GWDG

Grundlagen der Netzwerktechnik

- Aufbau, Management, Nutzung -

Erster Teil des Ausbildungsprogramms
„Fortbildung zum Netzwerkadministrator“

Dr. Holger Beck

Gesellschaft für wissenschaftliche Datenverarbeitung mbH Göttingen
Am Faßberg
D-37077 Göttingen

Version 1.1 Oktober 1997

Inhaltsverzeichnis

1. Vorwort

1.1. Überblick über das Ausbildungsprogramm „Fortbildung zum Netzwerkadministrator“

Zielsetzung des Ausbildungsprogramms:

Die Kursteilnehmer sollen in die Lage versetzt werden im Rahmen der im Kurs behandelten Netzwerksysteme, Routineaufgaben bei der Netzwerkadministration selbständig zu erledigen und komplexere Aufgabenstellungen zu verstehen und dadurch deren Lösung vorzubereiten oder solche mit Unterstützung von Experten zu lösen.

Aufteilung in zwei Kursabschnitte:

- Netzwerktechnik im allgemeinen im Kurs „Grundlagen der Netzwerktechnik - Aufbau, Management, Nutzung“
- Einführung in ein Netzwerkbetriebssystem, zur Zeit alternativ:
  - Administration von Novell-Netze
  - Administration von Microsoft-Netzen

1.2. Einordnung des Ausbildungsabschnitts „Grundlagen der Netzwerktechnik“ in das Ausbildungsprogramm „Fortbildung zum Netzwerkadministrator“

Zielsetzung des Ausbildungsabschnitts:

Erlernen theoretischer Grundlagen zum Verständnis von Netzen:

- Kenntnisse über Netzwerkinfrastrukturen
- Kenntnisse über Prinzipien von Vernetzungsprogrammen
- Prinzipien des Netzwerkmanagements
- Einblick in die Netzwerkstruktur im Bereich von Forschung und Lehre

In allen Fällen verbleibt die Vermittlung der Kenntnisse in diesem Kurs aufgrund der Kürze der Zeit nur auf der Ebene einer Einführung.

Das Ergebnis des Kurses sollte sein, daß die Teilnehmer danach in der Lage sind,

- Probleme wie die Planung von Übertragungsnetzen oder das Netzwerkmanagement zu verstehen und
- Netze ihrer Bestimmung gemäß zu nutzen, und
- die zum Verständnis der nachfolgenden Kursteile notwendigen Kenntnisse zu erwerben.

Komplexere Aufgaben werden nach wie vor Netzwerkexperten vorbehalten bleiben.

1.3. Gliederung des Kurses „Grundlagen der Netzwerktechnik - Aufbau, Management, Nutzung“

- Grundbegriffe
- Netzwerkarchitekturen
- Netzwerktechnologien im LAN-Bereich
- Internetworking
- Die IP-Protokollfamilie
- Netzwerkmanagement
- Funktion und Betriebsweise eines Universitätsnetzes

1.4. Literaturhinweise

Als allgemeine Einführung in das Thema des Kurses (und darüber hinaus):

A. Badach, E. Hoffmann, O. Knauer
High Speed Internetworking
Addison-Wesley 1994
ISBN 3-89319-713-3

Als Literatur zu Token-Ring-Netzen:

H.-G. Göhring, F.-J. Kauffels
Token Ring
DATACOM-Verlag 1990
ISBN 3-89238-026-0

Als Literatur zur FDDI- Netzen:

R. Jain
FDDI Handbook: High Speed Internetworking Using Fiber and Other Media
Addison-Wesley Publishing Company
ISBN 0-201-56376-2

Als Literatur zur Fehleranalyse in Netzen:

O. Kyas, T. Heim
Fehlersuche in lokalen Netzen
DATACOM-Verlag 1993
ISBN 3-89238-071-6

2. Datennetzwerke als moderne Kommunikationsstruktur

2.1. Historischer Rück- und Überblick

- Terminalarbeitsplätze an Großrechnern:
  - als Ersatz für offline-Eingaben über Lochkarten,
  - Einzelanbindung von Terminals an je einen Anschlußpunkt am Zielrechner,
  - später Terminalemulation auf Arbeitsplatzrechner mit der Möglichkeit des Datentransfers.
- Netze zum (lokalen) Datenaustausch:
  - schnellere Kommunikationsmedien,
  - von mehreren Rechnern gleichzeitig benutzte Medien,
  - Kopieren von Daten über das Netz,
  - Terminalemulation.
- Aufbau nationaler und internationaler Datennetze:
  - Elektronische Post,
  - Dateitransfer über weite Entfernungen.
- Netzwerkbetriebssysteme:
  - Einführung virtueller Netzwerkdienste (Drucker, Speicherkapazitäten),
  - Client-Server-Konzepte,
  - „Das Netzwerk als System“ (statt des Großrechners).
- Verteilte Systeme
- Multi-Media-Dienste und -Netze

3. Netzwerkdienste

Angebote/Möglichkeiten, die dem Nutzer durch das Netz eröffnet werden.

3.1. Kommunikationsmodelle

3.1.1. Client-Server-Modell

- Server

  Ein oder mehrere Netzwerkknoten stellen Dienste zur Verfügung

- Client

  Andere Rechner nutzen diese Dienste, ohne selbst Dienste anzubieten

- Gängiges Modell für größere Netze
- Die Trennung in Clienten und Server wird nicht bezüglich jeder Funktion immer 100%ig eingehalten.
- Hintergrund: Ablösung von Großrechnersystemen durch Client-Server-Konzepte

3.1.2. Peer-To-Peer-Netze

- Netzwerk aus gleichberechtigten Rechnern
- Alle Rechner bieten Dienste an, alle nutzen Dienste
- Für kleine Netze geeignet
- Preiswert, da keine dedizierten Server
- Leistungsgrenzen
- Problem Betriebssicherheit

3.1.3. Verteilte Systeme

- Stärkere Verteilung der Aufgaben auf mehrere Server mit spezielleren Aufgaben, Mischung von Client-Server-Rollen
- Mit der Ausdehnung der Netze bieten sich die Möglichkeiten zu weitergehender Vermaschung
- Grenzen zu Client-Server-Modell fließend

3.2. Arten von Netzwerkdiensten

- Netze als EDV-Hilfsmittel mit dem Ziel einer effiziente Nutzung von EDV-Resourcen:
  - Gemeinsame Nutzung von Druckern und anderen Peripheriegeräten
  - Gemeinsame Datenhaltung
  - Nutzung zentraler Archivierungs- und Sicherungssysteme
  - Zugriff auf entfernte Rechner und deren Kapazitäten
  - Hilfsmittel zum Datenaustausch (lokal)
- Netze als Hilfsmittel für Kommunikation und Informationsaustausch:

    - Funktion
        - Austausch von Daten (insbesondere über weitere Entfernungen)
        - Austausch von persönlichen Informationen
        - Allgemeine Informationsdienste
        - Diskussionsforen
    - Typische Anwendungen
        - Email
        - Diskussionslisten (News, Listserver)
        - Verteilte Informationssysteme (Gopher und World Wide Web)
- Zukünftige Ziele:
    - Multi-Media-Systeme: Integration aller Kommunikations- und Mediensysteme (Sprache, Bilder und Daten, Unterhaltung und Geschäftsleben)
- Unterteilungsmöglichkeit der Dienste nach typischen LAN- oder WAN-Diensten

3.3. Beispiel für Netzwerkdienste

3.3.1. Mehrfachnutzung von Ressourcen

- Massenspeichernutzung
    - File-Server
        - Benutzerdaten (Vorteil: gleiche Daten für alle, gleiche Daten überall, zentrale Sicherung)
        - Anonymous FTP
        - Typische Protokolle: IP/NFS, IPX, SMB, AppleTalk/AFP
    - Archiv-Server
    - Backup-Server
- Software-Nutzung
    - Nutzung zentral gehaltener und gepflegter Software (bei Nutzung der eigenen CPU)
        - Zentrale Pflege
        - Sicherheit (z.B. diskless Workstations)
        - Effiziente Nutzung von Lizenzen
    - Zugriff auf Software und CPU entfernter Rechner
- CPU-Nutzung
- Peripherie-Nutzung
    - Drucker
    - Plotter
    - Spezialausgabe-Geräte
    - Eingabegeräte (Bänder, Kassetten)
- Verteilte Datenbanken

- Spezielle Kombination von Speicher-, Software- und CPU-Nutzung
- Datenbankabfragesprache (SQL)
- Achtung: Unterschied zwischen SQL-Servern und Zugriff auf Datenbankdateien über File-Server!

3.3.2. Verteilte Systeme

- Verteilte Dateisysteme
  - NFS bei starker Verschachtelung der Server-Dienste
  - AFS
    - Vom Konzept her ein weltweites Dateisystem
- Verteilte Fenstertechnik
  - X-Window
  - Achtung bei den Begriffen: der Server ist der lokale Rechner (der den Bildschirm zur Verfügung stellt)
- Verteilte Datenbanken
  - Aufteilung von Datenbanken auf mehrere Server
- Verteilte Anwendungen / Parallelverarbeitung
  - nur mit Hochgeschwindigkeitsnetzen
- Verteilte Informationssysteme

3.3.3. Kommunikationsdienste

- Dateitransfer
- E-Mail
- Verteilung von Nachrichten (Broadcasts)
- Diskussionslisten
  - Per E-Mail (Listserver)
  - Als Diskussionsforum
    - Client-Server-Struktur
    - z.B. NetNews
- Informationsdienste
  - Gopher
  - World-Wide-Web
- Multimedia-Dienste

3.3.4. Mehrfachzugang zu Telekommunikationsdiensten

Übergang in andere Netze

- Gateways
  - Übergang LAN-Backbone
  - Übergang zu Weitverkehrsnetzen
- Telekom-Dienste
  - Datex-P/X.25

- ISDN
- Telex/Teletex
- FAX
- Btx

4. Grundbegriffe

4.1. Lokale Netze und Weitverkehrsnetze

In der Netzwerkwelt werden lokale Netze (Local Area Network, ***LAN***) und Weitverkehrsnetze (Wide Area Network, ***WAN***) unterschieden.

Die Grenzen zwischen den Typen sind nicht immer eindeutig bestimmt (z.B.: Ist eine Uni-Netz wie GÖNET ein LAN oder ein WAN?).

Als Unterscheidungskriterien zwischen LAN und WAN dienen:

Kriterium	LAN	WAN
Geographische Ausdehnung	Geographisch auf einzelne Gebäude oder Gebäudekomplexe beschränkt.	Verbindung weitentfernter LANs (oder MANs) miteinander.
Übertragungskapazitäten	Hohe Übertragungskapazität (10 MBit/s oder mehr).	Meist vergleichsweise geringe Übertragungskapazitäten (meist von ca. 10kbit/s bis 2MBit/s, erst neuere Versuche (ATM) bieten 34 MBit/s und mehr).
Dienstangebote	LANs dienen meist der Nutzung verteilter Resourcen wie Datei- und Druckerserver.	WANs dienen meist dem Zugriff auf entfernte Rechner (Terminalemulation), der Datenübertragung oder dem Informationsaustausch (Mail, Diskussionslisten, WWW usw.).
Vermittlungsfunktion	keine	Vermittlungsfunktion vorhanden
Eigentumsverhältnisse	Privates Netz	Meist öffentliche Netze
Nutzungsgebühren	Meist keine	Anschlußgebühren und/oder Nutzungsgebühren
Struktur	Shared Media	Punkt-zu-Punkt

Als eine Zwischenstufe zwischen LAN und WAN wird auch der Begriff des Metropolitan Area Network (***MAN***) benutzt. Darunter versteht man dann ein Netz mit LAN-Technologie (Zugriffsverfahren und Adressierung) und LAN-Geschwindigkeiten aber WAN-Ausdehnungen und Vermittlungsfunktionen. Zusätzlich werden hier z.T. auch virtuelle private Netze implementiert.

Im Rahmen dieses Kurses werden MANs weitgehend ausgeklammert oder als LANs betrachtet (insbesondere wird GÖNET, das unter die Einteilung MAN fallen würde, wie ein LAN behandelt).

4.2. Leitungsvermittlung und Paketvermittlung

Bei WANs wird zwischen Leitungs- und Paketvermittlung unterschieden:

Leitungsvermittlung:

- Schaltung einer dedizierten Leitung (eventuell mit Benutzung von Multiplexverfahren). Insofern ähnlich den ersten Terminalnetzen, bei denen dedizierte Leitungen von jedem Terminal zu einem dedizierten Anschluß am Großrechner

gezogen wurden oder dem Telefonnetz, bei dem Leitungen vorübergehend geschaltet werden, die dann für eine Verbindung dediziert benutzt werden.

- Nachteil, daß ihre Übertragungskapazität wegen anwendungsbedingter Übertragungspausen nicht vollständig ausgenutzt werden kann.
- Vorteil einer garantierten Übertragungskapazität.
- Flexibilität bei Kommunikationsprotokollen.

Paketvermittlung:

- Daten werden in kleinen Blöcke geteilt (Pakete), die dann unabhängig voneinander zwischen den Kommunikationspartnern übertragen werden.
- Nachteil, daß bei jedem Paket die Adressierungsinformation mitübertragen werden muß („Verschwendung“ von Übertragungskapazität).
- Die Übertragungswege können von mehreren Kommunikationen quasi zeitgleich genutzt werden.
- Eine verfügbare Übertragungskapazität kann einzelnen Kommunikationen nicht garantiert werden.
- In Vermittlungssystemen müssen Daten zwischengespeichert werden (Verzögerung, aufwendigere Vermittlungssysteme, Möglichkeit von Datenverlusten bei Stauungen auf Teilstrecken).

(In LANs und MANs werden Daten praktisch immer in Paketen übertragen, Vermittlungsfunktionen fehlen aber oft.)

4.3. Gemeinsam genutzte Medien

In LANs wird das Betriebsmittel Medium bzw. Übertragungskapazität typischerweise von allen Stationen gemeinsam genutzt (***Shared-LAN***).

Daher müssen in LANs Verfahren für die Erteilung einer Sendeberechtigung auf dem gemeinsamgenutzten Medium definiert werden (***Mediumzugriffsverfahren***, Medium Access Control, ***MAC***).

Dabei tritt bei Shared-LANs das Problem ***der Verteilung von Übertragungskapazitäten*** auf, die einerseits „gerecht“ sein, andererseits aber mit möglichst wenig Aufwand realisiert werden soll. Zudem kann das Problem auftreten, daß einzelnen Anwendungen im Netz wegen ihrer Wichtigkeit ***Prioritäten*** eingeräumt werden sollen.

Bei den Zugriffsverfahren, gibt es ***deterministische*** (z.B. Token-Ring, FDDI) und ***statistische*** Ansätze (z.B. Ethernet).

Neuere LAN-Techniken, die z.T. noch in der Entwicklung sind, versuchen über zentrale Knoten kurzzeitig zwischen Kommunikationspartnern dedizierte Verbindungen zu schalten (***Switching***). Solche LANs werden dann als ***Switched-LANs*** bezeichnet. Beispiele sind Switched-Ethernet, Switched-Token-Ring, Switched-FDDI oder ATM (letzteres nicht nur als LAN-Technik).

4.4. Netzwerktopologien

Netzwerktopologie: Art und Weise wie die Stationen im Netz miteinander verbunden werden. Dabei kann die physikalische Struktur von der logischen Struktur (Softwarekonzeptionen oder Protokoll) abweichen.

Bei WANs werden typischerweise Knotenrechner in einer baumförmigen oder vermaschten Struktur miteinander über dedizierte Leitungen verbunden (die dann von den Knotenrechnern mit Paketen beschickt werden oder im Multiplexverfahren in Kanäle aufgeteilt werden).

Im LAN treten folgende Topologien auf:

- Physikalische Topologie
  - Bustopologie
    - Anschluß aller Stationen an ein gemeinsames Kabel
    - Senden von Daten in alle Richtungen.
    - Keine Verteilerfunktionen nötig.
    - Geringer Platzbedarf für die Verkabelung, wenige Kabel
    - Jede Störung an Kabeln oder Endgeräten kann zu einem Totalausfall des Netzes führen.
  - Sterntopologie
    - Dedizierte Kabel von jeder Station zu einem zentralen Verteiler (der aber anders als bei Terminalvernetzungen oder WANs keine Endgeräte oder Vermittlungsfunktion hat).
    - Notwendigkeit von (mehr oder weniger intelligenten) Verteilern.
    - Hoher Aufwand bei Verkabelung
    - Flexibilität in der Konfiguration.
    - Geringe Anfälligkeit bei Störungen seitens der Verkabelung oder durch die Endgeräte, da ein Defekt jeweils nur eine Station stören.
    - Netzwerk-Managementfunktionen im bzw. mit Hilfe des Verteilers möglich.
  - Baumtopologie
    - Erweiterung der Sterntopologie durch Zusammenschaltung mehrerer Sterne mittels Leitungen zwischen den Verteilern
    - Vor- und Nachteile wie bei Sterntopologie.
  - Ringtopologie
    - Verbindung aller Stationen in Form eines Ringes.
    - Jede Station überträgt empfangene Daten an die nächste Station im Ring weiter.
    - Geringere Kabelmengen als bei Sterntopologie und kaum mehr als bei Bustopologie.
    - Ausfall einer Kabelstrecke oder einer Station kann zu einem Totalausfall führen.

      - Häufig Ausführung als Doppelring, um den Ausfall einer Verbindung oder einer Station kompensieren zu können.
- Logische Topologie
  - Bustopologie
  - Ringtopologie
  - Physikalische Stern- oder Baumtopologien werden durch entsprechende Verschaltung der Leitungen zu logischen Bussen oder Ringen verwandelt (anders bei WAN-Verbindungen, bei denen die Baumstruktur explizit berücksichtigt wird).

4.5. Zwei Grundregeln

Beim Entwurf einer Netzwerkarchitektur sind zwei Grundregeln zu berücksichtigen:

- Es ist davon auszugehen, daß Daten verfälscht werden können.
- Es ist davon auszugehen, daß Daten verloren gehen können.

4.6. Arten von Netzwerkkomponenten

Unterscheidung

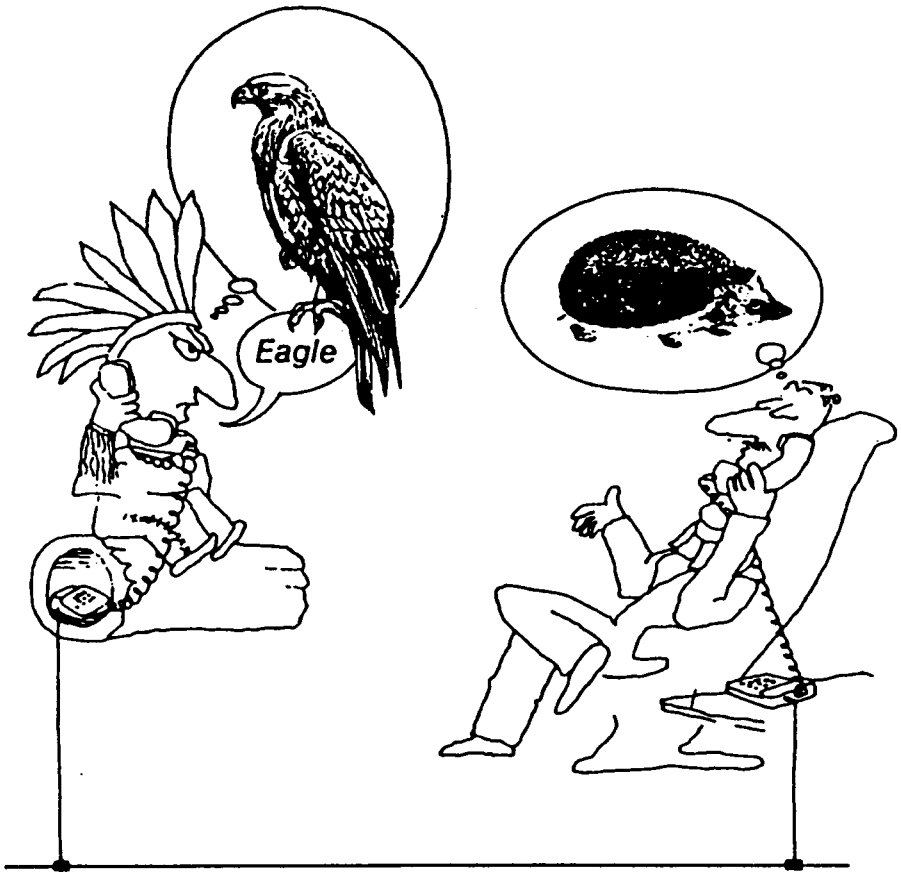
- ***Hardware***
  - ***Passive Komponenten***: Komponenten die über keine Stromversorgung verfügen
    - Kabel
    - Stecker
    - Passive Ringleitungsverteiler (im Token Ring)
  - ***Aktive Komponenten***: Komponenten, die eine Stromversorgung benötigen
    - Rechner
    - Internetworking Komponenten (Repeater, Brücken,Router usw.)
- ***Architekturen*** und ***Normen***
  - Modelle für Netzwerkverfahren
  - Normierungen von Netzwerktechnologien und Komponenten
- ***Software***
  - Netzwerkbetriebssysteme
  - Netzwerkanwendungen

5. Netzwerkarchitekturen

5.1. Struktur von Datenkommunikation

Definition: Datenkommunikation meint Austausch von Information zwischen oder mit Hilfe von Rechnersystemen.

Beispiel: Verbindung ist noch nicht Kommunikation:



Wie bei der verbalen Kommunikation gehört auch zur Datenkommunikation ein ***Regelwerk***.

Die ISO (International Standard Organisation) hat dazu ein Referenzmodell konzipiert, das ***OSI-Referenzmodell*** (OSI = Open System Interconnection).

Dieses Modell stellt nur eine Strukturierung der Datenkommunikation in Teilaufgaben dar, um dadurch die eigentliche „Sprache“ beschreiben zu können, jedoch noch keine Definition einer „Sprache“. Man bedenke die Spannweite der Datenkommunikation:

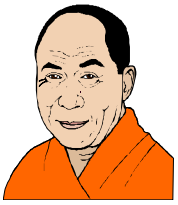
Geographische Spannweite

Technologische Spannweite der Datenkommunikation:

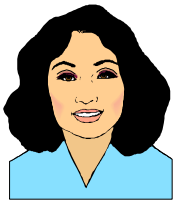
Auf der einen Seite - der ***Anwenderseite*** - erfolgt die Kommunikation z.B. durch den Befehl „senden“, den eine Person zwecks Versenden E-Mail abgibt. Auf der anderen Seite - der ***technischen Seite*** - werden elektrische Signale auf einem Kupferkabel erzeugt.

Beispiel: Zwei Philosophen unterschiedlicher Nationalität tauschen Ihre Gedanken aus (nach Kauffels, Einführung in die Datenkommunikation)

Der indische Philosoph schreibt seine Gedanken in Hindi nieder.



Die japanische Philosophin liest die Gedanken des indischen Kollegen.



Der Text wird einem Übersetzer übergeben.

Der Text wird der japanischen Philosophin übergeben.

Der Übersetzer überträgt die Gedanken des Philosophen in die lateinische Sprache.

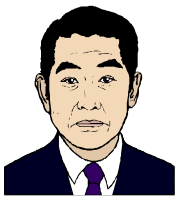
Die Übersetzerin übertragt den lateinischen Text in die japanische Sprache.

Der übersetzte Text wird einer Sekretärin zur weiteren Beförderung übergeben.

Der eingegangene Text wird an die Übersetzerin weitergeleitet.

Die Sekretärin sendet den Text per Fax an das Sekretariat der japanischen Philosophin.

Der Sekretär der japanischen Philosophin empfängt das Fax.



(Durchgezogenen Pfeile: reale Kommunikation, gestrichelte Pfeile: virtuelle Kommunikation.)

In diesem Beispiel kommunizieren die Philosophen untereinander in ihrer „Sprache“, d.h. in ihren Begriffen und Kategorien (vgl. oben: Anwenderseite), ebenso schreibt der eine Übersetzer gedanklich einen Brief an den anderen Übersetzer und die Sekretäre kommunizieren miteinander (technische Seite).

Andererseits bestehen direkte Kontakte (notwendigerweise) nur zwischen Philosophen und Übersetzern, zwischen Übersetzern und Sekretären und zwischen den Sekretären.

Dem Philosophen wird so das Problem der fremden Sprache oder auch der Bedienung eines Faxgeräts abgenommen. Der Übersetzer muß selbst keine philosophischen Gedanken entwickeln und auch Faxgeräte nicht bedienen können. Den Sekretären kann dafür der Inhalt der Faxe gänzlich gleichgültig sein.

Die Philosophen müssen die Sekretäre nicht einmal kennen (und umgekehrt).

5.2. Das OSI-Referenzmodell

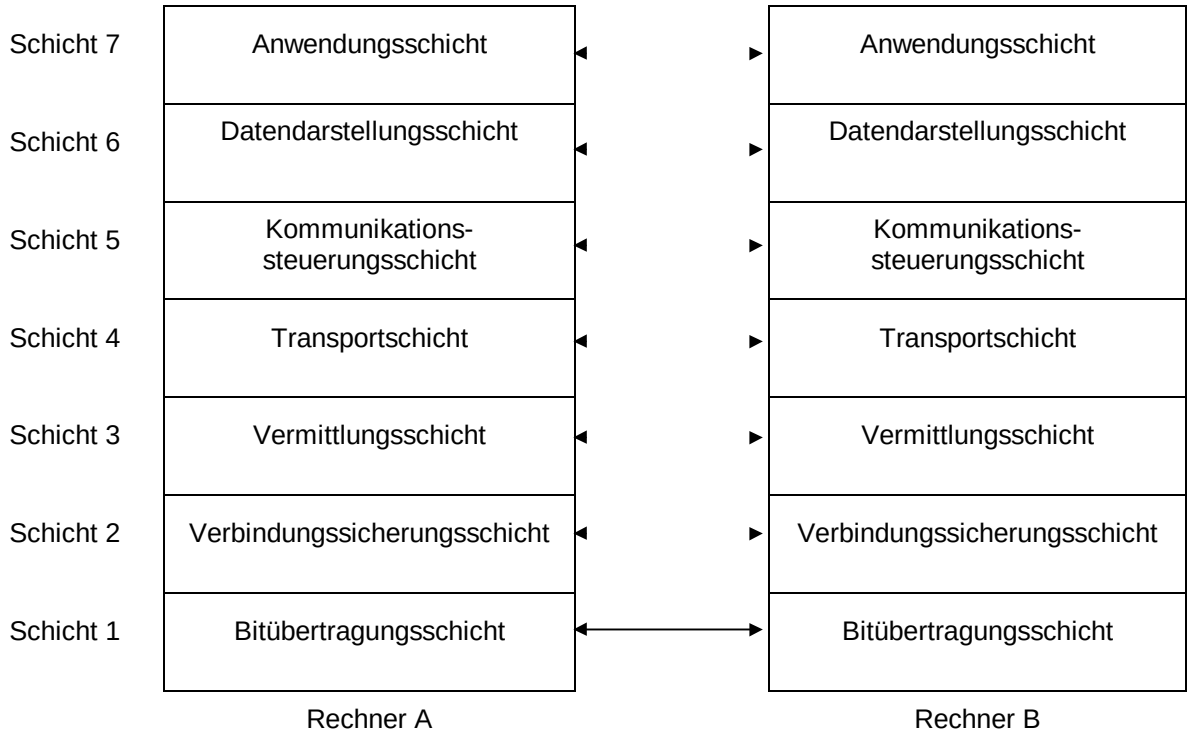
Analog dem obigen Beispiel wird die Kommunikation in Netzen in ***Schichten*** verschiedener Funktionalität eingeteilt.

Die ***Instanzen*** (Programme, Prozesse, Treiber, Firmware) jeder Schicht kennen nur die Schnittstellen zu der übergeordneten und der untergeordneten Schicht. An diesen Schnittstellen werden einige wenige ***Dienste*** (Programmschnittstellen) definiert. Die Instanzen jeder Schicht kommunizieren (virtuell) über das Netz nur mit Instanzen der gleichen Ebene beim Kommunikationspartner.

Dadurch lassen sich die einzelnen Schichten einfacher definieren, vielseitiger verwenden und flexibler kombinieren.

Die Schichten werden in zwei Gruppen unterteilt: ***Anwendungsbezogene Schichten***, die mit ***Informationstransfer*** beschäftigt sind, und ***netzwerkbezogene Schichten***, die sich mit ***Datentransfer*** befassen.

Das OSI-Referenzmodell definiert folgende Schichten:



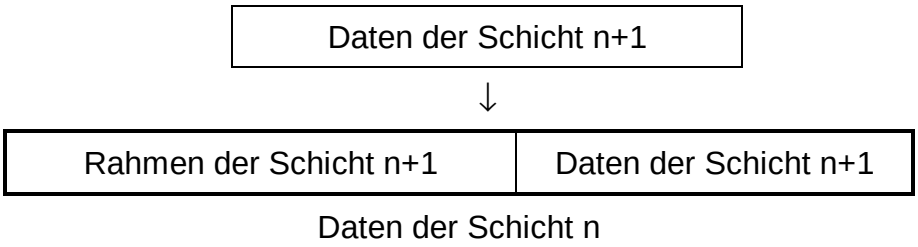
(Virtuelle Kommunikation gestrichelte, tatsächlicher Transport durchgezogene Pfeile)

Im OSI-Modell sind die Schichten 5-7 anwendungsbezogen, die Schichten 1-4 netzwerkbezogen.

In jeder Schicht können mehrere unabhängige Instanzen implementiert und (gleichzeitig) genutzt werden.

5.3. Rahmenstruktur

Die Daten, die von der einzelnen Schichten übertragen werden, müssen beim Übergang von einer höheren Schicht zu einer niederen Schicht (n+1- nach n-Schicht) um einen ***Rahmen*** erweitert werden, der die Informationen enthält, die zwischen den entsprechenden (n+1-) Schichten der Kommunikationspartner ausgetauscht werden (***Protokollinformationen*** zur Steuerung der Kommunikation).



Übergang zwischen zwei Schichten

Beim Übergang von der niedrigeren Schicht n zur höheren Schicht n+1 wird der Rahmen entsprechend von der Schicht n+1 interpretiert und entfernt.

Durch die Rahmenstruktur der Kommunikation entstehen Datenmengen, die zusätzlich zu den eigentlichen Nutzdaten übertragen werden müssen, der sogenannte ***Protokolloverhead***. Dieser kann je nach Größe der eigentlichen Nutzdaten erhebliche Einflüsse auf die Qualität der Netzdienste haben.

5.4. Die Netzwerkschichten

5.4.1. Schicht 1: Bitübertragungsschicht

Englische Bezeichnung: ***Physical Layer*** (Abkürzung: ***PHY***)

Andere Namen: Physikalische Ebene

Aufgaben:

- Festlegung von Kabeleigenschaften
- Festlegung physikalischer Eigenschaften von Anschlußkomponenten (Stecker usw.)
- Festlegung der Signalkodierung auf dem Medium (Spannungspegel bzw. optische Signale, Kodierungsverfahren, Modulation)

Auf der physikalischen Ebene können nur Rechner miteinander kommunizieren, die über eine direkte physikalische Verbindung zu einander verfügen (exklusive Nutzung eines Kabels oder gemeinsame Nutzung zusammen mit weiteren Rechnern)

5.4.2. Schicht 2: Sicherungsschicht

Englische Bezeichnung: ***Data Link Layer*** (***DLL***)

Andere Namen: Verbindungsebene, Verbindungssicherungsschicht

Die Schicht 2 wird in der Praxis in Unterschichten unterteilt:

- eine von der verwendeten Netzwerktechnik (z.B. Ethernet, Token-Ring, FDDI) abhängige Schicht, die Medienzugangskontrollschicht (Medium Access Control Layer, ***MAC-Layer***) und
- eine von der Netzwerktechnik unabhängige Schicht, die Kontrollschicht für logische Verbindungen (Logical Link Control Layer, ***LLC-Layer***)

Aufgaben:

- ***Zugangsregelung*** durch Festlegung von Mechanismen zur Vergabe von Sendeberechtigungen (insbesondere bei gemeinsamer Nutzung des Mediums durch mehrere Stationen). (MAC-Teilschicht)
- Vergabe von ***Stationskennungen*** zwecks Identifikation und Adressierbarkeit (Eindeutige Adressierung). (MAC-Teilschicht)
- ***Sicherung der Datenübertragung*** durch Überprüfung der korrekten Übertragung mittels Berechnung von ***Prüfsummen*** (Cyclic Redundancy Check, CRC) für das Datenfeld auf der Sender- und Empfängerseite und Vergleich nach dem Empfang mit der mitübertragenen Prüfsumme. (LLC-Teilschicht)
- ***Sicherung der Datenübertragung*** durch Protokolle zum Aufbau und Abbau ***virtueller Verbindungen*** und Festlegung von Mechanismen zur ***Rückmeldung*** des korrekten Empfangs an den Sender (optional). (LLC-Teilschicht)

5.4.3. Schicht 3: Vermittlungsschicht

Englische Bezeichnung: ***Network Layer***

Andere Namen: Netzwerkebene

Aufgaben:

- Ermöglicht durch Vermittlungsfunktion Datenaustausch über die Grenzen lokaler Netze hinweg (***Gesamtnetz***).
- Festlegung einer eindeutigen ***Adressierung*** im globalen Netz, die durch ihre Systematik eine Zustellung von Paketen erlaubt.
- Wegevermittlung und -verwaltung zwischen verschiedenen Netzen und durch Zwischennetze hindurch (***Routing***).
- Anpassung von Paketgrößen an Medienbeschränkungen (***Fragmentierung***).

5.4.4. Schicht 4: Transportschicht

Englische Bezeichnung: ***Transport Layer***

Andere Namen: -

Aufgaben:

- Kontrolle der Ende-zu-Ende-Verbindung (***Verbindungsaufbau und -abbau***).
- Sicherung der Datenübertragung und Übertragungsqualität durch Bestätigungsmeldungen vom Empfänger zum Sender (von Ende zu Ende), ***Flußkontrolle***.

- Bei Bedarf ***Segmentierung*** und Wiederzusammensetzung von Datenpaketen (übergeordnete Ebenen kennen die maximalen Größen nicht).
- Kennzeichnung der Pakete durch ***Numerierung***.

5.4.5. Schicht 5: Kommunikationsteuerungsschicht

Englische Bezeichnung: ***Session Layer***

Andere Namen: Sitzungsebene

Aufgabe:

- Aufbau und Abbau von Verbindungen zwischen Instanzen (Prozessen, Dienste) der kommunizierenden Endgeräte.
- Dialogsteuerung (Festlegung von Synchronisationspunkten zum eventuellen Wiederaufsetzen nach Abbrüchen)
- Aktivitätssteuerung (Pausieren von Kommunikationen)
- Meldung von Ausnahmezuständen (z.B. Fehler)

5.4.6. Schicht 6: Darstellungsschicht

Englische Bezeichnung: ***Presentation Layer***

Andere Namen: Präsentationsebene, Datendarstellungsschicht

Aufgabe:

- Formatumwandlung von lokalen Datenformaten in eine einheitliches Netzformat (z.B. Konvertierung von Zeichensätzen wie ASCII und EBCDIC)

5.4.7. Schicht 7: Verarbeitungsschicht

Englische Bezeichnung: ***Application Layer***

Andere Namen: Anwendungsebene

Aufgabe:

- Die Verarbeitungsschicht besteht aus den einzelnen Netzwerkanwendungen, wie sie sich den Anwendern des Netzes präsentieren.
- In der Verarbeitungsschicht ist die Bedienungsoberfläche gegenüber dem Benutzer definiert.
- Die Verarbeitungsschicht definiert die anwendungsbezogenen Kommunikation zwischen den Anwendungsprozessen der Endgeräte (z.B. Anforderungen zum Lesen oder Schreiben von Dateien bei einer Dateiübertragung einschließlich Namensgebung).
- Die Verarbeitungsschicht greift auf die Hilfsmittel der lokalen Betriebssysteme zu.

6. Netzwerktechnologien im LAN-Bereich

6.1. Überblick

Gängige Vernetzungstechnologien im LAN-Bereich sind:

- ***Terminalvernetzung***
  - Im wesentlichen veraltet, aber zum Teil noch vorhanden.
  - Statt einer direkten Verkabelung Terminal-Rechner erfolgt meist der Anschluß von Terminals an Terminalserver, die dann über ein LAN mit Rechnern kommunizieren.
  - Wird im weiteren nicht behandelt.
- ***Ethernet***
  - In LANs die am weitesten verbreitete Technologie.
  - Durch Bustopologie und weite Verbreitung sehr kostengünstig zu realisieren.
  - Mit einer Übertragungskapazität von 10 MBit/s ein LAN mittlerer Geschwindigkeit. (Realistische ist eine Auslastung von 30% die oberste Grenze.)
  - Ursprüngliche Entwicklung durch Digital, Intel und Xerox.
  - Statistische Zugriffskontrollverfahren.
  - Weiterentwicklungen zu ***Fast Ethernet*** mit 100MBit/s Übertragungskapazität.
- ***Token-Ring***
  - Von IBM entwickeltes Vernetzungssystem mit (logischer) Ringtopologie und in der Praxis physikalischer Sterntopologie als Konkurrenz zu Ethernet.
  - Durch Anforderungen an die Verkabelung, Netzwerkadapter und geringere Verbreitung teurer als Ethernet.
  - Mit einer Übertragungskapazität von 4 oder 16 MBit/s ein LAN mittlerer Geschwindigkeit.
  - Deterministisches Zugriffskontrollverfahren.
- ***FDDI***
  - Hochgeschwindigkeitsnetz für LAN und MAN (100 MBit/s)
  - Physikalische Doppelring und/oder Baumstruktur.
  - Logische Ringstruktur.
  - Deterministisches Zugriffskontrollverfahren.
- ***ATM***
  - Hochgeschwindigkeitsnetz für LAN und WAN.
  - Eignung für Multi-Media-Anwendungen.
  - Cell-Switching-Technologie.

- Standardisierung noch nicht abgeschlossen und bisher noch in der Erprobungsphase.
- Das Netz der Zukunft.
- Im weiteren nicht behandelt.

6.2. Ethernet

6.2.1. Medienzugriffsverfahren

Ethernet ist ursprünglich unter diesem Namen von Digital, Intel und Xerox als Ethernet Version 1 und Ethernet Version 2 „standardisiert“ worden. An manchen Stellen findet man daher das Kürzel DIX für die drei Entwicklerfirmen. Ethernet V.1 hat heute keinerlei Bedeutung mehr.

Später erfolgte eine Standardisierung durch internationale Gremien (IEEE und ISO), die allgemein unter der Bezeichnung 802.3 bekannt ist. Diese weicht geringfügig von Ethernet V.2 ab ist aber damit kompatibel.

Der Begriff Ethernet wird meist für beide Standards benutzt.

Das wesentliche Charakteristikum des Ethernet ist das Verfahren der Mediumzugriffskontrolle. Das Verfahren nennt sich CSMA/CD (Carrier Sense, Multiple Access with Collision Detection) und entspricht den Prinzipien einer Gesprächsrunde ohne Diskussionsleiter.

Bei einer solchen Diskussionsrunde gelten folgende Regeln:

- Jeder Teilnehmer kann anfangen zu reden, wenn nicht schon ein anderer redet.
- Sollten mehrere Teilnehmer zufällig gleichzeitig in einer Gesprächspause anfangen zu reden, so haben sie alle sofort ihren Beitrag abzubrechen.
- Durch zufällige Verzögerungen (oder Gesten) ergibt sich dann, wer als nächster reden darf.

Vorgehen bei Ethernet

- Sendewillige Stationen hören das Medium ab und warten bis es frei ist (Carrier Sense).
- Ist das Medium frei, so kann jede sendewillige Station nach einer Pause von 96 Bit (9,6µs, 12 Byte, ***Interframe Gap***) einen Sendevorgang beginnen (Multiple Access).
- Während des Sendens überprüft jede Station ob andere Stationen gleichzeitig senden, es also zu einer Kollision kommt (Collison Detection). Kollisionen werden an der Überlagerung von Signalen (überhöhte Signalpegel, Phasenverschiebung der Signale) erkannt.
- Nach dem Erkennen einer Kollision werden noch 4-6 weitere Byte (meist als 01-Bitmuster) gesendet, damit alle Stationen genügend Zeit haben, die Kollision zu erkennen (Jam Signal).
- Nach dem Ende aller Übertragungen während eines Kollisionsvorgangs warten alle Stationen 9,6µs (Interframe Gap).

- Die kollisionserzeugenden Stationen warten zusätzlich ein Vielfaches i der Slot time (512 Bit, 64 Byte, 51,2µs), wobei i eine Zufallszahl zwischen 0 und 2^k ist und k die Nummer des Übertragungsversuchs für ein bestimmtes Paket (maximal 10) ist. (***Backoff-Algorithmus***)
- Nach Ablauf der Wartezeit beginnt der Algorithmus von vorn.

(Sollte bei dem Versuch ein bestimmtes Paket zu senden 16mal eine Kollision auftreten, so wird ein Fehler (Excessive Collision) gemeldet und der Übertragungsversuch abgebrochen.)

6.2.2. Konsequenzen des CSMA/CD-Verfahrens

Aus der Notwendigkeit der Kollisionserkennung ergeben sich Konsequenzen:

- Die sendenden Stationen müssen eine Kollision vor dem Ende des jeweiligen Sendevorgangs erkennen. Beispiel:
  - Station A beginnt zu senden (Zeitpunkt 0).
  - Station B beginnt unmittelbar bevor sie das Signal von A erreicht zu senden (Zeitpunkt t).
  - Station B erkennt praktisch sofort die Kollision (Zeitpunkt t)
  - Station A erkennt die Kollision erst, wenn das Signal von B bei A angekommen ist (Zeitpunkt 2t).
  - Hätte Station A den Sendevorgang zum Zeitpunkt 2t schon beendet, so hätte A die Kollision nicht erkannt, wodurch das Verfahren zusammenbrechen würde (CD!).

  Folgerung: Die ***maximale Signallaufzeit*** zwischen zwei Stationen im Netz und die ***minimale Paketlänge*** müssen unter Berücksichtigung der ***Übertragungsrate*** so aufeinander abgestimmt sein, daß das Senden eines Pakets minimaler Größe länger als die doppelte maximale Signallaufzeit im Netz dauert.

  Im Ethernet müssen folgende Werte eingehalten werden:

  - Maximale Signallaufzeit: 25,6µs
  - Minimale Paketlänge: 64 Byte (512 Bit, 51,2µs)

  Die maximale Signallaufzeit ergibt sich aus der ***Ausbreitungsgeschwindigkeit*** des Signals auf dem Medium und den ***Verzögerungen*** durch die aktiven Komponenten im Netz wie Sendern, Empfängern oder Verstärkern (wobei die letzteren entscheidend sind!). Daher bedeutet die Beschränkung der Signallaufzeit eine Beschränkung in der Ausdehnung des Netzes, insbesondere eine Beschränkung der Anzahl der Verstärker zwischen je zwei Stationen. (Kabellängenrestriktionen wegen Dämpfung sind weniger restriktiv, Ausnahme: Fast Ethernet über Glasfaserkabel)

- Die obige Einschränkung führt effektiv auch zu einer Begrenzung der mit CSMA/CD-Verfahren möglichen Übertragungsrate, denn eine höhere Übertragungsrate verkürzt die für die Übertragung eines Pakets benötigte Zeit, während die Signallaufzeit durch die Verzögerungen in den aktiven Komponenten kaum kleiner wird. Um den CSMA/CD-Algorithmus weiterhin benutzen zu können, gibt es zwei Möglichkeiten:

  - Die minimale Paketlänge müßte erhöht werden. Dieses ist nicht praktikabel, weil damit ein erheblicher Teil der Netzbandbreite im Falle von Kollisionen verschwendet würde.
  - Die maximale Signallaufzeit müßte verkürzt werden (kürzere Kabel, weniger und schnellere Netzkomponenten zwischen den Endstationen). Dieses wird bei Fast Ethernet benutzt (2,56µs).
- Bei zunehmender Auslastung des Übertragungskanals und zunehmender Anzahl von beteiligten Stationen steigt die Kollisionswahrscheinlichkeit. Daher liegt die ***effektive Datenrate*** unter Umständen deutlich unter der ***nominellen Datenrate***.
- Je ausgedehnter ein Ethernet-Segment ist, desto länger ist die Risikophase in der Kollisionen auftreten können und je höher ist die Wahrscheinlichkeit, daß Kollisionen auftreten.

Andere Interpretation des CSMA/CD-Algorithmus:

- Warten auf freies Medium
- Belegen des Mediums
- Warten auf Bestätigung der Zugriffsberechtigung (keine Kollision innerhalb 51,2µs)

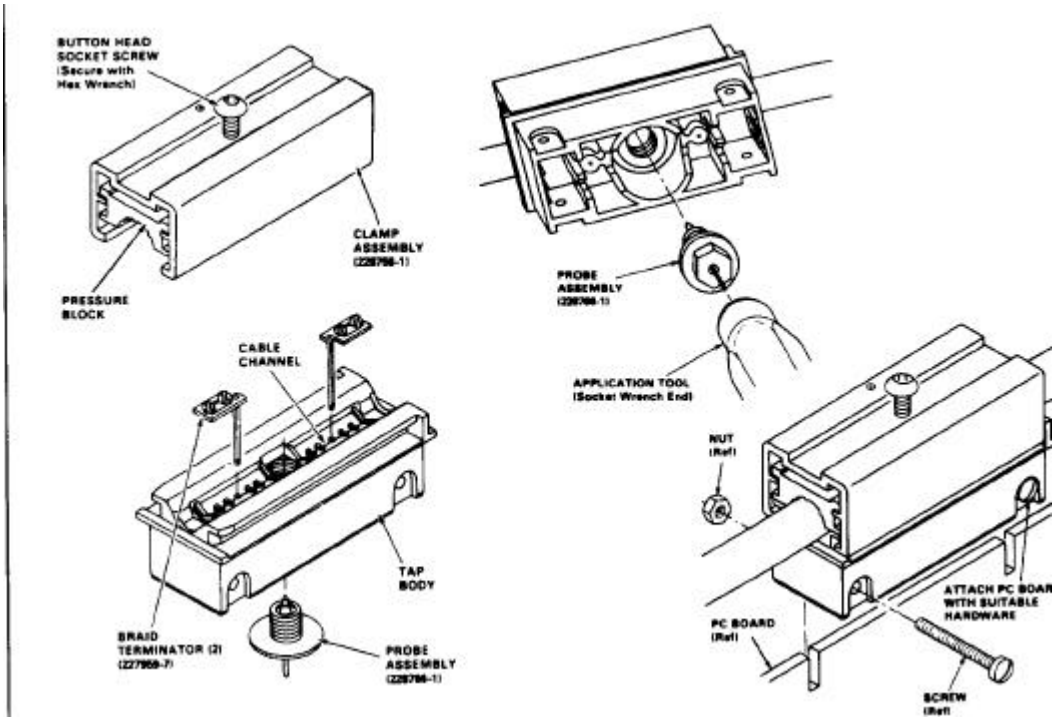
6.2.3. Ethernet-Varianten

6.2.3.1. 10 Base 5 oder Thickwire-Ethernet

- Ürsprüngliche Ethernet-Verkabelung
- Heute veraltet (höchstens noch in lokalen Backbones zu finden).
- 500 m maximale Segmentlänge
- Koaxialkabel mit
  - 50 Ω Wellenwiderstand
  - 0,77c Signalausbreitungsgeschwindigkeit (c=Lichtgeschwindigkeit=300.000 m/s)
  - ca. 1 cm Durchmesser
  - 25 cm Biegeradius (beim Verlegen einzuhaltender minimaler Radius einer Biegung des Kabels)

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	10.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,77	
Maximale Segmentlänge	l_{max}	500	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	2,166	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,1	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	23,08	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	21,66	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	51,2	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	11.817	m

- Maximale Anzahl Anschlüsse pro Segment: 100 MAUs (MAU=Media Access Unit, auch Transceiver genannt)
- Maximale Stationsanzahl im Netz (genauer: innerhalb einer Kollisionsdomäne): 1024
- Anschlüsse von Stationen durch
  - „Vampirklemmen“ (Taps) ohne Unterbrechung des Kabels oder



  - Steckverbinder (Installation nach Auftrennung des Kabels)
- Mindestabstand zwischen zwei Anschlüssen: 2,5 m
- Anschluß von Stationen an MAUs über Dropkabel mit
  - Maximaler Kabellänge von 50 m
  - Signalausbreitungsgeschwindigkeit 0,65c
  - Maximale Signallaufzeit von 0,257 µs

6.2.3.2. 10 Base 2 oder Thinwire-Ethernet

- Historisch die zweite Variante von Ethernet-Verkabelung
- Billigere und flexiblere Alternative zu 10 Base 5
- Maximale Länge eines Segments: 185 m
- Koaxialkabel mit
  - 50 Ω Wellenwiderstand
  - Signalausbreitungsgeschwindigkeit (ca.) 0,65c
  - Kabeldurchmesser ca. 0,5 cm
  - Minimaler Biegeradius bei Verlegung 5 cm
  - Leicht voneinander abweichende Kabeltypen (zusätzliche Schirmung, abweichende Signalausbreitungsgeschwindigkeiten)

Achtung: unterschiedliche Kabel sollten möglichst nicht vermischt werden!

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	10.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,65	
Maximale Segmentlänge	l_{max}	185	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	0,949	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,1	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	19,49	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	9,49	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	51,2	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	9.979	m

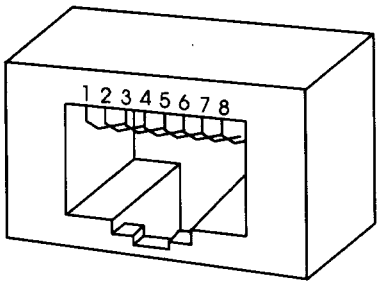
- Maximale Anzahl Anschlüsse pro Segment: 30
- Anschlußmöglichkeiten:
  - BNC-Steckverbinder
  - Unterbrechungsfreie Steckverbindungen / Dosen
- Mindestabstand zwischen zwei Anschlußstellen: 0,5 m

6.2.3.3. 10 Base T oder Twisted-Pair-Ethernet

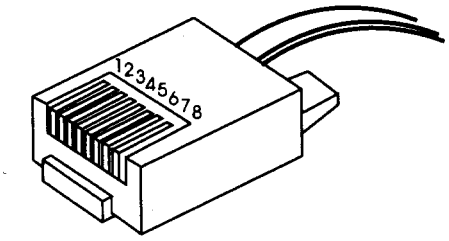
- Moderne Variante der Ethernet-Verkabelung
- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluß
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlußpunkt für jeden einzelnen Anschluß an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluß: 100 m
- Paarweise verdrillte Kabel mit
  - 100 Ω Wellenwiderstand
  - Signalausbreitungsgeschwindigkeit 0,585c bei ungeschirmten (UTP-) Kabeln
  - Signalausbreitungsgeschwindigkeit 0,75c bei geschirmten Kabeln des Typs „Kategorie 5“
  - Zweipaarige Kabel

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	10.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,75	
Maximale Segmentlänge	l_{max}	100	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	0,445	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,1	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	22,48	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	4,45	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	51,2	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	11.520	m

- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschlußtechnik: RJ45-Steckerverbinder



MAU MDI Connector



Twisted-Pair Link Segment Connector

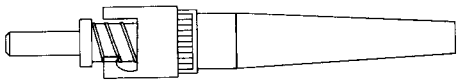
- Kostenintensivste (wegen Repeater) aber zukunftsicherste Verkabelungsvariante mit Kupferkabeln (bei Kategorie-5-Kabeln für andere Techniken bis 100 MHz)

6.2.3.4. 10 Base F oder Glasfaser-Ethernet

- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluß
- Auch für andere Netzwerktechniken nutzbar
- Eigener Anschlußpunkt für jeden einzelnen Anschluß an einem Sternkoppler
- Maximale Kabellänge für einen Anschluß:
  - 2000 m bei aktiven Sternkopplern
  - 500m bei passiven Sternkopplern (unüblich)
- Glasfaserkabel
  - In der Regel Gradientenkabel 62,5/125µ (in Europa abweichend oft 50/125µ)
  - Selten Monomodekabel 9/125µ
  - Zwei Fasern pro Verbindung
  - Signalausbreitungsgeschwindigkeit 0,68c

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	10.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,68	
Maximale Segmentlänge	l_{max}	2000	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	9,811	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,1	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	20,39	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	98,09	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	51,2	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	10.440	m

- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschlußtechnik: ST-Steckerverbinder



- Kostenintensive aber zukunftsichere Verkabelungsvariante
- Besser Abhörsicherheit als Kupferkabel
- Keine elektromagnetischen Beeinflußungen

6.2.4. Fast Ethernet

6.2.4.1. 100 Base TX

- Ethernet-Variante mit 100 MBit/s Übertragungsrate
- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluß
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlußpunkt für jeden einzelnen Anschluß an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluß: 100 m
- Paarweise verdrillte Kabel (wie bei 10 Base T) mit
  - 100 Ω Wellenwiderstand
  - Signalausbreitungsgeschwindigkeit 0,75c bei geschirmten Kabeln des Typs „Kategorie 5“
  - Zweipaarige Kabel der Kategorie 5

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	100.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,75	
Maximale Segmentlänge	l_{max}	100	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	0,445	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,01	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	2,25	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	44,44	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	5,12	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	1.152	m

- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschlußtechnik: RJ45-Steckerverbinder

6.2.4.2. 100 Base T4

- Ethernet-Variante mit 100 MBit/s Übertragungsrate
- Strukturierte Verkabelung
- Sternförmige Kabelführung zu jedem Anschluß
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlußpunkt für jeden einzelnen Anschluß an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluß: 100 m
- Paarweise verdrillte Kabel (wie bei 10 Base T) mit
  - 100 Ω Wellenwiderstand
  - Signalausbreitungsgeschwindigkeit 0,585c bei ungeschirmten (UTP-) Kabeln
  - Vierpaarige Kabel (auf ungeschirmten Kabeln der Kategorie 3 oder 4)

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	100.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,585	
Maximale Segmentlänge	l_{max}	100	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	0,570	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,01	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	1,754	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	57,013	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	5,12	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	898	m

- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschlußtechnik: RJ45-Steckerverbinder

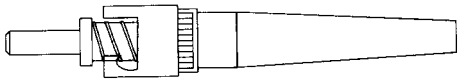
6.2.4.3. 100 Base FX

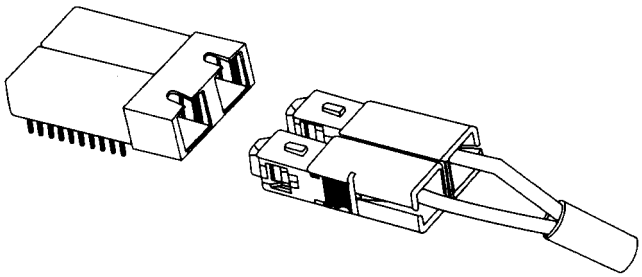
- Ethernet-Variante mit 100 MBit/s Übertragungsrate
- Strukturierte Verkabelung

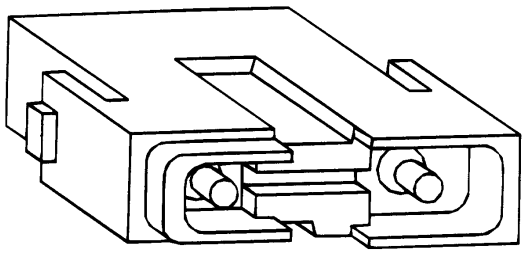
- Sternförmige Kabelführung zu jedem Anschluß
- Verkabelung mit Standardkabeln, die auch für andere Netzwerktechniken nutzbar sind.
- Eigener Anschlußpunkt für jeden einzelnen Anschluß an einem Verteiler mit Repeaterfunktion nötig
- Maximale Kabellänge für einen Anschluß: 450 m (bei Duplex-Übertragung bis 2000m)
- Glasfaserkabel
  - In der Regel Gradientenkabel 62,5/125µ (in Europa abweichend oft 50/125µ)
  - Selten Monomodekabel 9/125µ
  - Zwei Fasern pro Verbindung
  - Signalausbreitungsgeschwindigkeit 0,68c

Parameter	Bezeichnung / Formel	Wert	Einheit
Übertragungsrate	v	100.000.000	bit/s
Lichtgeschwindigkeit	c	299.792.458	m/s
Ausbreitungskoeffizient	n	0,68	
Maximale Segmentlänge	l_{max}	450	m
Maximale Signallaufzeit	$t_{max} = l_{max}/(nc)$	2,21	µs
Dauer eines Bits	$t_{bit} = 1/v$	0,01	µs
Länge eines Bits	$l_{bit} = nc/t_{bit}$	2,04	m
Anzahl Bits pro Segment	$b_{seg} = l_{max}/l_{bit}$	220,59	
Dauer von 64 Bytes	$t_{64Byte} = t_{bit} *8*64$	5,12	µs
Länge von 64 Bytes	$l_{64Byte} = l_{bit} *8*64$	1.044	m

- Maximale Anschlüsse pro Kabelsegment: 1 Station
- Anschlußtechnik: ST-, SC- oder MIC-Steckerverbinder





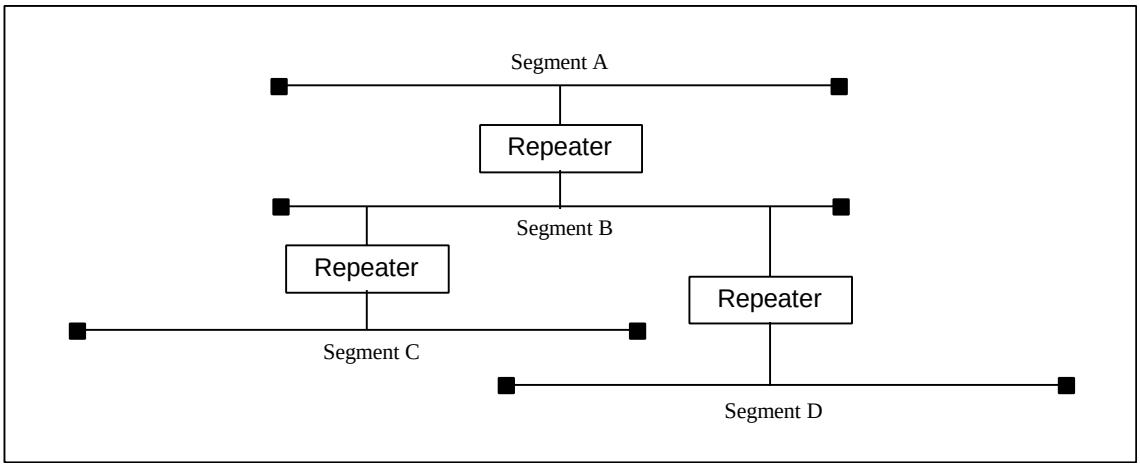


6.2.4.4. VG-AnyLAN

- Konkurrierende Entwicklung zu 100BaseXY-Standards
- Eigentlich kein Ethernet, da nicht CSMA/CD-Algorithmus
- Demand Priority Verfahren:
  - Vergabe der Zugriffsberechtigung durch den zentralen Verteiler
    - auf Anforderung
    - mit Möglichkeit von Prioritätenvergabe
    - in festgelegter Reihenfolge der Ports
- Standardisiert als IEEE 802.12 (nicht 802.3 wie alle Ethernet-Varianten)

6.2.5. Struktur einer Ethernet-Installation

- Einfachster Fall
  - Alle Stationen sind über ein Kabel in Reihe verbunden.
  - An den Enden des Kabel befindet sich je ein ***Abschlußwiderstand*** von 50 Ω.
- Problem der ***Dämpfung***
  - Wegen der immer vorhanden Abschwächung der Signal mit der Kabellänge, haben Netzkabel eine maximal zulässige Länge.
  - Bei Überschreiten der maximalen Länge müssen Verstärker (***Repeater***) eingesetzt werden.
  - Die Kabelabschnitte, die über Repeater verbunden werden, werden ***Segmente*** genannt.



6.2.6. Repeater

- Verstärkerfunktion
- Einsatzzweck: Überwindung von Längenrestriktionen durch Kabeldämpfungen
- Alle durch Repeater verbunden Segmente bilden bezüglich des CSMA/CD-Algorithmus eine Einheit (Kollisionsdomäne)

- Repeater verursachen eine Verzögerung der Signalübertragung (Faustregel: ein Repeater entspricht ungefähr einem 500m Segment).
- Anzahl der Repeater im Netz (oder genauer zwischen zwei beliebigen Stationen) ist begrenzt, wegen maximaler Signallaufzeit im Netz (Kollisionsfenster)
  - Repeaterregel:
    - maximal zwei Repeater zwischen zwei Stationen (drei Segmente) oder
    - maximal vier Repeater zwischen zwei Stationen (fünf Segmente), wenn zwei Segmente nur Link-Segmente sind (Remote-Repeater).
  - Bei 10 Base T sind alle Segmente, über die Repeater gekoppelt werden, Link-Segmente.
  - Bei 100 Base T maximal 2 Repeater (mit einem 5m Verbindungskabel)
- Durch Repeater darf kein Ringschluß entstehen
- Repeater-Varianten
  - Standard-Repeater mit zwei Ein- bzw. Ausgängen (Ports)
  - Multiport-Repeater mit mehr als zwei Ports
  - In Hubs integrierte Repeatermodule gelten zusammen als ein Repeater (soweit nicht zusätzliche Funktionen wie Aufteilung der Repeater auf interne Segmente implementiert sind).
  - Buffered Repeater
    - Zwischenspeicherung von Paketen bei besetzem Ausgang
    - Dadurch Unterbrechung der Kollisionsdomäne (mehr Repeater im Netz erlaubt)
- Repeater-Funktionalitäten
  - Auto-Partioning: automatische Abschaltung von gestörten Segmenten
  - Repeater-Jam:
    - Signalisierung von Kollisionen von einem Segment in ein anderes
    - Auf allen Segmenten wird ein Paket mit einem 01-Muster gesendet, das aber kürzer als minimal vorgeschrieben (also fehlerhaft) ist.

6.2.7. Adressierung

Jede Station im Ethernet muß eine eindeutige Adresse (***MAC-Adresse***) besitzen, um angesprochen werden zu können.

Der Standard legt fest, daß die MAC-Adressen ***48 Bit*** lang seien müssen.

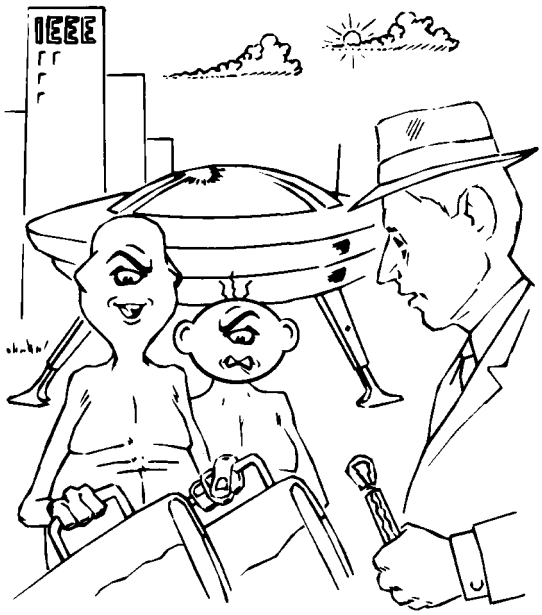
In der Praxis werden die Adressen von den Herstellern von Netzwerkadaptern festgelegt und bestehen aus einem 24 Bit langem Kode des Herstellers und einer ebensolangen Seriennummer (***Hardware-Adressen***).

Die MAC-Adressen weisen daher keine besondere Systematik bezogen auf die Netztopologie auf.

Neben Adressen für die einzelnen Stationen gibt es auch ***Gruppenadressen***, mit denen mehrere Stationen in Form eines Rundrufs angesprochen werden können. Solche Adressen sind dadurch erkennbar, daß das erste Bit der Adresse eine 1 ist.

Die bekannteste Gruppenadresse ist die ***Broadcast-Adresse*** (an alle). Sie besteht an allen Positionen aus Einsen (hexadezimal geschrieben FFFFFFFFFFFF). Die anderen Funktionsadressen werden als ***Multicast-Adressen*** bezeichnet (an viele).

Manche Software-Hersteller (z.B. Digital bei DECnet) benutzen nicht die vordefinierten, aber unsystematischen Hardware-Adressen, sondern definieren per Software andere MAC-Adressen, um eine Systematik der Adressen zu erhalten und in der Netzwerksoftware zu nutzen. Solche Adressen werden dadurch gekennzeichnet, daß das zweite Bit der Adresse den Wert 1 hat. Solche Adressen heißen dann ***lokale Adressen*** im Gegensatz zu den ***universalen Adressen*** mit einer 0 an Bitposition 2.



We are here to obtain a universal address from the IEEE.

6.2.8. Paketformate

Ethernetpakete sind wie folgt aufgebaut:

Ethernet V.2	PA	DA	SA	Typ	Data	FCS
Bytes	8	6	6	2	46-1500	4

802.3	PA	SFD	DA	SA	LEN	LLC	Data	FCS
Bytes	7	1	6	6	2	3	43-1497	4

Dabei sind :

PA:	Präambel zur Synchronisation des Empfängers auf den Takt des Senders 8 bzw. 7 Byte lang mit einer Folge von 0 und 1
SFD	Start Frame Delemiter, kennzeichnet den Beginn des eigentlichen Pakets und

	hat das Format 10101011.
DA	Destination Address, Zieladresse (6 Byte)
SA	Source Address, Quelladresse (6 Byte)
Typ	Typfeld zur Identifikation des Protokolls der MAC-Ebene (2 Byte)
Länge	Länge des Pakets (2 Byte)
LLC	„Logical Link Control“-Information (IEEE 802.2-Standard)
Data	Datenrahmen der übergeordneten Schichten
FCS	Prüfsumme, Frame Check Sequenz

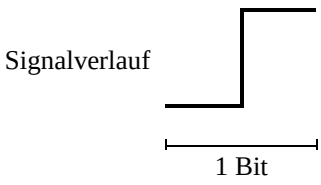
Die Übertragung der Bits eines jeden Bytes erfolgt mit dem niederwertigste Bit zuerst (***lsb***, least significant bit)

6.2.9. Arten fehlerhafter Pakete im Ethernet

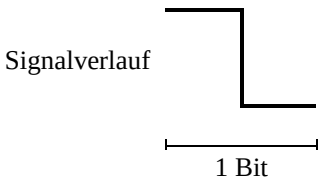
- CRC-Fehler: Die Prüfsumme ist falsch.
- Alignment-Fehler: Die Anzahl der Bits ist nicht durch 8 teilbar.
- Runt-Pakete: Pakete, die kürzer sind als die minimale Länge.
- Jabber- oder Giant-Pakete: Pakete mit Überlänge
- Late Collisions: Kollisionen, die nach mehr als 51,2 µs nach Beginn des Pakets auftreten.
- Excessive Collisions: 16 Kollisionen beim Versuch ein Paket zu senden.

6.2.10. Übertragungsverfahren

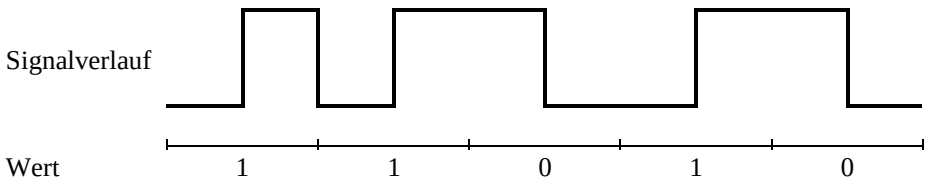
- Signalisierung mit Pegel zwischen 450 mV und 1315 mV
- Idle-Level: 0 mV ± 40 mV
- Gleichstromfreie Signalisierung
- Binäre Kodierung (nur 0 und 1)
- Signalisierung durch Spannungswechsel (nicht durch Spannungspegel)
- Selbstsynchronisation der Empfänger aus den Signalen
- Manchester-Codierung
  - 1 ist Übergang von negativem zu positivem Pegel



  - 0 ist Übergang von positivem zu negativem Pegel



- Beispiel



- Datenrate 10 MBit/s bei einer
- Bitrate (aus dem Kehrwert der Dauer eines Bits berechnet) von 10 MBit/s, einer
- Fundamentalfrequenz (Kehrwert aus der Dauer des kürzesten Signalzyklus) von 10 MHz und einer
- Baudrate oder Datentaktrate (Kehrwert der Dauer des kürzesten Impulses) von 20 Mbaud.
- Frequenz muß innerhalb minimaler Schwankungen bleiben
- Flankensteilheit muß innerhalb bestimmter Toleranzen liegen
- Für Fast Ethernet andere Kodierung (4B/5B Kodierung und Übertragung im MLT-3-Kode, s. FDDI)

6.3. Token Ring

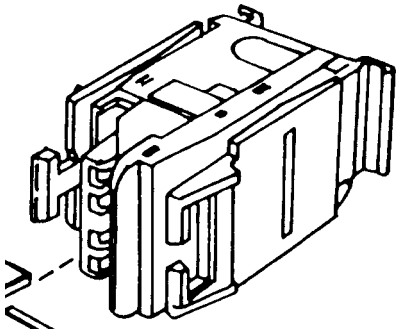
6.3.1. Überblick

- Logische Ringtopologie
- Physikalisch meist als Stern aufgebaut
- Durch physikalische Sternstruktur bessere Ausfallsicherheit
- Kopplung im Verteilerstandort durch passive oder aktive MAUs oder RLV (Medium Access Unit bzw. Ringleitungsverteiler)
- Deterministische Zugriffskontrollverfahren (Token-Prinzip)
- Zwei Varianten
  - 4 MBit/s Übertragungskazität (ursprünglicher Standard)
  - 16 MBit/s Übertragungskapazität (spätere Erweiterung)
- Von IBM entwickelt
- Als IEEE-Standard 802.5 normiert (bzw. ISO 8802.5)
- LLC-Protokoll 802.2 in Ebene 2 (wie bei Ethernet 802.3)

6.3.2. Medien

- Typisches Kabel: Geschirmte paarweise verdrillte Kabel vom IBM-Typ 1 oder 1M
- Andere Kabel: LWL und andere TP-Kabel
- Bei IBM-Typ-1-Verkabelung
  - geschirmte paarweise verdrillte Vierdrahtkabel mit
    - 150 Ω Wellenwiderstand

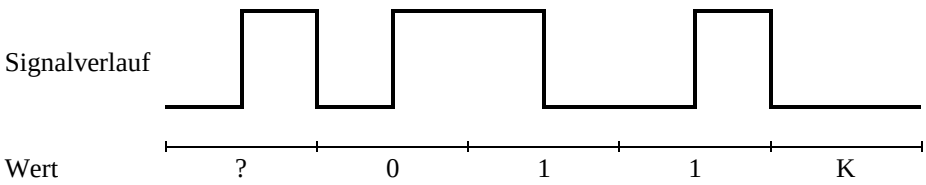
  - 0,64 cm Durchmesser
- Maximale Kabellänge zum Verteiler (Lobe-Kabel) 100 - 375 m abhängig von der Anzahl der Verteilerstandorte und Ringleitungsverteiler
- Maximal 260 Geräte in einem Ring
- Anschlußtechnik
  - Am Verteiler und an Anschlußdosen: hermaphroditischer IBM-Datenstecker (Würfel, Stecker und Buchse gleichzeitig)



  - Am Endgeräte: DB9-Buchse
- Ein Bit entspricht ca. 50m (bei 4 MBit/s) oder 12,5m (bei 16 MBit/s).

6.3.3. Übertragungsverfahren

- Jede Station regeneriert das Signal
- ***Differential-Manchester-Kodierung***
  - Abgeleitet vom Manchester-Code
  - Kodierung abhängig vom letzten Signal
    - Für 1: keine Umkehrung der Polarität am Signalanfang
    - Für 0: Umkehrung der Polarität am Signalanfang
    - In der Signalmitte bei 0 und 1 Polaritätsumkehrung
  - Zusätzliche Signale „J“ und „K“ ohne Polaritätsumkehr in der Signalmitte
    - „J“: keine Polaritätsumkehr am Anfang
    - „K“: Polaritätsumkehr am Anfang
  - Beispiel



- Datenrate 4 bzw. 16 MBit/s bei einer Bitrate von 4 bzw. 16 MBit/s, einer Fundamentalfrequenz von 4 bzw. 16 MHz und einer Baudrate von 8 bzw. 32 Mbaud.

6.3.4. Ringleitungsverteiler

- Zweck: Zusammenschluß der sternförmigen Verkabelung zu einem logischen Ring
- ***Überbrückungsfunktion*** bei nicht belegten Anschlüssen oder ausgeschalteten Endgeräten
- ***Aktive*** oder ***passive RLV***
  - Passive RLV arbeiten ohne Spannungsversorgung und schalten über elektromechanische Relais (bei Anlegen einer „Phantomspannung“ durch das Endgerät)
  - Aktive RLV regenerieren die Signale wie eine Endstation, benötigen aber dafür eine Stromversorgung
- Anschlußzahl pro RLV 8-20 (Original-IBM 8)
- RLV können über zwei zusätzliche spezielle Ports (Ring-In [***RI***] und Ring-Out [***RO***]) miteinander verbunden werden (jeweils RI mit RO).
- Bei Ausfall einer RI-RO-Verbindung wird eine Umleitung geschaltet (der zweite Ausfall teilt den Ring in zwei isolierte Ringe)

6.3.5. Token-Prinzip

- Auf dem Ring wird ein spezielle Paket erzeugt: das ***Token***
- Auf jedem Ring darf zu jedem Zeitpunkt nur ein Token vorhanden sein
- Länge des Token-Pakets: 3 Byte
- Spezielles Format des Token
- Senden darf nur die Station, bei der sich das Token befindet.
- Die sendende Station überträgt statt des Tokens einen Datenrahmen.
- Jeder Rahmen wird von allen Station unverändert weitergegeben (nur der Empfänger setzt ein Bit, um anzugeben, daß er den Rahmen erhalten hat, und der Monitor setzt ein Bit, um Rahemen, die nicht von der sendenden Satation entfernt wurden, erkennen zu können).
- Die sendende Station nimmt den Rahmen vom Ring und sendet das Token wieder aus. (Es ist nicht erlaubt, sofort einen weiteren Rahmen zu senden.)
- Eine einzige Station im Ring hat das Recht ein Token zu erzeugen und seine Existenz zu überwachen (***aktiver Monitor***)
- Zu einer Zeit darf nur eine Station aktiver Monitor sein.
- Jede Station kann aktiver Monitor sein.
- Bei der Initialisierungen oder beim Ausfall des aktuellen aktiven Monitors muß (über eine relativ aufwendigen Algorithmus) ein neuer aktiver Monitor bestimmt werden.
- Maximale Rahmenlänge im Token Ring: 10 ms (also 5.000 Byte bei 4 MBit/s und 20.000 Byte bei 16 MBit/s)

6.3.6. Adressierung

- MAC-Adressen wie bei Ethernet, nur mit umgekehrter Bit-Reihenfolge in den Bytes (***msb***, most significant bit, höchstwertigstes Bit)

6.3.7. Management-Protokoll

- Komplexität des Token-Ring durch verschiedene Management-Funktionen, die von jeder Station aus ausführbar sein müssen:
  - Jede Station muß die Funktion des aktiven Monitors übernehmen können.
  - Aufgaben des Management-Protokolls:
    - Sichergestellen, daß genau ein aktiver Monitor vorhanden ist.
    - Der aktive Monitor überwacht anhand von speziellen Bits in den Datenrahmen und über Management-Rahmen die Funktionsfähigkeit des Rings.
    - Mehrfachumkreisung von Rahmen im Ring verhindern (durch spezielles Bit im Rahmen).
    - Signalisierung von Fehlern durch den aktiven Monitor.
    - Feststellung des Nachbarn im Ring (MAC-Adresse)
  - Minimale Speicherkapazität von 24 Bit (Token-Länge) im Ring (entspricht bei 4 MBit/s ca 1.200m bzw. Bei 16 MBit/s 300m) bei Bedarf durch Pufferung durch aktiven Monitor
- Takt wird vom Monitor vorgegeben (keine Präambel zur Synchronisation), gegebenenfalls Aussenden von Idle-Signalen.

6.4. FDDI

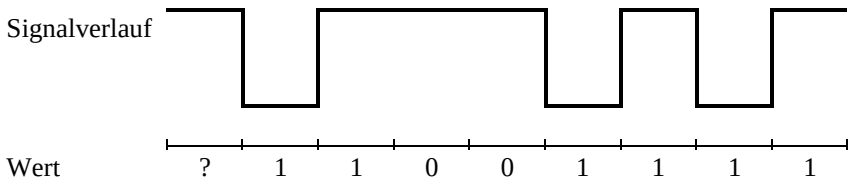
6.4.1. Überblick

- FDDI = Fiber Distributed Data Interface
- Ursprünglich nur für Glasfasern definiert.
- Hochgeschwindigkeitsnetz (100 MBit/s Datenrate)
- Normiert durch ANSI (X3T9.5)
- ***Token-Prinzip***
- Topologien
  - ***Doppelring*** oder
  - ***Baum*** oder
  - Kombination (***Dual Ring of Trees***)
- Maximale Ausdehnung des Gesamtrings (als Doppelring) 100 km bzw. 200 km bei Fehlerfällen (Rekonfiguration des Rings)
- Bis zu 500 Stationen im Ring
- Für lokale Nutzung neue Norm ***TPDDI*** (FDDI über TP-Kabel)
  - FDDI über Kupferkabel
  - Mit 100 MBit/s
  - Über Kategorie-5-Kabel

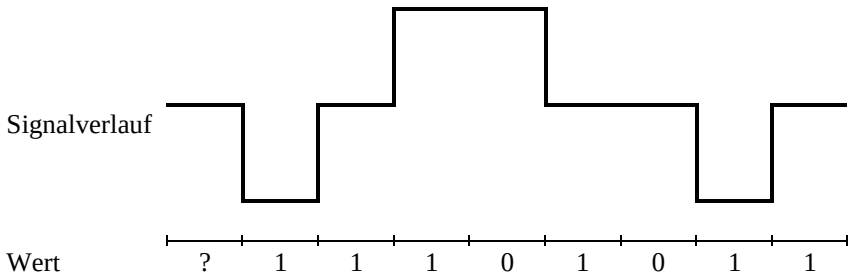
6.4.2. Übertragungstechnik

- 4B/5B-Kodierung:
  - Je 4 Bit werden in 5 Bit umgewandelt.

  - Dadurch 32 Bitkombinationen (oder Symbole) möglich, von den
    - 16 zur Datendarstellung und
    - 16 als Steuersignale genutzt werden können.
    - Auswahl der genutzten Kombinationen, so daß 0 und 1 möglichst gleichmäßig in den Symbolen vorkommen (Bei Licht: heißt das an/aus!)
  - Brutto 125 MBit/s bei Netto 100 MBit/s
- NRZI-Kodierung bei Übertragung über LWL
  - Non Return to Zero Inverted
  - (NRZ wäre:
    - 0 = Negativ (Licht aus)
    - 1 = Positiv (Licht an))
  - 1 durch Polaritätswechsel am Anfang dargestellt.
  - 0 durch keinen Polaritätswechsel dargestellt
  - Beispiel



  - Datenrate 100 MBit/s bei einer Bitrate von 125 MBit/s, einer Fundamentalfrequenz von 62,5 MHz und einer Baudrate von 125 Mbaud.
- MLT-3-Kodierung bei Übertragung über Kupferkabel
  - Dreistufige Kodierung (+,0,-)
  - Keine Änderung bedeutet 0
  - Jede Zustandsänderung (bei Beginn des Taktzyklus) bedeutet 1
  - Zustandsänderungen dürfen immer nur in eine vorgeschriebene Richtung erfolgen (0 → - → 0 → + → 0 → - → 0 usw.).
  - Beispiel



  - Datenrate 100 MBit/s bei einer Bitrate von 125 MBit/s, einer Fundamentalfrequenz von 31,25 MHz und einer Baudrate von 125 Mbaud.

6.4.3. Der Doppelring

- Ringtopologie ist bezüglich der Ausfallsicherheit ungünstig
- Um wenigstens einen Ausfall zu kompensieren, Doppelring aus
  - aktiven Ring (Primärring) und
  - Backup-Ring (Sekundärring, im Normalfall ungenutzt [keine Datenübertragung])
- Im Fehlerfall Umleitung über Backup-Ring:

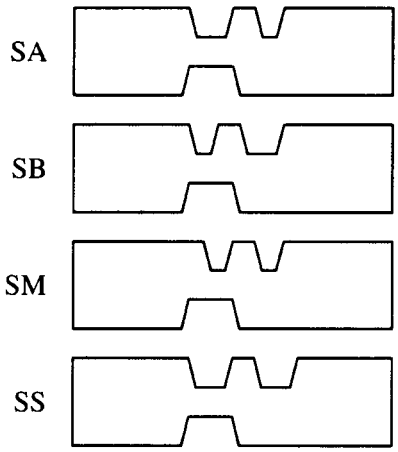
6.4.4. Typisierung aktiver Komponenten

- Unterscheidung: ***Ring-Anschluß oder Baum-Anschluß***
  - Ring:
    - Zwei Ports pro Station für Primär und Sekundärring
    - Bezeichnung: ***Dual Attached***
  - Baum:
    - Ein Port zum Anschluß an einen Konzentrator
    - Bezeichnung: ***Single Attached***
- Unterscheidung: ***Station oder Konzentrator***
  - Station: nur ein Anschluß an das Netz
  - Konzentrator: Mehrfacher Anschluß an das Netz
    - Mehrere Anschlüsse zum Anschluß weitere Geräte (nur Single Attached)
    - Ein Anschluß zur Anbindung an das übergeordnete Netz (Ring oder Baum)
    - Netzelement zum Aufbau von Baumstrukturen
- Vier Typen
  - ***DAS*** Dual Attached Station
  - ***SAS*** Single Attached Station
  - ***DAC*** Dual Attached Concentrator
  - ***SAC*** Single Attached Concentrator

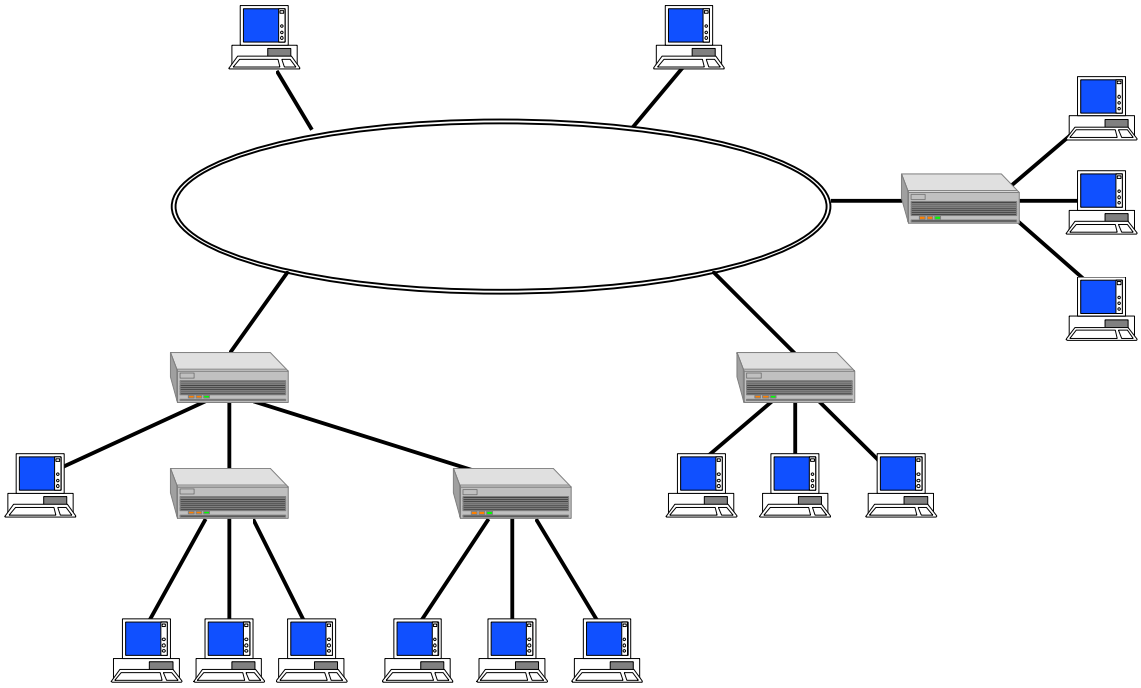
6.4.5. Port-Typen

- A-Port
  - Zum Anschluß an Doppelring
  - Empfang im Primärring
  - Senden (ggf) im Sekundärring
- B-Port
  - Zum Anschluß an Doppelring
  - Empfang (ggf) im Sekundärring
  - Senden im Primärring

- M-Port (Master)
  - Port eines Konzentrators zum Anschluß eines SAC oder einer SAS
- S-Port (Slave)
  - Port eines SAC oder einer SAS zum Anschluß an einen Konzentrator
- Kodierung der Porttypen auf der Oberseite des Steckers und des Fasertyps (MMF oder SMF) auf der Unterseite (keine Aussparung bei MMF):



6.4.6. Dual Ring of Trees



6.4.7. Verkabelungsoptionen

- Multimode Fiber (MMF-PMD)

  - Maximaler Abstand zwischen zwei Stationen: 2 km
  - Faserdurchmesser: 62,5/125µm oder 50/125 µm
  - Wellenlänge: 1300 nm
  - Anschlußtechnik: MIC-Stecker
  - Sender: LED
- Mono- oder Singlemode Fiber (SMF-PMD)
  - Maximaler Abstand zwischen zwei Stationen: 60 km
  - Faserdurchmesser: 9-10/125µm
  - Wellenlänge: 1300 nm
  - Anschlußtechnik: MIC-Stecker
  - Sender: Laserdiode
- Twisted-Pair (TP-PMD)
  - Maximaler Abstand zwischen zwei Stationen: 100 m
  - Paarweise verdrillte Vierdrahtleitung
  - Anschlußtechnik: RJ45-Stecker
  - Belegung der Paare 1,2 und 7,8 im Stecker (Ethernet 1,2 und 3,6, Token-Ring 1,2 und 4,5)
  - Übertragungsverfahren 4B/5B MLT-3
    - MLT-3: Multi Level Transition 3
    - Drei Zustände
    - Reduktion der Frequenz auf 31,5 MHz

6.5. ATM

6.5.1. Überblick

- ATM = Asynchronous Transfer Mode
- Weiterentwicklung aus ISDN und Breitband-ISDN
- Standardisierung/Entwicklung durch ITU und ATM-Forum (Herstellervereinigung)
- Abwandlung des synchronen Zeitmultiplexing (STM):
  - feste Zellstruktur (alle Pakete sind 53 Byte groß) analog STM,
  - in jeder Zelle 5 Byte Header (LAN-übliche Struktur),
  - verbindungsorientierte Kommunikation ähnlich Telekommunikationsdiensten
- Verbindungsorientierte Kommunikation
- Verschiedene Diensteklassen und Dienstgüten
- Geschaltete Leitungen (Switched Circuits)
- Verbindung über ATM-Switches als Vermittlungsstellen
- Zielsetzung: Integration von Sprach-, Bild und Datendiensten

6.5.2. Verbindungsmodell

- Verbindungsorientierte Kommunikation
- Zwischen zwei Kommunikationspartnern wird eine virtuelle Verbindung (Virtual Channel Connection, VCC) geschaltet.
  - Die Verbindungen werden durch eine Kombination von virtuelle Pfad- und Kanalnummern (Virtual Path Identifier und Virtual Channel Identifier, VPI/VCI) gekennzeichnet.
  - Die Pfade und Kanäle sind jeweils nur zwischen zwei ATM-Knoten definiert, die Knoten haben eine Umsetzungstabelle VPI/VCI-Eingangsport zu VPI/VCI-Ausgangsport.
- Arten von VCCs
  - Nach Art des Aufbaus der Kanäle:
    - feste definiert Kanäle (Permanent Virtual Circuits, VVC): vom Adminstrator permanent definiert.
    - dynamisch aufgebaute Kanäle (Switched Virtual Circuits, SVC): automatisch durch Kommunikation der Endgeräte und ATM-Verteiler
  - Nach Art der Kommunikationsstruktur
    - Punkt-zu-Punkt-Verbindungen
    - Punkt-zu-Mehrpunkt-Verbindungen

6.5.3. Dienstklassen

- Unterschiedliche Anforderungen bezüglich Datenraten und maximalen Verzögerungszeiten bei Audio- ,Video- und Datenübertragungen
- Definition verschiedener Diensteklassen
- Definition unterschiedlicher ATM-Varianten (Teilschichten im ATM-Protokoll): ATM Adaption Layer (AAL)
- Verschiedene Dienstequalitäten (Quality of Service, QOS):
  - konstante Bitraten (Constant Bitrate, CBR), z.B. für Sprache,
  - variable Bitraten mit Echtzeitanforderungen (realtime Variable Bitrate, rt-VBR), z.B. (komprimierte) Videos,
  - variable Bitraten ohne Echtzeitanforderungen (non realtime Variable Bitrate, nrt-VBR), z.B. Datenkommunikation,
  - nicht spezifizierte Bitraten (Unspezified Bitrate, UBR) oder
  - bestmögliche Bitrate (Available Bitrate, ABR), z.B. Datenkommunikation.

Dienstklasse	**A**	**B**	**C**	**D**
Dienst	Sprache	Video	LAN/MAN	
Zeitverhalten	isochron	nicht isochron		
Bitrate	konstant	variabel		
Quality of Service, QOS	CBR	rt-VBR	nrt-VBR	UBR, ABR
Kommunikationsart	verbindungsorientiert			verbindungslos
Adaptionsebene	AAL1	AAL2	AAL3/4	AAL5

6.5.4. Kommunikationsschnittstellen und deren Aufgaben

- Unterscheidung zwischen Endgeräten und Vermittlungsstellen:
  - User to Network Interface (UNI)
    - Auf- und Abbau von Verbindungen von Endrechnern zum Netzwerk und damit zu anderen Endgeräten
  - Network to Network Interface (NNI)
    - Schnittstelle eines ATM-Switches
    - Verbindung ATM-Switch zum Endgerät
    - Verbindung zwischen ATM-Switches
    - Aufbau von SVCs
    - Routenwahl (Hierarchische Routingstrukturen mit Source Routing)

6.5.5. Integration klassischer LANs

6.5.5.1. Grundproblem

- Klassische LANs („legacy LANS“) basieren von ihren Protokollen her auf der Möglichkeit des Rundsendens (Broadcast und Multicast).
- Klassische LANs kommunizieren verbindungslos.
- ATM unterstützt keine Broadcasts.
- ATM arbeitet (auf Schichten 2) verbindungsorientiert.

6.5.5.2. Classical IP over ATM

- IP über ATM-Netze,
- IP benutzt Broadcasts für ARP-Requests (Auflösung von MAC- (Schicht 2) zu IP-Adressen (Schicht 3)),
- Lösung des Broadcast-Problems durch Einführung eines ATM-ARP-Server,
- Definition von logischen IP-Subnetzen auf einem ATM-Netz (Logical IP Subnetworks, LIS),
- Einsatz von Routern zwischen LISs,
- LLC/SNAP-Protokoll,
- Lösung nur für IP.

6.5.5.3. LAN Emulation LANE

- Unterstützung mehrerer emulierter LANs (ELANs) in einem ATM-Netz
- Unterteilung der nach Funktionen in:
  - LAN Emulation Clients (LEC)
    - beliebige Endgeräte oder Edge-Devices (Übergangsstellen von ATM auf klassische Netze, z.B. ATM-Ethernet-Switches)
  - LAN Emulation Configuration Server (LECS)
    - zur Konfiguration der LEC’s mit
      - Zuordnung des LEC zu einem ELAN,
      - Weitergabe der LES-Adresse für das jeweilige ELAN

    - LAN Emulation Server (LES)
        - Auflösung von MAC-Adresse zu ATM-Adresse (LE_ARP),
        - Kontrollfunktionen,
        - Weitergabe der BUS-Adresse
    - Broadcast and Unknown Server (BUS)
        - Verteilung von Broadcasts (von LEC über Multicast-Send-VCC an BUS, dann über einen Multicast-Forward-VCC an alle LEC's)
        - Weiterleitung von Paketen, solange LE_ARP noch nicht erfolgreich war, über BUS,
- Einsatz von Routern zwischen ELANs,
- derzeitiger Standard LANE 1.0.

6.5.5.4. Multi Protocol over ATM

- Erweiterung von LANE um Routingfunktionalitäten,
- Shorts Cuts im Routing (Direkte Verbindungen zwischen Systemen verschiedener Subnetze, nur erstes Paket wird geroutet),
- eine lange Liste weitere Akronyme (hier nicht behandelt),
- Standardisierung noch nicht abgeschlossen.

7. Internetworking

7.1. Überblick

- Internetworking = Verknüpfung von Netzen
- Internetworking-Komponenten: Geräte zur Verknüpfung von Netzen
- Ziele bzw. Gründe für den Einsatz von Internetworking-Komponenten
  - Kopplung entferneter Netze
  - Medienbeschränkungen (z.B. maximale Kabellängen)
  - Systembedingte Grenzen (Signallaufzeiten, Anzahl Stationen)
  - Kapazitätsbeschränkungen (z.B. Lasttrennung)
  - Verknüpfung unterschiedlicher Netzwerktechnologien
- Internetworking-Komponenten:
  - Repeater (bedingt)
  - Brücken
  - Switches
  - Router
  - BRouter
  - Gateways
  - Hubs (bedingt)

7.2. Repeater

- Kopplung auf Schicht 1 (Bitübertragungsschicht) des OSI-Referenzmodells
- Verstärker zur Signalregenerierung
- Nicht sehr kostspielig
- Nur geringe Entfernungen zu überbrücken
- Abhilfe bei Erreichen der maximalen Kabellänge
- Keine Hilfe bei sonstigen Begrenzung, z.B. Lastproblemen
- Nur innerhalb einer Technologie einsetzbar, da auf Schicht 1 arbeitend.

7.3. Brücken

- Kopplung auf Schicht 2 (Sicherungsschicht) des OSI-Referenzmodells
  - Brücken interpretieren Datenrahmen der Schicht 2
  - Brücken verarbeiten (interpetieren) MAC-Adressen aber
  - sie verändern MAC-Adressen (oder sonstige Informationen) nicht.
  - Brücken arbeiten unabhängig von den Schichten 3 bis 7 (Transparenz)
- Filterung von Paketen
  - Zur Lasttrennung
  - Paket werden von der Brücke in ein anderes Segment weitergeleitet,

        - wenn der Zielrechner im anderen Segment ist oder
        - das Paket ein Broadcast- oder Multicast-Paket ist.
    - Zwei Möglichkeiten bei Paketen mit unbekanntem Ziel:
        - Fluten, d.h. weiterleiten auf Verdacht in alle Segmente (außer dem Quellsegment, die normale Variante)
        - Verwerfen, d.h. das Paket wird nicht weitergeleitet.
- Zwischenspeicherung von Paketen (Store & Forward)
    - Einlesen des gesamten Pakets, bevor mit der Weiterleitung begonnen wird.
    - Nachteil:
        - Verzögerung (Latency) im Netzverkehr
    - Vorteile:
        - Isolation von fehlerhaften Paketen
        - Trennung von Kollisionsdomänen
- Zweck des Brückeneinsatzes:
    - Lasttrennung
    - Entfernung fehlerhafter Pakete
    - Unterteilung in getrennte Kollisionsdomänen (beim Ethernet)
- Um die Filterung zu ermöglichen, benötigt die Brücke eine Tabelle von MAC-Adressen (Forwarding-Table) und deren Zuordnung zu den Schnittstellen:
    - Die Tabellen können statisch aufgebaut werden (selten) oder
    - die Tabellen werden dynamisch (selbstlernend durch Mitlesen von Paketen und darin enthaltenen Quelladressen) aufbebaut.
    - Manche Brücken erlauben die Konfiguration statischer Einträge zusätzlich zu dynamischen
    - Alterungsfunktion für dynamische Einträge
- Problem der Schleifenverhinderung
    - Schleifen sind verboten,
        - da sie zu einer Vervielfachung von Paketen führen würden und
        - die Forwarding-Table undefiniert wäre.
    - Erste Lösung:
        - Brücken dürfen nicht so platziert werden, daß Schleifen entstehen könnten.
    - Zweite Lösung (Spanning Tree):
        - Dynamische Abschaltung von Brücken, die zu einer Schleifenbildung beitragen würden.
        - Dazu tauschen Brücken untereinander Informationen aus, um Schleifenbildungen zu erkennen und zu verhindern (Spanning Tree Protokoll, IEEE 802.1d)
        - Vorteil: Ein redundanter Weg kann vorgehalten werden, der bei Ausfall einer Verbindung aktiviert werden kann.

  - Bei Ethernet und FDDI gängig
- Dritte Lösung (Source Routing):
  - Explizite Festlegung des Weges eines Paketes (d.h. welche Brücke benutzt werden soll) durch den Sender
  - Vorteil: Redundante Wege.
  - Nachteile:
    * Overhead in Paketen
    * Problem der Routenfindung (durch Explorerpakete)
  - Im Token-Ring benutzt

- Varianten von Brücken
  - Multiport-Brücken (mehr als zwei Ports)
  - Halbbrücken
    - Sparversion einer Brücke
    - Filterung nur in einer Richtung
    - MAC-Tabelle beschränkter Größe nur für einen Port (Workgroup-Seite)
    - Weiterleitung von Pakete aus der Backbone-Seite zur Workgroup-Seite nur, wenn Ziel in MAC-Tabelle
    - Weiterleitung von Pakete aus der Workgroup-Seite zur Backbone-Seite, wenn Ziel nicht in MAC-Tabelle
  - Remote-Brücken
    - Zur Kopplung von Netzen über andere Medien, insbesondere über Postleitungen
    - Je Brücke ein Remote und ein oder mehrere lokale Ports
    - Einsatz immer paarweise (meist baugleiche Brücken)
    - Ein Paar stellt funktional eine Brücke dar.
    - Andere Brücken heißen korrekt „lokale Brücken“
  - Translation-Brücken
    - Brücken zwischen verschiedenen Netzwerktechnologien
    - Bei verschiedener MAC-Teilschicht, aber gleicher LLC-Teilschicht
    - Probleme:
      * Anpassung der MAC-Adressen (lsb/msb)
      * Zwischenspeicherung bei unterschiedlichen Datenraten
      * Unterschiedliche maximale Paketlängen
        + Bei IP-Paketen Lösung durch Fragmentierung (eigentlich eine Funktion der Schicht 3 im IP),
        + sonst Datenverlust bei zu langen Paketen
        + oder Endstationen müssen MTU (Maximal Transmit Unit) aushandeln.

7.4. Switches

- Alternative zu Multiport-Repeatern oder Multiport-Brücken (je nach Variante)
- Schaltung von Verbindungen zwischen den Ports anhand der MAC-Adresse (analog Filterung bei Brücken)
- Existent für Ethernet, Token Ring, FDDI (ATM sowieso)
- Drei Varianten
  - Cut-Through-Switch
    - Switch schaltet nach Erkennung der Zieladresse (ggf.) sofort durch.
    - Sehr geringe Latenzzeit (30-40µs bei Ethernet)
    - Problem: Fehlerhafte Pakete und Kollisionsfragmente werden weitergeleitet.
    - Verwandtschaft mit Repeatern
  - Fragment-Free
    - Switch liest das Paket bis die minimale Paketlänge erreicht ist und beginnt dann die Übertragung.
    - Höhere Latenzzeit (ca.100µs bei Ethernet, aber Kollisionsfragmente werden nicht übertragen.
  - Store&Forward-Switch
    - Switch liest wie eine Brücke erst das ganze Paket
    - Größere Latenzzeit als die anderen Varianten (100-1200µs bei Ethernet)
    - Fehlerhafte Pakete und Kollisionsfragmente werden isoliert.
    - Implementierung von Filtern möglich
    - Unterschied zu Multiport-Brücke unklar
      - Schnellere interne Übertragungswege?
      - Höhere Portzahl?
      - Schaltung virtueller Leitungen?
      - Marketing-Trick?
  - Manche Switches erlauben eine Konfiguration der Variante, teilweise auch eine dynamische Umschaltung in Abhängigkeit der Kollisions und Fehlerraten.
- Häufig mit Uplink-Port zum Anschluß an einen schnelleren Backbone ausgestattet
- Bündelung von Ports für schnelle Switch-zu-Switch-Verbindungen bei einigen Herstellern (proprietäre Verfahren)
- Duplex-Optionen (gleichzeitiges Senden und Empfangen, aber proprietäre Verfahren)
- Technische Realisierungsvarianten:
  - Vermittlung
    - Matrix / Crossbar

  - Schneller interner Bus mit Cell- oder Frame-Switching
  - Shared Memory
- Verschiedene Prozessorarchitekturen
  - Paketprozessoren (ASICs) an jedem Port
  - Softwarelösung mit zentralen RISC-Prozessoren
- Eingangs- und/oder Ausgangspuffer
- Pufferung bei belegtem Ausgang
- Optional bewußte Kollisionserzeugung bei vollem Puffer (Contention Management)

7.5. Router

7.5.1. Überblick

- Kopplung auf Schicht 3 (Vermittlungsschicht)
- Einsatz zur Kopplung
  - LAN - LAN (auch bei verschiedenen Technologien)
  - LAN - WAN
  - LAN - LAN über ein WAN
- Vermittlungsfunktion (Routing) / Wegevermittlung (Routen)
- Redundante Wege sind erlaubt
- Router werden explizit angesprochen (anders als Brücken, die transparent sind).
- Keine Transparenz auf Schicht 2
  - Router arbeiten nur mit bestimmten Protokollen der Schicht 3
  - Rahmen der Schicht 2 werden vom Router bei der Weiterleitung neu erzeugt
- Router geben keine Broadcast- oder Multicast-Pakete weiter.
- Router haben größere Verzögerungszeiten als Brücken
- Heute üblich Multiprotokoll-Router (also für mehrere verschiedene Protokolle der Schicht 3 geeignet)
- Möglichkeiten zur Filterung auf Basis von Informationen der Schicht 3
- Durch Filtermöglichkeiten Sicherheitsvorteile

7.5.2. Kriterien für Routen

- Häufig existieren in der Netzwerk- oder Vermittlungsschicht alternative Wege
- Bei der Vermittlung muß der „günstigste“ Weg ausgewählt werden.
- Gewichtung von alternativen Wegen durch die Routing-Metrik
- Mögliche Kriterien zur Bestimmung einer Metrik und zum Auswahl eines Weges:
  1. Anzahl von Vermittlungsstellen auf dem Weg (Hops), „Distance-Vector“-Methode
  1. Übertragungskapazität auf dem Weg (Cost, Ticks)

1. Verzögerungszeit auf dem Weg (lastabhängig!)
1. Durchsatz (lastabhängig!)
1. Kosten (bei gemieteten Leitungen)
   - Die Kriterien 3 und 4 sind zustandsabhängig
   - Die Kriterien 1, 2 und 5 sind zustandsunabhängig

- Konfiguration eines Standardweg (Default Route) für unbekannte Ziele, um Routing-Tabelle nicht zu groß werden zu lassen.

7.5.3. Routenbestimmung

- Methoden
  - Manuelle Konfiguration fester Routen (statisches Routing)
    - Insbesondere bei Endgeräten ohne Alternativen in der Wegewahl
  - Automatische Konfiguration durch Kommunikation zwischen Routern (dynamisches oder adaptives Routing)
  - Mischung von dynamischen und statischen Routen
- Entscheidung über Routen
  - durch die Sender: Quellen- oder Source-Routing (praktisch nur bei Brükken im Token-Ring)
  - Verteiltes Routing
    - Jeder Router entscheidet aufgrund einer eigenen, selbst erstellten Tabelle.
    - Jeder Router kommuniziert mit jedem
    - Problem: relativ hohe Netzlast
  - Zentralisiertes Routing
    - Ein „Ober-Router“ errechnet zentral die Tabellen und verteilt sie.
  - Hierarchisches Routing

7.5.4. Variationen im dynamischen Routing

- Art des Austauschs von Routen
  - Fluten: jeder sendet die eigenen Information an alle
  - Selektives Fluten: jeder sendet nur an ausgewählte Router, die dann die anderen informieren
- Zeitpunkte des Routenaustauschs
  - Periodisch (bei alten Implementationen üblich), meist alle 10 bis 30 s
  - Bedarfsorientiert (bei neueren Protokollen üblich)
    - Routing-Information wird nur im Bedarfsfall ausgetauscht.
    - Zur Kontrolle werden periodisch kurze Hello-Pakete ausgetauscht.
- Inhalt des Routenaustauschs
  - Quantität
    - Kompletter Routing-Table oder

  - nur Informationen über eigenen Ports (und über externe Routen, die außerhalb des Bereichs liegen, in dem die Router kommunizieren [z.B. externe statische Routen])
- Qualität
  - Netzwerkadressen
  - Metrik
  - teilweise zusätzliche Informationen zur Struktur (z.B. Subnetzmasken bei IP)

7.6. BRouter

- Mischung aus Router und Brücke
- Routbare Protokolle werden (in der Regel) geroutet
- Sonstige Protokolle werden ggf. gebrückt
- Moderne Multiprotokoll-Router arbeiten meist als BRouter (im obigen Sinn)
- Achtung: Manche Hersteller bezeichnen Brücken (insbesondere Remote-Brücken) mit geringfügigen Vermittlungsfunktionen schon als BRouter

7.7. Gateways

- Kopplungsgeräte, die auf Schichten oberhalb der Netzwerkschicht (3) arbeiten
- Ziel ist die Umsetzung von Protokollen der Schichten 4 bis 7 (oder einzelner davon)
- Beispiele
  - Konvertierung von eMail-Formaten
  - Konvertierung zwischen Dateitransferanwendungen
  - Konvertierung zwischen Terminalemulationsprogrammen
- Achtung: Im IP-Bereich werden Router häufig auch als Gateways bezeichnet.

7.8. Hubs

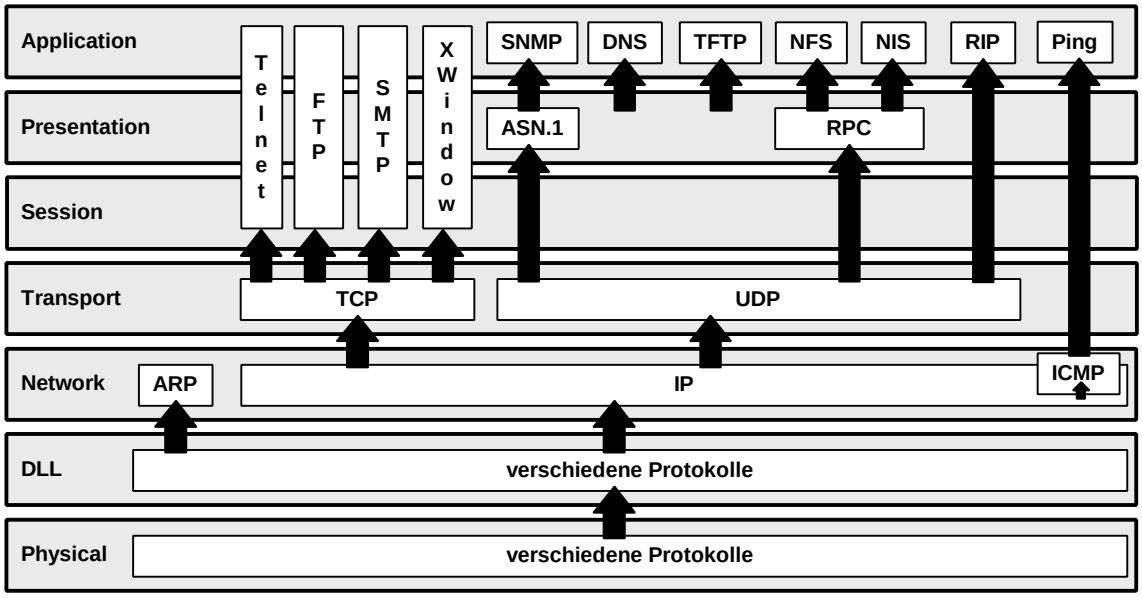
- Andere Bezeichnung: Konzentrator, Verteiler (ein Hersteller bezeichnet seine Geräte als Multi-Media-Access-Center, MMAC, dabei bezieht sich Multimedia auf verschiedene Medien im Sinne verschiedenen Verkabelungs- und/oder Netzwerktechniken)
- Varianten
  - Modulare Systeme
    - ein Gehäuse,
    - eine Stromversorgung für alle Komponenten,
    - modulare Einschübe mit unterschiedlichen Funktionen
      - Repeater (auch verschiedene Anschluß- und Verkabelungstechniken),
      - Ringleitungsverteiler (Token-Ring),
      - FDDI-Konzentratoren,

        - Brücken,
        - Switches,
        - Router,
        - Gateways.
    - Kopplung der Module über einen internen Bus (oder mehrere Busse oder Kanäle)
    - Bei Repeater-Modulen bilden alle Module zusammen einen Repeater (falls sie nicht auf verschiedenen Kanäle konfiguriert sind).
- Stackable Hubs
    - Einzelne, isoliert betriebsfähige Hubs
    - Meist mit Repeater-Funktionalität
    - Einzelne Teile könne durch spezielle externe Verkabelungen zu einem Hub zusammengeschaltet werden (der dann ggf. einen einzigen Repeater bildet).

8. Die IP-Protokoll-Familie als Beispiel

8.1. Überblick

- IP = Internet Protokoll
- Ursprung des Protokolls beim DoD (Department of Defence)
- Protokoll zur Kommunikation im weltweit größtem Netz (dem „Netz der Netze“)
- IP steht
  - einerseits für ein Protokoll der Schicht 3
  - andererseits für eine Familie von Protokollen der Schichten 3 bis 7
- Die IP-Protokoll-Familie hält sich nicht exakt an das OSI-Referenzmodell (sie ist ja auch älter als das Modell)
- Übersicht über die IP-Protokolle



8.2. IP als Protokoll der Schicht 3

8.2.1. Netzweite Adressierung

- 32-bit-Adressen
- ***Dotted Decimal Notation*** der Adressen:
  - Schreibweise als Quadrupel n.n.n.n
  - n jeweils 8 Bit, also zwischen 0 und 255
- Hierarchische Struktur der Adressen (wie Telefonnumern, Postleitzahlen)
- Aufteilung der Netze
  - anhand der Nummern (in [ ] Vergleich mit Telefonnummern)

Netz oder Network	Rechner oder Host
[Vorwahl]	[Durchwahl]

oder

Netz oder Network	Subnetz oder Subnet	Rechner oder Host
[Vorwahl]	[Nebenstellenanlage]	[Durchwahl]

- unterschiedlich lange Netznummern, aber mit der folgenden Systematik:
  - ***Class A Netze***
    - Bit 1 = 0
    - Adressen 1.0.0.0 bis 127.255.255.255
    - 7 Bit Netzadresse, 24 Bit Hostadresse
    - 127 Netze
    - 2^{24} -2 = 16.777.214 Rechner pro Netz
  - ***Class B Netze***
    - Bit 1-2 = 10
    - Adressen 128.0.0.0 bis 191.255.255.255
    - 14 Bit Netzadresse, 16 Bit Rechneradresse
    - 2^{14} = 16.284 Netze
    - 2^{16} - 2 = 65.534 Rechner pro Netz
  - ***Class C Netze***
    - Bit 1-3 = 110
    - Adressen 192.0.0.0 bis 223.255.255.255
    - 21 Bit Netzadresse, 8 Bit Rechneradresse
    - 2^{21} = 2.097.152 Netze
    - 2^{8}-2 = 254 Rechner pro Netz
  - ***Class D***
    - Bit 1-4 = 1110
    - Adressen 224.0.0.0 bis 239.255.255.255
    - IP-Multicasts
  - ***Class E***
    - Bit 1-4 = 1111
    - Adressen 240.0.0.0 aufwärts (außer 255.255.255.255, s.u)
    - reserviert
- Einführung von ***Subnetzen***
  - nur lokal bekannte Aufteilung (ähnlich Nebenstellenanlage beim Telefon)
  - Unterteilung eines der obengenanten Netze in durch Router getrennte Teilbereiche
  - Festlegung der Aufteilung durch „***Subnetzmaske***“
    - 32 Bit-Maske

        - An den Positionen, die zum Netzteil (inklusive Subnetz) der lokalen Adressen gehören stehen (binäre) Einsen, sonst Nullen
        - Dabei müssen die Einsen am Anfang, die Nullen am Ende der Maske stehen (keine Mischung)
        - Durch eine logische Und-Verknüpfung wird der Netz- vom Rechnerteil einer Adresse getrennt
        - Das jeweils erste (eigentlich, aber ..) und letzte (immer) Netz ist illegal (wegen der speziellen Adressen, s.u.)
      - Häufig muß in einem Netz die Subnetzmaske überall identisch sein (bei bestimmten Routingprotokollen [z.B. RIP])
      - Subnetze eines Netze dürfen nicht über ein anderes Netz verbunden werden.
    - Multinetting
      - Spezielle Option auf manchen Routern (den meisten besseren)
      - Betrieb mehrerer logischer Subnetze auf einem physikalischen Netz (hinter einer Router-Schnittstelle)
      - Manchmal nötig, wenn die Subnetzmaske im Netz einheitlich sein muß, aber unterschiedlich große Subnetze durch die Struktur nötig sind (z.B. im GÖNET).
- Spezielle Adressen
  - 0..0 im Hostteil = das Netz, das im Netzteil angegeben ist (z.B. im Routing Table verwendet)
  - 1..1 im Hostteil = an alle Rechner in dem Netz, das durch den Netzteil angegeben ist („Directed Broadcast“)
  - 1..1 in der gesamten Adresse = an Rechner im lokalen Netz (255.255.255.255)
  - 0..0 in der gesamten Adresse = Default Netz/Route
- Vergabe von Adressen pro Geräte-Schnittstelle
  - Wegen Identifikation des physikalischen Netzes aus dem Netzteil.
  - Jede Schnittstelle benötigt eine Adresse.
  - Rechner sind (bei mehreren Schnittstellen) nicht eindeutig durch die Adresse gekennzeichnet
    - Je nach verwendeter Adresse können Daten auf verschiedenen Wegen zu einem Rechner gelangen (mit ungewollten Seiteneffekten).
- Adressen sind ortsabhängig
  - Bei einem Ortswechsel des Rechners muß sich die Adresse u.U. ändern
- Beispiel: Adressen im GÖNET

8.2.2. Rahmen-Format

- Der IP-Rahmen (oder IP-Header) hat folgendes Format

Bit 1

<table>
<tr><td colspan="2">Version</td><td>Header-Länge</td><td>TOS (Type of Service)</td><td colspan="4">Länge des IP-Pakets</td></tr>
<tr><td colspan="4">Identifikation</td><td>0</td><td>DF</td><td>MF</td><td>Fragment-Offset (0 falls nicht Fragmentiert)</td></tr>
<tr><td colspan="2">TTL (Time to Live)</td><td>Protocol</td><td colspan="4">Checksum für den Header</td></tr>
<tr><td colspan="8">IP Source Address</td></tr>
<tr><td colspan="8">IP Destination Address</td></tr>
<tr><td colspan="6">Option (kann entfallen)</td><td colspan="2">Padding (Auffüllung, falls Option vorhanden)</td></tr>
</table>

- Falls auf dem Weg zwischen Quelle und Ziel ein Router feststellt,daß das Paket für ein Teilsegment zu lang ist, kann der Router es in Abhängigkeit vom DF-Bit in Fragmente teilen.
  - DF =1: don't fragment, darf nicht fragmentiert werden.
  - Weitere Information in Zusammenhang mit Fragmentierung:
    - MF =1: more fragments, das Paket ist nicht das letzte Fragment
    - Fragment offset: relative Position des ersten Bytes im Datenteil im ursprünglichen Paket
    - Identifikation: eindeutige Kennzeichnung des ursprünglichen Pakets, damit die richtigen Fragmente wieder zusammengesetzt werden können.
    - Eine empfangende Station startet bei Empfang des ersten Fragments einen Zeitzähler, innerhalb einer bestimmten Zeit müssen alle Teile eines Pakets eintreffen.
- Protocol: Angabe über übergeordnete Protokolle, z.B.
  - 1 = ICMP
  - 6 = TCP
  - 17 = UDP
- TTL: Time to Live
  - Zähler, der von jedem passierten Router um 1 dekrementiert wird
  - Sicherheitsmaßnahme gegen Schleifen
  - Bei TTL=0 wird das Paket von dem bearbeitenden Router verworfen.

8.3. ICMP

- Internet Control Message Protocol
- In Ebene 3 angeordnet, setzt aber auf IP auf.
- Funktionen
  - Tests der Netzfunktionalität
    - Echo Request
    - Echo Reply
    - Bei Anwendung „ping“ verwendet.
  - Fehlermeldungen
    - Destination unreachable (vom Router)
    - Source quench (vom Router bei Überlastung)
    - Redirect (vom Router: anderen Router benutzen)
    - Time exceed (TTL war 0)
    - Parameter Problem (Formatfehler im Header)
  - Informationsdienste
    - Information request/reply (IP-Adresse für sich selbst anfordern)
    - Adress mask request/reply (Subnetzmaske erfragen)
    - Timestamp request/reply (Zeitmarkierung)

8.4. ARP

- Adress Resolution Protocol
- Zweck Finden der MAC-Adresse zu einer IP-Adresse
- Vorgehen:
  - Broadcast senden mit Inhalt
    - eigener IP-Adresse
    - eigener MAC-Adresse
    - Ziel-IP-Adresse
    - Dummy-MAC-Adresse
  - Antwort vom Zielrechner (oder einem Proxy-ARP-Server)mit Inhalt
    - eigener IP-Adresse
    - eigener MAC-Adresse
    - Quellen-IP-Adresse
    - Quellen-MAC-Adresse
- Speicherung einmal ermittelter Umsetzungen (ARP-Cache, mit Alterungsfunktion)
- RARP (Reverse ARP) für Auflösung von MAC-Adresse zu IP-Adresse (nicht sehr häufig benutzt)

8.5. Routing-Protokolle

8.5.1. RIP

- Routing Information Protocol
- Austausch von Routing-Tabellen zwischen Routern
  - Senden einer Tabelle mit Netznummern (oder Subnetznummern) und Metriken
  - Metrik meist Hopcount
  - Metrik maximal 14 (konfigurierbar, aber besser nicht ändern)
  - Metrik = 15 bedeutet unreachable/Netz nicht erreichbar
- Paketformat
  - 14 Byte (!) lange Netznummer
  - 4 Byte Metrik
  - auch bei IPX- und XNS-Protokollfamilie fast identisch genutzt (dort aber Metrik als Ticks oder Hops wählbar)
- Probleme der Konvergenz
  - Beispiel
    - Netz A über Router R1 mit Router R2 verbunden
      - R1 gibt an A ist 1 Hop entfernt
      - R2 gibt an A ist 2 Hops entfernt (das wird auch R1 mitgeteilt)
    - Bei einem Ausfall der Verbindung von A zu R1 passiert folgendes:
      - R1 stellt fest, daß A über den bisherigen Weg nicht mehr erreichbar ist.
      - R1 stellt gleichzeitig fest, daß R2 A noch erreichen kann (mit Metrik 2)
      - R1 beschließt, daß er A mit Metrik 3 erreichen kann und teilt dies allen mit.
      - R2 sieht die Änderung der Metrik, die R1 für A angibt.
      - R2 Beschließt, daß er A mit Metrik 4 erreichen kann und teilt dies allen mit.
      - usw. bis R1 feststellt, daß die Metrik auf 15 steigt und endlich weiß, daß A nicht mehr erreichbar ist.
- Der komplette Routing-Table wird alle 30s verschickt.
- RIP wir auf Unix-Systemen von den Programmen routed und gated benutzt.
- Subnetting ist bei Verwendung von RIP nur mit einer einheitlichen Subnetzmaske im gesamten Netz möglich (da die Maske ja nicht in den Routing-Updates mitangegeben wird).

8.5.2. OSPF

- Open Shortest Path First
- Routing auf Basis von Kosten (z.B. ein Weg über Ethernet ist teurer als einer über FDDI)

- Router senden nur Informationen zu den eigenen Interfaces und externen Routen (nicht den kompletten Routing-Table)
  - Weniger Verkehr
  - Schnellere Konvergenz
  - Der Aufwand bei der Aufstellung der Tabellen der einzelnen Router ist für diese höher
- Routing-Updates nur bei Änderungen
- Routing-Updates werden nur an zwei Router gesendet
  - Designated Router und
  - Backup Designated Router
  - (die in der Initialisierungsphase bestimmt werden müssen)
  - Der Designated Router gibt den anderen dann Zusammenfassungen
- Hello-Pakete alle 60s (sonst würde eine Ausfall eines Routers nicht bemerkt)
- Übertragung in den Update-Paketen von
  - Netznummern,
  - Kosten und
  - Netzmaske
    - Unterstützung von variablen Subnetzmasken
- Optionaler Password-Schutz bei Übertragung von Hello- und Routing-Update-Paketen zur Authentifikation.

8.6. Protokolle der Schicht 4 (TCP und UDP)

8.6.1. Verbindungsorientierte und verbindungslose Kommunikation

- Verbindungsorientierte Kommunikation
  - ***Ende-zu-Ende-Kontrolle***
  - Auf- und Abbau von Verbindungen
  - ***Segmentierung*** zu sendender Daten im Quellrechner
  - Reihenfolgegarantie durch Sequenznummern
  - Zusammensetzung von Segmenten im Zielrechener (ggf.)
  - ***Flußsteuerung*** (ggf. Sendepausen verlangen, bremsen der Kommunikation)
  - ***Verlustsicherung***
    - Bestätigung erhaltener Pakete bzw.
    - Anforderung zur wiederholten Sendung fehlender oder fehlerhafter Pakete.
    - Beides über Sequenznummern (angegeben wird, welches Byte als nächstes erwartet wird)
  - Zusätzlicher Protokoll-Overhead
  - ***TCP*** (Transmission Control Protocol)
- ***Verbindungslose Kommunikation***

  - Versenden einzelner Pakete
    - ohne Vorbereitungen,
    - ohne Verlustsicherung,
    - ohne Segmentierung usw.
    - z.B.
      * bei Name-Server-Abfragen (kurze Pakete, Verlustsicherung wegen Anwendungszweck nicht nötig)
      * NFS als lokales Protokoll (geht von geringen Verlusten aus, erledigt Segmentierung selbst)
  - ***UDP*** (User Datagram Protocol)
- Gemeinsamkeiten
  - Bei beiden Varianten wird eine Angabe zur übergeordneten Instanz (Anwendung) verlangt.

8.6.2. Fenstertechnik zur Flußsteuerung

- Notwendigkeit zur Absicherung gegen Datenverlust bei unsicheren Wegen
- Notwendigkeit zur Flußsteuerung bei großen/langen Übertragungen und potentiell langsamen Empfängern (Festplatte zu langsam, Swap, ...)
- Einfacher Ansatz
  - Ein Paket senden
  - Bestätigung abwarten
  - nächstes Paket senden
  - usw.
  - Ineffizienz durch Wartezeit
- Fensteransatz (***Window***-Technik)
  - Vor Beginn der Übertragung wird ausgehandelt, wieviele Bytes (oder Pakete) gesendet werden dürfen, bevor auf eine Bestätigung gewartet werden muß (Window).
  - Im optimalen Fall keine Wartezeiten
- TCP benutzt Fenster auf Byte-Basis
- (DECnet benutzt Fenster auf Paket-Basis,
- Novell-IPX benutzt standardmäßig [kein Burst-Modus] keine Fenster)

8.6.3. Sockets

- UDP und TCP geben an, an welche Anwendungen Pakete gehen durch
  - vordefinierte „***Ports***“ (z.B. 23=Telnet, 25=SMTP-Mail, auf Unix-Rechnern in /etc/services definiert, immer kleiner als 1024)
  - Variable Portnummern, z.B. für möglicherweise verschiedene Telnet-Clienten-Prozesse (dynamisch vergeben, immer oberhalb 1023)
- Die Zusammenfassung eines Ports-Werts und einer IP-Adresse wird ***Socket*** gennannt und ist während eines Kommunikationsvorgangs unveränderlich.

8.7. Namen und Adressen

- In Internet-Anwendungen werden an der Benutzeroberfläche meist Namen statt der IP-Adressen verwendet.
- Der Namensraum ist hierarchisch aufgebaut und wird hierarchisch verwaltet.
- Die Namensteile in der Hierarchie werden durch Punkte getrennt.
- Die oberste Hierarchiestufe eines Namens steht am Ende
- Die in der obersten Hierarchiestufe lauten die Namen
  - xy (mit xy = zweibuchstabiger Ländercode, z.B. de für Deutschland, Ausnahme USA)
  - in den USA
    - com für Firmen
    - edu für (öffentliche) Forschung und Lehre
    - gov für Regierungseinrichtungen
    - mil für Militär
  - net für Netz-Service-Provider
  - org für (internationale) Organisationen
- Groß-/Kleinschreibung wird in den Namen ignoriert.
- Umsetzung von Namen zu Adressen und umgekehrt über ***Domain Name Server***
- Beispiele:
  - Asterix.III.Physik.Uni-Goettingen.de
  - ftp.microsoft.com

9. Funktionen und Ziele des Netzwerkmanagements

9.1. Überblick

- Unterteilung in die Teilbereiche (nach OSI)
  - Konfigurationsmanagement (Configuration Management)
  - Fehlermanagement (Fault Management)
  - Leistungsmanagement (Performance Management)
  - Sicherheitsmanagement (Security Management)
  - Abrechnungsmanagement (Accounting Management)

9.2. Konfigurationsmanagement

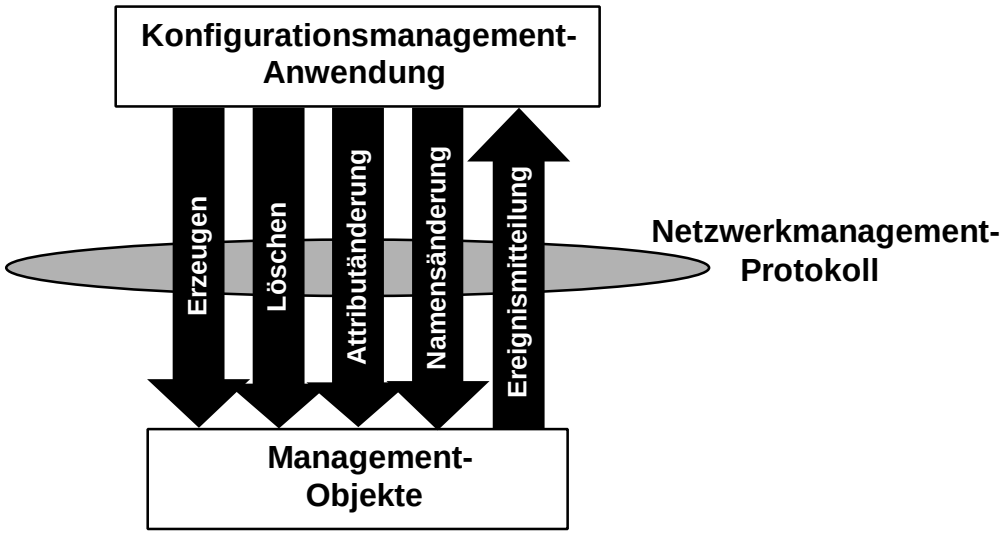
- Bestandsaufnahme
- Bestandsführung
- Manipulation

  } von Netzkomponenten

- Beschreibung der Komponenten und deren Elemente als ***abstrakte Objekte*** (nicht nur Hardware und Software)
- Pflege
- Zugänglichmachen
- Präsentation

  } von Datenbankobjekten

- Schema:



9.3. Fehlermanagement

- Unterteilung von Fehlermanagement in
  - Störungsmanagement und
  - Problemmanagement

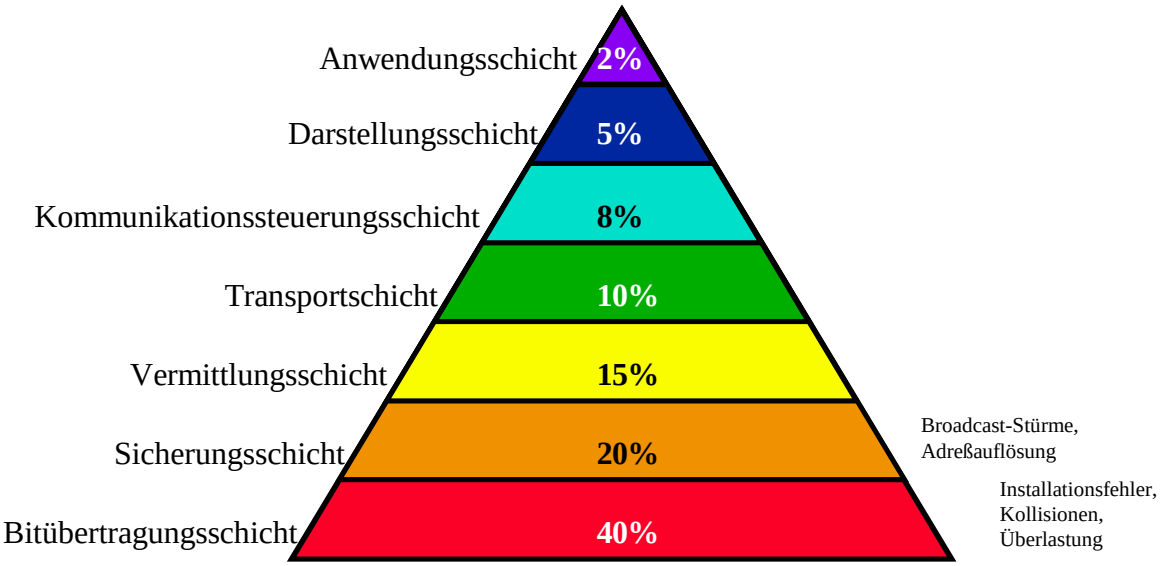
- Entdecken
- Analysieren
- Beheben

  ] von Fehlern
- im Kausalgeflecht von
  - Mensch (
    - Durchführung schädlicher Handlung oder
    - Unterlassen nötiger Handlungen

      aus
    - Unkenntnis,
    - Unvermögen oder
    - Absicht)
  - Umwelt, z.B.
    - elektromagnetische Strahlung,
    - Temperatur,
    - Feuchtigkeit,
    - Schmutz,
  - Technik, z.B.
    - Konstruktion
    - Fertigungsqualität
    - Transport,
    - Installation,
    - Instandhaltung,
    - korrekte Bedienung,
    - Verschleiß.
- Fehler durch
  - (Total-) Ausfall von Komponenten
  - (Strukturelle) Fehler in der Netzsoftware
  - Minderung der Dienstqualität
- Ablauf einer Fehleranalyse
  - Protokollierung von Zuständen
  - Auswertung der Daten
  - Klassifizierung von Fehlern
  - Alarmmeldung
  - Analyse
  - Rekonfiguration
  - Beseitigung oder Umgehung

    dabei
  - Mitwirkung verschiedener Personen

- Bedeutung des Benutzern nicht übersehen bei
  - Feststellung
  - Beseitigung
  - Informationspolitik
- Fehlerverteilung auf die Schichten des OSI-Referenzmodells (allgemeine Erfahrungswerte laut Literatur):

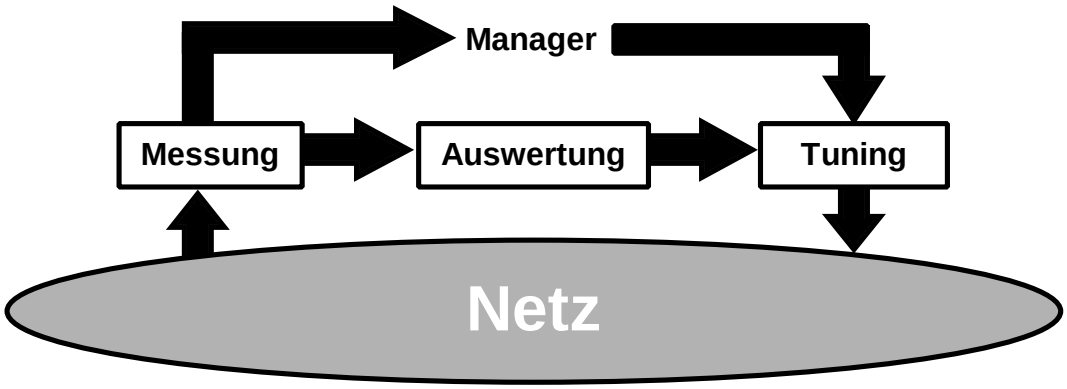


- Die Komplexität der Problematik der Fehleranalyse steigt mit der Schicht.

9.4. Leistungsmanagement

- Weiterführung des Fehlermanagements
- Sicherstellung der Effizienz und optimalen Funktion des Netzes durch
  - Überprüfung von Leistungskenngrößen
  - Überwachung von Leistungsengpässen
  - Messungen
  - Erfassung und Analyse von Managementdaten
  - Erstellen von Berichten
  - Tuning

- Schema:



- Problem der Belastung des Netzes durch die Messung
  - integrierte Messungen (SNMP)
    - über des Netz
    - automatisiert
  - isolierte Messungen (netzunabhängig, mit Analysator)
- Langfristige Messungen zur Trendanalyse

9.5. Sicherheitsmanagement

- Sicherstellung der Funktion des Netzes (Schutz)
- Aufgaben:
  - Überwachung und Erkennen von Angriffen auf die Sicherheit des Netzes,
  - Datenverschlüsselung,
  - Authentifizierung,
  - Ergreifen von Sicherheitsmaßnahmen.
- Unterteilung der Maßnahmen:
  - bau- und versorgungstechnische,
  - organisatorische,
  - technologische,
    - gerätetechnische,
    - programmtechnische.
- Gegensatz: sicheres und offenes Netz
- Dienste des Sicherheitsmanagements
  - Authentisierung (Identitätsprüfung)
  - Zugriffskontrolle (Prüfung von Rechten)
  - Vertraulichkeit (Schutz vor unauthorisiertem Zugriff)
  - Datenintegrität (Schutz vor unauthorisierter Modifikation)

9.6. Abrechnungsmanagement

- Kostenmanagement

- Aufgaben:
  - Erfassung
  - Abrechnung
  - Aufbereitung

  } von Leistungen
  - Kontrolle von Limitierungen
  - Speicherung von Abrechnungsdaten

10. Netzwerkmanagement-Werkzeuge

10.1. Dokumentation

- Verkabelungspläne
  - Kabelverlauf
  - Position von Anschlüssen
- Meßprotokolle
  - Korrekte Verlegung und korrekte Auflegung
    - Kurzschlüsse
    - Adernvertauschung
  - Dämpfung
  - Übersprechen
  - Schleifenwiderstand
  - Kapazität
  - TDR-Messung (Time-Domain-Reflektometer) / Oszilloskop
- Dokumentation der Verteilerfelder
  - Übergang vom Verteilerfeld zum Endgerät
  - Übergang vom Verteilerfeld zum Verteiler
- Dokumentation der Umgebungsbedingungen
  - Zugangsregelungen
  - Elektrische Sicherungen
- Dokumentation der aktiven Komponenten
  - Netzverteiler,
  - Internetworking-Komponenten
  - Endgeräte

    bezüglich
  - Aufstellung
    - Raum
    - Anschlußdose
  - Anschlüsse
    - Adaptertyp
  - Konfiguration
    - MAC-Adresse
    - Protokolladressen (IP, DECnet, IPX usw.)
    - eingesetzte Software (Typ und Release)

10.2. Ausbildung

- Einweisung von

    - Personal und
    - Benutzern
- Zum Schutz vor
    - Fehlbedienung,
    - ineffizienter Benutzung
    - Fehlalarmen

10.3. Meßgeräte zur Überprüfung der Funktionalität der Bitübertragungsschicht

- Kabeltester unterschiedlicher Güte
    - Von Spannungsmessungen bis zum
    - Autotest aller Kabelkenngrößen
- Messung mit TDR
    - Aussenden von kurzen Testimpulsen
    - Messung von Reflektionen mit Oszilloskop
    - Suche nach Störstellen im Kabel
- Spezialmeßgeräte zur Überprüfung der aktiven Stationen auf
    - Einhaltung des Takts
    - Signalformen
    - Signalpegel
    - Rauschen
- Aufgaben:
    - vorsorgliche Messung vor Inbetriebnahme
    - Hilfsmittel bei Fehlersuche auf Bitübertragungsschicht

10.4. Netzwerkanalysatoren

10.4.1. Allgemeine Eigenschaften

- Aktive Komponenten, die Netzverkehr mitlesen und auswerten.
- Varianten:
    - Portable Rechner mit Spezialsoftware und/oder -hardware
    - Fernabfragbare Komponenten
        - RMON-Standard oder
        - proprietäre Lösungen
- Unterschiedliche Qualität und Quantität der Auswertung
    - Globale statistische Werte
        - Netzlast
        - Fehlerraten
        - Kollisionsraten

        - Aufzeichnung
            - kumulativ oder
            - zeitabhängig
    - Statistische Werte bezogen auf einzelne Teilnehmer
        - Last stationsbezogen (Senden und Empfangen),
        - Fehler stationsbezogen,
        - Kommunikationsmatrixen
        - Betrachtung unterschiedlicher Ebenen
            - Sicherungsschicht oder
            - Vermittlungsschicht
    - Datenaufzeichnung
        - mit offline-Protokolldekodierung oder
        - mit online-Protokolldekodierung
    - Expertensysteme
        - Automatische Protokollanalyse auf Fehlerzustände und Symptome
            - online oder
            - offline
- Unterschiedung
    - spezielle Meßhardware oder
    - normale Endgeräte und Netzkarten mit zusätzlicher Software
- Lastgenerierung
- Durchsatzmessungen
- Immer wichtig: die Erfahrung des Bedieners

10.4.2. Beispiele

10.4.2.1. Etherload

- Public-Domain-Software für Intel-PCs
- Setzt auf Standardtreibern auf (ODI, NDIS, Paket, DEC-DLL)
- Veranlaßt Treiber alle Pakete an das Programm zu leiten (promiscuos mode)
- Eingeschränkte Möglichkkeit zur Aufzeichnung
- Allgemeine Statistik nur eingeschränkt
    - keine Information über Kollisionen (von Karte nicht weitergegeben)
    - eingeschränkte Informationen über Fehler (vom Netztreiber abhängig, ODI günstiger)
- Interpretation von Paketen der Schichten 2 bis (teilweise) 7
    - online
    - statistische Darstellung
    - keine Expertenfunktion

- Praktisches Problem: nicht für Dauerbetrieb geeignet, da der PC irgendwann einfach hängt (persönliche Erfahrung)

10.4.2.2. RMON-Probes

- Fernabfragbare Netzwerkmonitore
- Standardisierter Leistungsumfang (eventuell mir proprietären Erweiterungen)
- Darreichungsformen:
  - Als Black-Box mit Netzanschluß und IP-Adresse
  - oder in Hubs und Repeatern, Brücken oder Switches integriert
- Funktionen
  - globale Statistik
  - Hostliste mit Statistik
  - History über globale Parameter
  - Kommunikationsmatrix auf Schicht 2
  - konfigurierbare Alarme
  - Datenaufzeichnung (Capture, ohne Dekodierung, aber mit Filterungsoption)
- Zugriff auf gesammelte Daten
  - über SNMP von einer Managementsstation oder
  - über eine lokale Terminalschnittstelle.
- Zugriff über das überwachte Netz oder eine zusätzliche Netzschnittstelle
- Datenauswertung offline
- Standardisiert für
  - Ethernet
  - Token Ring
- Eignung
  - lang- und mittelfristige Überwachung
  - Analyse sporadisch auftretender Probleme
  - für akute Fehleranalyse bedingt geeignet

10.4.2.3. Dedizierte Analysatoren

- Spezielle Meßhardware (keine normalen Netzadapter)
  - daher auch Meßung von
    - Kollisionen und
    - fehlerhaften Paketen
  - in normalen PCs
- Optionen für
  - Ethernet
  - Token Ring
  - FDDI

    - ATM
    - Serielle Leitungen (WAN)
    - ISDN u.a.
- Meist Multiprozessor-Design
    - eigener Prozessor für Meßaufgabe
    - PC nur zur Datendarstellung und Abspeicherung
- Ergebnisse
    - globale Statistik
    - stationsbezogenen Statistik auf Schicht 2
    - Paketaufzeichnung (einschl. Filterung)
    - Paketdekodierung (meist offline)
    - zeitabhängige Darstellung globaler Parameter
- Option zur Lastgenerierung / Replay
- Durchsatzmessungen (mit mehreren Interfacekarten)
- Funktionen ähnlich RMON-Probe, aber vor Ort direkt einsetzbar (keine Management-Station, Erfassung und Analyse direkt am Gerät)
- Eignung:
    - akute Fehleranalyse (vor allem auf Schicht 2)

10.4.2.4. Expertensysteme

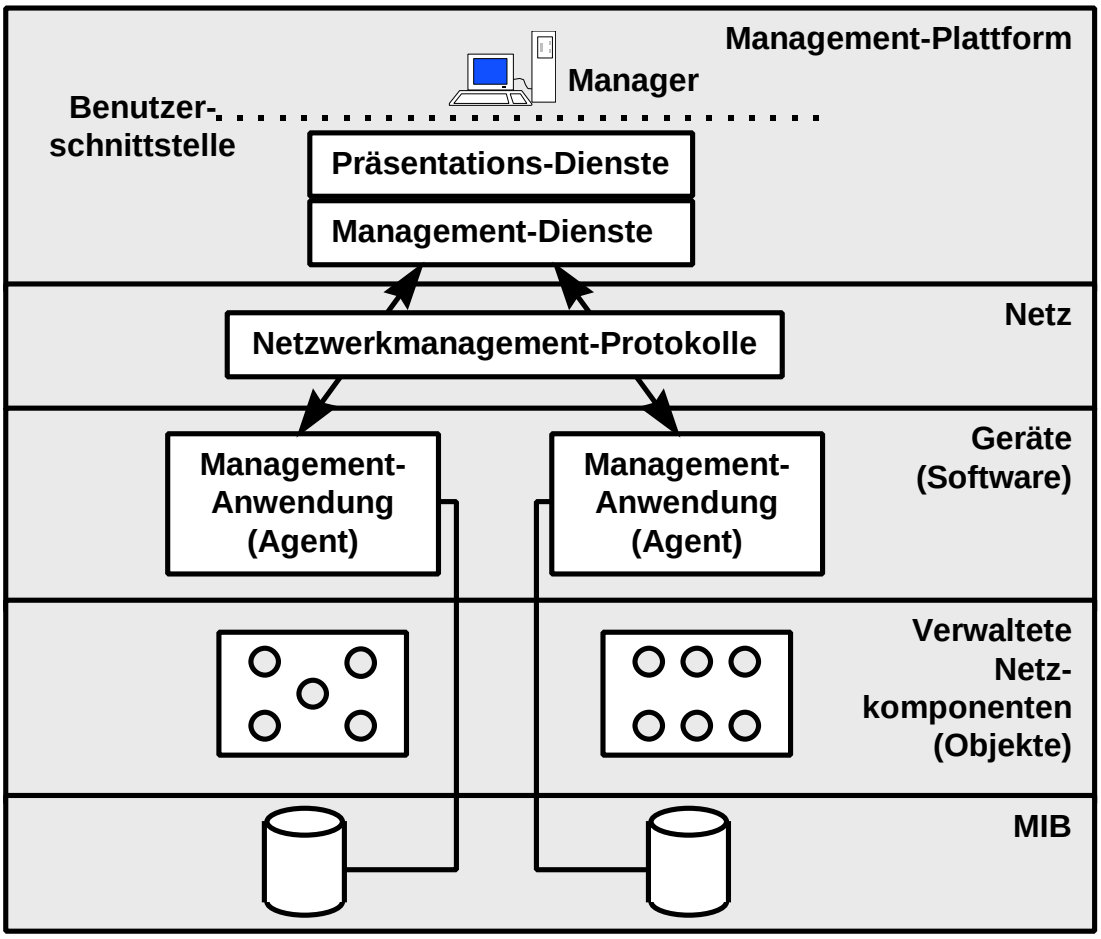
- Insbesondere „Expert-Sniffer“ von Network General
- PC mit leicht modifiziertem Netzwerk-Adapter für
    - Ethernet und
    - Token-Ring
    - (FDDI nur Sniffer, nicht Expert)
- Nur eine CPU
- Ergebnisse
    - globale Statistik
    - stationsbezogene Statistiken auf allen Schichten (ab 2)
    - Paketaufzeichnung einschließlich Filter
    - Paketanalyse
    - Paketdekodierung
    - Analyse von Fehlern und Symptomen in den Schichten 2 bis 7
        - online und
        - offline.
- Lastgenerierung
- Eignung:
    - akute Fehleranalyse auf allen Netzwerkschichten
    - regelmäßige Kontrolle im Sinne des Leistungsmanagement

- Variante als Remote Sniffer (fernbedient)

10.5. Netzwerkmanagement-Systeme

10.5.1. Prinzipien

- Ziel: Überwachung und Management von größeren Netzen
- bisherige Tools realisieren nur geringe Teile der obengenannten Management-funktionalitäten
- verteilte Intelligenz im Netz (bei allen aktiven Netzwerkkomponenten, ***Agenten***)
- Zentrale oder hierarchische Überwachung und Auswertung (Netzwerkmanagement-Station bzw. -Anwendung)
- Kommunikation über Netzwerkmanagement-Protokolle
- Allgemeine Struktur:



- Begriffe:
  - Management-Objekte
    - definiert über

        - Existenz
        - Attribute
        - mögliche Zustände
        - Relationen zu anderen Objekten (Vater, Kind)
      - Baumstruktur
      - Attribute
        - Identifikatoren (zur Wiederfindung)
          - Namen
          - Position in MIB
        - Beschreibende Attribute
          - Funktionalität
          - Leistungsmerkmale
          - Herkunft
          - Rechte
        - Zeitattribute
        - Statusattribute
    - Agent
      - Softwaremodul in einer Netzwerkkomponente
      - Erfaßt selbständig Parameter von Management-Objekten.
      - Kann Parameter von Management-Objekten auf Anweisung ändern
      - Parameter sind strukturiert und werden lokal in einer MIB gespeichert.
    - MIB
      - Management Information Base
      - abstrakte Darstellung der Netzkomponenten als Management-Objekte
      - Baumstruktur
    - Netzwerkmanagement-Protokolle
      - SNMP
        - Simple Network Management Protocol
        - im Internet (und überhaupt) üblich
      - CMIP
        - Common Management Information Protocol
        - OSI-Protokoll
- Kommunikation
    - Polling
      - explizite Abfrage vom Netzwerkmanagement-System zum Agenten
        - periodisch oder
        - bedarfsorientiert
      - vom Netzwerkmanagement-System induziert

    - Traps
        - selbständige Meldung des Agenten an das System
- Managementstrukturen
    - bei Aufteilung der Manager-Aufgaben auf mehrere Netzwerkmanagement-Systeme:
        - zentral
        - symmetrisch (mehrere gleichberechtigte Manager)
        - hierarchisch
- Zielsetzungen und Eignungen:
    - Im Prinzip alle Netzwerkmanagement-Funktionen
    - Abhängigkeit von Funktionalität der Agenten
    - weniger für akute Fehler mit Totalausfall (auf Schicht 1/2) geeignet
    - Konfigurationsmanagement gut
    - langfristige Analyse (Leistungsmanagement)
    - Fehler in Anwendungsebene meist nicht erkennbar
    - Problem: Analyse der Datenmengen
- Allgemeines Problem: In der Regel ein Inband-Management

10.5.2. Netzwerkmanagement-Systeme in der Internet-Umgebung

10.5.2.1. Einfache Netzwerktests

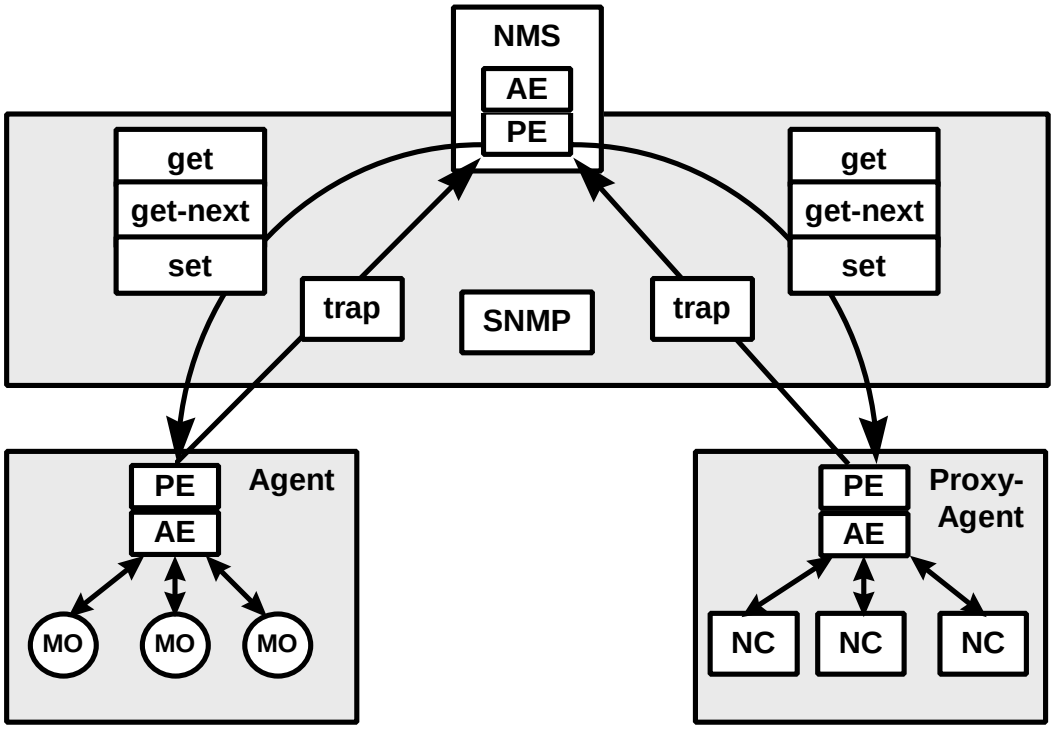
- Überprüfung der Erreichbarkeit von Endstationen mit ICMP-Echo-Requests
    - PING
- Überprüfung der verwendeten Routen mit ICMP
    - traceroute (unter MS-Windows tracert)
    - Reihe von Echo-Requests mit TTLs 1,2,...
    - Antwort der Router mit ICMP-Time exceed

10.5.2.2. Management mit SNMP

- Simple Network Management Protocol
- Aufteilung in
    - Management-Modell
    - Management-Informationsmodell
    - Management-Protokoll
- Das Management-Modell
    - Beschreibung der Management-Elemente und -Funktionen
    - Elemente sind
        - Manager (Management-Stationen, nicht Personen)
        - Agenten
        - Proxy-Agenten (Stellvertreter, die den Zugriff auf Komponenten, die kein SNMP sondern andere Protokolle unterstützen, erlauben)

  - Managed Objects
- Funktionen
  - get, get-next: Abfrage des Wertes eines Attributs eines Managed Object durch den Manager
  - set: Setzen des Wertes eines Attributs eines Managed Object durch den Manager
  - trap: Meldung von Attributen durch Agenten
- In der Praxis dominiert das Polling
- Austausch der Nachrichten über IP/UDP

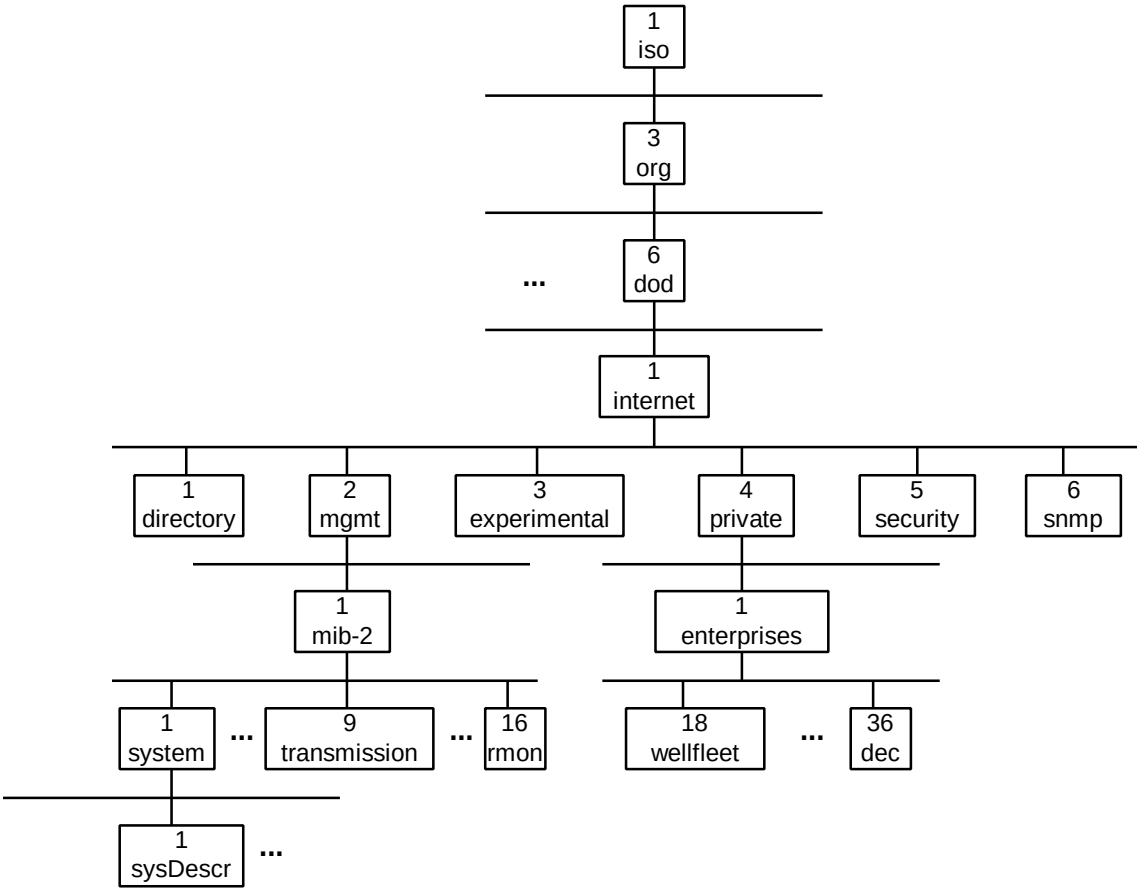
Schema



NMS: Network Management System
AE: Application Entity
PE: Protocol Entity
MO: Managed Object
NC: Network Component

  - Managed Objects können beliebige Objekte sein (nicht nur netzwerkbezogene)
- Management-Informationsmodell
  - Festlegung der Darstellung und das Zugriffs auf Management-Informationen
  - Organisation in einer Baumstruktur (MIB, Management Information Base)
  - Standardisierung des Baumes mit
  - Möglichkeiten zur Erweiterung mit firmenspezifischen oder hardwarespezifischen Ergänzungen
  - Standard-MIB (ursprüngliche Variante und erweiterte MIB-II)

- Bezeichnung der Objekte durch
  - Nummern und
  - Namen (in der Praxis optional, aber nach Möglichkeit benutzt)
- Ausschnitt aus der SNMP-MIB

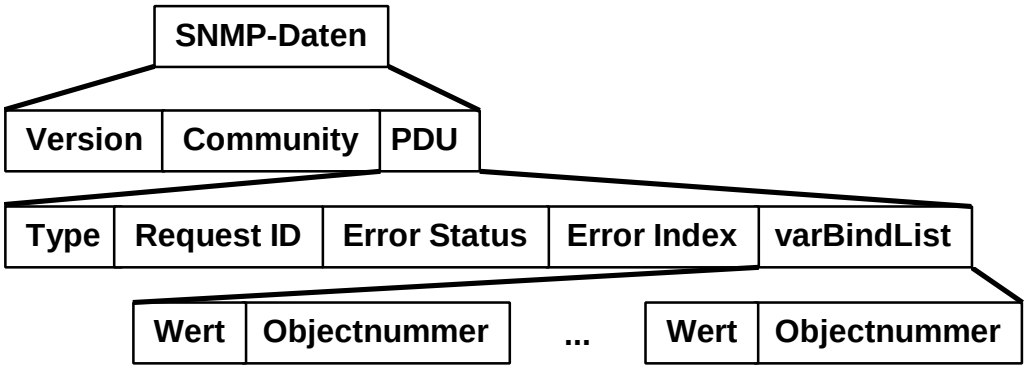


- Beschreibung de Objekte in einem Subset von ASN.1 (Abstract Syntax Notation)
  - Beschreibung von
    - Relationen,
    - Formaten,
    - Zugriffsrechten,
    - Status und
    - Beschreibung / Erklärung von Objekten
  - Typen von Objekten
    - Network Address (MAC)
    - Internet Address
    - Counter (von 0 bis 2^{32}-1 heraufgezählt, dann wieder 0 gesetzt)
    - Gauge (32-Bit-Zähler, der auch dekrementiert werden kann)
    - Timeticks (in 1/100 s)

        - Opaque (zur Definition weiterer Typen)
        - SEQUENCE OF (Record-Definition)
        - OCTET STRING
    - Zugriffsrechte
        - read-only
        - read-write
        - write-only
        - not accessible
    - Status
        - mandatory (zwingend vorgeschrieben)
        - optional
        - obsolete (veraltet)
    - Beispiel: Definition des Objekts ipInDelivers

```
ipInDelivers OBJECT TYPE
        SYNTAX      Counter
        ACCESS      read-only
        STATUS      mandatory
        DESCRIPTION
                „ The total number of input datagrams
                successfully delivered to IP user protocols
                (including ICMP)“
        ::= { ip 9 }
```

- Management-Protokoll SNMP (Version 1)
    - Setzt auf IP und UDP auf
- Paketformat für get/get-next/set:



    - Community (eine Art Password)
    - PDU: Protocol Data Unit
    - Type:
        - get
        - get-next
        - set

        - trap
    - RequestID zur Identifikation und Zuordnung von Requests zu Replies
    - Error Status: Fehlerart
    - Error Index: Fehlernummer
    - Wert bei get/get-next im Request auf Null gesetzt
  - trap-PDU

Type	Enterprise	Agent-Adr.	Generic Trap	Specific Trap	Timestamp	varBindList

    - Enterprise: Wert des Managed Objects sysObjectId des Agenten zur Identifikation des Agententyps
    - Agent Adress: IP-Addresse des Agenten
    - Generic Trap: Nummer eines standardisierten Traps:
        - coldStart
        - warmStart
        - linkDown
        - linkUp
        - authenticationFailure
        - egpNeighbourLoss
        - enterpriseSpecific
    - herstellerspezifische Traps (falls Generic Trap = enterpriseSpecific)
        - definiert in privaten MIBs
    - Timestamp: Zeitstempel mit Uptime des Agenten
- Bewertung von SNMP
  - wenig Ansprüche an Agenten
  - weitverbreitet (der Quasi-Standard)
  - Sicherheitsschwächen

10.5.2.3. SNMP Version 2

- Erweiterung von SNMP
- Schwächen von SNMP
  - hohe Netzlast durch Übertragung der Informationen
  - schwache Sicherheitskonzepte
  - kein hierarchisches Management
- Neu bei SNMPv2
  - erweitertes Kommunikationsmodell Manager-Agent
  - neue Sicherheitskonzepte
  - Übertragung größerer Datenmengen in einer Nachricht
  - Manager-zu-Manager-Kommunikation

    - Erweiterung des Agenten-Konzepts
    - unterschiedliche Transport-Protokolle
- Bisher noch nicht durchgesetzt
- Komplexere Agenten

10.5.2.4. SNMP-Netzwerkmanagement-Systeme

- Verbreitete Netzwerkmanagement-Systeme (unter Unix)
    - OpenView (HP, auch unter Windows, aber mit deutlich geringerer Funktionalität)
    - Spectrum (Cabletron)
    - NetView (IBM, auf Basis HP-OpenView)
    - Polycenter (DEC, SNMP-Teil auf Basis NetView)
    - Transview (SNI)
- Spezielle Tools für spezielle Komponenten
    - graphische Darstellung von speziellen Netzkomponenten
    - herstellerspezifische Erweiterung
    - angepaßt auf private MIBs und spezielle Eigenschaften
    - integriert in Netzwerkmanagement-System oder als Standalone-Programm
- Funktionen eines modernen SNMP-Managers
    - Integration privater MIBs
    - Integration zusätzlicher Anwendungen
    - Erstellen von Anwendungen
        - als Tabellen oder
        - einfache Diagramme
    - Graphische Darstellung der Netzwerktopologie
    - Automatische Ermittlung der Netzwerktopologie
    - Automatische Überwachungsfunktionen
        - Einfache Erreichbarkeitstest mit ICMP
            * periodisch
            * für Endgeräte ohne SNMP-Agenten
        - Überwachung von Schwellwerten (in MIBS der Agenten)
        - Annahme und Interpretation von Traps
        - Konfigurierbare Reaktionen auf Änderung von Netzzuständen
            * Log
            * Mail
            * Pager
            * SNMP-Set
            * Beliebige Unix-Programme
        - Automatische Sammlung von Werten

- Manuelle Überwachungsfunktionen
  - Gezielte Abfrage von Management-Objektwerten
  - Graphische Darstellung der Werte
  - Erstellung von Berichten

11. Netzwerkdienste im GÖNET

11.1. Allgemeine Funktion des Netzes

- Bereitstellung einer lokalen Netzwerk-Infrastruktur
- Lokale Nutzung der Netzwerk-Infrastruktur
  - File- und Printserver-Dienste in Arbeitsgruppen, Abteilungen, Instituten oder Fachbereichen
  - Datenbanken

11.2. Unterstützte Netzwerkprotokolle

- Lokal beliebige Protokolle möglich
- Im Gesamtnetz
  - TCP/IP
  - Novell IPX
  - DECnet (Phase IV)
  - Appletalk
  - LAT

11.3. Dienste der GWDG

11.3.1. Zugang zu klassischen Rechenzentrumsdiensten

11.3.1.1. Rechenanlagen der GWDG als Compute-Server

- UNIX-Cluster
- VAX-Cluster
- Parallelrechner

11.3.1.2. Serverfunktionen im UNIX-Cluster

11.3.1.2.1. Zugriff auf den File-Server des Clusters

- Über NFS
  - auf Antrag
  - geeignete Methode für andere UNIX-Workstations
  - mount von fs?.gwdg.de
- Über PC-NFS
  - Zur Zeit nicht realisiert, aber technisch kein Problem
  - geeignet für PCs mit PC-NFS-Software
- Über NetBIOS-TCP/IP
  - für alle registrierten Benutzer verfügbar
  - realisiert über Public-Domain-Software SAMBA

        - installiert auf gwdu19
        - nutzbar mit verschiedener Client-Software
            - Windows für Workgroups
            - Windows 95
            - Windows NT
            - LAN-Manager
            - PATHworks-TCP/IP
        - Probleme bei der Nutzung
            - basiert auf Broadcast, die im Backbone aber nicht übertragen werden
            - Nutzung von WINS-Servern nötig (IP-Adressen 134.76.11.71 und 134.76.11.72)
            - oder statische Listen (LMHOSTS-Datei) zur Umsetzung von Namen in IP-Adressen
    - Über NetBIOS-DECnet
        - auslaufendes Modell
        - geeignet für PATHworks-DECnet-Clienten
        - installiert auf GWDU02 (DECnet-Node 1.47)
    - Über Novell IPX
        - zur Zeit nicht möglich
        - zur Zeit keine Lösung geplant
    - Über Appletalk
        - über Helios Ethershare (kommerzielle Software)
        - installiert auf gwdu19 (in Zone GWDG)

11.3.1.2.2. Zugriff auf den Archiv-Server des Clusters

- Über NFS
    - wie bei Fileserver,
    - aber mount von archiv.gwdg.de
- NetBIOS und Appletalk
    - direkt nicht möglich
    - indirekt über den File-Server-Zugriff, falls im UNIX-Cluster ein geeigneter Link erzeugt wurde
      (z.B.: ln -s $AHOME $HOME/archiv)
    - auf demselben Weg auch Zugriff auf temporäre Massenspeicherbereiche ($THOME)

11.3.1.2.3. Zugriff auf Print-Server-Dienste

- Über LPR
    - für auf Antrag möglich
        - UNIX-Cluster als Server
            * mit Workstations als Clienten

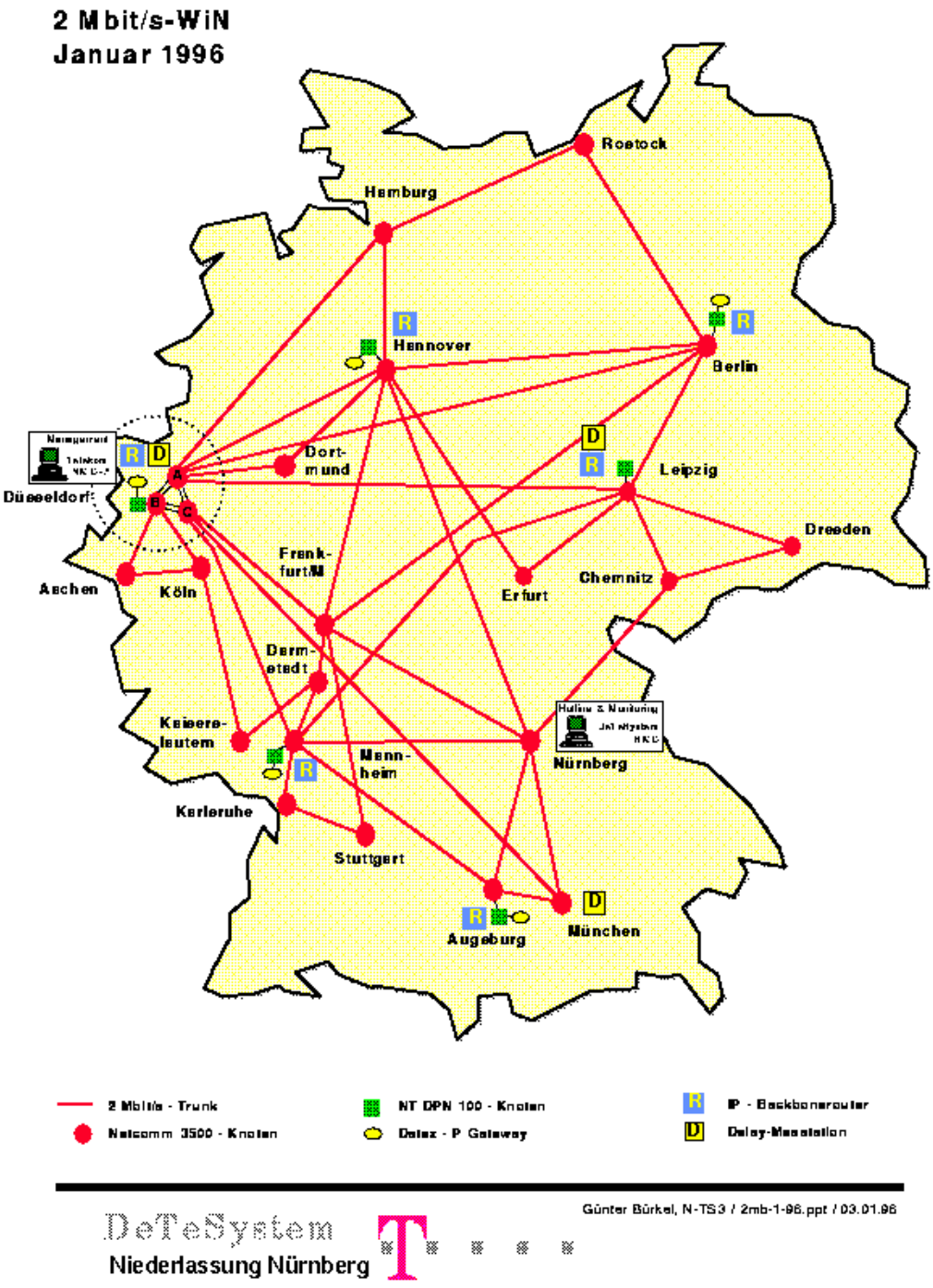
        - insbesondere zum Zugriff auf Spezialdrucker
            + Farblaser
            + Thermotranferdrucker
            + Thermosublimationsdrucker
            + Farbausgabe auf DIN A0-Format (Tintenstrahl-Technik)
            + DIN A0-Plotter
            + Dia-Belichtung
    - UNIX-Cluster als Client
        - mit geeigneten lokalen Servern mit LPD-Dienst
        - zur lokalen Ausgabe aus dem UNIX-Cluster heraus
- Über NetBIOS-TCP/IP
    - für alle registrierten Benutzer möglich
    - UNIX-Cluster als Server
    - Dienste wie bei LPR
    - Clienten-Software wie bei File-Server
    - realisiert über gwdu19 (oder GWDG-PC-S1 im PC-Netz)

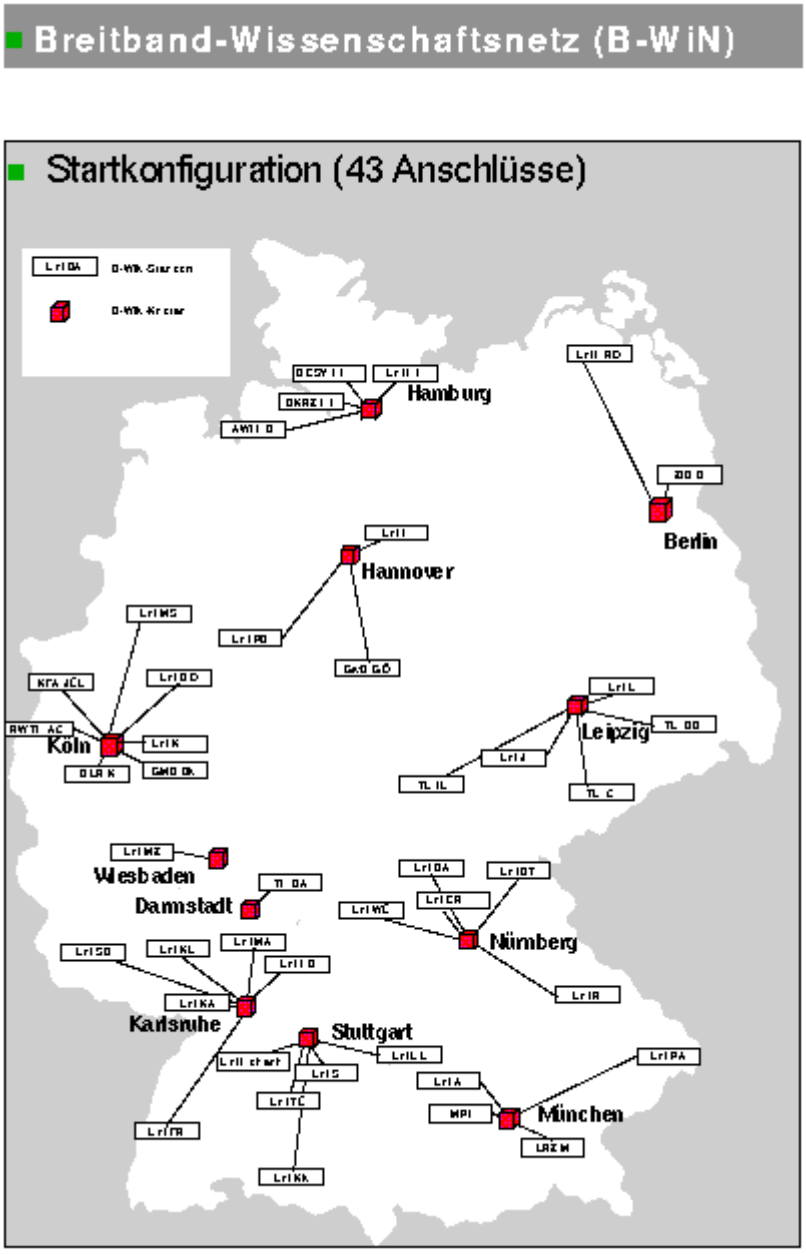
11.3.2. Zugang zu und von nationalen und internationalen Netzen

11.3.2.1. Wissenschaftsnetz (WiN) und Internet

11.3.2.1.1. Anschluß an das WiN

- Forschungsnetz
- Von der Telekom bereitgestellt im Auftrag des DFN-Vereins (DFN=Deutsches ForschungsNetz)
- Anschluß z.Z. über eine 2MBit/s-Verbindung
- Interne Kommunikation über X.25-Protokoll
- Ab April 1996 mit 34 MBit/s (ATM-Netz, zunächst kein X.25 mehr)
- Kommunikation mit TCP/IP-Protokollen in X.25-Paketen verpackt (später in ATM-Zellen)


2 Mbit/s-WiN
Januar 1996
Rostock
Hamburg
Hannover
Berlin
Dort-
mund
Leipzig
Düsseldorf
Dresden
Frank-
furt/M
Chemnitz
Aachen
Köln
Erfurt
Darm-
stadt
Kaiserslautern
Nürnberg
Mann-
heim
Karlsruhe
Stuttgart
Augsburg
München
2 Mbit/s - Trunk
Netcomm 3500 - Knoten
NT DPN 100 - Knoten
Datex - P Gateway
IP - Backbonerouter
Delay-Messstation
Günter Bürkel, N-TS3 / 2mb-1-96.ppt / 03.01.96
DeTeSystem
Niederlassung Nürnberg



11.3.2.1.2. Anschluß an das Internet

- Anbindung an das weltweit größte Netz
- Kommunikation mit TCP/IP-Protokollen, insbesondere SMTP-Mail, FTP, Telnet, Gopher, NetNews, WWW (auch X.400-Mail, X.500-Directory-Service)
- Als Zugang zum Internet und Zugang von Internet zum GÖNET
- Anbindung über vom DFN-Verein bereitgestellte Übergänge (z.Z. von Düsseldorf nach USA, Ebone-Netz in Europa) - „Mehrwertdienste“ des DFN-Vereins
- Pauschale Bezahlung des WiN-Anschlusses (500.000 DM/Jahr für 34 MBit/s) und der „Mehrwertdienste“ (87.000 DM/Jahr) durch die GWDG
- Abrechnung gegenüber den Instituten (bei GWDG) in Arbeitseinheiten (AE)

11.3.2.2. Zugang über Telefonnetz und Modem

11.3.2.2.1. Anbindung über Terminalemulation an das UNIX-Cluster

- Zeichenorientierte Anbindung an die Rechner der GWDG
- Indirekt funktional eingeschränkter Zugang zum GÖNET und Internet
- Modems mit 28800 bit/s Übertragungsrate
- Erreichbar unter (05 51) 5 02 67 10
- Voraussetzung: Benutzerkennung bei der GWDG

11.3.2.2.2. Anbindung über PPP-Protokoll an das Internet

- Direkte Netzanbindung über Modem
- Endgerät wird direkt Teil des Internet bzw. GÖNET
- Volle Funktionalität im Internet
- Zugangskontrolle über das PC-Netz der GWDG
- Zugang zum PC-Netz der GWDG
- Modems mit 28.800 bit/s Übertragungsrate
- Erreichbar unter (05 51) 2 01 18 88
- Voraussetzung: Benutzerkennung bei der GWDG
- Weiterer Zugang über den UNIX-Cluster der GWDG im Test

11.3.3. Kommunikations- und Informationsdienste

11.3.3.1. Mail

11.3.3.1.1. SMTP-Mail

- Internet-Mail-Protokoll (Simple Mail Transfer Protokol)
- Direkte Ende-zu-Ende-Kommunikation (meistens)
- oder Nutzung von Mail-Relais oder Mailern (Rechnern zur Zwischenspeicherung)
- Unter Mehrbenutzersystemen wie UNIX und VMS üblich
- Aufgabenteilung:
  - Mail-Frontend-Programm zum Schreiben und Lesen von Mails, Verwalten von Adressbüchern (hat mit SMTP und Netzen noch nichts zu tun)
  - Mail-Programm zum Versenden und Empfangen von Mail (mit Warteschlangen- und Wiederholungsfunktion für den Fall vorübergehend unerreichbarer Zielrechner)
- Problem: Zielrechner muß (fast) permanent über Netz erreichbar sein.
- Problem: Keine Authentifikationsfunktionen
- Im GÖNET: von vielen lokalen Rechnern (meist UNIX-Systeme), insbesondere auch von den Rechnern im UNIX-Cluster der GWDG (Mail-Adresse: user@gwdg.de oder user@Uni-Goettingen.de)

11.3.3.1.2. Mail-Relay (Mailer)

- Zwischenspeicherungsfunktion durch Rechner mit erhöhter Betriebssicherheit und Verfügbarkeit (Vergleichbar mit Sekretariat)
- Übliche Kommunikationswege mit Mailern:
  Sender ⇒ lokaler Mailer ⇒ entfernter Mailer ⇒Empfänger
- Der Sendevorgang erfolgt aktiv, der Empfangsvorgang passiv, d.h. der Empfänger muß zu nicht vorhersehbaren Zeiten empfangsbereit sein
- Mail-Adresse ist Name des Endrechners
- Eventuelle Gateway-Funktionen (Übergänge zu anderen Mail-Protokollen)
- Im GÖNET: mailer.gwdg.de

11.3.3.1.3. POP-Mail-Server

- Post Office Protokoll
- Client-Server-Konzept
- Üblicher Kommunikationsweg:
  Sendender POP-Mail-Client ⇒lokaler SMTP-Mail-Server ⇒ empfangender POP-Mail-Server ⇒ empfangender POP-Mail-Client
- Die POP-Mail-Clienten arbeiten aktiv, der POP-Mail-Server passiv (der SMTP-Server arbeitet wie ein Mailer).
- Kommunikationsprotokolle:
  - SMTP bei Sendevorgängen
  - POP beim Lesen der Mail vom POP-Mail-Server
- Mail-Adresse ist der (ein, jeder) Name des POP-Mail-Servers
- Im GÖNET:
  - Server: popper.gwdg.de
  - Mail-Adresse: user@gwdg.de (oder user@popper.gwdg.de oder user@Uni-Goettingen.de)
  - Voraussetzung: Benutzerkennung bei der GWDG
  - Alternativ lokale Server von Instituten oder Fachbereichen
- Verfügbare POP-Clienten
  - Für Apple Macintosh: Pegasus-Mail, Eudora (Freeware)
  - Für PCs mit Windows: Pegasus-Mail (auch für Mail über Novell-Server), Eudora
  - Demnächst POP-Mail-Client in Netscape integriert (für Mac, PC, UNIX)

11.3.3.1.4. X.400-Mail

- OSI-Mail-Protokoll
- Im Internet-Bereich weniger verbreitet
- Bei GWDG möglich (als Zieladresse user@gwdg.d400.de)
- Übergänge über Mail-Gateway-Funktionen (DFN-Verein/Mehrwertdienste)

11.3.3.1.5. DECnet-Mail

- Mail-Protokoll in der DECnet-Protokoll-Familie
- Gateway zwischen SMTP-Mail und DECnet-Mail bei GWDG (Rechner GWDGI)
- Senden vom DECnet ins Internet über Adresse GWDGI::“SMTP-Adresse“ (““ mit eingeben)
- Senden vom Internet ins DECnet über Adresse user@DECnet-Name.dnet.gwdg.de

11.3.3.1.6. Versenden von Dateien

- Problem: Mit SMTP ist nur die Übertragung von 7-bit-Zeichen vorgesehen, also keine Umlaute, keine Binärdaten
- Lösung: Kodierungsverfahren zur Umsetzung in einen 7-bit-Kode
- Drei gängige Kodierungsverfahren: uuencode/uudecode (kommt aus der UNIX-Welt: uu=Unix-to-Unix), BinHex (kommt aus der Mac-Welt) und MIME (Internet-Standard, Multipurpose Internet Mail Extensions)
- Unterstützung durch Mail-Cienten: pine (MIME), Eudora (BinHex), Pegasus-Mail (alle drei), Netscape (MIME)

11.3.3.2. Gopher

- Informationsdienst
- Client-Server-Konzept
- Strukturiert in
  - Dokumente und
  - Verzeichnisse
- Dokumente üblicherweise als reine ASCII-Texte (keine Umlaute, keine Formatierungen)
- Neuere Clienten erlauben andere Formate durch Aufruf von Zusatzprogrammen (external viewer)
- Verzweigung zu Terminalemulationen möglich
- Verknüpfung zu weltweitem Informationssystem durch Verweise auf andere Server in den Verzeichniseinträgen
- Clienten unter verschiedenen Betriebssystemen
- Zugriff auf Server erfolgt anonym
- Wird durch WWW ersetzt
- Bei GWDG:
  - Server gopher.gwdg.de
  - Clienten im UNIX-Cluster (gopher) und PC-Netz (als Windows-Anwendung)

11.3.3.3. WWW

- Informationsdienst
- Client-Server-Konzept

- Weltweites Informationssystem
- Funktionalitäten
  - Dokumente in Textform
  - Graphiken (vor allem GIF-Format)
  - Formulare
  - Datenbank-Schnittstellen
  - Integration von
    - Dateitransfer mit FTP
    - Gopher
    - NetNews
  - Einbindung anderer Applikationen
    - Telnet
    - Video
    - Audio
    - beliebige „external viewer“
- Dokumente in HTML-Format
- Hypertext-Strukturierung
- Keine Unterteilung in Verzeichnisse und Dokumenten, sondern Verknüpfung zwischen Dokumenten über Querverweise (Hyperlinks) im Dokument
- Clienten („Browser“, Freeware für Unis) für
  - UNIX-Systeme (Netscape, Mosaic)
  - Windows / Windows NT / Windows 95 (Netscape, Mosaic, MS-Internet Explorer)
  - Mac (Netscape, Mosaic)
- Ersetzt zusehends Gopher-Systeme
- Im GÖNET:
  - Server der GWDG: www.gwdg.de (Proxy-Server für HTTP,FTP,Gopher)
  - Server der Uni (Abteilung Medizinische Statistik) www.Uni-Goettingen.de
  - Clienten bei der GWDG unter UNIX und im PC-Netz
- Netscape als WWW-Browser auch als News- und POP-Mail-Client einsetzbar

11.3.3.4. NetNews

- Diskussionsforum
- Client-Server-Konzept
- Verteilung von Servern mit gleichem Inhalt (abgesehen von technisch bedingten Verzögerungen)
- hierarchisch organisierte Verteilung der Inhalte zwischen den Servern
- Aufteilung der Diskussionen in hierarchisch organisiert Diskussionsgruppen (thematisch sortiert)
- Möglichkeit zur Einrichtung lokaler News-Gruppen

- Begrenzte Speicherungsdauer von Beiträgen auf den Servern (je nach Konfiguration der Server)
- Zugriff auf die Diskussionsbeiträge durch Abfrage eines News-Servers
- Versenden von Beiträgen an einen News-Server (der dies akzeptieren muß)
- Im GÖNET:
  - Server news.gwdg.de
  - Lokale News-Gruppen (gwdg.xxx)
  - Zugriff:
    - Im UNIX-Cluster mit nn oder tin (zeichenorientiert)
    - Im PC-Netz mit WinVN oder Netscape unter Windows (auch für PCs in Instituten)

11.3.3.5. Listserver

- Diskussionsgruppen
- Verschiedenste von einander unabhängige Server
- Auf Mail-basierend
- Diskussionsbeiträge werden an alle Teilnehmer vom Server per Mail verschickt.
- Diskussionsbeiträge werden an die Liste durch Mail an eine Listen-Mail-Adresse gesendet.
- Aufnahme in eine Liste nach einer speziellen Mail an den List-Server
- Im GÖNET
  - Server listproc@gwdg.de
  - Listen (z.B.)
    - goenet@gwdg.de
    - mpg-info@gwdg.de

11.3.4. Netz-interne Dienste

- DNS
  - Domain Name Server
  - Umsetzung zwischen IP-Adresse und Internet-Name (in beiden Richtungen)
  - Hierarchisches System von Servern
  - Verschiedene Servertypen (primary, secondary, caching, forwarder)
  - Bei GWDG
    - Server für Domänen gwdg.de, Uni-Goettingen.de, mpg.de
    - Server für IP-Netz 134.76.0.0
    - Adressen der Server 134.76.10.46 und 134.76.98.2
    - Delegation von Subdomänen an lokale Server möglich
    - Einrichtung und Nutzung von lokalen Secondary-Servern mit eine Kopie der Datenbasis zum Schutz vor Ausfällen
- NIS

  - Network Information Service
  - Früherer Name Yellow Pages (YP)
  - Verteilte Datenbestände, insbesonders von Benutzern, Gruppen, Rechnern vor allem bei UNIX-Rechnern zur Bildung lokaler Cluster
  - Lokal eingesetzt oder an Domäne der GWDG angegliedert bei Rechnern die voll von der GWDG betrieben werden.
- BOOTP
  - Umsetzung zwischen MAC-Adresse und IP-Adresse (eine Richtung)
  - Vorteil: Endgerät wird von zentraler Stelle mit IP-Adresse versorgt (keine lokale Konfiguration nötig)
  - Nachteile: Abhängigkeit vom Netz und Server, Verwaltungsaufwand
  - Insbesondere bei Rechnern, die über Netz gebootet werden, eingesetzt
  - Bei Bedarf bei GWDG verfügbar, aber theoretisch auch auf jedem UNIX-Rechner (und z.T. auch auf anderen Systemen)
- Windows-NT-Domänen
  - Benutzer- und Rechteverwaltung unter Windows NT
  - Domäne GWDG-PC für das PC-Netz der GWDG (kann auch von außerhalb benutzt werden)
- WINS
  - Windows Name Server
  - Umsetzung von NetBIOS-Namen in IP-Adressen
  - Registrierung und Zuteilung von NetBIOS-Namen
  - Nur für Microsoft-Netze relevant
  - Im GÖNET: Server 134.76.11.71 und 134.76.11.72 (NT-Server GWDG-PC-S1 und GWDG-PC-S2)
  - Bei Microsoft Netzen (Windows für Workgroups, Windows 95) im GÖNET unbedingt eintragen
- Zeit-Synchronisation
  - Über NTP-Protokoll
    - Server der GWDG: ntps1.gwdg.de, ntps2.gwdg.de, ntps3.gwdg.de
    - Synchronisiert auf Funkuhr
  - Bei PCs mit Windows für Workgroups mit net time \\gwdu19 /set /yes

11.4. Dienste der Staats- und Universitätsbibliothek

11.4.1. OPAC

- Online Public Access Catalog
- Bestände, Ausleihe, Verlängerung
- Über Terminalemulationsprogramme mit Telnet-Protokoll unter OPAC.SUB.Uni-Goettingen.de erreichbar
- Im GÖNET und im gesamten Internet zugänglich

11.4.2. PICA-Katalogisierung

- Dienst für Institutsbibliotheken zur Katalogisierung im Verbundssystem

11.4.3. CD-ROM-Server

- Server der SUB für Datenbanken auf CD-ROM
- Realisiert über Novell-Netware-Server
- Nur von PCs (80x86) mit Novell-Netz-Anbindung unter DOS (nicht unter Windows) erreichbar
- Menügeführtes System zur Auswahl verschiedener Datenbanken
- Zwei Server:
  - GOSUB5 in der SUB
  - SUBMED in der Teilbibliothek Medizin
- Login als Benutzer CDPUBLIC (ohne Password)

11.5. Andere Dienste

- Im einzelnen bisher nicht erfaßt
- Vor allem WWW-, auch FTP-Server
- Insbesondere www.Uni-Goettingen.de (z.Z. bei der Medizinischen Statistik)

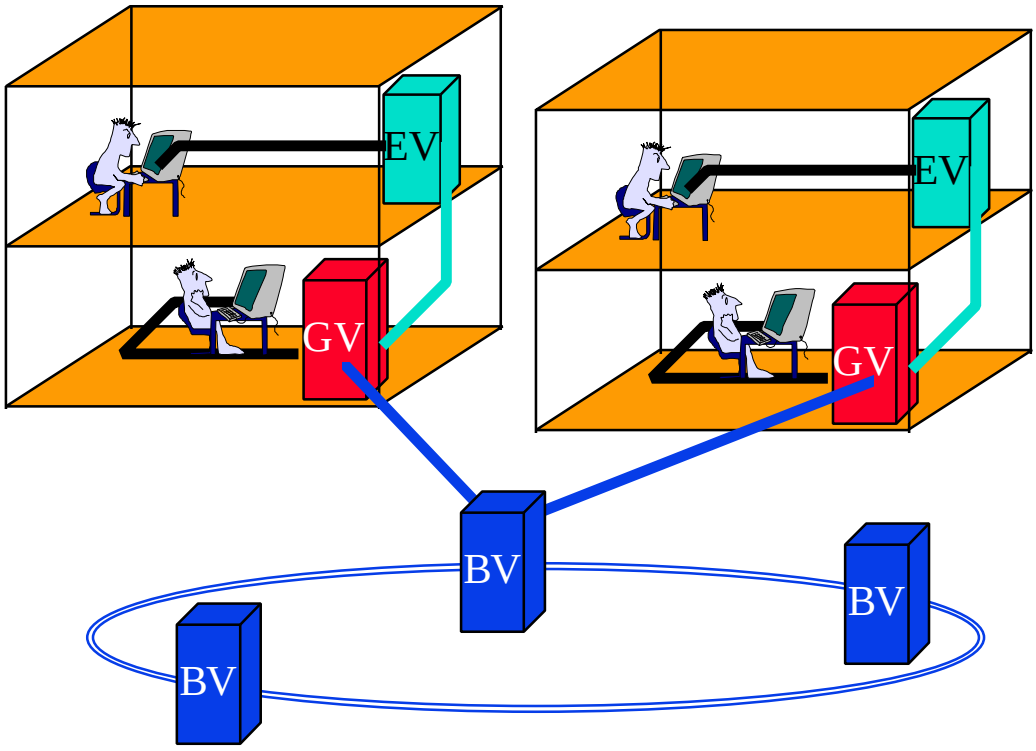
12. Technische Realisierung eines Universitätsnetzes

12.1. Funktionale Strukturierung eines Universitätsnetzes

12.1.1. Strukturierungsprinzipien

Aufteilung des Netzes in Funktionsbereiche

- Etagenbereich oder Tertiärbereich
- Steigebereich oder Sekundärbereich (innerhalb eines Gebäudes)
- Gebäudeanschluß oder Primärbereich
- Hintergrundnetz oder Backbone



12.1.2. Backbone

- Prinzipiell
  - Schnelles Hintergrundnetz (¤ 100 MBit/s)
  - Bildung von Konzentrationspunkten (Backbone-Knoten)
  - Verbindung der Konzentrationspunkte
  - Glasfaser-Verkabelung
  - Router als Backbone-Knoten
- Im GÖNET
  - Backbonenetz mit 12 Monomodeglasfasern 9/125µm (plus vier Fasern der Max-Planck-Institute für Strömungsforschung und Experimentelle Medizin)
  - Betrieb als FDDI-Netz
  - Logischer-Ring, aber physikalisch eine einzige Strecke mit einer Verzweigung in der Hospitalstraße zum Südbereich und zur Sternwarte

- 10 Backboneknoten
  - GWDG
  - Forstwissenschaftlicher Fachbereich (Router im Büsgenweg 5)
  - Nordbereich (unterhalb Bereich Forst) mit Router in der Anorganischen Chemie
  - Fernmeldezentrale (Anschluß von entfernten Netzen über Telefonleitungen)
  - Neues Klinikum
  - Bereich Altes Klinikum und Agrarwissenschaften mit Router in der Physiologie
  - Bereich GWZ mit Router im Theologicum
  - Hospitalstraße
  - Südbereich mit Router in der III.Physik
  - Sternwarte
- 10 Wellfleet BCN-Router mit FDDI-Schnittstellen als Backboneknoten
- Ethernet- und Token-Ring-Schnittstellen im Backbone-Router für Primäranschlüsse (FDDI bei GWDG)

12.1.3. Primärbereich

- Allgemein
  - Anschlußtechnik
    - Glasfaserverbindung von jedem Gebäude zum Backboneknoten (soweit finanzierbar und technisch möglich)
    - Verbindung über Modem-Strecken im Telefonnetz andernfalls
  - Anbindung mit 10-100 MBit/s bei Glasfaserkabeln und 64 kBit/s bis 2 MBit/s bei Modemverbindungen
  - Gebäudehauptverteiler mit Ethernet-, Token-Ring- oder FDDI-Technik (nach Bedarf und Möglichkeit)
  - Router-, Brücken-, Switch- oder Repeaterfunktionalität (bedarfsabhängig)
  - Einsatz von erweiterbaren Verteilern (quantitativ und qualitativ)
- Im GÖNET
  - Anschlußtechnik
    - Ansteuerung jedes Gebäudes mit 12 Gradienten-Glasfassern 50/125 µm
    - oder Modemverbindung
      - mit 512 kBit/s bei Neuinstallationen
      - alte Verbindungen 64-160 kBit/s
      - für die Zukunft geplant 2 MBit/s
  - Anschluß jedes Gebäudes
    - im Falle Glasfaseranschluß an eigene Routerschnittstelle,
    - aller Modemverbindungen an eine Routerschnittstelle im FMZ über Remote-Ethernet-Brücken
  - Primärverteiler in Hub-Technologie
  - Primärverteiler
    - mit Repeaterfunktionalität bei kleinen Gebäuden/Netzen
    - mit Brückenfunktionalität bei größeren Gebäuden/Netzen

  - mit Switchfunktionalität in der Sternwarte (und zukünftig statt Brücken)

12.1.4. Sekundärbereich

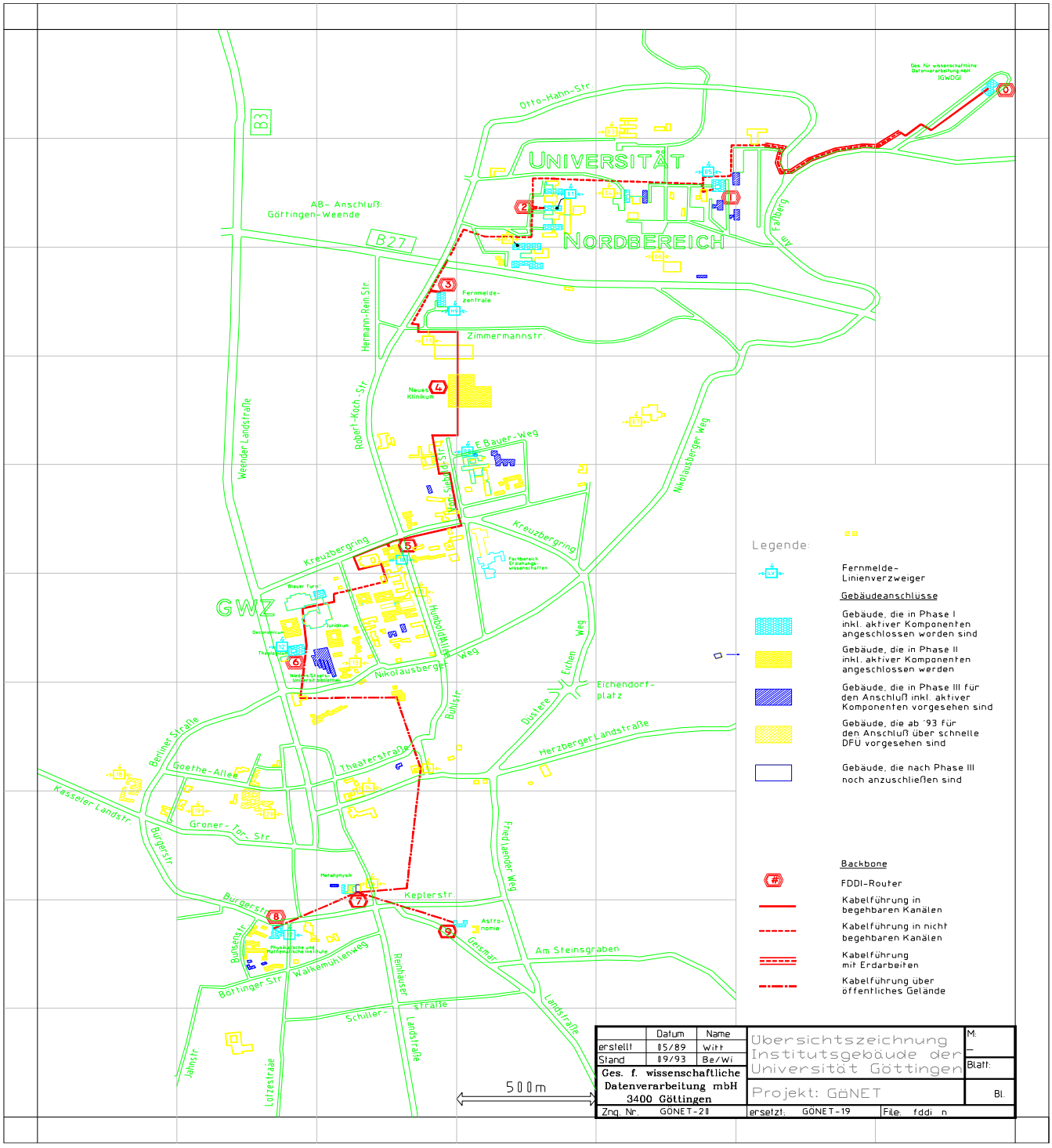
- Allgemein
  - Etagen- oder Bereichsverteiler (Sekundärverteiler)
  - Verkabelung zwischen Primär und Sekundärverteiler (meist Verteilung in der Vertikalen, daher auch Steigebereich genannt)
  - Verkabelung in Glasfasertechnik
  - Sekundärverteiler
    - in Ethernet-, Token-Ring oder FDDI-Technik (ggf. auch gemischt)
    - je nach Bedarf mit Repeater-, Brücken-, Switch- oder (selten) Routerfunktionalität
  - Einsatz von erweiterbaren Verteilern (quantitativ und qualitativ)
  - Anschlußpunkt für Etagenverkabelung
  - Kann in kleineren Gebäuden entfallen, wenn der Primärverteiler die Funktion mit übernimmt
- Im GÖNET
  - Steigeverkabelung mit 12 Gradienten-Glasfasern 50/125µm
  - Ethernet- und Token-Ring-Technik (FDDI nur bei GWDG und einigen Max-Planck-Instituten)
  - In der Regel Repeater-Funktionalität (einmal eine Brücke)
  - Modulare Hubsysteme oder Stackable Hubs
  - Fehlt in den meisten Gebäuden, da Verkabelung direkt zum Primärverteiler geht.
  - Anschlußtechnik entsprechend Tertiärverkabelung
    - BNC-Buchsen für 10Base2-Ethernet
    - RJ45-Buchsen für 10BaseT-Ethernet
    - IBM-Würfel-Stecker, RJ45- DB9-Buchsen für Token-Ring

12.1.5. Tertiärbereich

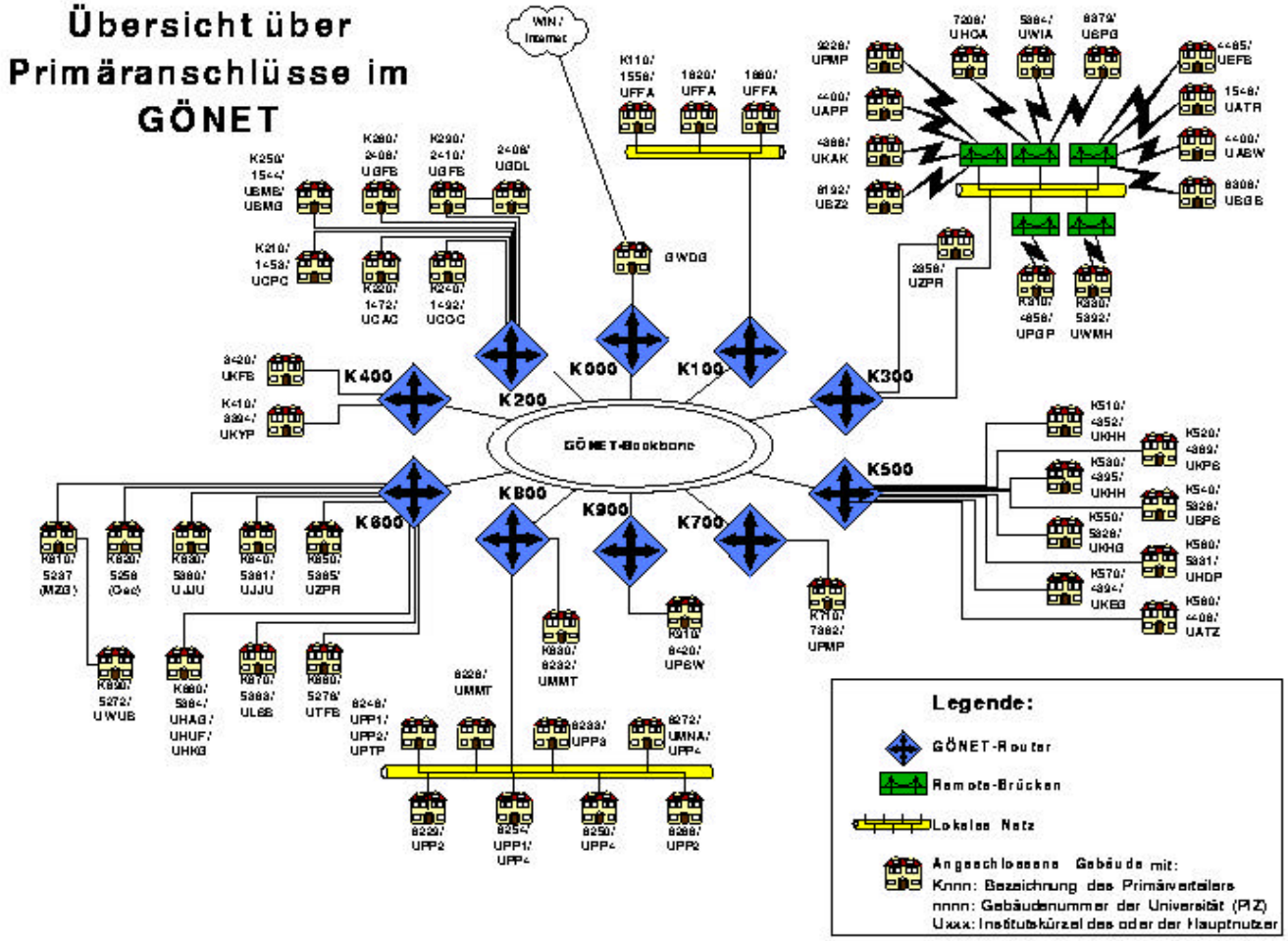
- Allgemein
  - Verkabelung vom Sekundärverteiler bis zur Anschlußdose für Endgeräte
  - Bei Neuverkabelung
    - Sternförmige Verkabelung
      - wegen Flexibilität bezüglich Netztechnik und logischer Strukturierung
      - TP-Verkabelung mit Kategorie-5-Kabel (bis 100 MHz und 100 m Kabellänge geeignet, 100 Ω)
      - Glasfaser-Verkabelung bei elektromagnetisch belasteter Umgebung oder Sicherheitsbedürfnissen oder großen Entfernungen.
  - Bei Altverkabelung auch Koaxialkabel, IBM-Typ-1-Kabel
- Im GÖNET
  - Viele Altverkabelungen, da in der ersten Phase (fast) nur bestehende Netze angeschlossen wurden.
  - Neuverkabelungen mit Kategorie-5-Verkabelung (Ausnahme im Bereich des WiSo-Rechenzentrums: IBM Typ 1)

12.2. Topologie des Göttinger Universitätsnetzes

12.2.1. Physikalische Struktur



12.2.2. Logische Struktur



12.3. Konfiguration des Netzes

12.3.1. IP-Routing

- Für jedes Gebäude ein eigenes IP-Subnetz (Ausnahme: Anschlüsse über Remote-Brücken und Modem)
- Subnetzmaske 8 Bit (Maske 255.255.255.0 bzw. FF.FF.FF.00)
- Bei größeren Gebäuden mehrere logische Subnetze für ein physikalische Netz (Multi-netting)
- Empfehlung für Endgeräte
  - Subnetting ignorieren
  - Subnetzmaske 255.255.0.0 bzw. FF.FF.00.00 einstellen
  - Broadcast-Adresse mit 255.255.255.255 oder 134.76.255.255 einstellen
  - Proxy-ARP auf dem Router löst Adressen in entfernten Subnetzen auf
  - Statische Route (Default-Route zum Netz 0.0.0.0) auf 134.76.x.254 (mit x=eigene Subnetznummer)

    - Dynamische Routing mit RIP möglich, aber nicht empfohlen, solange nur ein Weg existiert
- Filter gegen IP-Spoofing (vortäuschen falscher IP-Adressen aus fremden Subnetzen heraus)
- OSPF als Router-Protokoll im Backbone

12.3.2. Novell-IPX-Routing

- Netzwerktyp oder Frame-Format:
    - Ethernet_802.3 im Ethernet
    - 802.2 im Token Ring
    - SNAP im FDDI (Probleme bei Brücken zwischen FDDI und Ethernet)
- Externe Netzwerknummer für Server: IP-Subnetz (in hexadecimal geschrieben, ggf. Subnetz mit der niedrigsten Nummer im Falle von Multinetting)
- Interne Netzwerknummer für Server: externe Netzwerknummer mit 01,02, usw. an der letzten Stelle.
- Z.Z. keinerlei Filter implementiert

12.3.3. DECnet-Routing

- Area-Routing auf den Backbone-Routern
- In der Regel Area 10, mit Ausnahmen
    - Area 2 für Südbereich
    - Area 3 für MPI für Stömungsforschung
    - Area 4 für Sternwarte
    - Area 11 für Forstwissenschaftlihen Fachbereich
    - Area 12 für Abteilung Medizinische Statistik (mit eigenem Area-Router)

12.3.4. Appletalk-Routing

- Konfiguration der Backbone-Router als Seed-Router
- Netznummer = Nummer des IP-Subnetzes * 100
- Network-Range von 10 Netznummern
- Zonennamen im Format Uni-Fachbereich-Institut
- Ggf. mehrere Zonen auf einem physikalischen Netz

12.3.5. Brückenfunktionalität der Router

- Translation-Bridging zwischen FDDI und Ethernet bzw. Token-Ring
- nicht mehr unterstützt und aktiviert