

1. HERSTELLERUNABHÄNGIGE KOMMUNIKATION

1.1 Rückblick

Sehr früh wurde von den Herstellern die Möglichkeit geboten, interaktiv mit ihren Computern zu arbeiten bzw. die Computer zu vernetzen. Jeder Hersteller entwickelte sein eigenes Verfahren:

- IBM - System Network Architecture (SNA)
- Digital Equipment - Digital Network Architecture (DNA)
- Siemens - Transdata
- u. a. m.

Die Verfahren sind nicht kompatibel, d. h. ein Computer der Firma A kann mit einem Computer der Firma B *nicht* kommunizieren.

Lösung:

- Emulation des Verfahrens der Firma A auf dem Computer der Firma B ($n^*(n-1)$ Emulationen)
- Herstellerunabhängige Verfahren bzw. Protokolle

Protokoll:

Ein Satz von Regeln für den Ablauf der Kommunikation zwischen zwei oder mehreren Partnern (z. B. Protokoll bei Hof, diplomatisches Protokoll).

1.2 OSI-Referenzmodell

OSI - Open System Interconnection

7-Schichtenmodell

- festgelegt von ISO (International Standard Organisation)
- Standards für Netzwerkaufbau
- Basis für die Kommunikation in unterschiedlichsten Netzwerken

Das Schichtenmodell wurde aufgrund einer eingehenden Analyse des Kommunikationsablaufs zwischen zwei Endstellen entworfen.

Sinn eines Schichtenmodells:

- Komplexität der Netzwerkkommunikation soll reduziert (bzw. in den Griff bekommen) werden, indem jede Schicht die Verantwortung über genau ein Teilproblem übernimmt.
- die einzelnen Schichten sind in sich abgeschlossen (mit wohldefinierten Schnittstellen)
- die benachbarten Schichten können davon ausgehen, dass die jeweilige Schicht "ihre Aufgabe ordentlich" erledigt
- überschaubar (geringere Komplexität: Vorteil bei Codierung und Fehlerlokalisierung)

1.2.1 Schichten des OSI-Referenzmodells

Schichten 1 bis 4 sind für die eigentliche, gesicherte Datenübertragung verantwortlich. Pro Schicht wird an die Daten der vorigen Schicht ein eigener Header angefügt. Jede Schicht gibt daher nach unten Daten mit einem bestimmten Aufbau (und einem bestimmten Namen) weiter:

Schicht	Bezeichnung der Dateneinheit
Application Layer	APDU (Application Protocol Data Units)
Presentation Layer	PPDU (Presentation Protocol Data Units)
Session Layer	SPDU (Session Protocol Data Units)
Transport Layer	TPDU (Transport Protocol Data Units)
Network Layer	Packets (Frames plus zugehöriger Header)
Data Link Layer	Frames (Bits plus zugehöriger Header)
Physical Layer	Bits

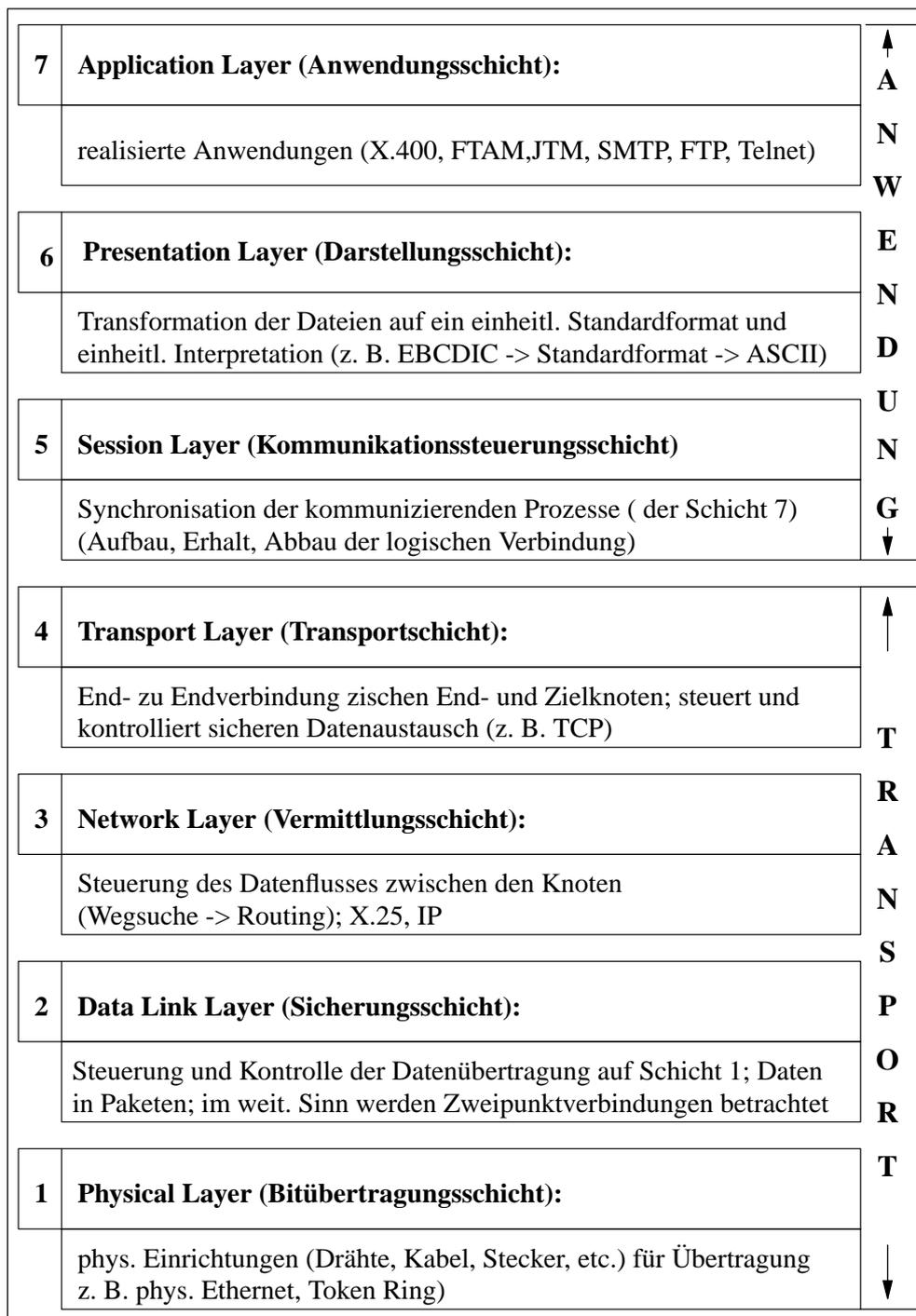


Abbildung 1. ISO/OSI Schichtenmodell

1.2.2 Normen im Bereich von OSI

Ursprünglich bestand die Absicht, eine OSI-Protokollfamilie zu definieren und zu implementieren. Diese Absicht wurde von der Entwicklung überholt (Internet mit TCP/IP). Geblieben ist daher primär das Referenzmodell als Hilfsmittel zum Entwurf, Darstellung und Analyse von Netzwerken, das nicht nur für OSI-Netzwerke nutzbar ist. Vereinzelt gab und gibt es noch Elemente aus der OSI-Protokollfamilie.

Physikalische Ebene - Layer 1

OSI, TCP u. a.:

Ethernet V2.0, IEEE 802.x, X.21

Data Link Layer - Layer 2

OSI, TCP u. a.:

Ethernet, V2.0 IEEE 802.x, Higher Level Data Link Protocol (HDLC)

Netzwerkebene - Layer 3

OSI:

X.25 (verbindungsorientiert, zusammen mit TP2)

TCP:

IP (verbindungslos; Datagram-Dienst)

Transportebene - Layer 4

OSI:

TP0: keine Flusskontrolle, keine Fehlerkorrekturen

TP1: einfache Fehlerkorrekturen

TP2: Multiplexen von Transportverbindungen und Flusskontrolle, sonst wie TP0

TP3: im wesentlichen Funktion von TP1 und TP2

TP4: wie TP3, zusätzlich Erkennung und Behebung von Fehlern, die von darunterliegender Schicht nicht erkannt werden; wurde von TCP abgeleitet.

TCP:

entspricht der Schicht 4 im OSI Referenzmodell

Applikationsebene - Schicht 7

OSI:

X.400 - E-Mail

FTAM - File Transfer

X.500 - Directory Service

JTM - Job Transfer Mode

X.3, X.29 - Remote Login

TCP:

SMTP - E-Mail

FTP - File Transfer

Telnet - Remote Login

REXEC - Remote Execution

RPC - Remote Procedure Call

NFS - Network File System

Kerberos - Identification/Authentication
LPR - Line Printer
WWW - World Wide Web
Archie
u.v.a.

2. NETZWERKTYPEN

Zusammenhang zwischen einsetzbaren Technologien und geographischer Ausdehnung:

- Lokale Netzwerke - Local Area Networks - LAN
- Weitbereichsnetzwerke - Wide Area Networks - WAN

Früher auch

- "Stadtnetzwerke" - Metropolitan Area Networks - MAN

um auch Netzwerke mit speziellen Techniken für mittlere Ausdehnungen (> LAN) zu erfassen. Heute gibt es diese Unterscheidung nicht mehr, weil

- sich LANs mit Einsatz spezieller Glasfasern (Monomodefasern) und Geräte weiter ausdehnen lassen, z. B. FDDI bis 40 km
- die Bezeichnung MAN für eine spezielle Technik, DQDB, reserviert ist, die auch wieder in WANs eingesetzt werden kann

3. ÜBERTRAGUNGSMEDIEN

3.1 Qualitätsmerkmale

- Übertragungsbandbreite:

Hz pro Sekunde

bit pro Sekunde

Baud: Signalgeschwindigkeit, gibt an, wie oft in der Sekunde das Signal seinen Wert (Spannung) ändert. Werden nur die Werte Null und Eins verwendet, dann sind Bitrate und Baudrate gleich

- Elektromagnetische Verträglichkeit (EMV, Electromagnetic Compatibility - EMC)

Auswirkung der elektromagnetischen Ausstrahlung auf die Umwelt (Funktionsstörungen, Gesundheitsstörungen)

- Dämpfung (Attenuation):

Energieverlust während der Signalausbreitung; das Signal ist keine einfache Welle, sondern besteht aus einer Reihe von Fourierkomponenten. Der Energieverlust ist für jede dieser Komponenten unterschiedlich, daher führt der Verlust nicht nur zu einer Verringerung der Amplitude, sondern auch zu einer Verzerrung und kann daher nicht mehr erkannt bzw. rekonstruiert werden. Es muss daher sichergestellt sein, dass das Signal verarbeitet wird, bevor es unkenntlich ist. Damit gibt es ein Limit für die maximale Signallaufzeit und als Folge eine maximale Kabellänge.

Die Dämpfung ist abhängig von der Kabelqualität und der Frequenz (Mhz). Je größer die Frequenz ist, umso stärker die Dämpfung. Für ein Kabel bestimmter Qualität (z. B. CAT5) ist eine maximale Dämpfung für bestimmte Frequenzen vorgegeben. Die Dämpfung wird in Dezibel (dB) angegeben.¹

- Laufzeitverzerrung:

Die Fourierkomponenten bewegen sich auch mit unterschiedlicher Geschwindigkeit. Dies kann dazu führen, dass die schnellen Komponenten eines Bits die langsamen Komponenten eines vorausgehenden Bits ein- bzw. überholen, die Bits vermischen sich und verursachen einen Übertragungsfehler.

- Rauschen

ist eine unerwünschte Energie von anderen Quellen, z. B. thermisches Rauschen, das durch Zufallsbewegungen von Elektronen verursacht wird. Der Rauschpegel beeinflusst die Dämpfung: fällt das Signal unter den Rauschpegel ab, ist es nicht mehr erkennbar.

Die wichtigste Rauschstörung ist das *Nebensprechen* (Near-End Crosstalk - NEXT). Es wird durch induktive Kopplung zwischen zwei eng benachbarten Drähten verursacht.

- Abhörsicherheit:

Aufgrund der elektromagnetischen Strahlung ist es möglich, das Signal auch mit Geräten zu empfangen, die *nicht* mit dem Kabel verbunden sind.

1. $\text{dB} = 10 \log_{10} \frac{S}{N}$
S: Signalstärke
N: Rauschstärke

3.2 Aerische und terrestrische Medien

Für den Aufbau der physikalischen Netzwerke stehen Kabel (terrestrisch) und drahtlose Einrichtungen (aerisch) zur Verfügung. In lokalen Netzwerken dominiert das Kabel, weil drahtlose Einrichtungen nicht die notwendige Übertragungskapazität oder Sicherheit bieten. Drahtlose Übertragung wird daher eingesetzt

- in Gebäuden, die nicht verkabelt werden können
- zur vorübergehenden Anbindung von Räumen und Gebäuden
- für mobile Stationen, z. B. in der Logistik
- zur Überbrückung von öffentlichen Einrichtungen (Straßen)

Im Weitbereich kann derzeit ein forciertes Ausbauen von Kabelnetzwerken *und* von drahtlosen Netzwerken festgestellt werden. Die große Anzahl neuer Telekomgesellschaften führt derzeit zu einer gewissen Trendumkehr. Während früher im Bereich Wähllamt - Endbenutzer (Local Loop) das Kabel und im Weitbereich drahtlose Einrichtungen forciert wurden, liegt nunmehr die umgekehrte Situation vor.

Häufig wird auch von einem Konkurrenzkampf zwischen Kabel und Satellit gesprochen. Zugunsten des Satelliten wird der niedrige Preis aufgrund der großen Übertragungsbandbreite angeführt. Dabei darf allerdings nicht übersehen werden, dass neue Techniken, wie Dense Wave Division Multiplexing (DWDM) die Kapazität von Glasfasernetzwerken enorm erhöhen. Darüber hinaus dürfte die Lebensdauer von Glasfaserkabel größer sein als die von Satelliten. Mit Hilfe von Satelliten können Gebiete, die keine Infrastruktur haben, rasch erschlossen werden, Informationen können an viele gleichzeitig übermittelt werden (Broadcast). Glasfaser dagegen ist weniger störanfällig und sicherer. Der Autor geht daher davon aus, dass beide Medien parallel und gezielt eingesetzt werden.

Aufgrund der Dominanz des Kabels - vor allem im LAN - werden die drahtlosen Übertragungseinrichtungen nur kurz angeführt.

3.2.1 Drahtlose Übertragungseinrichtungen

- Radioübertragung
 - rundstrahlend, daher keine sorgfältige Ausrichtung von Sender und Empfänger notwendig
 - durchdringt Gebäude
 - Leistung stark frequenzabhängig
 - reagieren stark auf Witterung und Störungen durch Elektroanlagen
- Mikrowelle
 - im Bereich ≥ 100 Mhz
 - erfordert Sichtverbindung zwischen den Stationen
 - stellt hohe Übertragungskapazitäten zur Verfügung
 - reagiert auf atmosphärische Störungen und erfordert daher Ausweichmöglichkeiten
 - ermöglicht den raschen Aufbau von leistungsstarken Netzwerken
- Infrarot
 - einfach und billig
 - durchdringt keine festen Gegenstände (abhörsicher)

- nur für den Betrieb in Räumen geeignet

- Laser

- erfordert exakte Ausrichtung von Sender und Empfänger
- kann Regen und starken Nebel nicht durchdringen
- gefährdet Lebewesen

3.2.2 Kabel

3.2.2.1 Koaxialkabel

- Aufbau:

Kern aus steifem Kupferdraht, umwickelt mit Isolationsmaterial; darüber zylindrischer Leiter (Drahtgeflecht), geschützt mit Kunststoffmantel

- Typen

50 Ohm für digitale Übertragung im LAN und WAN (Basisband)

75 Ohm für analoge Übertragung (Breitband)

- Nutzen einen Frequenzbereich bis zu 300 Mhz
- wird in Kanäle aufgeteilt (Mischung von TV, Audio, Datenübertragung)
- erfordert sorgfältige Ausmessung, bei Hinzufügen eines neuen Knotens muss neuerlich abgestimmt werden
- weit verbreitet (Kabelfernsehen, CATV)²

Nutzung für das Internet erfordert Rückkanal (Benützer muss auch senden können), sowie spezielle "Modems", um Geräte an CATV anschliessen zu können.

Standardisierungen sind im Gange:

- IEEE 802.14 (basiert auf ATM)
- Multimedia Cable Network System (MCNS) Data over Cable Service Interface Specification (DOCSIS) (basiert auf Ethernet)
- wird durch neue Techniken, wie z. B. ATM, abgelöst

- Reichweite

1 - 2 Gbps bei einem Kilometer

- Koax wurde bzw. wird im LAN durch Twisted Pair und Glasfaser, im WAN durch Glasfaser abgelöst

3.2.2.2 Verdrilltes Kabelpaar (Twisted Pair)

- Kupferkabel, je 2 Adern verdrillt (twisted)

Verdrillen reduziert elektromagnetischen Störungen durch benachbarte Leitungen

2. Solche Netzwerke sind interessant, um Internet und Telefonie zum Endbenützer zu bringen. Lokale Netzwerke wird man wegen der bestehenden Probleme mit dieser Technik nicht aufbauen. Eher wird man lokale Netzwerke mit geeigneter Technik (z. B. ATM) so erweitern, dass sie auch für den Transport von TV genutzt werden können. Daher werden im folgenden Text CATV-Netzwerke nicht behandelt.

- Typen
 - geschirmtes Kabel (Shielded Twisted Pair - STP)
 - ungeschirmtes Kabel (Unshielded Twisted Pair - UTP)
 - Screened Unshielded Twisted Pair (SUTP)
 - Einzelheiten siehe Anhang 1
- Verschiedene Kategorien (1 - 5) bzw. Klassen (A - D)
- Normen
 - EIA/TIA 568A + 568 B
Commercial Building Telecommunications Wiring Standard (USA)
 - ISO/IEC IS 11801
Generic Cabling for Customer Premises
 - EN 50173
Informationstechnik - Anwendungsneutrale Verkabelungssysteme (Europa)
- heute Klasse D bzw. Kategorie 5 (CAT5) üblich
 - 100 MHz Übertragungsbandbreite mit maximal 22 dB
erlaubt auch Geschwindigkeit von 155 Mbps, d. h. dass z. B. ATM auf zwei Kabelpaaren (vorwärts - rückwärts) möglich ist³
 - RJ45-Stecker
 - *Alle* Komponenten (Verbindungskabel, Dosen, Stecker etc.) müssen so konstruiert sein, dass die CAT5-Norm eingehalten wird
 - Längenbeschränkung zwischen den Endpunkten (max. 90 bzw. 100 m)
 - Konfektionierung:
4 Paare pro Kabel, üblicherweise werden aber nur zwei Paare pro Gerät benötigt (Ausnahme: Gigabit Ethernet)
 - Herstellung:
Lieferant muss mittels Messprotokoll nachweisen, dass die Verkabelung der Klasse D bzw. CAT5 entspricht
- Weiterentwicklungen: Klasse E und CAT6, sowie Klasse F und CAT7
 - derzeit Klasse E 250 Mhz und RJ45-Stecker, der verbessert werden muss, Klasse F 600 Mhz, Stecker noch nicht definiert
 - es ist noch kein Standard verabschiedet, Spezifikationen ändern sich noch
 - Klasse F erfordert auf jeden Fall Neukonfektionierung der Kabel mit Steckern, etc
 - Zukunft ungewiss, Initiative kommt aus Europa, Chancen hängen davon ab, ob USA mitziehen oder nicht
 - primär Reaktion der Kupferkabelhersteller auf Bestreben, Glasfaser bis zum Endgerät zu verlegen
 - Nachweis im Feld, ob Verkabelung tatsächlich CAT6 bzw. CAT7 ist nicht möglich

3. Dies ist nicht das theoretische Maximum nach dem Nyquist-Shannon-Theorem. Zur Theorie der Datenübertragung siehe z. B. Andrew S. Tannenbaum, Computernetzwerke, Prentice Hall

— *Es wird CAT6 und sogar CAT7-Verkabelung angeboten. Dies bedeutet aber nur, dass ein für CAT6 bzw. 7 geeignetes Kabel verlegt wird. Das Gesamtsystem ist aber nach wie vor CAT5.*

3.2.2.3 Lichtwellenleiter (LWL)

- Aufbau:

Kern aus Glasfaser mit Glasumhüllung mit niedrigerem Brechungsindex als Kern (hält gesamtes Licht im Kern), Ummantelung aus Kunststoff; Fasern werden gebündelt und mit Außenhülle geschützt

- Multimodefaser

Kerndurchmesser 50 Mikrometer (Europa) bzw. 62,5 Mikrometer (USA)

Licht wird mit LEDs (lichtemittierende Dioden) in die Faser eingespeist

Jeder Strahl wird im Kern reflektiert, aber mit einem verschiedenen Winkel; jeder Strahl hat anderen Modus, daher Multimodefaser

- Monomodefaser

Kerndurchmesser 8 bis 10 Mikrometer, lässt nur mehr eine Wellenlänge durch, daher Monomodefaser

Licht wird mit Laserdioden eingespeist, pflanzt sich ohne Reflexion fort

Reichweite 30 - 40 km mit hohen Datenraten (2,5 Gbps), wird laufend verbessert

- Wellenlängen:

850, 1300 und 1550 Nanometer

Jedes Band 25.000 bis 30.000 GHz breit

- Eigenschaften

geringe Dämpfung,⁴ (z. B. 850 nm 0,8 dB/km, 1300 nm ~ 0,3 dB/km)

unempfindlich gegen elektromagnetische Störungen

keine Emission, daher kein Problem mit EMV

keine gegenseitige Störungen in der Glasfaser selbst

- Weiterentwicklungen:

DWDM (Dense Wave Division Multiplexing), derzeit 64 Kanäle zu 2,5 Gbps, in Kürze 128 Kanäle zu 10 Gbps

Entwicklung von optischen Repeatern und Switches zur Vermeidung der opto-elektrischen Umsetzung zur Signalerneuerung bzw. Weiterschaltung der Signale

- Einsatz:

im WAN wird nur mehr Glasfaser verlegt, im LAN in den Ebenen 1 und 2

4. Dämpfung in Dezibel = $10 \log_{10}(\text{Übertragene Leistung}/\text{empfangene Leistung})$
Angabe erfolgt in dB/km

4. LOKALE NETZE

- Innerhalb eines Gebäudes oder zwischen Gebäuden einer Institution
- Ausdehnung zwischen 2,5 und 4 km
- Verbindet PCs und Workstations, auch Einbindung von Mainframes und Spezialrechnern

4.1 Verkabelung

Mit Einführung von Ethernet wurde die sternförmige Verkabelung für Terminalnetzwerke durch Busverkabelungen abgelöst. Heute wird wieder etagen- oder gebäudeweise sternförmig verkabelt:

- es können beliebige Strukturen hergestellt werden
- höhere Betriebssicherheit (nur ein Gerät pro Kabel)
- höhere Datensicherheit (Abhörgefahr wird reduziert)
- mehr Kapazität

3-Ebenen-Verkabelung nach den Normen EN 50173 und ISO/IEC 11801

- Ebene 1: zwischen den Gebäuden mit Glasfaser
- Ebene 2: Verbindung der Etagen im Gebäude mit Glasfaser
- Ebene 3: Etagen mit Twisted Pair Kabel
- Tendenz zum "Collapsed Backbone", d. h. Ebene 2 entfällt

Häufig wird Cable Sharing eingesetzt. Pro Kabel sind vier Adernpaare verfügbar, pro Gerät werden aber nur zwei gebraucht. Mit speziellen Steckern und Dosen ist es möglich, mit einem Kabel zwei Geräte zu versorgen. Dies reduziert die Kosten der Verkabelung. Bei Einsatz neuer Techniken, wie z. B. Gigabit Ethernet, wird aber die Anzahl der Anschlüsse halbiert. Auf der anderen Seite ist es fraglich, ob jemals bzw. wann mehr als 622 Mbps am Arbeitsplatz benötigt werden. Eine Neuverkabelung wird höchstwahrscheinlich mit Glasfaser bis zum Arbeitsplatz erfolgen.

Üblicherweise werden Endgeräte mit Kupferkabel an das Netzwerk angeschlossen. Lichtwellenleiter (LWL) (Fiber to the Office, Fiber to the Desk) haben jedoch Vorteile:

- weitaus größere Reichweite als Kupfer⁵ (erleichtert Errichtung von "Collapsed Backbone")
- kein Probleme mit elektromagnetischen Störungen
- kein Problem mit Cable Sharing, aufgrund der Eigenschaften des LWLs werden immer zwei Fasern pro Gerät reichen
- zukunftssicherer
- keine Normen wie für Kupferverkabelung (Steckervielfalt), an der Normierung wird jedoch gearbeitet
- neue Techniken in der Konfektionierung (Kleben statt Spleissen) verbilligt Arbeit und Geräte und kann daher auch vom eigenen Personal durchgeführt werden
- reine Verkabelung kaum noch teurer als Kupferverkabelung

5. Bisher konnte beim Einsatz von LWL die Reichweite ausser Acht gelassen werden. Mit steigender Frequenz (Mhz) kann aber die Reichweite der Multimodefaser nicht mehr ignoriert werden.

- Aktivkomponenten für LWL sind vor allem wegen der geringen Portdichte wesentlich teurer als die Komponenten für Kupfer

Obwohl Glasfaserkomponenten noch teurer sind als Kupferkomponenten, wird empfohlen, bei Neuverkabelungen einen Preisvergleich durchzuführen. Ein Collapsed Backbone benötigt weniger Platz (für Etagenverteiler) und weniger Aktivkomponenten. Beim Vergleich ist die höhere Lebensdauer der Glasfaserverkabelung (Verkabelungskosten!) und die unsichere Lage bezüglich der Weiterentwicklung der Kupferverkabelung zu berücksichtigen. Es muss allerdings auch angemerkt werden, dass 155 bzw. 622 Mbps, die auf Kupfer möglich sind, noch Jahre ausreichen werden. Höhere Bandbreiten bis zum Arbeitsplatz werden die Ausnahme sein.

4.2 Ethernet

Eigenschaften:

- logischer Bus
- Geräte sind an diesen Bus mittels Adapter (Netzwerkkarten) angeschlossen
- Daten des Senders sind auf gesamten Bus verteilt (Broadcast), jeder kann lesen !
- erfordert spezielles Verfahren, um Zugriff auf den Bus zu steuern:
 - CSMA/CD - Carrier Sense Multiple Access with Collision Detection
 - sendewilliges Gerät prüft, ob Bus frei ist
 - Bus ist frei, wenn **kein** Trägersignal (Carrier) vorhanden ist (daher Carrier Sense)
 - Gerät beginnt zu senden
 - Gerät muss weiterhin Trägersignal prüfen, weil auch andere Geräte mit Senden beginnen können (Multiple Access)
 - senden mehrere, sind Daten wegen Überlagerung unbrauchbar, es besteht eine Kollision, die erkannt werden muss (Collision Detection)
 - wenn Kollision, stellen *alle* das Senden ein
 - es wird für jedes Gerät eine Wartezeit berechnet, nach deren Ablauf wieder mit dem Senden begonnen werden darf
 - Stochastisches Verfahren
 - Anzahl der Kollisionen nehmen dramatisch zu, Nutzleistung geht gegen Null bis zum Zusammenbruch
- Geschwindigkeit: 10 Mbps (Megabit/sec)
- Broadcastmedium bzw. Shared Medium, d. h. alle Geräte, die mit einem logischen Bus verbunden sind, teilen sich die Kapazität

Typischer Aufbau:

- früher
 - Lichtwellenleiter zwischen den Gebäuden
 - Thickwire Ethernet Cable zwischen den Stockwerken (10Base5)
 - Thinwire Ethernet Cable in den Stockwerken (10Base2)
- heute Sternverkabelung

Komponenten:

- Netzwerkkarte (und Treibersoftware) im Gerät mit verschiedenen Anschlußtypen (BNC, RJ45, AUI)
- Netzwerkdose: Anschlußpunkt im Netzwerk
- Lobekabel, auch Patchkabel verbindet Karte mit Anschlußpunkt
- Repeater verbindet Kabel zum Gesamtnetz und erneuert Signal, bevor es aufgrund der Dämpfung nicht mehr rekonstruierbar ist; max zwei (Ethernet V2) bzw. vier (IEEE802.3) Repeater zwischen zwei Geräten
- Halfrepeater ist ein geteilter Repeater, dessen Hälften über Glasfaser verbunden sind
- Bridge verbindet zwei Ethernets

Probleme:

- Abhörgefahr
- Überlastung (stochastisches Verhalten)
- Abhilfe durch Segmentierung mittels Brücken (Bridges)

Varianten und Normen

- Ethernet Version 1.0 (DIX - Digital Equipment Intel Xerox), abgelöst von
- Ethernet Version 2.0 heute Industriestandard, allgemein im Einsatz
- IEEE 802.3 bzw. ISO 8802.3 unterscheidet sich von Ethernet V2.0 in einer einzigen Position des Ethernetframes
Koexistenz aber keine Kommunikation
physikal. Netze folgen dem 802.3-Standard

Weiterentwicklungen:

- 10BaseT: Standard für Twisted Pair (anstelle von Thinwire)
- 10BaseFL: Standard für Lichtwellenleiter
- 100BaseTX bzw. FX:
 - Standard für 100 Mbps Ethernet (Fast Ethernet)
 - nur mehr mit TP- oder LWL-Kabel
 - Netzwerkkarten und Geräte unterstützen 10 und 100 Mbps (Autosensing)
- 1000BaseX:
 - Gigabitethernet
 - ursprünglich nur für Glasfaser
seit Juli 1999 auch Standard (IEEE 802.3ab) für TP; es werden 4 (!) Kabelpaare verwendet
 - gegenüber 10 bzw. 100 Mbps Ethernet modifiziert (im Prinzip kein Ethernet mehr)
 - primär für Backbone und Anschluß von Server gedacht
- 10Gigabitethernet
 - im Entstehen begriffen

- derzeit nur für Monomode Glasfaserkabel
- zwei Versionen (10 Gbps und 9,95 Gbps)
- zweite Version setzt auf SDH (OC192/STM64) -> Einsatz im WAN
- kein CSMA/CD und nur Full Duplex; defacto kein Ethernet, es wird nur das Ethernet Frame verwendet
- 100BaseAnyLAN:
 - AnyLAN - sowohl Ethernet als auch Token Ring werden unterstützt
 - Twisted Pair 4*25 Mb
 - neue Zugriffstechnik (kein CSMA/CD), aber Gerätetreiber können weiterverwendet werden
 - entwickelt von Hewlett Packard u.a.
 - hat sich *nicht* durchgesetzt!

Switched Ethernet

beruht auf einer Weiterentwicklung der Bridges zu Multiport Bridges, jetzt Switches genannt:

- ermöglicht starke Segmentierung des Netzwerks in einzelne Ethernets
- im Idealfall pro Anschlußpunkt (Port) des Switches nur *ein* Gerät
- Bandbreite (10, 100 oder 1000 Mbps) stehen pro Port zur Verfügung
- mit TP- oder LWL-Verkabelung Full Duplex Betrieb möglich, d.h. es kann gleichzeitig gesendet und empfangen werden (Kapazitätsverdoppelung)
- erhöht Betriebssicherheit und reduziert Abhörgefahr
- Voraussetzung für One-to-Many bzw. Many-to-Many-Verbindungen (Multicast)

In die Ethernetstandards bzw. LAN Standards (LLC 802.1) wurden Funktionen für VLANs (802.1q) und Priorisierung (802.1p) eingebaut. Mit Link Aggregation soll es in Zukunft möglich sein, mehrere Ethernetkanäle zusammenzufassen, sodaß auch Zwischenstufen (z. B. zwischen 10 und 100 Mbps) möglich sind. Die Skalierbarkeit wird verbessert. Der Author rechnet damit, daß weitere Funktionen für Quality of Service (QoS) in die Standards eingebaut werden, damit isochrone Dienste besser servisiert werden können. Für den Einsatz von Telefonie wird empfohlen, die maximale Datenlänge (Maximum Transmission Unit) deutlich unter der maximalen Framelänge festzusetzen.

4.3 Token Ring

Eigenschaften:

- logischer Ring
- Geräte sind an diesen Ring mittels Adapter (Netzwerkkarten) angeschlossen
- Daten des Senders sind auf gesamten Ring verteilt (Broadcast), jeder kann lesen!
- erfordert spezielles Verfahren, um Zugriff auf den Ring zu steuern:
 - Token Passing
 - ein Gerät, das im Besitz des Tokens ist, darf senden
 - jedes Gerät auf dem Weg zum Empfänger prüft, ob es der Empfänger ist

- Empfänger prüft Daten und merkt fehlerfreie oder fehlerhafte Übertragung im Token an
- Token und Daten gehen zum Absender zurück
- Absender verarbeitet Informationen im Token
- Absender ist verpflichtet, den Token weiterzugeben, u. zw. auch dann, wenn er weiterhin Daten zum Senden hat
- Deterministisches Verfahren
 - Antwortzeit läßt sich in Abhängigkeit von der Anzahl aktiver Geräte genau bestimmen
 - Netzwerk bricht nicht zusammen, es steigen nur Antwortzeiten immens an
 - geeignet für Echtzeitsysteme
- Geschwindigkeit: 4 Mbps bzw. 16 Mbps (Autosensing)
- Broadcastmedium bzw. Shared Medium, d. h. alle Geräte, die mit einem logischen Ring verbunden sind, teilen sich die Kapazität

Typischer Aufbau:

- auch früher fast immer physikalischer Stern, kaum echte physikalische Ringe
- Lichtwellenleiter zwischen den Gebäuden und den Stockwerken bzw. Ringverteiler
- Twisted Pair vom Gerät zum Ringverteiler

Komponenten:

- Netzwerkkarte (und Treibersoftware) im Gerät
- Netzwerkdose: Anschlußpunkt im Netzwerk
- Lobekabel, auch Patchkabel verbindet Karte mit Anschlußpunkt
- Token Ring Verteiler verbindet die sternförmig verlegten TP-Kabel zu einem Ring; passives Gerät
- Bridge verbindet zwei Token Ring Netzwerke, max. sieben Bridges zwischen zwei Geräten

Probleme:

- Abhörgefahr
- Überlastung, auch bei deterministischem Verfahren
- Abhilfe durch Segmentierung mittels Brücken (Bridges)

Normen

- von IBM entwickelt
- IEEE 802.5 bzw. ISO 8802.5

Weiterentwicklungen:

- lange Zeit keine Weiterentwicklungen, IBM tendierte zu ATM mit 25 Mbps
- High Speed Token Ring (100 Mbps) fertig
- Gigabit Token Ring im Gespräch

Switched Token Ring analog zu Switched Ethernet

Vergleich Ethernet - Token Ring

Obwohl Token Ring theoretisch ein weitaus stabileres Verhalten hat als Ethernet, findet sich Token Ring primär in Institutionen mit IBM Equipment. Die TR-Installationen betragen nur ca. 10 % der Ethernet Installationen. Die höhere Bandbreite - Token Ring hatte ursprünglich nur 4 Mbps - und die geringeren Preise des Ethernets waren wohl ausschlaggebend. Dazu kommt, dass die Nachteile des stochastischen Verhaltens kaum oder nicht wirksam werden, weil aus Kapazitätsgründen die Netzwerke in kleinere Einheiten zerlegt wurden (Bridges und Router).

4.4 Fiber Distributed Data Interface (FDDI)

Eigenschaften:

- logischer Doppelring, daher sehr ausfallssicher (self healing)
- Geräte sind an diesen Doppelring mittels Adapter (Netzwerkkarten) oder Konzentratoren angeschlossen
- Konzentratoren (Dual Attached) zum Anschluß von Geräten mit FDDI-Adapter (Single Attached); billiger als Direktanschluß
- Zugriff auf den Ring wird mit Token Passing gesteuert (ähnlich wie Token Ring)
- Deterministisches Verfahren
- Wegen der hohen Kosten (insb. Adapter) wurde bzw. wird FDDI primär als Backbonenetzwerk zur Verbindung von Ethernet- oder Token Ring Netzwerke eingesetzt
- Geschwindigkeit: 100 Mbps
- Broadcastmedium bzw. Shared Medium, d. h. alle Geräte, die mit einem logischen Bus verbunden sind, teilen sich die Kapazität

Typischer Aufbau

- Dual Ring in Glasfaser für Backbone Netzwerk
- Stern zwischen Geräten und Konzentratoren (TP oder Koax)
- Translation Bridges zum Anschluß von Ethernet- oder Token Ring LANs
- Router zum Anschluß von Ethernet, Token Ring etc.

Komponenten

- Netzwerkkarte (und Treibersoftware) im Gerät
- Konzentratoren (Dual Attached) zum Anschluß von Geräten mit FDDI Adapter (Single Attached)
- Patchkabel (Glasfaser oder TP bzw. Koax)
- Translation Bridges oder Router

Probleme: ähnlich Ethernet bzw. Token Ring

Normen:

ANSI X39T, ISO 9314 Standards

Weiterentwicklungen:

- CDDI - Copper Distributed Data Interface:
Twisted Pair zwischen Gerät und Konzentrador
- FDDI-II:
Erweiterung für isochrone Dienste, z. B. Sprachübertragung
- FFOL:
FDDI Follow up

Switched FDDI analog zu Ethernet

FDDI verliert zusehends an Bedeutung, Neuinstallationen gibt es kaum noch. Die Weiterentwicklungen wurden aufgegeben. Die relativ junge Technik ATM ist für Sprach- und Multimedia (isochrone Dienste) wesentlich besser geeignet als Weiterentwicklungen von FDDI. ATM-Komponenten waren rasch billiger als FDDI-Komponenten. Neue Netzwerke für anspruchsvolle Dienste wurden daher mit ATM gebildet, FDDI-Netzwerke wurden auf ATM umgerüstet. Die Weiterentwicklung von Ethernet zu Fast Ethernet, das wesentlich billiger ist als FDDI, führte teilweise sogar zur Aufgabe von FDDI in einfachen Datennetzwerken, obwohl FDDI im Vergleich zu Fast Ethernet Vorteile hat (deterministisches Verhalten, Redundanz).

4.5 Zusammenfassung

Die angeführten Techniken sind "Shared Media" bzw. "Broadcast Media". Dies bedeutet

- jedes aktive Gerät kann den gesamten Verkehr mitverfolgen
- die aktiven Geräte teilen sich die Kapazität

Für bestimmte Anwendungen

- Multicast (one-to-many, many-to-many)
- Broadcast (to-all)

ist dies ein Vorteil. Die Nachteile (Abhörgefahr, Kapazitätsengpässe) überwiegen aber. Durch Switching werden die Nachteile reduziert, ev. sogar eliminiert. In Hinblick auf die steigende Bedeutung von Multicast scheinen diese Techniken in ihrer Switched Version ideal zu sein. Es handelt sich aber nach wie vor um "Shared Media", weil es die Technik nicht erlaubt, Punkt-zu-Punkt-Verbindungen mit einem reservierten Kanal aufzubauen. Ab bzw. bis zu einem Sammelpunkt wird die Übertragungseinrichtung der Technik entsprechend wieder gemeinsam (shared) verwendet.

4.6 Virtuelle LANs (VLANs)

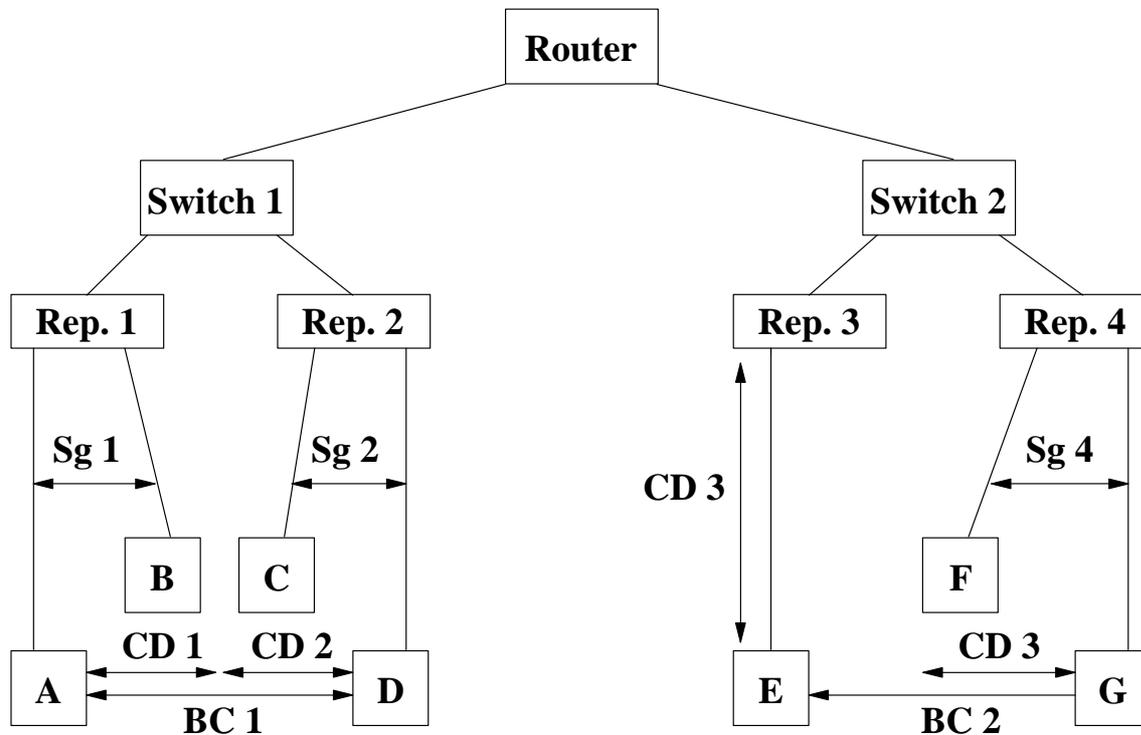
In einem LAN existieren folgende Komponenten:

- Segment: eine Übertragungseinrichtung, die zumindest zwei Geräte miteinander verbindet. Eines dieser Geräte kann ein Repeater sein.
- Repeater: ein Gerät, das zumindest zwei Segmente miteinander verbindet. Ein Repeater sorgt dafür, dass ein Signal, das in einem Segment entsteht, auf alle anderen Segmente übertragen wird. Alle Geräte, die über Repeater verbunden sind, gehören *einem* Collision Domain an. Der Zugriff innerhalb eines Collision Domains wird über einen Algorithmus gesteuert, z. B. CSMA/CD (s. Anhang 3).
- Bridge: ein Gerät, das ein Collision Domain in zwei oder mehrere⁶ Collision Domains trennt. Alle Collision Domains, die über Bridges verbunden sind, bilden *ein* Broadcast Domain, d. h. eine Nachricht, die als Broadcast versendet wird, geht an alle Geräte im Broadcast Domain. Ein Broadcast

6. man spricht dann von Multiport Bridges bzw. Switches

Domain ist *identisch* mit einem LAN.

- Router: ein Gerät, das ein Broadcast Domain in zwei oder mehrere Broadcast Domains trennt.



Legende:

Rep: Repeater

Sg: Segment

CD: Collision Domain

BC: Broadcast Domain

Entnommen aus: Robert Breyer, Sean Riley, *Switched, Fast and Gigabit Ethernet*, 3. Edition, S 167

Abbildung 2. LAN

Werden Switches mit entsprechender Software eingesetzt, dann ist es möglich, Broadcast Domains weitgehend unabhängig von der physikalischen Anbindung zu bilden, z. B. über Stockwerke und Gebäude hinweg. Auf diese Weise entstehen virtuelle LANs (VLANs). Ein Broadcast in einem VLAN wird an alle Geräte dieses VLANs verteilt, egal wo sich das Gerät befindet. Der Switch sorgt aber auch dafür, dass das Broadcast nicht an alle an ihn angeschlossenen Geräte verteilt wird, sondern nur an jene, die zum betroffenen VLAN gehören.

Merkmale:

- die Geräte eines VLANs bilden ein Broadcast Domain

- es gibt keine physikalischen Grenzen bei der Bildung von VLANs
- VLANs können nur über Router miteinander kommunizieren. Es gibt spezielle Switches, die auch Routingfunktionen haben (Layer 2/Layer 3 Switches), was die Kommunikation beschleunigt.
- ein Gerät kann Mitglied mehrerer VLANs sein. Dies ermöglicht den Zugriff auf einen Server aus mehreren VLANs ohne Router. Router sind Mitglied jedes VLANs, das sie bedienen.
- VLANs erhöhen die Sicherheit, weil sie die Bildung von logisch zusammengehörigen Gruppen erlauben und diese von einander abgrenzen.
- es wird angestrebt, die Technik so zu entwickeln, dass die Ortsänderung eines Rechners eines VLANs ohne manuelle Eingriffe erkannt wird und sich das Netzwerk quasi selbst rekonfiguriert.

Typen von VLANs:

- Port Based
 - leicht zu installieren und überschaubar
 - erfordern manuelle Verwaltung
 - erfordert Rekonfiguration bei Ortsänderung
- MAC Address Based
 - bleibt im VLAN bei Ortsänderung (Adresse wandert mit)
 - erfordert manuelle Eingabe der Adresse, aber wenig Aufwand im Switch beim Betrieb
- Layer 3 Protocol Base
 - hohe Flexibilität bei Ortsänderung
 - relativ hoher Aufwand im Switch
- Layer 3 Address Based
- Layer 3 Subnet Address Based
- Layer 4 Port Based
- Kombination verschiedener Verfahren.

VLANs wurden erstmals im Zusammenhang mit ATM vom ATM Forum spezifiziert. Seit 1999 gibt es auch einen Standard für herkömmliche LANs (802.1Q). Trotz des angestrebten Ziels, die Rekonfiguration zu automatisieren, ist der Verwaltungsaufwand doch sehr groß. Ortswechsel sind nicht die einzigen Änderungen, die ein VLAN betreffen. Es ist daher fraglich, ob sich VLANs tatsächlich durchsetzen werden. Es gibt Ansätze, pro Rechner bzw. Benutzer festzulegen, was mit wem getan werden darf.⁷ Das Prinzip des benutzerbezogenen Ansatzes soll als Directory Enabled Networks (DEN) standardisiert werden.

7. Z. B. Fast Secure Ethernet von Cabletron.

5. WEITBEREICHSNETZWERKE - WIDE AREA NETWORKS (WAN)

Zum Aufbau von WANs werden Telefonleitungen (Standleitungen, leased lines) bzw. Festverbindungen oder Dienste der Telekoms verwendet.

5.1 Standleitungen - Festverbindungen

- immer Punkt-zu-Punkt-Verbindungen
- beliebige Strukturen
- bei Einsatz von entsprechenden Endgeräten können Netzwerke aufgebaut werden, die den Diensten der Telekoms entsprechen

5.2 Dienste

No Broadcast Multiple Access (NBMA):

- beliebig viele Teilnehmer werden an das den Dienst realisierende Netzwerk angebunden
- jeder Teilnehmer kann mit *einem* Anschluß mit n ($n \geq 1$) Teilnehmern virtuelle Verbindungen aufbauen
- die Verbindung wird nach Abschluß der Kommunikation wieder abgebaut (Switched Virtual Circuit - SVC)
- mittels Verschlüsselung oder Zugangskontrolle können Privatnetzwerke (Virtual Private Network - VPN) aufgebaut werden
- permanente Verbindungen (Permanent Virtual Circuit - PVC) stehen meistens ebenfalls zur Verfügung
- pro Anschluß kann mehr als ein PVC aufgebaut werden!

5.3 Standleitungen versus Dienste

Primär eine Frage der Kosten:

- Kosten der Festverbindung: Standorte
- Nutzung der Verbindungen: Kosten der Dienste oft Entfernungs-, Dauer- und Zeitabhängig; auch Grundgebühren
- Wartungs- und Betriebskosten: z. B. Kosten des eigenen Netzwerkteams
- Sicherheit des Betriebs: Kosten einer Backuplösung bei Leitungsausfall; bei Verwendung eines Dienstes ist dies Angelegenheit des Diensteanbieters

5.4 Beispiele für Dienste

Bei den angeführten Diensten handelt es sich eigentlich um Protokolle auf OSI Layer 2 oder 3, mit denen der Dienst aufgebaut wird. Die Telekoms verwenden Produktnamen zur Bezeichnung der Dienste, z. B. bezeichnet die Datakom Austria mit Datex-P einen auf X.25 basierenden Dienst.

5.4.1 X.25

- altes, sehr sicheres Protokoll (OSI Layer 3)
- verbindungsorientiert (wie Telefon)

- Paketdienste; Daten werden in Paketen unterschiedlicher Länge zerlegt und übertragen
- entstanden zu einer Zeit, in der Leitungsqualität sehr schlecht war
- daher umfangreiche Fehlerprüfung und -korrektur in den Netzwerkknoten
- Geschwindigkeit 300 bps bis 64 Kbps
- Varianten bis zu 2 Mbps (Maximum dieses Verfahrens)
- meisten SVCs, aber auch PVCs
- weltweit verbreitet; oft einzige Möglichkeit, qualitativ gute Verbindungen nach Entwicklungsländern aufzubauen

5.4.2 Frame Relay

- ähnlich wie X.25 (verbindungsorientiert, Paketdienst)
- OSI Layer 2
- bis zu 2 Mbps, Varianten bis zu 34 Mbps
- Standard kennt nur PVCs, proprietäre Lösungen bieten auch SVCs (Standard wird überarbeitet)
- effizienter als X.25, weil keine aufwendigen Fehlerprüfungen und -korrekturen im Netzwerkknoten
- erfordert Verbindungen mit hoher Qualität

5.4.3 B-ISDN

B-ISDN: Breitband ISDN

ISDN: Integrated Services Digital Network

- basiert auf MAN (Distributed Queue Dual Bus; IEEE 802.6) oder ATM (Asynchronous Transfer Mode)
- MAN bereits wieder bedeutungslos
- Kapazität nach oben praktisch unbeschränkt
- derzeit üblicherweise bis zu 155 Mbps
- nur wenig Funktionen von ATM werden von Telekoms angeboten
- derzeit nur PVCs mit konstanter Bitrate (Constant Bit Rate - CBR)

6. ASYNCHRONOUS TRANSFER MODE (ATM)

Für jede Aufgabe existiert(e) ein eigenes Netzwerk:

- Sprache (Telefonie)
- Daten (häufig Telefonleitungen, X.25)
- Fernsehen
- Bilder
- ?

Es ist kein Kapazitätsausgleich möglich. Es wurden daher Verfahren geschaffen, mit deren Hilfe mehrere Netzwerke auf einer physikalischen Verbindung abgebildet werden können (Multiplexing). ATM ist das bisher beste Verfahren für diesen Zweck, weil es aufgrund seines asynchronen Ansatzes freie Kapazitäten besser und ohne Rekonfiguration nutzen kann als synchrone Verfahren. Darüber hinaus bietet ATM die Möglichkeit, für jede Verbindung Parameter vorzugeben, die einzuhalten sind. Können die Parameter nicht garantiert werden, wird die Verbindung nicht aufgebaut. Auf diese Art und Weise können Anwendungen mit unterschiedlichen Anforderungen an Bandbreite, Übertragungszeit und Datenintegrität parallel effizient übertragen werden.

Parameter:⁸

- Quality of Service
Übertragungszeit, Variation der Übertragungszeit, Fehlerrate, Verlustrate, u. a.
- Traffic Descriptors:
minimale Kapazität, maximale Kapazität, u. a. (in Zellen zu je 53 Bytes)
- Service Categories:
konstante Bitrate, variable Bitrate, nichtspezifizierte Bitrate, u. a.

Diese Parameter können entsprechend den Bedürfnissen der Anwendung kombiniert werden. Z. B. für Videokonferenzen ist eine geringe Übertragungszeit und vor allem eine geringe Variation der Übertragungszeit (delay variation) erforderlich, während der Verlust eines Bildes nicht so gravierend ist. Bei Electronic Mail spielt die Übertragungszeit bzw. ihre Variation keine große Rolle, ein Verlust einer Zeile kann jedoch die gesamte Mail unbrauchbar machen.

Eigenschaften:

- Technik für WAN *und* LAN
- kein "Shared Medium", d. h. Kapazität steht jedem Gerät voll zur Verfügung
- Schnittstellen sind definiert für
 - 1,5 bzw. 2 Mbps
 - 25 Mbps
 - 34 bzw. 45 Mbps
 - 51 Mbps
 - 155 Mbps

8. unvollständig, nur beispielhaft

- 622 Mbps
- 2,5 Gbps (bereits verfügbar)

Normen:

Die Entwicklung von ATM wird primär von einer Benützervereinigung (ATM Forum) vorangetrieben, die eine Reihe von Spezifikationen entwickelt hat (<http://www.atmforum.com>).

Die International Telecommunication Union - Telecommunication Subsection (ITU-T) entwickelt Standards speziell für die Anwendung in WANs. Beide Gremien arbeiten eng zusammen.

Probleme:

In lokalen Netzen können die Eigenschaften von ATM nicht ausgeschöpft werden, weil die bestehenden Netzwerke nicht einfach abgelöst werden können. Es ist vielmehr notwendig, ATM und die bestehenden Netzwerke (Legacy LANs) zu integrieren. Die Abbildung von Ethernet und Token Ring auf ein ATM-Netzwerk wird als LAN Emulation (LANE) bezeichnet.

Die Weiterentwicklung von Ethernet mit preiswerten Netzwerkkadaptern hat dazu geführt, dass im Bereich von ATM (noch?) nicht jene Stückzahlen erreicht wurden, die für eine Produktion von preisgünstigen Adaptern und Switches notwendig sind. In LANs wird daher ATM primär im Backbone und zum Anschluß von Servern verwendet.

7. TENDENZEN

Shared Media haben den Nachteil, dass sich die aktiven Geräte die vorhandene Bandbreite teilen müssen. Dies hat zur Folge, dass die Kapazität des Netzwerks als zu gering empfunden wird, obwohl es nur wenig Anwendungen gibt, die wirklich mehr als 2 Mbps (full duplex) benötigen.

Tatsächlich besteht aber das Problem darin, dass mit diesen Techniken nicht garantiert werden kann, dass zwischen zwei Endgeräten eine bestimmte Bandbreite zu einem bestimmten Zeitpunkt für ein bestimmtes Zeitintervall zur Verfügung steht. Dies kann nur dann sichergestellt werden, wenn Bandbreitenmanagement erfolgt oder die Bandbreite so groß ist, dass sie auch während Spitzenzeiten nur gering belastet ist.

Mit ATM wurde ein derartiges Management eingeführt, was vorerst ATM auch begünstigte. Aus Kostengründen hat sich ATM bis zum Desktop bisher nicht durchgesetzt. Im WAN haben die Telekoms nur wenig der ATM-Spezifikationen implementiert. Multimediaanwendungen bzw. zeitkritische Anwendungen, die gewisse Garantien benötigen, werden aber auch noch nicht sehr häufig verwendet, sodass dies noch nicht sehr problematisch ist.

In den USA besteht derzeit die Tendenz, die Probleme mit Bandbreitenvergrößerung zu lösen. Ist die Bandbreite groß genug, dann ist die Wahrscheinlichkeit, dass für (zeit)kritische Anwendungen die notwendigen Ressourcen und Bedingungen nicht vorliegen, gering. Der Aufwand für Bandbreitenmanagement kann daher eingespart werden. Netzwerkadapter und Geräte können daher billiger hergestellt werden. Da Europa den USA nachfolgt, kann es durchaus geschehen, dass ATM trotz seiner Vorteile nicht überlebt.

Theoretisch ist Bandbreite kein Problem. Mit Wave Division Multiplexing (WDM) können derzeit pro Glasfaserpaar $10 \times 2,5$ Gbps übertragen werden. In Kürze werden es 128×10 Gbps sein. Es sind allerdings Monomodefasern notwendig, die in lokalen Netzwerken bisher kaum installiert sind. Darüber hinaus ist es zumindest derzeit fraglich, ob die Geräte so billig hergestellt werden können, dass ein ökonomischer Einsatz auch in lokalen Netzwerken möglich ist.

In WANs wird WDM eingesetzt, um die vorhandenen Glasfasern besser nutzen zu können und somit das teurere Verlegen zusätzlicher Fasern zu vermeiden. Dies bedeutet aber, dass gerade im WAN-Bereich **nicht** erwartet werden kann, dass unbegrenzte Bandbreite zur Verfügung steht. Bandbreitenmanagement wird daher notwendig sein.

Auch für lokale Netzwerke wurden und werden Techniken entwickelt, welche diesem Trend entsprechen (Gigabit Ethernet, 10Gigabit Ethernet etc). Trotzdem hat man das Problem von Kapazitätsengpässen. Sind im Durchschnitt mehr als 10 Stationen mit Fast-Ethernet-Anbindung aktiv, dann ist ein Gigabit-Ethernet-Kanal bereits überlastet. Es gibt daher auch bereits die ersten Normen, die ein Bandbreitenmanagement im Ethernet vorsehen. Ihre Anwendung wird ev. den Einsatz von ATM wieder stimulieren, nicht zuletzt deshalb, weil in ATM bereits jetzt 2,5 Gbps zur Verfügung stehen.

Es ist anzunehmen, dass in den nächsten Jahren Bandbreitenmanagement und simple Bandbreitenerhöhung im o. a. Sinn parallel eingesetzt werden. Vielfach wird damit gerechnet, dass mit steigendem Einsatz von Multimediapplikationen, ibs. Videokonferenzen, Teleteaching etc. ATM wieder forciert werden wird.

8. KOMMUNIKATIONSABLAUF IN NETZWERKEN

Das OSI Referenzmodell zeigt, wie eine Kommunikation abläuft:

- Die Daten durchlaufen alle Schichten nach unten und am Ende wieder nach oben. Schichtenrelevante Informationen werden hinzugefügt bzw. entfernt
- Die Schichten 1 - 3 können auf dem Weg mehrmals durchlaufen werden.
- Nur über die Schicht 3 können Netzwerke mit unterschiedlichen Techniken (Token Ring, Ethernet,..) miteinander verbunden werden. Die Schicht 3 legt den Weg durch das Netzwerk fest (Routing).
- Die Schicht 4 wird nur zweimal aktiv und bildet die Endpunkte des Transportweges (END-to-END Connection). Diese Schicht sorgt dafür, dass die Daten korrekt (Summenprüfung, Wiederanforderung) und in der richtigen Reihenfolge an die obere Schicht übergeben werden.

Die Kommunikation zwischen Protokollen gleicher Ebene erfolgt so, als ob keine anderen Protokolle (anderer Ebenen) involviert wären (Peer-to-Peer Communication).

Wie auf Ebene 1 und 2 gibt es auch auf Ebene 3 und 4 unterschiedliche Verfahren, z. B. X.25, IP, IPX auf Ebene 3, u. zw. unabhängig von den Verfahren auf Ebene 2. Daraus folgt, dass

- ein Endsystem sowohl auf Ebene 3 als auch auf Ebene 2 identifizierbar (=adressierbar) sein muss
- zwischen den Adressen auf diesen Ebenen eine Abbildung notwendig ist (Adress Resolution)
- es unterschiedliche Methoden für die Festlegung des Weges von Datenpaketen durch ein Netzwerk gibt (Routing)

Adressierung erfolgt nicht nur in den Transportschichten. Auch die Beziehung auf Applikationsebene (Client-Server) muss eindeutig identifizierbar sein, denn eine bestimmte Serverapplikation auf einem System kann parallel mehrere Clients bedienen.

8.1 Adressen in Netzwerken

Adreßabbildung und Adressierung auf Applikationsebene werden im Kapitel TCP/IP behandelt.

8.1.1 Geräteadressen (Schicht 2)

auch MAC-Level Adresse (Medium Access Control)

Ethernet, Token Ring, FDDI:

- 16- bzw. 48-Bit, gebräuchlich sind 48 Bit
- weltweit einmalig
- in der Hardware kodiert (aber überschreibbar)
- auch Multicastadressen

8.1.2 Netzwerkadressen (Schicht 3)

Die Gestaltung der Adressen ist protokollabhängig. So hat z.B. eine X.25 Adresse des Datex-P-Dienstes der Telekom Austria das Aussehen einer Telefonnummer (15 Stellen):

z. B. Uni Linz 232 2 6 73 1 034 xxx:

232 Österreich
2 Datex-P (der Post)
6 9,6 kbit/sec

73 Area Code
1 Zugangsart
034 laufende Nummer
xxx Subadresse

Im Internet Protocol (IP), Version 4, besteht eine Adresse aus 4 Okteten zu je 8 Bits. Sie wird in Netzwerk- und Hostadresse untergliedert (Details siehe Kapitel über Internet). In Version 6 besteht eine Adresse aus 128 Bit.

8.2 Routing

Routing findet sowohl auf Ebene 2 als auch auf Ebene 3 statt. Auf Ebene 2 ist dies aber so einfach, dass der Begriff "Routing" automatisch mit Ebene 3 in Beziehung gesetzt wird. Eine Ausnahme bildet das verbindungsorientierte ATM (Ebene 2), das ein ebenso komplexes Routing erfordert wie Protokolle der Ebene 3.

Zwei Verfahren:

- **verbindungsorientiert:**

beim Verbindungsaufbau (angestossen durch die Applikation) und *vor* Versenden des ersten Datenpakets wird der Weg durch das Netzwerk zwischen den Endpunkten fixiert. In jedem Netzwerkknoten erfolgt eine Eintragung in eine Tabelle. Da auf jeder physikalischen Verbindung mehrere logische Verbindungen realisiert werden können, besteht jede Eintragung aus vier Werten:

(physikal. Interface, logisches Interface) am Eingang
(physikal. Interface, logisches Interface) am Ausgang

Im Paket erfolgt ein Austausch der Werte (Labelswitching), das Paket wird am angegebenen Interface gesendet.

Vor- und Nachteile:

- dem schnelleren Transport (verglichen mit verbindungslosen Verfahren) steht Zeit für Verbindungsauf- und -abbau gegenüber. Effizient, wenn viele Pakete pro Verbindung ausgetauscht werden
- Pakete treffen in der gleichen Reihenfolge ein, mit der sie gesendet wurden, daher geringerer Aufwand auf Ebene 4
- Fällt ein Netzwerkknoten aus, muss die Verbindung neu aufgebaut werden

- **verbindungslos:**

Jeder Host und jeder Netzwerkknoten (= Router) enthält eine Routingtabelle. Im Endsystem enthält diese Tabelle meist nur die Information, zu welchem Router das Datagramm gesendet werden muss, wenn der Empfänger nicht im eigenem Netzwerk ist (Defaultroute).

Enthält die Tabelle des Routers einen Eintrag für das Netzwerk des Empfängers, dann wird das Paket auf dem angegebenen Interface gesendet bzw. dem Empfänger direkt zugestellt. Ansonsten wird die Defaultroute verwendet. Der Vorgang wird solange wiederholt, bis das Paket zugestellt oder gelöscht wurde.

Vor- und Nachteile:

- kein Verbindungsaufbau, dafür Berechnung des Weges in jedem Netzwerkknoten für jedes Datagramm
- jedes Datagramm kann einen anderen Weg nehmen, die korrekte Reihenfolge beim Empfänger ist daher nicht garantiert und muss in der Schicht 4 geprüft und hergestellt werden
- fällt ein Netzwerkknoten aus, wird das Datagramm sofort auf einen anderen Weg umgeleitet, wenn Alternativen existieren

Obwohl sich bei der Benutzung des Webs (Surfen) der Zielhost häufig ändert, ist nicht sicher, dass verbindungslose Protokolle für das Internet vorzuziehen sind, weil die Berechnung von Routen sehr aufwendig ist. Es werden daher Verfahren entwickelt,⁹ die vorkalkulierte Routen einrichten und versuchen, die Schicht 3 weitgehend zu reduzieren (Layer-3-Switching). Diese Tendenz wird durch ATM (verbindungsorientiert auf Schicht 2) verstärkt.

9. z. B. Multiprotocol Label Switching (MPLS)

9. TCP/IP

9.1 Aufbau

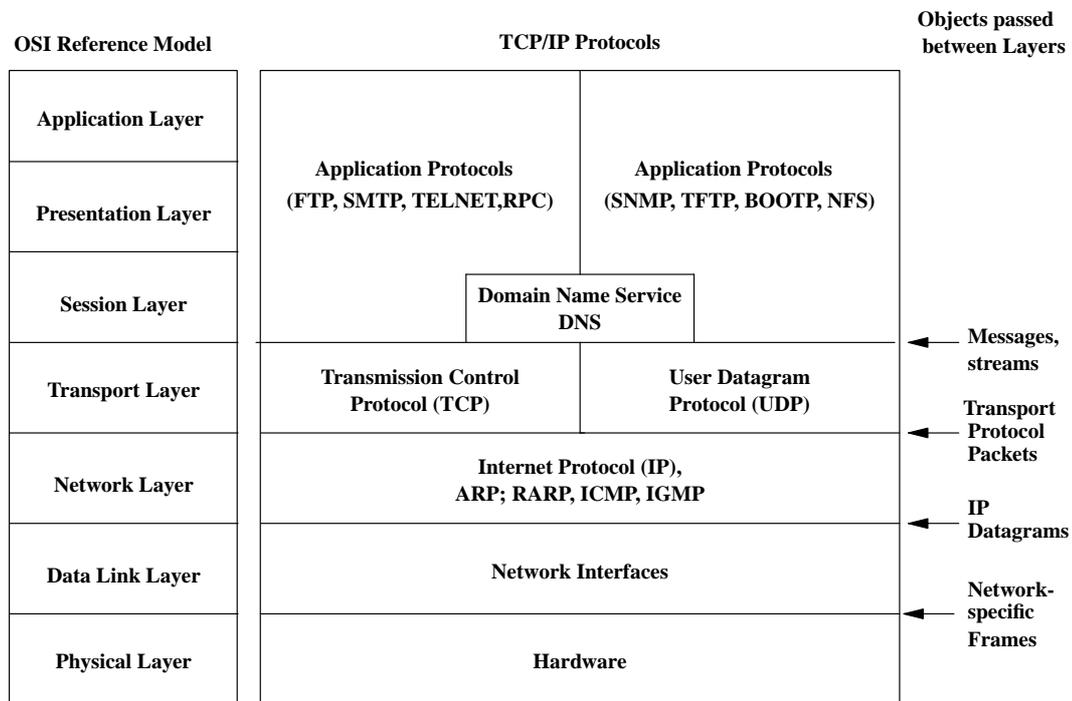


Abbildung 3. TCP/IP Protokolle¹⁰

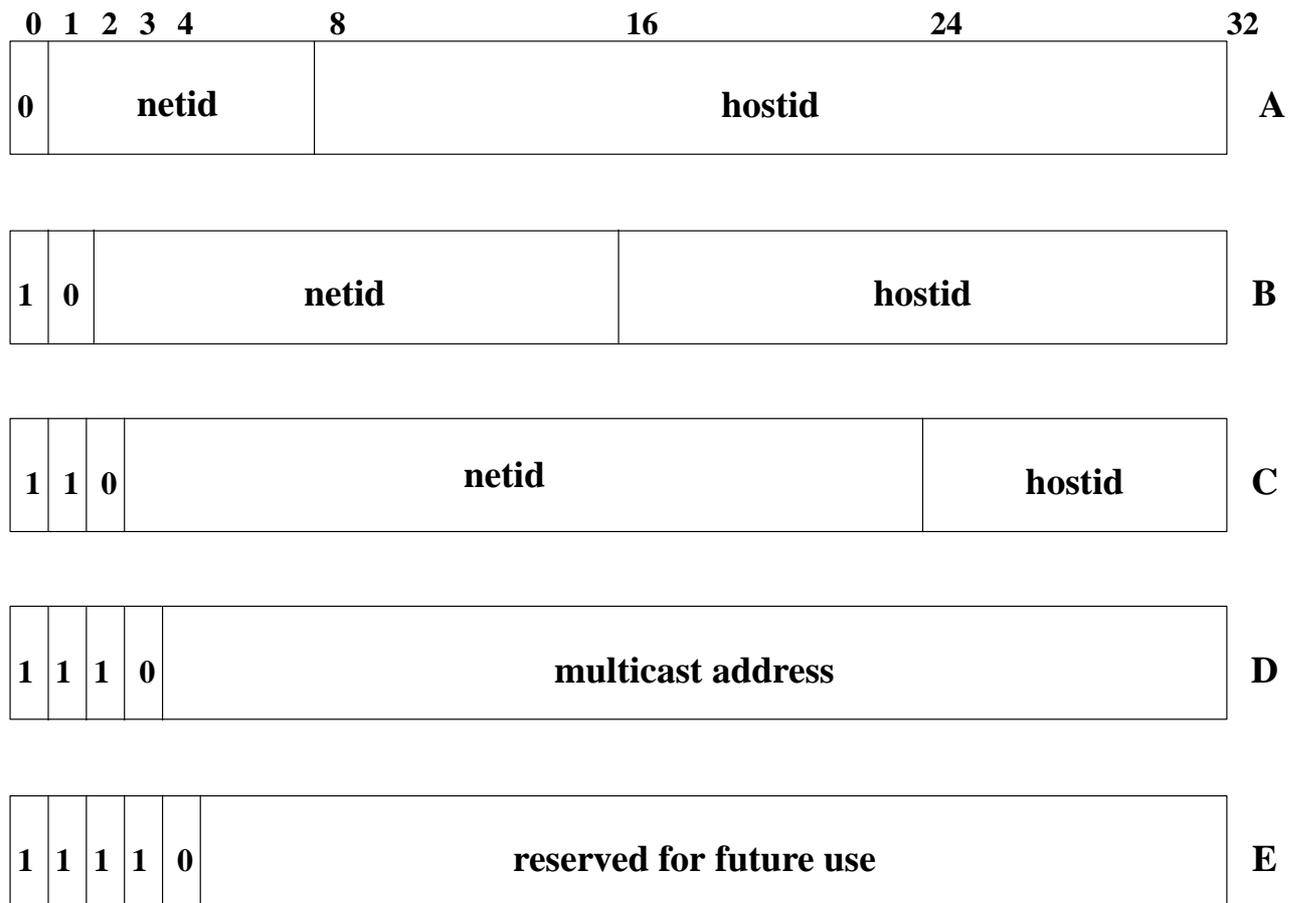
9.2 Adressen im IP (Schicht 3)

Adreissklassen

Class	Oktet	Verwendung
A	0 1-3	Netzwerkadresse (1-127) Hostadresse
B	0-1 2-3	Netzwerkadresse (ab 128 - 191.255) Hostadresse
C	0-2 3	Netzwerkadresse (ab 192 - 223.255.255) Hostadresse
D		multicast (ab 224)
E		reserviert (ab 240)

Eine Netzwerkadresse soll nicht mit 0, 127 oder 255 beginnen

10. entnommen aus: Kosiur, Dave, IP Multicasting, John Wiley & Sons, 1998, S 31

Abbildung 4. Adreßklassen¹¹**Spezielle Adressen**

- Hostadresse **0**
bedeutet "dieser Host", Netzwerkadresse **0** ist "dieses Netzwerk". Wird von Hosts benutzt, die ihre Adresse noch nicht kennen. Diese Adressen werden daher nicht vergeben (z. B. 128.6.4.0). In alten Implementationen wurde Hostadresse 0 als Broadcastadresse benutzt.
- Netzwerkadresse **127** ist für Loopback reserviert und wird zum Test auf der lokalen Maschine verwendet. Die Hostadresse ist beliebig, aber meist 1.
- **255** bedeutet Broadcast, z. B. 128.6.4.255, Broadcast im Netz 128.6.4.0. Jeder Host *muss* das Paket verarbeiten. 255.255.255.255 ist ein Broadcast im lokalen Netz und **nicht** im Internet und wird auch von 128.6.4.0 verstanden.

11. nach Douglas E. Comer, Internetworking with TCP/IP, Prentice HALL, 1991, S 62

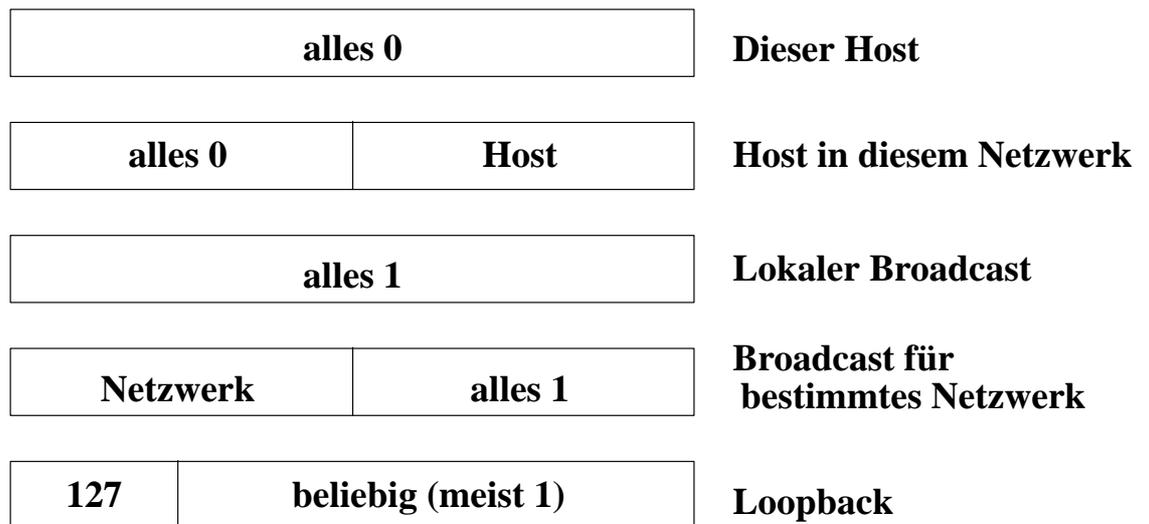


Abbildung 5. Adreßkonventionen (Zusammenfassung)¹²

9.3 Abbildung von Netzwerkadressen in MAC-Adressen

Abbildung von Netzwerkadressen auf Geräteadressen:

- Tabellen
- Address Resolution Protocol (ARP)
Mit Broadcast wird allen Rechnern im eigenem Netz mitgeteilt, dass die zu einer bestimmten IP-Adresse gehörige MAC-Adresse gesucht wird

Proxy ARP: ein Rechner gibt vor, der Gesuchte zu sein, empfängt die Daten und leitet sie weiter (Security!)
- Reverse Address Resolution Protocol (RARP)
ermöglicht Geräten ohne Festplatte, ihre IP-Adresse aufgrund der MAC-Adresse festzustellen (RARP Server)

9.4 TCP-Verbindungen

Grundsätzlich kann

- jeder Host Server und Client sein
- ein Service auf einem Host mehrere Clients parallel bedienen; die Clients können beliebig auf ein oder mehrere Hosts verteilt sein

Jede Verbindung zwischen *einem* Client und dem Server ist eine eigene Verbindung (connection), die eindeutig identifizierbar sein muss.

Port:

Eine 16-bit Nummer, die zur Unterscheidung zwischen Prozessen (auf einem Host) dient. Sie wird vom System an den Prozeß vergeben und ist auf dem jeweiligen System eindeutig

Well known Port: Eine Portnummer, die in engem Zusammenhang mit bestimmten Services steht (z. B. 25

12. nach Douglas E. Comer, Internetworking with TCP/IP, Prentice Hall, 1991, S 67

für SMTP). Ein derartiger Port darf vom Betriebssystem nicht vergeben werden.

Das Paar (IP-Adresse, Port) charakterisiert Endpunkte einer Verbindung:

- jeder Client erhält einen Port, der im lokalen System eindeutig ist (kein well known port!)
- jedes Service hat einen eindeutigen (well known) Port (z. B. Telnet 23)
- Die Kombination beider Paare, die in jedem Datenpaket aufscheint, identifiziert eine Verbindung *eindeutig*

9.5 Point to Multipoint (IP Multicast)

Multicast bedeutet, dass ein Paket an mehrere Empfänger gesendet wird, z. B. im Rahmen einer Videokonferenz. Multicast gewinnt zunehmend an Bedeutung. Die Engpaßprobleme im Internet, die quasi immer bestehen, erfordern den Einsatz von Proxyservern oder gespiegelten Servern. Die Verteilung der Datenbestände an diese Server erfolgt sinnvoll unter Verwendung von Multicast.

Die Quelle sendet nur ein Paket. Eine Vervielfältigung erfolgt erst dort, wo eine Verzweigung auftritt.

IP Multicast:

- Class D Adresse (nur Zieladresse, keine Sourceadresse!) charakterisiert Multicast Gruppe
- Multicast Gateways bzw. Router zum Transport über das Internet
- TTL (Time To Live) begrenzt Reichweite
- Benutzt Hardware Multicast (z. B. Ethernet Multicast Adresse wird aus 23 low order bits der IP Multicast Adresse erstellt)
- 224.0.0.1 all host groups dient zur Anmeldung an eine Multicast Gruppe (nur lokal, Weitergabe der Pakete erfolgt durch Router)
- Internet Group Management Protocol (IGMP) zum Austausch von Group Membership Informationen

MBone (Multicast Backbone) ist eine Infrastruktur, die über das Internet gelegt wurde und für Videokonferenzen oder Verteilung anderer Ereignisse verwendet wird.

MBone Communication Tools sind ein Satz von Programmen für Videokonferenzen, die im Rahmen von verschiedenen Projekten im Zusammenhang mit MBone integriert wurden.

9.6 Domainnamen

9.6.1 Prinzip der Domainnamen

Im allgemeinen sind Namen leichter merkbar als Adressen. Die Verwendung von Namen ermöglicht auch, Services nach Bedarf auf mehrere Hosts aufzuteilen bzw. zusammenzufassen oder zu verlagern.

Der Name eines Hosts (full qualified hostname) muss in einem Internet eindeutig sein. Eine Struktur ist daher notwendig:

hostname.domain-(n-x).....domain-(n-1).domain-1

Das äusserst rechte Domain (Top Level Domain, TLD) bildet die höchste Hierarchiestufe. Die Namen sind **nicht** "case sensitiv".

Top Level Domains:

- EDU, GOV, MIL, ORG, COM
Originaldomains, wurden in den USA festgelegt
- zweibuchstabile ISO Country Code für jedes Land, z. B. AT für Österreich
- TLDs, die vor kurzem geschaffen wurden:
 - FIRM - für Geschäftszwecke und Firmen
 - STORE - Für Geschäfte, die Waren zum Kauf anbieten
 - WEB - für Organisationen, die sich primär auf WWW Aktivitäten konzentrieren
 - ARTS - für Kultur und Unterhaltung
 - REC - für Freizeit und Unterhaltung
 - INFO - für Informationsdienste
 - NOM - für individuelle oder persönliche Nomenklatur

Unterhalb des TLD kann jedes Land frei gestalten, z. B. in Österreich

- AC - Academic
- OR - Organiation
- CO - Commercial
- GV - Government

Diese Einteilung ist in Österreich **nicht** mehr zwingend vorgeschrieben.

Das Domain bzw. sein Name sind im Internet bekannt und offiziell registriert. Innerhalb eines Domains kann weiter strukturiert werden, die dadurch entstehenden Subdomains sind aber nicht registriert.

Beispiel: Hostname im Domain donau-uni.ac.at

Um Mailssysteme flexibel gestalten zu können, wird in Mailadressen nicht der (full qualified) Hostname, sondern nur ein Teil davon, das sogenannte Maildomain verwendet, z. B.

user@donau-uni.ac.at

9.6.2 Abbildung von Domainnamen auf IP-Adressen

Tabellen:

Eine zentrale Stelle sammelt Hostnamen und ihre Adressen, faßt sie in einer Tabelle zusammen und verteilt sie. Dieses Verfahren reicht für kleine Netze, wurde aber im Internet rasch unhandlich und unbrauchbar.

Verteilte Datenbanken

Jedes Domain verwaltet für sich eine Tabelle und betreibt einen sogenannten Domain Name Server (DNS). Diese Server kommunizieren untereinander und bilden den Namen auf eine Adresse ab. Die Kommunikation entspricht der Struktur des Domainnamens. Die Auflösung beginnt bei den Root Name Servern.

- Root Name Server:
kennen die DNS aller Top Level Domains
- TLD Name Server:
kennen die DNS der nächsten Hierarchiestufe
- Für jede Stufe des Domainnames muss es einen DNS geben. Innerhalb des Domains kann weiter strukturiert werden (Subdomains).

9.7 IP Version 6 (IPv6)

Probleme mit IPv4

- limitierter Adressraum (32 bit)
- schwierige Konfiguration ibs. des Routings
- Probleme beim Providerwechsel (derzeit sind IP-Adressen an den Provider gebunden)

fürten Anfang 1990 zur Entwicklung eines neuen Protokolls, IPv6.¹³

Die wichtigsten Änderungen sind

- IP-Adresse mit 128 Bit (bisher 32)

Die Adresse wird, vereinfacht ausgedrückt, in einen Endbenutzer und in einen ISP-Teil unterteilt. Der ISP-Teil¹⁴ wird so strukturiert, dass die zum Routen notwendigen Informationen nach oben aggregiert werden und somit das Routing vereinfacht wird.

Adressen werden nur mehr dynamisch vergeben, der ISP-Teil muss erst dann hinzugefügt werden, wenn das Paket das lokale Netzwerk verlässt. Ein Wechsel des ISP erfordert keine Rekonfiguration.

- Leistungsverbesserung

Headerformat und Behandlung der Optionen wurde vereinfacht, ein Paket kann daher schneller verarbeitet werden.

- Erweiterung von Header und Optionen ist vorgesehen, auf neue Anforderungen kann daher rasch reagiert werden.
- Quality of Services

Spezielle Felder bzw. Optionen sind vorgesehen, um bestimmten Diensten ein verlangtes Service garantieren zu können¹⁵

- Sicherheit

Erweiterung für Authentication und Integrität

IPv6 ist ein neues Protokoll und kann daher nicht ohne weiteres eingeführt werden. Ein Übergang muss definiert werden, Gateways zwischen beiden Welten sind notwendig. Die gesamte Software, wie z. B. Routingsoftware muss für IPv6 adaptiert werden. Es war daher klar, dass der Adressraum von IPv4 vor seiner Ablöse durch IPv6 erschöpft sein wird. Es wurden daher Maßnahmen zur besseren Nutzung des Adressraums und für verbessertes Routing entwickelt:

- Classless Inter Domain Routing (CIDR)

IP-Adressen werden lückenlos aufsteigend in Gruppen vergeben. Im Routingprozess muss nur mehr die Gruppe und nicht jede einzelne Adresse geprüft werden

- Network Address Translation (NAT)

Die lokale Adresse¹⁶ wird beim Verlassen des lokalen Netzwerkes in eine offiziell vergeben Adresse

13. Für Details wird auf die IPv6 Home Page verwiesen: <http://playground.sun.com/pub/ipng/html/ipng-main.html>

14. Das genaue Format liegt noch nicht fest

15. IPv6 hat dafür nur beschränkte Möglichkeiten und bietet eigentlich nur "Best Effort"

übersetzt. Bei einem Providerwechsel muss nur der NAT-Prozess geändert werden. Da nicht jedes Gerät einen Zugang zum Internet benötigt bzw. da nicht alle Geräte parallel im Internet arbeiten, lässt sich durch NAT die Anzahl der notwendigen, offiziellen Adressen einschränken.

- Masquerading

Durch Manipulation des Ausgangsports kann mit einer IP-Adresse ein ganzes Netzwerk versorgt werden.

Die Umstellung von IPv4 auf IPv6 ist sehr aufwendig und langwierig. Es ist daher nicht sicher, dass das gegenwärtige Internet jemals auf IPv6 umgerüstet wird. Möglicherweise werden neue Anwendungen, wie z. B. Kontrolle von Verkehrsampeln etc, von vornherein auf IPv6 aufgesetzt. Defacto wird es dann über Jahrzehnte hinweg zwei Internets geben, die über Gateways miteinander kommunizieren und mit Hilfe von Encapsulation¹⁷ die Infrastrukturen gemeinsam nutzen.

16. Dies kann eine der sogenannten privaten Adressen sein, die im Internet nicht geroutet werden (10.0.0.0, 192.168.0.0 etc)

17. Ein IPv4 Packet wird in ein IPv6 Packet eingepackt (und umgekehrt)

10. HINWEISE ZUR PLANUNG VON NETZWERKEN

Planung ist nicht nur vor der erstmaligen Errichtung eines Netzwerks erforderlich, sondern auch für die laufende Anpassung des Netzwerks an geänderte Umweltverhältnisse. Sehr wichtig ist, parallel dazu das Netzwerkmanagement zu planen *und* zu installieren.

Das Netzwerkmanagement darf nicht aus finanziellen Gründen ignoriert werden. Störungen im Netzwerk müssen rasch erkannt und beseitigt werden. Ungebührlich lange Stillstandzeiten sind wesentlich teurer als ein Netzwerkmanagement. Die nachträgliche Einführung eines Netzwerkmanagements ist kostspielig und aufwendig, weil vielfach eine Reorganisation des Netzwerks erforderlich ist. Dies entspricht praktisch einer Neuplanung.

Planung inkl. des Netzwerkmanagements ist auf allen Ebenen erforderlich. Es gibt aber Größen, die relativ fix sind und daher Planung und Entscheidung erleichtern.

Ebene 1 (Kabel etc):

Die Verkabelung wurde ausführlich im Kapitel "Lokale Netze" diskutiert. Die erste Entscheidung muss zwischen Kupfer und Glasfaser unter Einbeziehung der Telefonie fallen. Wahrscheinliche Entwicklungen sind zu berücksichtigen. In Hinblick auf die geplante Entwicklung von Ethernet stellt sich im Backbonebereich bereits die Frage, ob Multimode oder Monomode Glasfaser gewählt werden soll.

Es müssten die Gesamtkosten für die geplante oder erwartete Lebensdauer der Verkabelung ermittelt werden. Manche Kosten, wie z. B. die Preise für Glasfaserports der Aktivkomponenten sind aber nur schwer zu bestimmen. Ebenso schwierig ist einzuschätzen, wie sich drahtlose Übertragungseinrichtungen und die Entwicklung im persönlichen Sektor (UMTS?) auf Nutzung und Gestaltung von Netzwerken, wie sie heute bekannt sind, auswirken werden.

Ebene 2 (LAN-Technik):

Ethernet dominiert im LAN, andere Techniken werden wahrscheinlich nur geringe Bedeutung haben oder verschwinden. Diese Entwicklung wird durch Switchen und Full Duplex unterstützt, weil keine Steuerung des Zugriffs auf das Netzwerk mehr erforderlich ist, d. h. die Unterschiede zwischen den Techniken verwischen bzw. bestehen nur mehr in den Formaten der Frames.

Ethernet ist wegen CSMA/CD keine Backbonetechnik (siehe jedoch oben) und hat auch Probleme bei der Rekonfiguration des Netzwerks im Störfall.¹⁸

ATM soll dort eingesetzt werden, wo effizientes Ressourcenmanagement notwendig ist. Die Priorisierung, wie sie derzeit in 802.1p existiert, garantiert keine absoluten Werte für Bandbreite, Delay, Jitter und andere QoS Größen.

ATM ist hervorragend geeignet, verschiedene Techniken (Ethernet, Token Ring etc.) in ein Netzwerk zu integrieren bzw. von einer Technik auf die andere zu migrieren.¹⁹

Wegen der geringen Stückzahlen sind die Kosten für ATM höher als die für Gigabit Ethernet. Dies mag auch dort zugunsten von Ethernet sprechen, wo ATM aus technischen Gründen vorteilhafter wäre. Dies kann bzw. wird dazu führen, dass die Entwicklung von ATM, insbesondere für den LAN Bereich, endgültig

18. Im Ethernet darf es keine parallelen Pfade zwischen den Geräten geben. Dies wird mit dem Spanning Tree Algorithmus sichergestellt. Physikalisch vorhandene Parallelwege dürfen daher erst nach Unterbrechung eines Weges aktiviert werden. Der Zeitaufwand ist so groß, dass die Verbindung zwischen Server und Client auf jeden Fall unterbrochen wird.

19. siehe Multi Protocol Over ATM (MPOA)

eingestellt wird.

Ebene 3 und 4

TCP/IP dominiert, alle anderen Protokolle verschwinden. Eine Entscheidung über IPV6 ist derzeit nicht aktuell, weil noch Unklarheiten bestehen und ein Mangel an ausgereiften Produkten bestehen. Der Einsatz von IPV6 und der Betrieb eines Gateways zu IPV4 würde den Einsatz von Spezialisten erfordern.

Leistungsfaktoren für Backbone²⁰

Folgende Faktoren müssen bei der Dimensionierung des Backbones berücksichtigt werden:

- Kapazität
 - Datenübertragung: Anzahl der Server x 1 Gbps²¹
 - Sprache: Anzahl Telefone x 0,5 x 256 Kbps
 - Video: Anzahl Desktops x 0,5 x 1,5 Mbps
- Mittlere und maximale Verzögerungszeit (Delay)
 - Filetransfer: 10 Millisekunden
 - Verteilte Datenbankanwendung: 1 Millisekunden
 - Performance Cluster: 0,1 Millisekunden
 - Sprache: 100 Millisekunden
 - Video: 40 Millisekunden
 - Bei Sprache und Video ist zusätzlich die Verzögerung des Endgeräts zu beachten
- Verfügbarkeit
- Fehlertrennung
- Skalierbarkeit
- Nutzungszeit

20. s. Jürgen Suppan, Gigabit-Ethernet als Königsweg?, in: Datakom, 4, April 2000, 17. Jahrgang, S 38ff

21. Bei den Kapazitätsangaben ist allerdings zu beachten, dass von Haus aus ein Gigabit Ethernet Anschluss bei den Servern angenommen wird. Ob dies derzeit erforderlich oder realistisch ist, sei dahingestellt. In einem Beispiel geht Suppan sogar davon aus, dass sämtliche Server parallel und permanent genutzt werden.

11. DIENSTE UND DIENSTEBIANBIETER

11.1 Transportnetzwerke

Transportnetzwerk: nationales oder internationales sogenanntes Backbonenetzwerk

Merkmale:

- Bestandteil des Internets
- bietet Transatlantikverbindungen
- eventuell auf bestimmten Benutzerkreis ausgerichtet
- häufig Mehrfachfunktionen (z. B. Internet Service Provider, geschlossene Benutzergruppen)
- Übergänge zu anderen Transportnetzwerken (Peering)
- keine Unterstützung bei Aufbau des Kundennetzwerks, Konfiguration von PC's, Nutzung der Internetdienste etc.

11.1.1 Rückblick

ab 1984

European Academic and Research Network (**EARN**)

- basiert auf IBM Technologie
- in Österreich seit 15. 7. 1985 über Universität Linz
- erster Ansatz eines akademischen Netzwerks in Österreich
- verwendet Standleitungen
- erste Versuche zum Aufbau eines europäischen Backbonenetzwerks
- existiert als Netzwerk seit 1997 nicht mehr
- Netzwerkinfrastruktur teilweise noch vorhanden

etwa zur gleichen Zeit **EUNET**

- in Österreich TU Wien
- basiert auf UNIX (UUCP)
- verwendet Wählleitungen
- wichtigster Beitrag: News
- mit Einsatz von IP kein Unterschied mehr zwischen Internet und EUNET
- EUNET verschwindet aus akademischen Bereich und wird kommerzieller Anbieter

ab 1990

erste Ansätze von Internet in Österreich

- internationale Anbindungen über Universität Linz und Universität Wien
- Aufbau eines akademischen Netzwerks in Österreich (ACONet)

ab 1992

Konzentration aller Aktivitäten an der Universität Wien

11.1.2 European Backbone Network (Ebone)

Ebone bietet ein europaweites Backbonenetzwerk mit Transatlantikverbindungen an. Es war ursprünglich als Übergang zu einer endgültigen europäischen Lösung (Europanet, TEN34, TEN155) gedacht, entwickelte aber seine eigene Dynamik und ist heute ein kommerzieller Anbieter.

Organisation

Ebone Verein

- Benützer konnten Mitglieder des Vereins und somit Eigentümer der Gesellschaft werden
- Mitgliedschaft "policy free"

Ebone Ltd.

- existierte seit ca. Mitte 1996
- Gesellschaft nach dänischem Recht
- stand im Eigentum des Ebone Vereins bzw. seit ca. Mitte 1998 mehrheitlich bzw. seit kurzem vollständig im Eigentum eines amerikanischen Infrastrukturproviders (Verein wurde aufgelöst)

Anbindung

EBS - Ebone Boundary System

- Anschlußpunkt für Kunden
- Leitungen zumindest zu zwei weiteren EBS
- mehrere Transatlantikleitungen
- Universität Wien betreibt EBS

RBS - Regional Boundary System

- regionaler Anschlußpunkt
- Kunden werden über diesen Anschlußpunkt gemeinsam an einen EBS geführt
- Backup zu einem weiteren EBS möglich

<http://www.ebone.net>

11.1.3 TEN-155

TEN-155 ist ein europäisches Forschungsnetzwerk auf ATM-Basis, das ein Backbonenetzwerk mit 155 Mbps anbietet. Die Zuleitungen der einzelnen Teilnehmer zum Backbone haben zumeist eine Kapazität von 34 Mbps. Transatlantikverbindungen stehen im Rahmen des Projekts nicht zur Verfügung, werden aber vom Betreiber angeboten und sind extra zu bezahlen. ACONet verwendet für Transatlantikverkehr Ebone oder eigene Verbindungen.

- ein Projekt der EU (+Tschechien, Slowenien, Schweiz, Israel) und der Forschungsnetzwerke der Mitgliedsstaaten (gemeinsame Finanzierung)
- organisiert und verwaltet von Dante Ltd, UK

- **nicht** "policy free"
- Österreich (ACONet) mit 34 Mbps an den Knoten in Wien angebunden
- wird Kapazitäten für Projekte (Breitbandapplikationen) zur Verfügung stellen
- Vorgänger: IXI, Europanet, TEN-34

<http://www.dante.net/ten-155.html>

11.1.4 ACONet

ACONet ist das österreichische akademische Netzwerk, das Universitäten, Schulen und anderen Einrichtungen des BMWV zur Verfügung steht. Gemeinnützige Einrichtungen, z. B. Bildungseinrichtungen können auf Antrag teilnehmen.

Wurzeln

- EARN Österreich (SNA-Netzwerk, IBM)
- Universitätsnetz Austria (DNA über Datex-P, DEC)
- EUNET Österreich (Wählverbindungen)

Promotor

- ACONet-Verein, gegründet 1986

Entwicklung

- 1990 (2. Hälfte)
 - gemeinsames Netzwerk auf Basis X.25 (Ringnetzwerk)
 - Anbindung an Internet (Ebone) über Genf (Wien) und Amsterdam (Linz)
 - Verbindungen zu Nachbarländer über Linz und Wien
- 1992
 - Umstellung auf IP (Dreieck Wien - Linz - Graz)
 - Anbindung an Internet (Ebone) und Nachbarländer über Wien (EBS)
- 1994 (Mai) Umstellung auf MAN-Dienst der PTT (logischer Stern)
- 1996 (März) Umstellung von Linz und Graz auf ATM
- 1997 Umstellung der Standorte Innsbruck, Leoben, Klagenfurt und Salzburg auf ATM

Anbindung

- über EBS an der Universität Wien

Details s. <http://www.aco.net>

11.2 Diensteanbieter(Internet Service Provider)

Internet Service Provider (ISP) sind Firmen, die ihren Kunden Internetzugänge anbieten (Access Provider).

Merkmale:

- Nationale und internationale Provider
- Zugang über regionale Anschlußpunkte, häufig von Sub Providern betrieben
- Unterstützen Kunden mit Software, Installation und Beratung, Erstellung von WEB-Seiten, Speicherplatz, Einbindung der Seiten in den ISP-Server
- Proxyserver und ähnliche Einrichtungen dienen primär zur Entlastung des Netzwerkes und sind daher nur indirekt Kundendienst
- zur Benutzung des Internets muss sich Kunde in einen Access Server einwählen, sich identifizieren und authentifizieren
- auch Standleitungsservice für Kunden
- meist eigenes Transportnetzwerk, jedoch auch Nutzung anderer Transportnetzwerke

Bemerkung:

ISP ist jedes Unternehmen, das Internetzugänge anbietet und seinen eigenen Zugang zum Internet hat!

ISPA - Internet Service Provider Austria, Vereinigung der

Die Anzahl der internationalen und nationalen ISP steigt an. Es finden ständig Ankäufe, Verschmelzungen und Neugründungen statt. <http://www.ispa.at> gibt einen Überblick über die ISP Österreichs, die dort als Access Provider bezeichnet werden.²²

11.3 Geschlossene Benutzergruppen

Profit oder Non Profit Organisationen, die Dienste und Inhalte (Content) anbieten, welche nur ihren Kunden/Mitgliedern zur Verfügung stehen (auch Content Provider).

Merkmale:

- bietet spezielle Dienste an (z. B. Forumdienste, spezielles Mailservice)
- ev. Dienste, die auf einen rechtlich geschützten Input zurückgehen (Diensteanbieter löst rechtliches Problem)
- zur Benutzung der Dienste muss sich Kunde in einen Server einwählen, sich identifizieren und authentifizieren
- vor oder parallel zum Internet entstanden
- früher häufig eigenes Transportnetzwerk, jedoch auch Nutzung anderer Transportnetzwerke
- bietet ev. Kunden Zugang zum Server über Internet an (Kunde verfügt über einen Internetanschluß)
- bietet Zugang zum Internet voll oder teilweise (ist also auch Internet Service Provider)
- bereitet Internetdienste speziell für seine Kunden auf

22. Manche Autoren unterscheiden zwischen Access Provider, Space Provider und Content Provider.

11.3.1 FIDONET

existiert seit 1984. Es ist ein Amateurnetzwerk, welches das Ziel hat, die Basisnetzwerkdienste möglichst billig zur Verfügung zu stellen. Derzeit umfaßt das Netzwerk 30000 Knoten. Der Hauptzweck besteht heute darin ein Gateway zwischen Fidonet und Internet zur Verfügung zu stellen.

Merkmale:

- kein wie immer gearteter kommerzieller Verkehr
- streng hierarchischer Aufbau nach Zonen, Regionen und Netzwerke
- proprietäres Protokoll (billiger Transport)
- nur Mail, Internet News, Fido Newsletters
- nur Wählleitungen
Organisation orientiert sich nach Tarifzonen
Übertragung in festgelegtem Zeitintervall (Zone Mail Hour)
- jeder Knoten in gemeinsamer Tabelle (wird wöchentlich verteilt)
- kein Austausch von Mail/Files zwischen Fidonetknoten über Internet !

<http://www.fidonet.org>

11.3.2 AOL - America OnLine

AOL ist auf Unterhaltung, Spiel, etc. ausgerichtet. Es gibt Diskussionsgruppen (im weiteren Sinn) für alle möglichen Zwecke bzw. Personengruppen

- Traumanalysen
- extreme Fans (Sportler bis ins Schlafzimmer verfolgt)
- Gruppe für Schlaflose
- Moms Online
- Newsgroup Scope
- Comics
- Kids only
- Senior Net (über 55)
- u. v. a.

Weitere spezielle Dienste sind

- Software Center (z. B. spezielle Down Load Software)
- Zeitungskiosk
- Kumpelliste
- chats
- Internet
- etc.

<http://www.aol.com>

AOL wurde Anfangs 2000 vom TV-Anbieter Warners übernommen.

11.3.3 AMDA bzw. AMANDA

AMDA - Austrian MacIntosh Development Association (in OÖ. AMANDA) ist ein Beispiel für eine österreichische Gruppe. Für die Bereitstellung der Dienste wird FirstClass verwendet. Es gibt Clients für Mac und DOS/Windows.

Dienste

- Electronic Mail, erweitert um Formulare
- File Transfer
- News
- Chat
- Informationsbibliotheken
- Bulletin Boards, Konferenzen
- Gateways zu Internet, Fidonet, MicroSoftMail, QuickMail

AMDA kann auch vom Internet aus erreicht werden.

12. VERWALTUNG DES INTERNETS

Internet ist ein Netzwerk, das auf "Freiwilligkeit" beruhte und immer noch beruht. D. h. i. b. s., dass es keine von oben verordnete Verwaltung gibt. Notwendige Maßnahmen wurden von Institutionen übernommen. Mit zunehmenden Anwachsen der Aufgaben wurden Organisationen zur Bewältigung dieser Aufgaben gegründet, die vom Staat (USA) und den Nutzniessern finanziert wurden bzw. werden. Seit der Kommerzialisierung des Internets haben Regierungen den Trend, sich als Sponsor zurückzuziehen.

Sehr häufig findet man Baumstrukturen, d. h. es gibt eine zentrale Stelle, welche die Aufgaben dann an regionale (kontinentale) Stellen delegiert, die sie ihrerseits an nationale Einrichtungen weitergeben. Als Beispiel sei die Adreßvergabe angeführt:

- weltweit gesteuert durch IANA (Internet Assigned Numbers Authority) (<http://www.iana.org>)
- Europa hat ein Kontigent von Adressen, die von RIPE (<http://www.ripe.net>) verwaltet werden
- RIPE gibt wieder Kontigente an ISP ab, die sie ihren Kunden zur Verfügung stellen

Ähnlich läuft die Entwicklung von Internet Standards ab. Im Prinzip hat jeder die Möglichkeit, an der Entwicklung von Standards (Drafts), die dann in sogenannten RFCs (Request for Comments) niedergelegt werden, mitzuarbeiten. Formal eingebunden ist diese Aufgabe in der Internet Engineering Taks Force, IETF (<http://www.ietf.org>) , die ihrerseits vom Internet Architecture Board, IAB (<http://www.iab.org>) , gesteuert wird. Innerhalb des IAB gibt es noch die Internet Research Task Force, die sich mit Forschungen im Bereich von TCP/IP und Internetarchitektur beschäftigt.

Andere Organisationen, wie z. B. CERT, befassen sich mit Sicherheitsproblemen.

Anhang 1. Literaturhinweise*Bücher:*

Tannenbaum, Andreas, S., Computernetzwerke, 3. revidierte Auflage, Prentice Hall, 1998

Das Buch enthält eine umfassende Darstellung der Materie, beginnend mit theoretischen Grundlagen über Kabel bis zu Applikationen etc. Es ist in einigen wenigen Bereichen nicht auf den letzten Stand, was aber heute aufgrund der rasanten Entwicklung in einem Buch gar nicht mehr möglich ist.

Robert Breyer, Sean Riley, Switched, Fast and Gigabit Ethernet, 3. Auflage, MacMillan Network & Architecture Series

Ein sehr guter Überblick über die Geschichte und Entwicklung von Ethernet; weiters werden VLAN, Layer 2 und Layer 3 Switching, aber auch Verkabelung behandelt.

Jim Geir, Wireless LANs, MacMillan Network & Architecture Series, 1999

Die Grundlagen von Wireless LANs werden beschrieben. Der Autor konzentriert sich dann auf den Standard 802.11. Aufgrund des Erscheinungsjahrs fehlt natürlich die neueste Version von 802.11. Der Autor benutzt sehr viele Fallbeispiele. Der Planungsprozess wird ausführlich an Hand eines Falls beschrieben. Das Buch ist auch für Nichttechniker und Manager geeignet.

Zeitschriften:

The Internet Protocol Journal, CISCO, vierteljährlich, im WEB verfügbar (<http://www.cisco.com/ipj>)

Die Zeitschrift befasst sich mit Themen und Problemen aus dem Betrieb des Internets und ist für jene interessant, die ein Internet/Intranet verwalten, ibs. wenn dieses Netzwerk mit dem globalen Internet verbunden ist.

Datacom, Das Management Magazin für Daten- und Telekommunikation, monatlich

Breit gestreute Themen aus dem Bereich der IT, nur wenig technische Artikel; der Verlag Datakom gibt auch Bücher heraus, die einen guten Überblick über einzelne Themen bieten, aber kritisch betrachtet werden müssen, weil sie zum Teil rasch produziert werden.

Normen:

Wer sich für technische Details interessiert, soll oder muss Normen studieren.

Lokale Netze: <http://www.ieee.org>

Weitbereichsnetze und Telefonie: <http://www.itu.org>

Anhang 2. Comparison of STP and UTP

<http://www.anixter.com/techlib/vendor/cabling/attup.htm>

UTP vs. STP: A Comparison of Cables, Systems, and
Performance Carrying High-Data-Rate Signals

Contents:

- * Introduction
- * UTP Cable vs STP Cable
- * UTP Cabling Systems vs STP Cabling Systems
- * UTP vs STP Cabling Systems and Electromagnetic Compatibility (EMC)
- * UTP Cabling Systems and High-Speed Data Transmission
- * The Advantages of Using UTP Cabling Systems

Introduction

Recently, debate has arisen on the advantages and disadvantages of shielded twisted pair (STP) cable and unshielded twisted pair (UTP) cable. Advocates of STP cable (a category that includes screened twisted pair cable and foil twisted pair cable) have attempted to claim that their product is superior to UTP cable without adequately presenting both sides of the story. While it is true that STP cable and UTP cable are inherently different in design and manufacture, their purpose should be the same, to provide reliable connectivity of electronic equipment. Although, in theory, both types of cable should perform this task successfully, the true test comes when you look at the performance of each of these cable types within its respective end-to-end system.

UTP Cable vs STP Cable

Two copper wires, each encased in its own color-coded insulation, are twisted together to form a twisted pair. Multiple twisted pairs are packaged in an outer sheath, or jacket, to form twisted pair cable. By varying the length of the twists in nearby pairs, the possibility of interference between pairs in the same cable sheath can be minimized.

Twisted pair cable has been around for quite a while. In fact, early telephone signals were sent over a type of twisted pair cable, and just about every building today still uses twisted pair cable to carry telephone and other signals. However, signals have become more complex over the years, evolving from 1200 bps to over 100 Mbps. And there are many more sources of interference that might disrupt those signals today than there were at the turn of the century. Coaxial cable and fiber optic cable were developed to handle higher-bandwidth applications, and to support emerging technologies. But twisted pair cable, too, has evolved so that it can now carry high-data-rate signals.

Some twisted pair cables contain a metal shield to reduce the potential for electromagnetic interference (EMI). EMI is caused by signals from other sources such as electric motors, power lines, high-power radio and radar signals in the vicinity that may cause disruptions or interference, called noise. Shielded twisted pair (STP) cable encases the signal-carrying wires in a conducting shield. At first glance, it may appear that because STP cable is physically encased in a shield, all outside interference is automatically blocked; however, this is not true.

Just like a wire, the shield acts as an antenna, converting received noise into current flowing in the shield when it has been properly grounded. This current, in turn, induces an equal and opposite current flowing in

the twisted pairs. As long as the two currents are symmetrical, they cancel each other out and deliver no net noise to the receiver. However, any discontinuity in the shield or other asymmetry between the current in the shield and the current in the twisted pairs is interpreted as noise. STP cable is only effective at preventing radiation or blocking interference as long as the entire end-to-end link is shielded and properly grounded. To work properly, every component of a shielded cabling system must be just that fully shielded.

STP cable also has drawbacks; for example, its attenuation may increase at high frequencies, and its balance (or longitudinal conversion loss) may decrease if the effects of the shield are not compensated for, which leads to crosstalk and signal noise. The shielding effectiveness depends on the material of the shield, its thickness, the type of EMI noise field, its frequency, the distance from the noise source to the shield, any shield discontinuity, and the grounding structure used. Nor can it always be guaranteed that the shield itself will contain no imperfections.

Some STP cables use a thick braided shield. These cables are heavier, thicker, and harder to install than their UTP counterparts. Some STP cables only use a relatively thin overall outer foil shield. These cables, called screened twisted pair (ScTP) cables or foil twisted pair (FTP) cables, are thinner and less expensive than braided STP cable. However, they are not any easier to install the minimum bending radius and maximum pulling tension force must be rigidly observed when these cables are installed; otherwise, the shield may experience a tear.

Unshielded twisted pair (UTP) cable, on the other hand, does not rely on physical shielding to block interference, but on balancing and filtering techniques through media filters and/or baluns. Noise is induced equally on two conductors, which cancels out at the receiver. With properly designed and manufactured UTP cable, this technique is easier to maintain than the shielding continuity and grounding of an STP cable.

UTP cable has evolved over the years, and different varieties are available for different needs. Basic telephone cable, also known as direct-inside wire (or DIW), is still available. Improvements over the years, such as variations in the twists or in individual wire sheaths or overall cable jackets, have led to the development of EIA/TIA-568 standard-compliant Category 3 (for specifications on signal bandwidth up to 16 MHz), Category 4 (for specifications on signal bandwidth up to 20 MHz), and Category 5 (for specifications on signal bandwidth up to 100 MHz and greater) UTP cable. Because UTP cable is lightweight, thin, and flexible, as well as versatile, reliable, and inexpensive, millions of nodes have been and continue to be wired with UTP cable, even for high-data-rate applications. For the best performance, UTP cable should be used as part of a well engineered structured cabling system.

UTP Cabling Systems vs STP Cabling Systems

If STP cable is combined with improperly shielded connectors, connecting hardware, or outlets, or if the foil shield itself is damaged, overall signal quality will be degraded. This can result in degradation of emission and immunity performance. Therefore, for a shielded cabling system to succeed totally in interference reduction, every component within that system must be fully and seamlessly shielded, as well as properly installed and maintained.

Likewise, an STP cabling system requires good grounding and earthing practices. An improperly grounded system can be a primary source of emissions and interference. Whether this ground is at one end or both ends of the cable run depends on the frequency of the application. For high-frequency signals, an STP cabling system must be grounded, at a minimum, at both ends of the cable run, and it must be continuous. A shield grounded at one end only has no effect against magnetic field interference. The length of the ground conductor itself can also be a source of problems. If it is too long, it no longer acts as a ground. Therefore, optimum grounding for an STP cabling system is not possible, since it depends on the application. UTP cabling systems do not have this problem.

While an STP cabling system is dependent on such factors as physical continuity of the cable shield itself

or installation with adequately shielded and grounded components, a UTP cabling system inherently has fewer points for potential failure and is easier to install. For UTP cabling systems such as Lucent Technologies' SYSTIMAX® Structured Cabling Systems (SCS), all of the individual products certified for use are manufactured by Lucent Technologies and individually tested, as well as tested in conjunction with other products in the SYSTIMAX SCS offering. All cables, for example, are tested on the reel at the point of manufacture, and are also tested as a complete cabling system within the individual applications for which they are certified. All products certified for use in SYSTIMAX SCS also carry a 15-year warranty.

SYSTIMAX SCS utilizes Lucent Technologies/Bell Laboratories-developed design rules for all certified end-to-end applications. Such design rules, which are fully documented in Lucent Technologies' application guidelines, cite which products may be used (for example, only Category 5 products for some higher-speed applications), how cable must be terminated and administered, and maximum distances for cable runs. All applications are also tested in Lucent Technologies/Bell Laboratories test labs and are certified for a period of 15 years. Consequently, both products and systems are fully tested and warranted.

UTP vs STP Cabling Systems and Electromagnetic Compatibility (EMC)

In addition to precision design and manufacture, as well as end-to-end integrity, another factor to consider when choosing a cabling system relates to the recent adoption of electromagnetic compatibility (EMC) directive. EMC refers to the ability of an electronic system to function properly in its environment that is, an environment where several pieces of equipment are located in the same workspace, each radiating electromagnetic emissions. With the increased amount of electronic equipment in the average workspace, EMC becomes increasingly more important excess radiation from one piece of equipment can adversely affect performance of another piece of equipment. This means that every electronic system, which includes either an STP or UTP cabling system, must meet this directive.

In some countries, such as the U.S. and Germany, EMC regulations have existed for years. However, the implementation of the European EMC Directive in 1989 has refocused attention on EMC. The European EMC Directive 89/336/EEC states that all electronic equipment and apparatus must comply with the directive. These systems must pass the essential requirements of the directive before they can be sold anywhere in the European Economic Area (EEA). Some national regulations (such as Amtsblatt Verfassung 243/91 of Germany) currently exempt STP based systems from immunity testing. However, as of January 1, 1996, these national regulations will no longer apply, and all systems must be tested. Those that do not pass will not be able to be sold in the EEA.

How well do UTP and STP based systems stand up to rigorous EMC testing? Contrary to some popular assumptions, not all STP based systems can automatically pass EMC tests, while a well designed UTP cabling system can.

EMC Fribourg, a Swiss testing facility, conducted comparative EMC tests on four STP cabling systems and one UTP cabling system. All were configured to support the IBM 16 Mbps Token Ring local area network (LAN) application according to ISO 8802.5 standards, using personal computers (PCs) with IBM Token Ring Adapter Cards.

For the UTP cabling system, SYSTIMAX SCS 1061 Category 5 24 AWG High-Performance 4-pair UTP cable was chosen, with an M1000 MULTIMAX Panel and M100-type information outlets (IOs) used as the connecting hardware, and a 370C1 Adapter (media filter) used to link the IBM card to the SYSTIMAX SCS UTP system.

Test results were as follows:

* In radiated emissions testing for a frequency range of 30 MHz 1 GHz in an anechoic chamber and in an open area test site (OATS), the SYSTIMAX SCS UTP system met CISPR 22/EN5022 Class B

requirements (Class B requirements are for residential use, and are more stringent than the Class A requirements for commercial use) with a more-than-adequate margin. * In conducting emissions on signal port testing at lower frequencies (150 kHz 30 MHz) with a current probe, the SYSTIMAX SCS UTP system met the proposed CISPR 22/EN55022 class B requirements. * In IEC 801.4 electrical fast transient (EFT) noise-burst testing, the SYSTIMAX SCS UTP system did not fail even when subjected to the most strenuous test at 4,000 V. None of the STP cabling systems survived to that level. * In IEC 801.3 radiated immunity testing, which tests the ability of a system to withstand electromagnetic interference at defined severity levels (26 MHz 1 GHz), the SYSTIMAX SCS UTP system experienced no errors. The one STP cabling system tested experienced errors when the media filter was used instead of the shielded work area cable at the PC.

EMC Fribourg concluded that UTP cabling systems, and, more specifically, SYSTIMAX SCS UTP systems, can meet the above EMC requirements.

UTP Cabling Systems and High-Speed Data Transmission

Tests conducted in well known testing facilities show that UTP cabling systems and, specifically, SYSTIMAX SCS using UTP cable, can meet standards specifications for transmitting high-speed data within acceptable levels and can pass all required tests.

EMC tests were conducted on an ISO 8802.3 10 Mbps 10BASE-T system that used SYSTIMAX SCS 1061 Category 5 24 AWG High-Performance 4-pair UTP cable, with Category 5 patch panels, Category 5 M100-type IOs, and Category 5 patch cords, along with 486-type PCs and electronics from several major vendors. The tests were done at the Lucent Technologies/Bell Laboratories Global Product Compliance Laboratory in Holmdel, NJ, and were sent to a German notified and competent body, Bundesamt für Zulassungen in der Telekommunikation (BZT) for certification. The SYSTIMAX SCS UTP system passed every test, in some cases even exceeding the current requirements under the EMC Directive.

The tests were as follows:

* Radiated Emissions; specifications EN 55022, 1987, Class B Limit * Conducted Emissions (AC Mains); specifications EN 55022, 1987, Class B Limit * Conducted Emissions (Signal Ports); specifications EN 50081-1, 1992, Informative Annex A, CISPR 22 Amendment, CISPR/G (Sec 65), 1993, Class B Limit * Electrostatic Discharge (ESD) Immunity; specifications IEC 801.2, 1991, IEC CISPR 24, Part 2, prEN 55024, Part 2, Contact Discharge at 4,000 V (Level 2), Air Discharge at 8,000 V (Level 3) * Radiated Field Immunity; specifications IEC 801.3, 1992, IEC CISPR 24, Part 3, prEN 55024, Part 3, 3 V/m (Level 2), 10 V/m (Level 3) * EFT/Burst Immunity; IEC 801.4, 1988, IEC CISPR 24, Part 4, prEN 55024, Part 4, AC Mains at 1.0 kV (Level 2), Signal/Control Lines at 0.5 kV (Level 2) and 1.75 kV (Level 3)

EMC tests were also conducted on an ISO 9314 (ANSI X3T9.5) 100 Mbps TP-PMD LAN that used SYSTIMAX SCS 1061 Category 5 24 AWG High-Performance 4-pair UTP cable, with Category 5 patch panels, Category 5 M100-type IOs, and Category 5 patch cords, along with 486-type PCs and electronics from several major vendors. The tests were done at the Lucent Technologies/Bell Laboratories Global Product Compliance Laboratory in Holmdel, NJ, and were sent to BZT in Germany for certification. The SYSTIMAX SCS UTP system again passed every test, in some cases even exceeding the current requirements under the EMC Directive.

The tests were as follows:

* Radiated Emissions; specifications EN 55022, 1987, Class B Limit * Conducted Emissions (AC Mains); specifications EN 55022, 1987, Class B Limit * Conducted Emissions (Signal Ports); specifications EN 50081-1, 1992, Informative Annex A, CISPR 22 Amendment, CISPR/G (Sec 65), 1993, Class B Limit * ESD Immunity; specifications IEC 801.2, 1991, IEC CISPR 24, Part 2, prEN 55024, Part 2, Contact

Discharge at 4,000 V (Level 2), Air Discharge at 8,000 V (Level 3) * Radiated Field Immunity; specifications IEC 801.3, 1992, IEC CISPR 24, Part 3, prEN 55024, Part 3, 3 V/m (Level 2) * EFT/Burst Immunity; IEC 801.4, 1988, IEC CISPR 24, Part 4, prEN 55024, Part 4, AC Mains at 1.0 kV (Level 2), Signal/Control Lines at 0.5 kV (Level 2)

Furthermore, research conducted by the SYSTIMAX SCS Department of Lucent Technologies/Bell Laboratories together with the Advanced Multimedia Communications Department of Lucent Technologies/Bell Laboratories has demonstrated that SYSTIMAX SCS UTP systems, using 328 ft (100 m) of 1061 Category 5 24 AWG High-Performance 4-pair UTP cable, with M1000 MULTIMAX Panels and M100-type IOs for connecting hardware along with Category 5 D8AU patch cords, can successfully transmit up to 622 Mbps the equivalent of 23,000 pages of text per second.

The test used off-the-shelf high-quality red/green/blue (RGB) video equipment to provide the data stream. A studio-quality RGB video camera was used to capture a full-motion high-resolution image. Using a codec, the analog video signal from the camera was converted to an industry-standard D1 protocol digital video data stream and, at the transmitter, encoded into a 64-point Carrierless Amplitude and Phase (64 CAP) signal. The 64 CAP encoding method was used to partition the data stream into four 155-Mbps "channels" at the transmitter, which were each then sent over one pair of the 4-pair cable, and then decoded and recombined into a single 622 Mbps data stream at the receiver end of the link. A codec at this end converted the signal back into an analog RGB video signal that was displayed on the monitor.

The Advantages of Using UTP Cabling Systems

STP cabling systems are more expensive and harder to install and maintain than UTP cabling systems, but are not necessarily better. As demonstrated in EMC and other test results, UTP cabling systems succeeded even excelled in rigorous testing. Furthermore, because it was chosen as the representative UTP cabling system, SYSTIMAX SCS demonstrated even more fully the benefits of Lucent Technologies' extensive testing and precision manufacturing under rigid ISO 9000 quality control conditions. This underscores the importance of using a structured cabling system made up of products designed and manufactured to work together that meet or exceed international standards.

Return to: [Technical Library](#) | [Vendor Technical Papers](#)

[About Anixter](#) | [Solutions](#) | [Special Programs](#) | [Service](#) | [Home](#) | [What's New](#) | [Technical Library](#) | [Catalog](#) | [Search](#) | [Site Index](#) | [Contact Us](#)

All contents © 1997 Anixter Inc.

Anhang 3. CSMA/CD

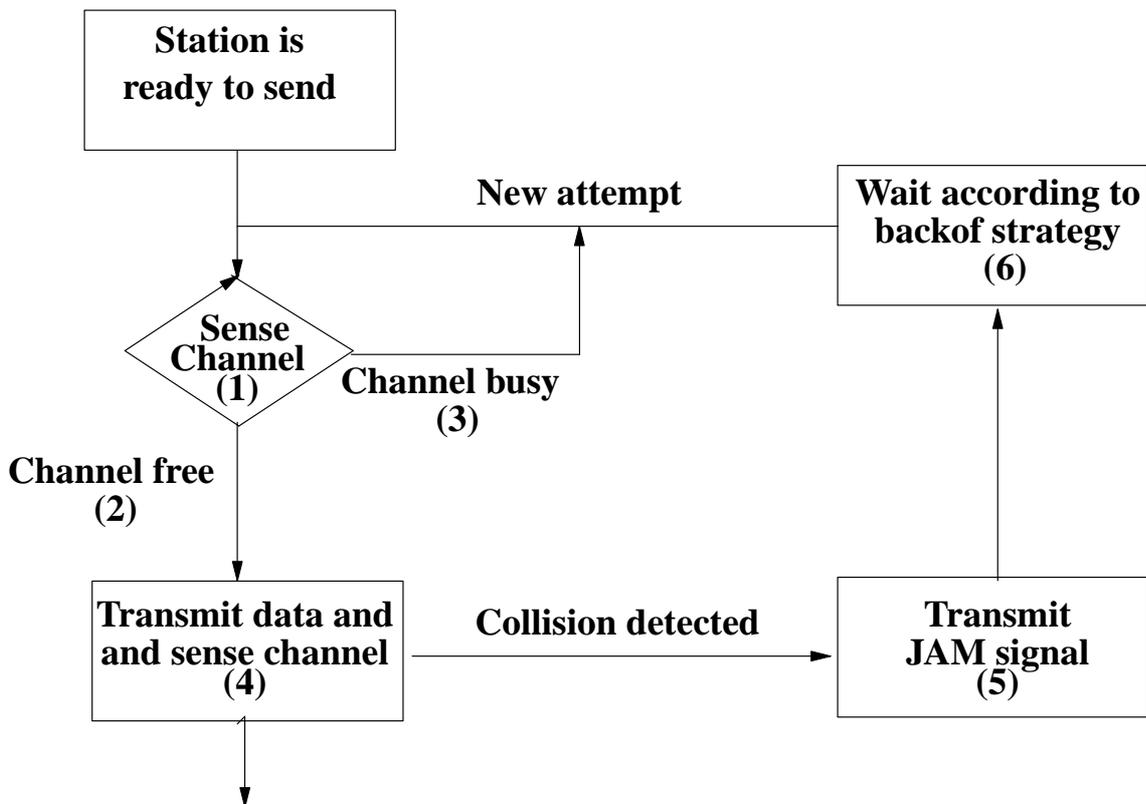


Abbildung 6. CSMA/CD

1. Es muss sichergestellt sein, dass keine andere Station das »shared Medium« benutzt (carrier sense oder »listen before talking)
2. Sende, falls Kanal für eine bestimmte Zeit (interframe gap) frei (»talk if quiet)
3. Falls besetzt, prüfe solange, bis Kanal wieder für eine bestimmte Zeit frei ist (multiple access oder »wait for quiet before talking«)
4. Sende Daten und prüfe weiterhin Kanal auf Signale anderer Stationen (Collision detection oder »listen while talking«)
5. Sende JAM, um sicherzustellen, dass andere Stationen Kollision entdecken (Collision detection oder »one talker at a time«)
6. Nach einer Wartezeit, die mit einer Zufallsfunktion bestimmt wird, kann Vorgang wieder gestartet werden.²³

23. Nach Robert Breyer, Sean Riley, Switched, Fast und Gigabit Ethernet, 3. Auflage, S 88f

1. HERSTELLERUNABHÄNGIGE KOMMUNIKATION	1
1.1 Rückblick	1
1.2 OSI-Referenzmodell	1
1.2.1 Schichten des OSI-Referenzmodells	1
1.2.2 Normen im Bereich von OSI	4
2. NETZWERKTYPEN	6
3. ÜBERTRAGUNGSMEDIEN	7
3.1 Qualitätsmerkmale	7
3.2 Aerische und terrestrische Medien	8
3.2.1 Drahtlose Übertragungseinrichtungen	8
3.2.2 Kabel	9
4. LOKALE NETZE	12
4.1 Verkabelung	12
4.2 Ethernet	13
4.3 Token Ring	15
4.4 Fiber Distributed Data Interface (FDDI)	17
4.5 Zusammenfassung	18
4.6 Virtuelle LANs (VLANs)	18
5. WEITBEREICHSNETZWERKE - WIDE AREA NETWORKS (WAN)	21
5.1 Standleitungen - Festverbindungen	21
5.2 Dienste	21
5.3 Standleitungen versus Dienste	21
5.4 Beispiele für Dienste	21
5.4.1 X.25	21
5.4.2 Frame Relay	22
5.4.3 B-ISDN	22
6. ASYNCHRONOUS TRANSFER MODE (ATM)	23
7. TENDENZEN	25
8. KOMMUNIKATIONSABLAUF IN NETZWERKEN	26
8.1 Adressen in Netzwerken	26
8.1.1 Geräteadressen (Schicht 2)	26
8.1.2 Netzwerkadressen (Schicht 3)	26
8.2 Routing	27
9. TCP/IP	29
9.1 Aufbau	29
9.2 Adressen im IP (Schicht 3)	29
9.3 Abbildung von Netzwerkadressen in MAC-Adressen	31
9.4 TCP-Verbindungen	31
9.5 Point to Multipoint (IP Multicast)	32
9.6 Domainnamen	32
9.6.1 Prinzip der Domainnamen	32
9.6.2 Abbildung von Domainnamen auf IP-Adressen	32

9.7 IP Version 6 (IPv6)	33
10. HINWEISE ZUR PLANUNG VON NETZWERKEN	36
11. DIENSTE UND DIENSTEANBIETER	38
11.1 Transportnetzwerke	38
11.1.1 Rückblick	38
11.1.2 European Backbone Network (Ebone)	39
11.1.3 TEN-155	39
11.1.4 ACONet	40
11.2 Diensteanbieter(Internet Service Provider)	41
11.3 Geschlossene Benutzergruppen	41
11.3.1 FIDONET	42
11.3.2 AOL - America OnLine	42
11.3.3 AMDA bzw. AMANDA	43
12. VERWALTUNG DES INTERNETS	

.....	44
Verzeichnis der Abbildungen	

Abbildung 1. ISO/OSI Schichtenmodell	3
Abbildung 2. LAN	19
Abbildung 3. TCP/IP Protokolle ¹⁰	29
Abbildung 4. Adreßklassen ¹¹	30
Abbildung 5. Adreßkonventionen (Zusammenfassung) ¹²	31
Abbildung 6. CSMA/CD	51

Verzeichnis der Anhänge

Anhang 1. Literaturhinweise	45
Anhang 2. Comparison of STP and UTP	46
Anhang 3. CSMA/CD	51