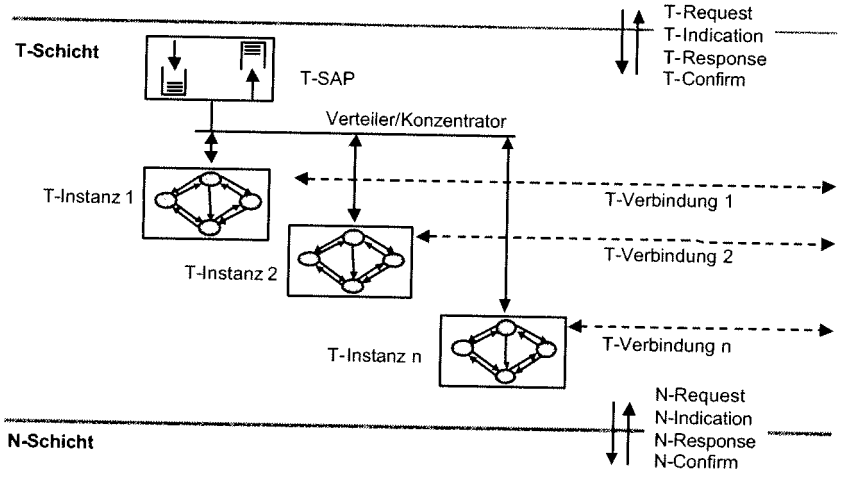


Bild: Peer-to-Peer Verbindungen

Das Bild weist nochmals daraufhin, dass ein Instanz-Paar für jede bgische Verbindung existieren muss. Im Bild ist auch zu sehen, dass mehrere logischen Verbindungen über einen Dienstzugangspunkt zur nächsthöheren Schicht geleitet werden können. In diesem Fall werden die Einzelverbindungen mit eine Verbindungskennung (Connection Endpoint Identifier, CEI) auseinander gehalten.

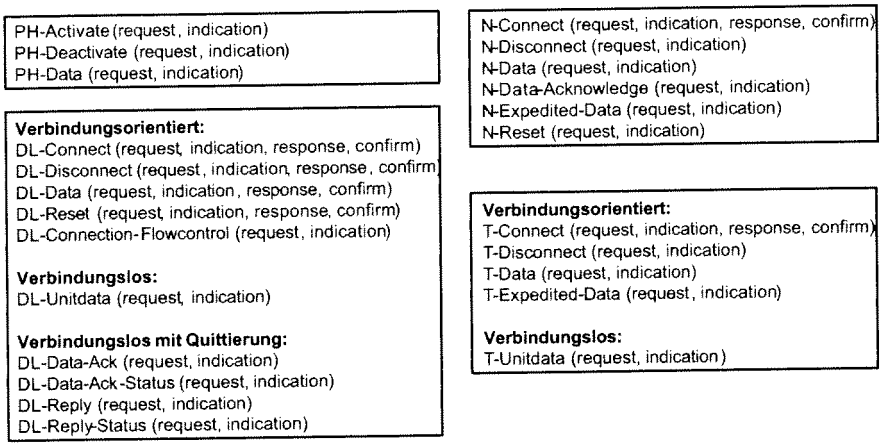


Bild: Zusammenfassung der Primitive der Schichten 1 bis 4

Im Bild sind die Primitive der unteren vier Schichten zusammengestellt.

- Auf der Bitübertragungsschicht spricht man von activate/deactivate statt connect/disconnect.
- Auf den Schichten 3 und 4 ist mit Expedited-Data einen priorisierter Datentransfer möglich.
- Auf den Schichten 2 und 4 wird unterschieden zwischen verbindungsorientierten und verbindungslosen Verbindungen.
- Beim verbindungslosen Betrieb verwendet man Unitdata.
- Auf Schicht 2 kann den verbindungslosen Rahmentransfer speziell quittiert werden.

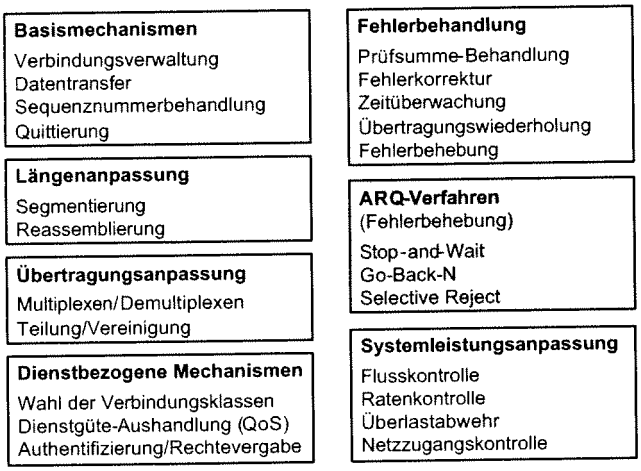


Bild: Gliederung von gemeinsamen Protokollmechanismen

Protokollmechanismen

Protokolle der verschiedenen OSI-Schichten enthalten zum Teil vergleichbare Funktionen. Deshalb gibt es gemeinsame und schichtenspezifischen Protokollmechanismen bzw. Protokollfunktionen Protokolle.

Im Bild sind die gemeinsamen Protokollelemente klassifiziert in sieben Bereiche.

- Die Basismechanismen werden unten kurz zusammengefasst.
- Die Längenanpassung und Übertragungsanpassung wurden oben in diesem Kapitel betrachtet.
- Die Fehlerbehandlung, die ARQ-Verfahren und die Systemleistungsanpassung werden im Teil 2 des Skripts behandelt.

Basis-Protokollmechanismen

Verbindungsverwaltung: Sorgt primär für den erfolgreichen Verbindungsaufbau. Eine Ablehnung der Verbindung durch den Empfänger (caller) oder den verwendeten Dienst wird dem Sender (Initiator, callee) mitgeteilt. Der Protokollmechanismus muss mit verlorenen, duplizierten oder verspäteten Datenblöcken zurechtkommen. Weiter realisiert er die bestätigte Dienstfunktion Verbindungsabbau (disconnect) und die unbestätigte Dienstfunktion Verbindungsabbruch (abort). Im ersten Fall können ausstehende Übertragungen noch ausgeführt werden, im zweiten Fall nicht.

Datentransfer: Dieser Protokollmechanismus wird fast überall benötigt, meistens bezieht er sich auf einen gewöhnlichen Transfer von Datenblöcken. Abhängig von der Schicht betrachtet man Rahmen (frames), Pakete (packets), Zellen (cells) oder Nachrichten (messages). Zusätzlich kann ein Prioritäts-Datentransfer (expedited data transfer) sinnvoll sein, dessen Daten vor den normalen Daten ausgeliefert werden. Die prioritären Daten können dabei früher gesendete, normale Daten überholen.

Sequenznummern: Für die Fehlerbehandlung (auch Auslieferung in der richtigen Reihenfolge) und die Systemleistungsanpassung sind nummerierte Datenblöcke erforderlich.

Quittierung: Der korrekte Empfang von Datenblöcken wird vom Empfänger quittiert. Dazu kann eine eigene Quittungseinheit (ACK, Acknowledgment) verwendet werden oder die Quittung wird einem Datenblock, das in der Gegenrichtung übertragen wird, mitgegeben. Diese Variante wird als Huckepack-Quittung (piggy back acknowledgment) bezeichnet. Quittungen können sich auf mehrere, korrekt empfangene Datenblöcke beziehen.