Vorlesungsscript FH Friedberg *(Hessen)*

Skript zu Rechnernetzwerke

Prof. Dr. Karim Roger Kremer

21. März 2005

Inhaltsverzeichnis

Kapitel 1

Einführung: ISO/OSI-Referenzmodell

Gegenüber zentralisierten Systemen bieten Rechnernetze aus autonomen Rechnern, die über ein Kommunikationsnetz miteinander verbunden sind, folgende Vorteile:

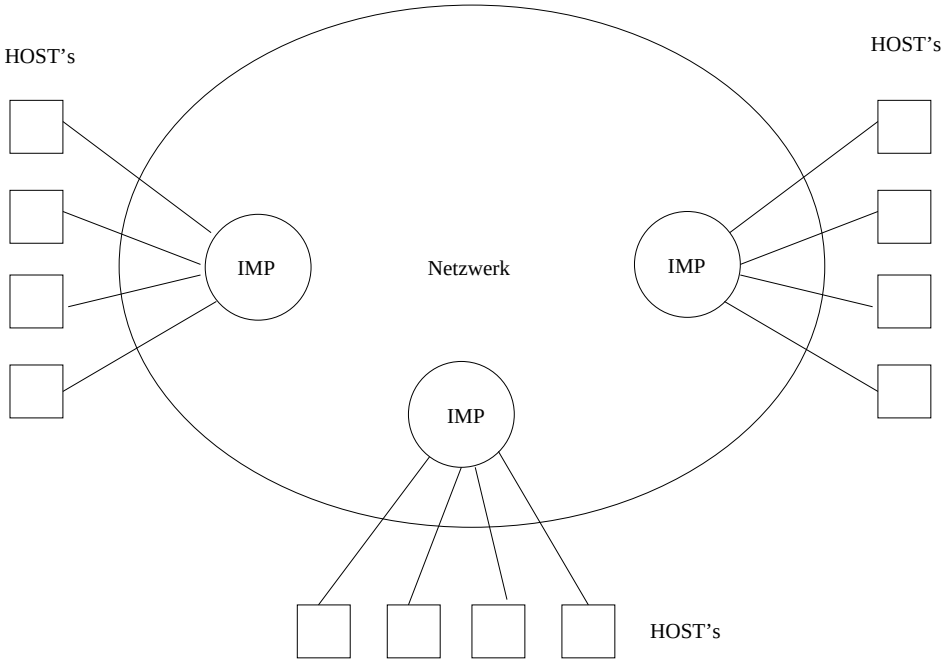
Leistungsverbund: Leistung einzelner Rechner lässt sich durch Hinzuschalten weiterer Rechner erhöhen.

Erhöhte Zuverlässigkeit:Bei Ausfall eines oder mehrerer Rechner kann auf andere Rechner zurückgegriffen werden.

Lastverteilung: Überlastete Rechner werden durch Übertragung von Aufgaben auf unterlastete Rechner entlastet.

Besseres Dienstleistungsangebot: Das Spektrum der Dienstleistungen von Anwender-Programmen aber auch spezialisierter oder dedizierter Hardware, wie spezielle Drucker-, Datei-, Datenbank- oder Rechen-Server wird vergrößert.

Die Aufgabe des Rechnernetzwerks besteht darin, Daten zwischen den Endknoten, den sog. Host's, zu übertragen. Dazu verfügt das Netzwerk über Leitungen und spezielle Prozessoren, die bestimmte Verbindungen miteinander verschalten. Solche Prozessoren werden Interface Message Processors (IMP's) genannt. Einheitliche Kommunikationsverfahren sog. Protokolle definieren die Schnittstelle der Host's zu den IMP's bzw. zum Netzwerk.



Rechnernetze lassen sich nach einer Vielzahl von Kriterien unterteilen. Ein Kriterium ist z.B. die größenordnungsmäßige Länge der Verbindungsleitungen. Bei höchstens ca. 10 km spricht man von einem lokalen Netz (Local Area Network, LAN) anderenfalls von einem globalen Netz oder Weitverkehrsnetz (Global Area Network, GAN oder Wide Area Network, WAN). Manche Autoren geben auch noch eine weitere Gruppe von sog. Metropolitan Area Networks (MAN's) an. Außer der Länge weisen globale und lokale Netze eine Reihe von weiteren Unterschieden auf.

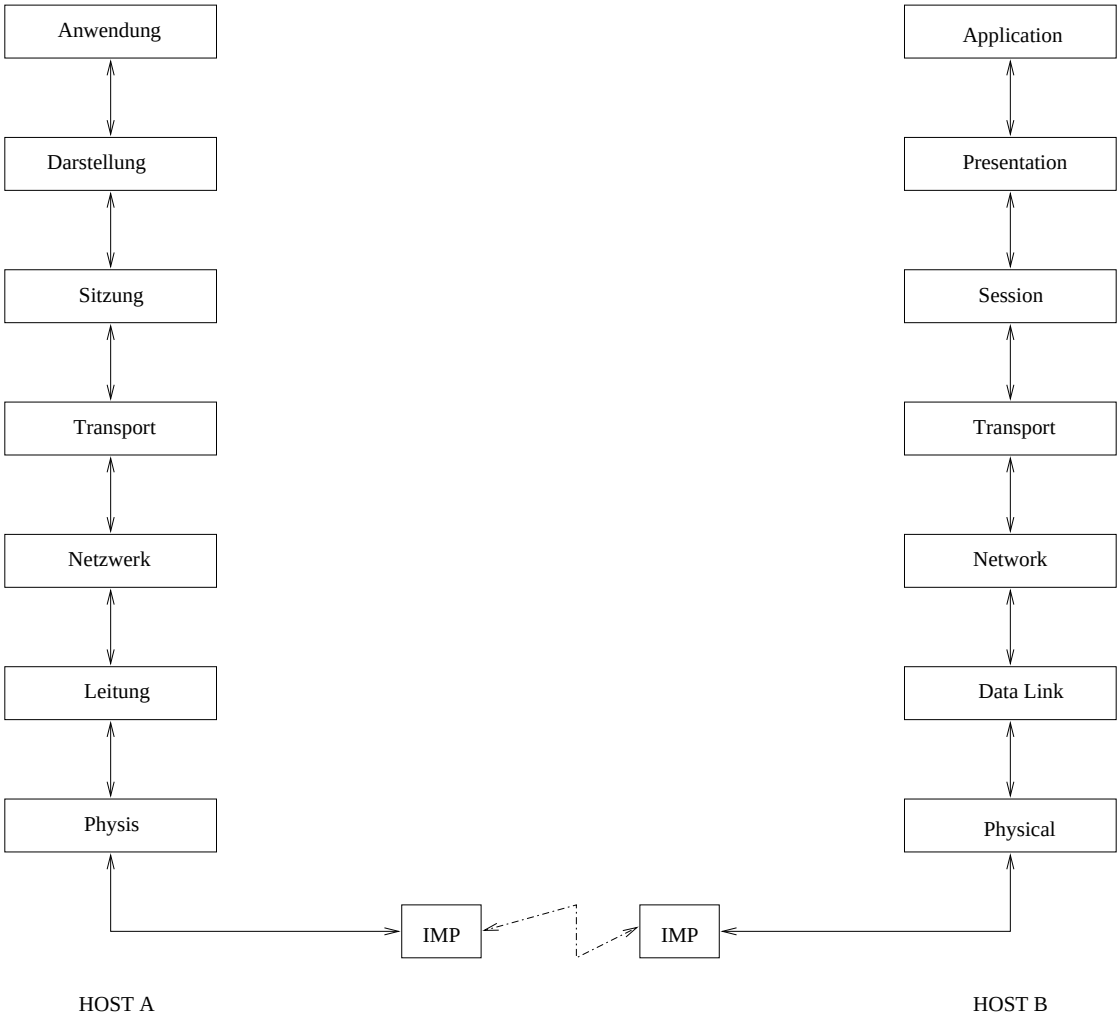
Für diese unterschiedlichen Netze sind zahlreiche komplexe Protokolle erforderlich. Diese dienen dazu, die physikalischen Netze aus logischer Sicht einheitlich zu handhaben. Die Protokolle werden in verschiedenen logischen Ebenen organisiert, wobei zwischen netzwerkabhängigen, netzwerkunabhängigen und anwendungsbezogenen Ebenen unterschieden wird. Zur Beschreibung der Architektur eines Netzes wird das 7-Schichten-ISO/OSI-Referenzmodell verwendet.

So wie sich ein Rechner in einer Hierarchie von Ebenen beschreiben lässt (CPU, Arbeitsspeicher, Maschinensprache, Assembler, Betriebssystem, Compiler, Anwendungen), können auch bei der Kommunikation verschiedene Abstraktionsebenen unterschieden werden. Will ein Benutzer z.B. mit einem Programm Daten bearbeiten, die sich auf der Festplatte eines anderen Rechners befinden, so muss der lokale Rechner transparent für den Benutzer die Kommunikationssoftware starten, die den Datentransfer auf der höchsten logischen Ebene bewerkstelligt. Diese Softwareebene hat aber kein Wissen über das physikalische Medium, über

das die Daten transferiert werden. Dieses Wissen hat der zugeordnete IMP (z.B. die Netzwerkkarte im PC an einem LAN). Die Daten werden vom IMP geeignet kodiert, um Fehler bei der Übertragung zu erkennen und ggfs. zu beseitigen. Auf der anderen Seite des Empfänger-IMP's müssen die Daten wieder dekodiert werden. Außerdem muss eine Anpassung an das physikalische Medium erfolgen (z.B. Koaxial-Kabel, Twisted-Pair-Kabel, FDDI-Glasfaser).

Das ISO/OSI-Referenzmodell ist eine Standardisierung der verschiedenen Ebenen in datenverarbeitende, transportierende und physikalische Funktionen. Jede Ebene stellt der logisch darüber stehenden Ebene wohldefinierte Funktionen zur Verfügung. Weiterhin bearbeitet jede Ebene eine abgeschlossene Aufgabe, so dass der Informationsaustausch mit der darüber stehenden Ebene möglichst gering ist.

Das folgende Bild gibt einen Überblick über den Aufbau des ISO-Referenzmodells. Wesentlich am ISO/OSI-Referenzmodell ist, dass die Durchführung der Kommunikation in den unteren Ebenen völlig transparent für die darüber liegenden Ebenen ist.



Man unterscheidet zwischen Punkt-zu-Punkt-Netzen (Point-to-Point-Networks) und Broadcast-Netzen.

Bei Punkt-zu-Punkt-Netzen sind die IMP's zweier Rechner entweder direkt oder indirekt über andere IMP's in einem Store-and-Forward-Netz miteinander verbunden. Im Store-and-Forward-Netz sind die Zwischenstationen-IMP's in der Lage, die Daten bei belegten Leitungen zwischenzuspeichern und nach Freiwerden der Leitungen weiterzuleiten. Bei mehreren Leitungen kann ein IMP ggfs. auch eine freie Leitung wählen.

Beim Broadcast-Netz teilen sich alle IMP's einen einzigen Kanal. Ausgesendete Daten eines IMP stehen an allen anderen IMP's zur Verfügung. Beide Netzformen sind i.d.R. also nicht konfliktfrei.

Die verschiedenen Netzwerktypen, wie Ethernet, Token-Ring und Fibre Distributed Data Interface (FDDI) unterscheiden sich auf den unteren 3 Ebenen des ISO/OSI-Referenzmodells. Deswegen werden sie als netzwerkorientierte Ebenen bezeichnet. Ziel des Referenzmodells ist eine Übereinstimmung verschiedener Netzwerke auf den darüber liegenden Ebenen.

Die Ebenen lassen sich wie folgt beschreiben:

Ebene 1 ist die physikalische Ebene. Sie beschreibt die Übertragung der Bits über eine Verbindungsleitung. Dabei sind u.a. folgende Aspekte interessant:

- Wieviel Volt werden für eine duale 1, 0 benötigt?
- Wieviel Zeit wird für eine duale 1, 0 benötigt?
- Welches Medium wird verwendet?
- Wie lang ist die Übertragungsstrecke?
- Wie erfolgt die Übertragung - simplex, d.h. nur in eine Richtung, halb-duplex, d.h. zeitlich abwechselnd in beide Richtungen oder voll-duplex, d.h. gleichzeitig in beide Richtungen?
- Welche Stecker werden benutzt?
- Welche zusätzlichen Übertragungseinrichtungen wie Modems oder ISDN-Adapter werden benutzt?

Ein häufiger Fall ist z.B., dass analoge Telefonleitungen zur Datenübertragung genutzt werden. Dabei sind digitale Daten des Rechners in analoge Signale der Leitung umzuwandeln und umgekehrt. Diese Aufgaben übernimmt ein sog. Modem (Modulator-Demodulator). Ein Rechner oder Terminal wird hierbei über eine bitserielle V.24-Schnittstelle an das Modem angeschlossen. Es ist jedoch auch möglich, zwei Rechner mit ihren V24-Schnittstellen über kürzere Distanz direkt in einer sog. Nullmodemschaltung ohne Modems zu verbinden.

Für digitale Übertragungsleitungen ohne Modem kann z.B. ein Interface nach der X.21-Empfehlung verwendet werden. Sowohl V.24 als auch X.21 sind bitserielle Verfahren, d.h. zu einer Zeit wird nur ein Bit übertragen und nicht mehrere Bits gleichzeitig.

Für kürzere Distanzen sind auch bitparallele Verfahren gebräuchlich, z.B. in den Bussen von Rechnern. Über längere Strecken treten bei bitparallelen Verfahren allerdings Synchronisationsprobleme durch unterschiedliche Laufzeiten der parallel übertragenen Bits auf, weshalb dort meist bitserielle Verfahren verwendet werden.

Die Ebene 2 ist die sog. Leitungsebene (Data-Link-Layer). Zu ihren Aufgaben gehört der Aufbau der Datenverbindung zwischen zwei unmittelbar benachbarten Kommunikationseinheiten (IMP's oder Host's). Weiterhin werden Datenübertragungsfehler der physikalischen Ebene erkannt und falls möglich korrigiert. Hierzu dienen Verfahren zur Fehlererkennung und -korrektur. Erkannte aber nicht korrigierbare Fehler werden an die nächst höhere Ebene zur weiteren Behandlung weitergegeben. Zur Fehlerbehandlung werden die Daten in Blöcke unterteilt und geeignet kodiert blockweise übertragen. Einige der Aufgaben des Leitungsprotokolls sind:

- Angabe von Anfang und Ende eines Datenblocks,
- Erkennung und Behandlung von Übertragungsfehlern,
- Senden und Empfangen einzelner Datenblöcke in richtiger Reihenfolge,
- Adressierung einer zusammengehörenden Menge von Datenblöcken,
- Flusssteuerung, d.h. Anpassung der Sendegeschwindigkeit an den Empfänger, um Datenverluste zu vermeiden.

Ein einfaches Verfahren zur Flusssteuerung ist das Stop-and-Wait-Verfahren, bei dem nach einem Frame auf die Bestätigung des Empfängers gewartet wird, bevor der nächste Frame gesendet wird.

Die Netzwerk-Ebene (Ebene 3) betrachtet das gesamte Netzwerk aus logischer Sicht. Es wird der Transport von Daten zwischen Quelle und Ziel ggfs. über Zwischenstationen bewerkstelligt. Routing-Verfahren bestimmen hierbei den Weg, den die Daten im Netz zurücklegen. Routing ist also die Wegfindung im Netzwerk. Als Relaying bezeichnet man die Wegsteuerung im Netz, d.h. die Vermittlung der Datenpakete im Netz. Bezüglich der Dienstleistungen für die darüberliegende Transport-Ebene lassen sich zwei verschiedene Dienstarten unterscheiden:

Virtual Circuit Service: Hierbei wird dem Host ein perfekter logischer Kanal zur Verfügung gestellt, mit Verbindungsauf- und abbau und fehlerfreier, vollständiger Datenübertragung

Datagram Service: Hierbei werden Datenpakete (Datagramme) von einem Host angenommen und isoliert weiterübertragen. Die Reihenfolge der Datagramme sowie die Zuverlässigkeit der Übertragung werden nicht garantiert.

Der Virtual Circuit Service hat seine Entsprechung beim Telefondienst, bei dem der Anrufer erst wählt dann spricht und schließlich auflegt. Alle Abläufe im Telefonnetz sind für den Nutzer transparent. Er hat es scheinbar mit einer fehlerfreien Punkt-zu-Punkt-Verbindung zu tun.

Der Datagram Service ist zum Briefverkehr analog. Jeder Brief wird isoliert befördert. Dazu muss er eine vollständige Adresse enthalten. Bei Verlust eines Briefes verschickt die Post nicht automatisch ein Duplikat. Datagramme, die auf dem Weg z.B. wegen zu geringer Empfangspuffergröße verloren gehen, werden ebenfalls nicht automatisch erneut gesendet. Weiterhin kommen Datagramme wie Briefe auch nicht notwendigerweise in der Reihenfolge des Absendens beim Empfänger an.

Während der Datagram Service auch bei kurzen Nachrichten effizient arbeitet, ist der Virtual Circuit Service wegen Verbindungsauf- und abbau dort ineffizient. Ferner kann der Datagram Service an die Belastung des Netzwerks angepasst werden, denn jedes Paket kann potentiell lastabhängig seinen eigenen Weg durch das Netz gehen. Die Implementierung des Datagramm Service ist einfacher, denn es brauchen keine Informationen über bestehende Verbindungen in den Host's und IMP's gehalten werden. Wesentlicher Nachteil des Datagram Service ist das Eintreffen der Nachrichtenpakete in einer falschen Reihenfolge beim Empfänger. Durch das dynamische Routing sind Überholvorgänge der Datagramme im Netzwerk möglich.

Ebene 4 ist die Transportebene. Ihre Aufgabe ist einen zuverlässigen, effizienten End-to-End Transportservice zwischen Benutzerprozessen auf verschiedenen Host's zu gewährleisten. Hier wird also nicht mehr die maschinennahe Host-IMP-Schnittstelle betrachtet, d.h. das unterliegende Netz ist für die Schicht 4 nicht relevant. Die Transportebene empfängt Daten aus der Ebene 5, unterteilt sie in kleinere Einheiten und versieht sie mit Kontrolldaten und Identifikatoren in einem sog. Header. Anschließend überträgt sie diese Daten u.U. über mehrere verschiedene Netze zur Transportebene eines anderen Host's. Einige wichtige Funktionen der Transportebene sind:

- Aufbau, Durchführung und Beendigung eines Datentransfers zwischen Benutzerprozessen,
- Multiplex einer Netzverbindung, d.h. Nutzung einer Netzverbindung für mehrere Transportverbindungen oder auch Nutzung mehrerer Netzverbindungen für eine Transportverbindung zur Leistungssteigerung,
- Segmentierung, d.h. Zusammenfassen, von Blöcken der Schicht 5,
- Synchronisation und Flusskontrolle auf der Basis von End-to-End Benutzerprozessen,
- Maßnahmen zur Fehlererkennung und Fehlerkorrektur über Ebene 2 hinaus.

Die Komplexität des Transportprotokolls hängt wesentlich von der Qualität des Fehlerverhaltens der tieferen Ebenen ab. Dabei können drei Fehlerarten in tieferen Ebenen klassifiziert werden:

1. Der Fehler wird auf einer Ebene entdeckt und dort auch behoben.
2. Der Fehler wird auf einer Ebene entdeckt, kann aber dort nicht behoben werden, sondern wird an eine höhere Ebene weitergemeldet.
3. Der Fehler wird auf einer Ebene nicht entdeckt und deshalb auch nicht behoben und weitergemeldet.

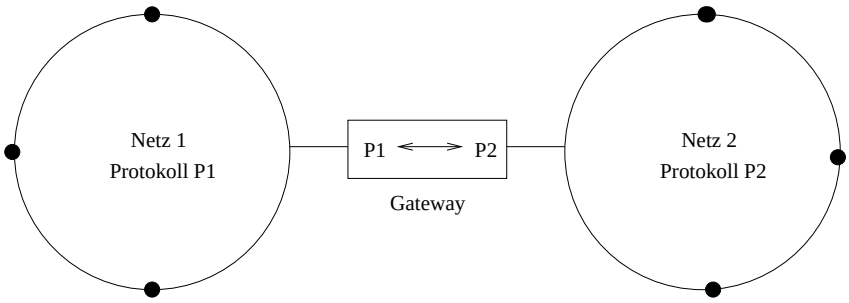
Nach dieser Fehlerdifferenzierung können drei Netztypen unterschieden werden:

- Netzverbindungen mit akzeptabler Rate von Fehlern der Art 1. und 2. und keinen Fehlern der Art 3, d.h. alle Fehler werden zumindest unterhalb Schicht 4 erkannt. Hier ist der zusätzliche Aufwand zur Fehlerbehandlung in Schicht 4 gering.
- Netzverbindungen mit akzeptabler Fehlerrate der Art 3. aber nicht akzeptabler Rate der Art 2.
- Netzverbindungen mit nicht akzeptabler Rate der Art 3.

Der Aufwand zur Fehlerbehandlung steigt hierbei, so dass bei dem letzten Netztyp die gesamte Fehlerbehandlungs-Funktionalität in die Ebene 4 verlagert wurde. Allgemein gilt, dass man umso mehr Fehlerbehandlungs-Funktionalität in die Ebene 4 verlagert je zuverlässiger das Übertragungsmedium ist. Denn der Aufwand in Ebene 2, Fehlerbehandlung zu betreiben, wäre dann aufgrund der seltenen Fehlerfälle ineffizient. Hierzu zwei Beispiele:

1. Überregionale Netze auf der Basis konventioneller Leitungen (Kupferdraht):
   - Medium unzuverlässig (z.B. Bit error rate 10^{-6}),
   - aufwendiges Netzprotokoll der ersten 3 Ebenen z.B. X.25 mit Virtual Circuit Service,
   - einfaches Transportprotokoll.
2. Lokales Netz auf Koaxialkabel-, Twisted Pair- oder Glasfaser-Basis:
   - Medium sehr zuverlässig (z.B. Bit error rate 10^{-9}),
   - einfaches Netzprotokoll mit Datagram Service,
   - Ebene 4 beinhaltet Maßnahmen für seltene Fehler.

Eine weitere Aufgabe der Transportebene ist das sog. Internetworking, d.h. die Verbindung von verschiedenen Netzen, die u.U. unterschiedliche Protokolle auf den Ebenen 1 bis 3 verwenden. Dazu gibt es an den Berührungspunkten solcher Netze sog. Gateways oder Gateway-Rechner, die die unterschiedlichen Protokolle ineinander umwandeln.



Die Dienste der Transportebene ermöglichen der Sitzungsebene (Session Layer, Ebene 5) von allen Hardware-, Software- und Topologie-Details der beteiligten Netze zu abstrahieren.

Die Sitzungsebene (Session Layer, Ebene 5) regelt die Nutzung der Transportebene z.B. bzgl. Zugriffsrechten, Kommunikationsart und Abrechnungsmodalitäten. Im sog. Binding wird dementsprechend ein Aufbauwunsch für eine Verbindung akzeptiert oder abgelehnt.

Die Darstellungsebene (Presentation Layer, Ebene 6) hat die Kodierung der Daten in eine gemeinsame Sprache eines offenen Systems zur Aufgabe. Hierzu wird aus der Normierung verschiedener konkreter Syntaxen unterschiedlicher Systeme eine gemeinsame abstrakte Syntax formuliert. Eine Sprache in abstrakter Syntaxnotation wird als Abstract Syntax Notation (ASN) bezeichnet. Anwendungs-Beispiele für ASN's sind:

- Datenkompression,
- Verschlüsselung,
- ASCII/EBCDIC-Konvertierung,
- 32 Bit-Zahl-/64 Bit-Zahl-Konvertierung,
- Umwandlung verschiedener Dateiformate.

Zur sicheren Übertragung von Daten im Sinne eines Schutzes gegen unberechtigtes Abhören der Nachrichten durch Dritte werden Daten verschlüsselt. In einem Broadcast-Netz z.B. Ethernet kann eine an einen bestimmten Adressaten

gerichtete Nachricht von vielen anderen Stationen empfangen werden. Mit der Verschlüsselung beschäftigt sich die Kryptologie mit ihren beiden Unterdisziplinen der Kryptographie (erkennbarer) Geheimschriften und der Kryptoanalysis der (unautorisierten) Entzifferung.

Die Anwendungsebene (Application Layer, Ebene 7) beschäftigt sich mit Kommunikationsfunktionen, die aus der Sicht des Netzanwenders interessieren. Dienste werden also nicht für andere ISO/OSI-Ebenen sondern für Anwendungsprozesse zur Verfügung gestellt. Wegen der Anwendungsorientierung sind einheitliche Protokolle auf dieser Ebene kaum möglich. Es gibt aber eine Reihe von Standardfunktionen, die für viele Anwendungen von Bedeutung sind und deren Protokolle zumindest teilweise standardisiert sind. Dazu gehören:

- Remote Job Entry (RJE),
- Electronic Mail (Mail Transfer Protocol, MTP),
- ortstransparente Dateiverwaltung (z.B. Network File System, NFS),
- Dateitransfer (z.B. File Transfer Protocol, FTP).

Es gibt viele weitere Protokolle für spezielle Anwendungszwecke, z.B. für:

- elektronischer Bankverkehr (Electronic Founds Transfer),
- Lastverteilung von Programmen auf mehrere Rechner,
- verteilte Betriebssysteme,
- verteilte Datenbanken.

Ein typisches Beispiel für ein Anwendungsprotokoll sind verteilte Datenbanken. Dabei wird ein logisch zusammengehörender Datenbestand auf geographisch getrennte Rechner verteilt. Das Anwendungsprotokoll hat jetzt z.B. die Ortstransparenz zu gewährleisten, d.h. der Nutzer kennt nicht die physikalische Verteilung der Daten. Vorteile verteilter Datenbanken sind u.a. die erhöhte Zuverlässigkeit gegenüber zentralisierten Systemen sowie die leichtere Erweiterbarkeit und Flexibilität bei Änderungen der Anwendungen.

Kapitel 2

Grundlagen der Rechnernetzwerke

2.1 Eigenschaften und Unterschiede lokaler und globaler Rechnernetzwerke

Die wichtigsten Eigenschaften lokaler Rechnernetzwerke lassen sich wie folgt zusammenfassen. Diese Eigenschaften grenzen lokale Netze insbesondere auch gegen klassische globale Netze ab:

1. Die Leitungen sind höchstens 10 km, meist jedoch weniger als 1-2 km lang. Typischerweise verläuft ein LAN innerhalb eines Hauses oder mehrerer Häuser auf einem Firmengelände. Es gibt keine postalischen Vorschriften für das Privatgelände.

2. Das Übertragungsmedium besitzt hohe Bandbreite, z.B. durch Verwendung von Koaxial-,Twisted Pair- oder Glasfaserkabeln. Um diese Bandbreiten von 10 MBit/s bis zu einigen GBit/s zu erreichen, müssen die Leitungslängen, wie unter 1. angegeben, beschränkt sein.

3. Die Antwortzeiten für interaktive Benutzung liegen unter ca. 10 ms.

4. Die Anzahl der angeschlossenen Hosts und Endgeräte bleibt im wesentlichen konstant, bis auf Ausfälle und Hinzunahmen von Hosts und Endgeräten.

5. Die Kommunikation zwischen den Komponenten ist ausfallsicher. Kosten entstehen nur für Installation und Wartung nicht aber für die Nutzung des Netzes.

6. Erweiterungen oder Veränderungen sind ohne größere Unterbrechungen des laufenden Betriebs möglich.

Lokale Netze ermöglichen die Integration von Terminals, PC's, Workstations und Spezial- und Großrechnern zu einem gemeinsamen Netz, in dem verteilte Dienste von unterschiedlichen Orten aus genutzt werden können. Die Anforderung an die LAN-Technik steigt aufgrund höherer Last auf den Netzwerken z.B. durch verstärkten Einsatz leistungsfähiger Server in Client/Server-Applikationen. Auch die Integration von Video-, Audio- und Grafikapplikationen erhöhen die notwendige Bandbreite und fordern geringe Verzögerungszeiten der Kommunikation. Traditionelle LAN's erfüllen diese Forderungen nur teilweise, weswegen momentan neue Techniken entwickelt und erprobt werden.

Globale Netze sind von lokalen Netzen u.a. durch folgende Eigenschaften abgegrenzt:

1. Das Netz ist in seiner räumlichen Ausdehnung unbeschränkt.
2. Das physikalische Medium verfügt i.a. über geringere Übertragungskapazität als bei lokalen Netzen (Ausnahme z.B. Satellitenstrecken).
3. Die Antwortzeiten sind länger, z.B. typischerweise 100 ms.
4. Die Kommunikation zwischen den Netzkomponenten ist mit hohen Kosten für Installation, Betrieb und Wartung verbunden.
5. Die Anzahl angeschlossener Endgeräte ändert sich zeitlich. Verbindungen werden meist für jede Datenkommunikation neu aufgebaut.
6. Die Nutzung des Netzes ist durch gesetzliche Vorschriften geregelt.
7. Die Netzarchitektur ist technisch und rechtlich offen. Letzteres bedeutet, dass ein öffentliches Netz von jedem genutzt werden darf, der die technischen Voraussetzungen für einen Netzanschluss erfüllt und die anfallenden Gebühren bezahlt.

Punkt 5 besagt, dass es sich bei einem globalen Netz i.a. um ein Wählnetz mit wenigen Standleitungen handelt. Vor allen Dingen die Punkte 2 und 3, also Übertragungsbandbreite und Antwortzeiten, müssen insbesondere im Hinblick auf die wachsenden Anforderungen im Internet (z.B. Integration digitalisierter Telekommunikationsdienste) verbessert werden und LAN-Qualität erreichen.

2.2 Übertragungsmedien

Für verschiedene Signaltypen werden folgende Arten von Übertragungsmedien eingesetzt:

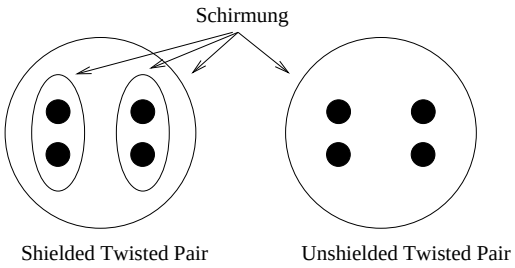
- elektrische Leitungen,
- Lichtwellenleiter,
- Mikrowellen.

Als elektrische Leitungen werden meist Koaxialkabel sowie 2- und 4-Drahtleitungen verwendet. 2- und 4-Drahtleitungen werden meist mit verdrillten Leiterpaaren als sog. Twisted Pair-Kabel produziert. Durch die Verdrillung bekommen die elektromagnetischen Strahlungsfelder entgegengesetzte Richtungen und neutralisieren sich so gegenseitig. So wird die resultierende Störstrahlung des Kabels sehr gering. Falls mehrere Paare von Leitungen in einem Kabel untergebracht sind, wird hierdurch eine Minimierung des sog. Nebensprechens, d.h. der Störung der Leitungspaare untereinander erreicht. Je enger die Verdrillung ist, d.h. je größer die Anzahl Wicklungen pro Länge ist, desto niedriger sind Strahlung und Nebensprechen.

Man unterscheidet zwei Arten von Twisted Pair-4-Drahtkabeln:

Shielded Twisted Pair (STP): Hierbei sind die Leiterpaare von einer Schirmung aus geflochtener Kupferlitze oder spiralförmiger Metallfolie umgeben. Dies erhöht die Störfestigkeit gegen Rauschen aus der Umgebung weiter und reduziert die ausgestrahlte Energie.

Unshielded Twisted Pair (UTP): Hierbei gibt es nur eine äußere Schirmung der 4-Drahtleitung.



STP-Kabel werden vor allem für Token-Ring-Netze eingesetzt und sind in der Regel teurer als UTP-Kabel; sie übertreffen i.d.R. die Spezifikation von UTP-Kabeln. Für UTP gibt es verschiedene Kabel-Kategorien:

Kategorie 1: Nachrichtenkabel für niedrige Frequenzen bis 100 KHz, z.B. für Alarmsysteme

Kategorie 2: Nachrichtenkabel für Frequenzen bis 4 MHz, z.B. für den ISDN-Basisanschluss mit 144 KBit/s

Kategorie 3: Sprachkabel (Voice Grade) für Übertragung mit Frequenzen bis 16 MHz auch zur Datenübertragung verwendet

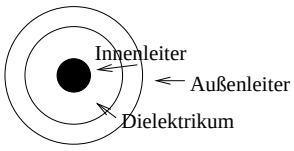
Kategorie 4: Datenkabel (Data Grade) für Frequenzen bis 20 MHz

Kategorie 5: Datenkabel für Frequenzen bis 100 MHz

Die Mehrzahl der installierten Kabelinfrastrukturen sind heute UTP Kategorie 3. Mit neuen Übertragungstechniken werden dort heute 100 MBit/s und mehr erreicht. Neue Kabel für Hochgeschwindigkeitsnetze werden meist aus der Kategorie 5 gewählt. Die Kategorie 6 entsteht gerade mit Frequenzbereichen bis zu 600 MHz.

Zwischen der Grenzfrequenz f_g in Hz und der Schrittgeschwindigkeit v_T in Baud besteht folgender Zusammenhang als Faustregel: $v_t = 1.25\ f_g$. Die Begründung hierfür ist, dass die Sprungantwort eines idealen Tiefpasses mit Grenzfrequenz f_g eine Einschwingzeit t_e von ungefähr $t_e = 1/2f_g$ benötigt. Setzt man die kürzeste Signaldauer oder den Schritt mit $T > t_e = 1/2f_g$ an, z.B. $T = 0.8\frac{1}{f_g}$, so erhält man für $v_T = 1/T = 1.25\ f_g$.

Koaxialkabel bestehen aus zwei Leitern - einem zentralen Innenleiter und einem Außenleiter, der den Innenleiter umhüllt. Die Leiter sind durch ein Dielektrikum gegeneinander isoliert. Koaxialkabel werden hauptsächlich zur Verkabelung von TV's verwendet. Bei Standard-LAN's spielen sie heute kaum noch eine Rolle, obwohl sie in ihren physikalischen Eigenschaften den Twisted-Pair-Kabeln überlegen sind. Die Bandbreite von Koaxialkabeln beträgt je nach Typ 450, 750 oder 1000 MHz.



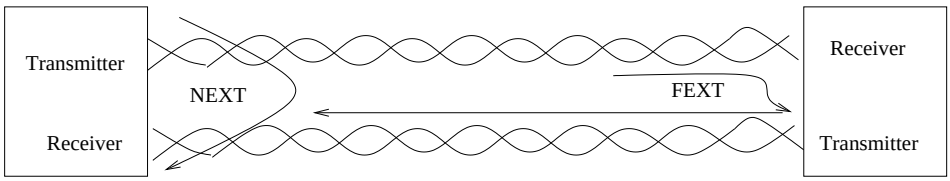
Koaxialkabel

Die Übertragungsleistung von Kabeln wird hauptsächlich durch Dämpfung, Nebensprechen und Rauschen begrenzt. Diese Faktoren setzen Grenzen für die Genauigkeit, mit der Bits beim Empfänger erkannt werden können.

Bei der Dämpfung fällt der Signalpegel in Abhängigkeit von elektrischen Eigenschaften (Impedanz) der Leitung, der Leistung des Senders, der Frequenz des Signals und der Entfernung. Deshalb müssen Verstärker, sog. Repeater, eingesetzt werden, um über größere Entfernungen Signale übertragen zu können.

Nebensprechen tritt vor allem bei Parallelleitern (Twisted Pair) auf. Hierunter versteht man den Übergang eines Teils der Signalenergie von einem Leiterpaar auf ein anderes. Besonders im Vollduplex-Betrieb und in Leitungsbündeln an Netzsternpunkten tritt Nebensprechen verstärkt auf. Beim gleichzeitigen Senden in beide Richtungen im Vollduplex-Betrieb unterscheidet man Nah- und Fernnebensprechen (Near End Crosstalk, NEXT und Far End Crosstalk, FEXT). Bei NEXT geht die Energie vom Transmitter in den Receiver derselben Station über. Bei FEXT geht die Energie vom Transmitter der ersten Station an den Transmitter der zweiten Station und gelangt auf diesem Weg zum falschen Receiver.

Nebensprechen kann durch enge Verdrillung und gute Abschirmung reduziert werden. Darüberhinaus werden in High-Speed-Netzen digitale Signalprozessoren (DSP's) eingesetzt, um die Informationen aus dem überlagerten Empfangssignal zu gewinnen.



Eine weitere Möglichkeit zur Reduzierung des Nebensprechens ist das Verfahren Time-Compression-Multiplexing, bei dem beide Seiten nicht gleichzeitig, sondern in kurzen Abständen zeitversetzt senden.

Lichtwellenleiter (LWL), auch optischen Fasern (Optical Fibre) genannt, sind sehr dünne Fasern, die meist aus Glas machmal auch Kunststoff bestehen. Vorteile von LWL sind u.a.:

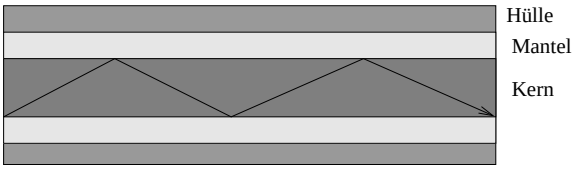
- große Bandbreite,
- große Reichweite,
- niedrige Fehlerrate,
- elektromagnetische Verträglichkeit,
- Sicherheit.

Die Bandbreite von LWL wuchs von 45 MBit/s Ende der 70'er Jahre auf 20 GBit/s Ende der 90'er Jahre. Die meisten Installationen arbeiten heute mit 2,5 GBit/s. (Ein TV-Signal benötigt größenordnungmäßig 10 MBit/s, d.h. bei dieser Bandbreite können 250 TV-Kanäle parallel über den LWL übertragen werden.) Licht ist nahezu immun gegen elektromagnetische Felder und strahlt fast keine Energie

in die Umgebung ab. Außerdem ist es schwierig, Singnalel aus einem LWL abzuhören, da sich dies in einem deutlichen Signalabfall äußert. Es gibt sogar Geräte, mit denen man die Eingriffsstelle orten kann.

Trotz der Fortschritte bei der Technik der Kupferleitungen, sind LWL bei Kommunikation mit hohen Bandbreiten, hoher Sicherheit und niedriger Fehlerrate unschlagbar. Zwar sind die Glasfaserkabel im Preis-Leistungs-Vergleich zu Kupferkabeln nicht zu teuer, aber die Sende- und Empfangseinrichtungen schlagen kostenmäßig stärker zu Buche.

Ein LWL besteht aus drei Schichten, einem Kern, einem Mantel und einer Schutzhülle. Der Kern leitet das Lichtsignal. Diese Faser umgibt ein Mantel mit kleinerem Brechungsindex, wodurch die Strahlen an der Grenzschicht vom Kern zum Mantel durch Totalreflexion im Kern bleiben. Die Schutzhülle umgibt den Mantel vor allem, um das Kabel vor Biegedefekten zu schützen.



Lichtwellenleiter mit Totalreflexion

Als Kenngröße wird der Durchmesser der Kernfaser und der Durchmesser des Mantels in der Form d_1/d_2 z.B. $85/125\ \mu m$ angegeben. Die Dämpfung in Silizium Fasern hat typischerweise einen Wert von $0,2\ dB/km$ bei $1550\ nm$und $0,35\ dB/km$ bei $1310\ nm$ Wellenlänge. Sie stellt i.d.R. also ein geringeres Problem als die sog. Dispersion dar. Hierbei ist die Ausbreitungsgeschwindigkeit im Medium von der Wellenlänge des Lichtsignals abhängig. Es kommt zur Verbreiterung der optischen Impulse und hiermit durch Interferenz zu einer höheren Bitfehlerrate. Die Dispersion ist jedoch in bestimmten Wellenlängenbereichen gering, so dass sie vernachlässigt oder rückgängig gemacht werden kann. Gebräuchlich sind folgende LWL-Normen:

G.652: Dispersion-unshifted Fibre mit minimaler Dispersion im $1310nm$-Fenster,

G.653: Dispersion-shifted Fibre mit rückgängig machbarer Dispersion im $1550nm$-Fenster.

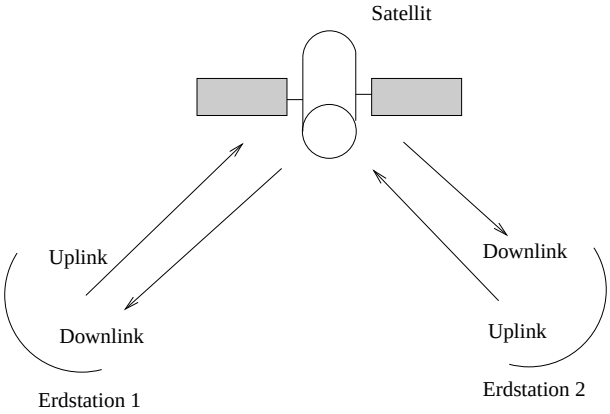
Weiterhin unterscheidet man zwischen Multimodefasern mit mehreren 100 diskreten Wellen und Monomodefasern mit nur einer ausbreitungsfähigen Welle. Während die Wellenausbreitung in Multimodefasern aufgrund der Totalreflexion an der Grenzschicht zum Mantel der Faser beruht, erfolgt die Wellenausbreitung

in Monomodefasern i.w. geradlinig entlang der Faserachse. Dispersion spielt bei Monomodefasern kaum eine Rolle. Allerding muss der Kerndurchmesser in der Größe der Wellenlänge des Lichts liegen, z.B. $6 - 7\ \mu m$ bei $1300\ nm$ Wellenlänge. Die Einspeisung der Sendeleistung kann bei Monomodefasern nur mit teureren Laserdioden nicht mit billigeren LED's wie bei Multimodefasern erfolgen.

Richtfunkstrecken und Satellitenverbindungen arbeiten im Mikrowellenbereich, d.h. grob zwischen 1 und 100 GHz. Beiden Übertragungsarten ist gemeinsam, dass sie einfach abgehört werden können. Daher müssen geheimzuhaltende Informationen verschlüsselt übermittelt werden.

Richtfunkstrecken sind relativ teuer, da man viele terrestrische Antennen und Sender (Relais-Stationen) bedingt durch Erdkrümmung, Berge und Bebauung benötigt. (Mikrowellen breiten sich geradlinig ähnlich wie Lichtstrahlen aus.) Weiterhin stört atmosphärisches Rauschen die Mikrowellenübertragung. I.d.R. werden für Richtfunkstrecken Frequenzen zwischen 2 und 40 GHz mit Übertragungsraten bis zu einigen 100 MBit/s verwendet.

Bei Kommunikations-Satelliten (es gibt weitere Satellitentypen, wie Wetter- oder Aufklärungs-Satelliten) wird der Satellit als Relais-Station meist auf einer geostationären Umlaufbahn (36000 km) zwischen zwei Erdstationen verwendet.



Satelliten nutzen das sog. Radiofenster als Frequenzbereich zur Übertragung, das zwischen 1-10 GHz liegt. Das Radiofenster ist von unten durch kosmisches Rauschen und von oben durch atmosphärisches Rauschen begrenzt. Zur Zeit werden über Satelliten Breitbandübertragungen von 155 MBit/s durchgeführt. Das Hauptproblem der Signalübertragung durch Satelliten liegt in der hohen Laufzeitverzögerung von etwa 0,25 s durch die Strecke von 72000 km. Diese Verzögerungen sollen in Zukunft verstärkt durch Satelliten mit niedrigeren Umlaufbahnen verkürzt werden, die dann natürlich nicht geostationär sein können. Auf diese Weise sollen auch interaktive Kommunikationen verbessert durch Satelliten übertragen werden können. Man unterscheidet drei Typen von Satelliten:

- GEO: Geostationary Earth Orbit,
- MEO: Medium Earth Orbit,
- LEO: Low Earth Orbit.

2.3 Übertragungstechnik

2.3.1 Kodierung

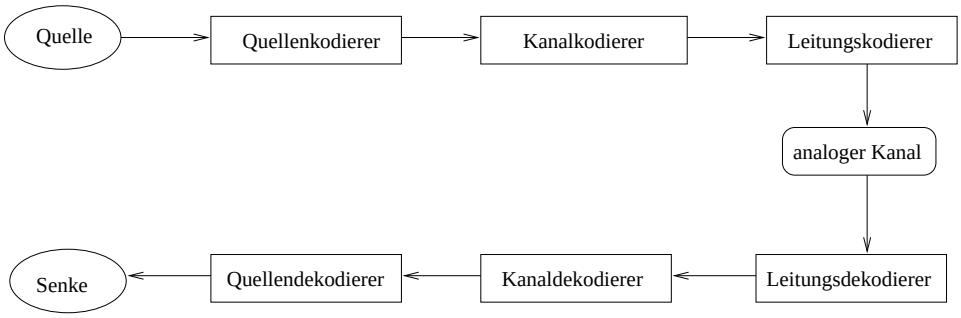
Ein Kode ist eine Vorschrift zur Darstellung von Informationen. Ziel der Kodierung ist, mit möglichst hoher Geschwindigkeit möglichst störsicher Informationen über einen gestörten Kanal zu übertragen. Man unterscheidet Quellen-, Kanal- und Leitungskodierung.

Ziel der Quellenkodierung ist eine möglichst geringe mittlere Anzahl zu übertragender Zeichen zu erreichen. Ein Beispiel für eine solche Kodierung ist der Morsecode, bei dem häufig auftretende Zeichen durch möglichst kurze Signalfolgen kodiert werden. Für die Quellenkodierung gibt es eine entscheidende Erkenntnis, die im Satz von Shannon über die Entropie der Quelle zum Ausdruck kommt. Dabei ist die Entropie definiert als der mittlere Informationsgehalt eines Zeichens der Quelle: $H(x) = -\sum p_i * log_2 p_i \; bit$, wobei $p_1, p_2, \ldots, p_n$ die Auftretenswahrscheinlichkeiten der Zeichen $1, 2, \ldots, n$ und $-log_2 p_i \; bit$ der Informationsgehalt des Zeichens i ist. (Der Informationsgehalt eines Zeichens ist umso höher, je geringer seine Wahrscheinlichkeit ist.)

Ziel der Kanalkodierung ist, gezielte Redundanz für fehlererkennende und fehlerkorrigierende Codes in den Code einzubauen. Hierbei wird die Gesamtmenge möglicher Codeworte in zugelassene und nicht zugelassene (falsche) unterteilt, so dass die Verfälschung eines Codewortes erkannt werden kann. Neben Linearcodes wie Parity Check, Blocksicherung, Blockkodierung und gleichgewichtige Codes, gibt es zyklische Codes, bei denen die Kodierung und Prüfung durch Schieberegister und XOR-Schaltungen (XOR = logische Exclusiv Or Funktion) erfolgen kann.

Ziel der Leitungskodierung ist es, das digitale Signal in ein möglichst einfaches störsicheres analoges Signal zur Übertragung über das Medium zu kodieren.

Beim Sender folgt der Quellenkodierung die Kanalkodierung und der Kanalkodierung die Leitungskodierung. Beim Empfänger erfolgt die Dekodierung in umgekehrter Reihenfolge.



Die entscheidende Definition zur Fehlererkennung und Fehlerkorrektur bei der Kanalkodierung ist die sog. Hamming-Distanz. Die Hamming-Distanz ist wie folgt definiert:

Die Hamming-Distanz d zwischen je zwei Codeworten ist die Anzahl unterschiedlicher Bits der Codeworte.

Die Hamming-Distanz d eines Codes ist der Mindestabstand zwischen je zwei Codeworten eines Codes.

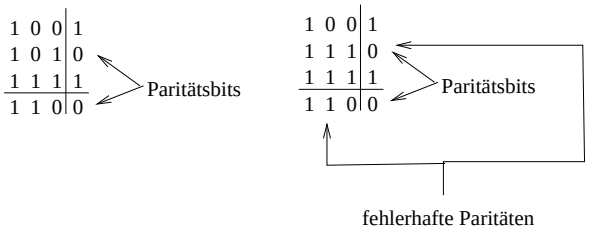
Das einfachste Verfahren der Kanalkodierung ist die mehrfache Übertragung von Zeichen. Eine 2-fache Übertragung ist fehlererkennend mit einer Redundanz von 50%. Die Redundanz ist wie folgt definiert: $R = \frac{n-i}{n}$, wobei n die Gesamtzahl der Bits und i die Anzahl informationstragender Bits ist. Die 3-fache Übertragung hat eine Redundanz von $66,7\%$, wobei der Code durch das Verhältnis $2:1$ fehlerkorrigierend sein kann.

Erwartungsgemäß ist die Redundanz der mehrfach-Übertragungen hoch. Der meist bekannte Parity-Check-Code erkennt z.B. einen Fehler pro Zeichen durch ein Prüfbit Redundanz, so dass die Summe der 1-sen eines Zeichens gerade oder ungerade ist (gerade oder ungerade Parität). Dazu ist z.B. bei 6-Bit Worten eine Redundanz von $16,7\%$ notwendig.

Bei gleichgewichtigen Codes der Länge n mit Gewicht w werden von den n Stellen pro Zeichen genau w Stellen mit einer 1 besetzt. Der Fernschreibcode ist 7-stellig mit Gewicht 3. Es gibt also $\left(\begin{array}{c} 7 \\ 3 \end{array} \right) = \frac{7*6*5}{3*2} = 35$ verschiedene Codeworte. Die Redundanz berechnet sich also zu $R = \frac{7-log_2 35}{7} = 26,7\%$. Worte mit einem Gewicht ungleich w sind bei gleichgewichtigen Codes fehlerhaft.

Die Blocksicherung ist eine Kombination aus Längs- und Querparität, wobei man mehrere Codeworte in einer Matrix anordnet. Einfache Fehler können in einem Block korrigiert werden. Doppelte Fehler können jedoch nicht korrigiert werden, wenn sie in einer Zeile oder Spalte liegen, da dann die Zeilen- oder

Spaltenparität richtig bleibt und damit die falschen Stellen nicht geortet werden können.



Die Redundanz bei einem Blocksicherungsverfahren mit $n * n$ -Blöcken ist $R = \frac{n^2-(n-1)^2}{n^2} = \frac{2n-1}{n^2}$, z.B. bei $n = 4$: $R = \frac{7}{16} = 43,7\%$.

Bei den Hamming-Codes (Blockkodierung) wird ebenfalls eine Parität zur Überprüfung von Übertragungsfehlern benutzt. Dabei wird ein Vektor $(x_{k+1}, ..., x_{k+p})$ aus mehreren Paritätsbits durch Multiplikation eines Vektors der Informationsbits $(x_1, ..., x_k)$ mit einer Paritätsmatrix berechnet:

$$(x_{k+1}, ..., x_{k+p}) = (x_1, ..., x_k) * \begin{pmatrix} g_{11} & \cdots & g_{1p} \\ \cdots & \cdots & \cdots \\ g_{k1} & \cdots & g_{kp} \end{pmatrix}$$

Beim Empfänger werden alle Bits mit einer um eine $p * p$-Einheitsmatrix vergrößerten Paritätsmatrix multipliziert. Dabei werden die übertragenen Paritätsbits auf die errechneten addiert. Es ergibt sich ein Resultatvektor, bei dem bei fehlerfreier Übertragung sämtliche Stellen 0 sind. Wie man leicht sieht, ist der Resultatvektor bei einem Fehler an der Stelle x_i gleich den Werten der $i-$ten Zeile $(g_{i1}, ..., g_{ip})$ der Paritätsmatrix. Wenn alle Zeilen der Paritätsmatrix verschieden sind, kann ein solcher Fehler also korrigiert werden. Ist die Paritätsmatrix linear unabhängig, so können sogar alle Mehrfachfehler erkannt werden:

$$(x_1, ..., x_k, x_{k+1}, ..., x_{k+p}) * \begin{pmatrix} g_{11} & \cdots & g_{1p} \\ \cdots & \cdots & \cdots \\ g_{k1} & \cdots & g_{kp} \\ 1 & 0 & \cdots \\ 0 & 1 & \\ \cdots & \cdots & \cdots \\ 0 & \cdots & 1 \end{pmatrix} =$$

$$= \begin{cases} 0 \, kein \, Fehler \\ (g_{i1}, ..., g_{ip}) \, Fehler \, an \, Stelle \; i \\ a \neq 0 \, Fehler \end{cases}$$

Die minimale Anzahl Paritätsbits, um einfache Fehler korrigieren zu können, ergibt sich aus der Bedingung $k + p \leq 2^p$, da es 2^p verschiedene Paritätszeilen gibt. Für $k = 4$ ergibt sich $p = 3$ als niedrigste Anzahl Paritätsbits für die einfache Fehlerkorrektur.

Der bekannteste zyklische Code, der z.B. im Ethernet-Übertragungsprotokoll verwendet wird, ist der Cyclic Redundancy Check (CRC). Die Idee des CRC ist, aus einer zu übertragenden Informationsfolge I eine Folge T zu machen, die durch eine fest vordefinierte Folge G teilbar ist. Nachdem T übertragen wurde, wird die empfangene Folge $T\prime$ wieder durch G geteilt. Entsteht dabei ein Rest $R \neq 0$, so ist ein Übertragungsfehler passiert.

Im CRC-Verfahren werden Generatorpolynome $G(x)$ verwendet. Gängige Generatorpolynome sind:

CRC-16: $x^{16} + x^{15} + x^2 + 1$

CRC-CCITT: $x^{16} + x^{12} + x^5 + 1$

CRC-32: $x^{32} + x^{25} + x^{22} + x^{16} + x^{12} + x^{11} + x^{10} + x^8 + x^7 + x^5 + x^4 + x^2 + x + 1$

CRC-32 wird z.B. bei Ethernet verwendet. Das CRC-Verfahren arbeitet wie folgt:

1. An die Nutzinformation werden k 0-Bits angehängt, wenn G den Grad k hat. Es entsteht dadurch $x^k * I(x)$ mit dem Polynom $I(x)$ mit Koeffizienten aus den Bitstellen von I, z.B: $I = 10010000$ergibt $I(x) = x^7 + x^4$.

2. $x^k I(x)$ wird durch $G(x)$ dividiert. Es entsteht das Restpolynom $R(x)$, das höchstens vom Grad $k - 1$ ist. Die Koeffizienten von $R(x)$ belegen also höchstens k Bits.

3. Nun werden die Koeffizienten von $R(x)$ anstelle der k 0-Bits an die Nutzinformation angehangen. Es entsteht das Polynom $x^k * I(x) + R(x)$. Da Addition, Subtraktion und exklusives Oder in der Boole'schen Algebra dasselbe bewirken, ist dies auch gleich dem Polynom $x^k * I(x) - R(x)$, das durch $G(x)$ teilbar ist.

4. Wenn bei der Übertragung ein Fehler passiert, entspricht dies der Übertragung eines Fehlerpolynoms $E(x) : T\prime(x) = T(x) + E(x)$. Ein solcher Fehler wird nun nur dann nicht erkannt, wenn $E(x)$ ein Vielfaches von $G(x)$ ist. Damit ist klar, dass alle Mehrfachfehler mit höchstens sovielen Fehlerstellen erkannt werden, wie der Grad von $G(x)$ angibt.

Für die CRC-Codes ergibt sich:

CRC-16: erkennt alle Fehler mit einer Bitanzahl von höchstens 16 Stellen und 99,997% aller längeren Fehler,

CRC-32: erkennt alle Fehler mit einer Bitanzahl von höchstens 32 Stellen und 99,99999995% aller längeren Fehler.

Zusammenfassend kann größenordnungsmäßig die Reduzierung von Fehlern um folgende Faktoren durch verschiedene Codes festgehalten werden:

- 10 Parity-Check-Code,
- 10^3 Blocksicherung,
- 10^5 Blockkodierung,
- $10^5 - 10^{10}$ Zyklische Blocksicherung (CRC).

2.3.2 Basisband- und Breitbandübertragung

Bei der Basisbandübertragung werden Signale des Leitungscode ohne weitere Umformung über die Leitung übertragen. Eine Leitung wird deshalb meist nur durch einen Übertragungskanal genutzt. Mehrere Informationsströme können jedoch auch im Zeitmultiplex-Verfahren (Time Division Multiplexing, TDM) im Basisband übertragen werden.

Basisbandnetze haben folgende Kennzeichen:

- relativ wenig Kosten,
- leicht handhab- und erweiterbar,
- beschränkte Bandbreite (i.a. höchstens 1 GBit/s),
- weniger gute Auslastung der Übertragungsleitungen,
- geringe überbrückbare Entfernungen.

Für die Basisbandübertragung gibt es verschiedene Leitungscodes. Als Codeelement bezeichnet man die kleinste übertragbare Einheit. Das Codeelement ist meist 1 Bit könnte aber auch ein Signal mit 3 oder mehr Zuständen sein. Man spricht z.B. von binärem, ternärem, quaternärem Code. Für die Übertragung eines Codeelements wird nun die Zeit T benötigt. Dann definiert man die Schrittgeschwindigkeit $v_T = 1/T\, Baud$. Die Übertragungsgeschwindigkeit in Bit/s ergibt sich als $v_U = v_T * log_2 n$, wenn das Codeelement n verschiedene Zustände annehmen kann.

Mehrere Codeelemente können zu einem Codewort zusammengefasst werden. Bei ISDN wird z.B. auf dem Teilnehmeranschluss die sog. 4BT3-Code verwendet. Hierbei werden 4 Bit in 3 ternären Codeelementen kodiert ($2^4 = 16$ Zustände sind in $3^3 = 27$ Zuständen kodierbar). Da die Übertragungsgeschwindigkeit v_U mit der Anzahl der Zustände des Codeelements wächst, könnte man nun meinen,

die Übertragungsgeschwindigkeit durch mehr Zustände des Codeelements ohne großen Aufwand steigern zu können. Leider werden aber die Anforderungen an Sender, Empfänger und Medium durch Dämpfung, Rauschen usw. für mehr als 3 Zustände rasch sehr hoch. Deshalb werden meist binäre oder ternäre Codeelemente verwendet, die sich leicht in Signale umsetzen lassen, z.B. binär : U_L, U_H ternär: $-U_H, 0, +U_H$.

Weitere Anforderungen an Leitungscodes im Basisband sind Gleichstromfreiheit und die Möglichkeit der Taktrückgewinnung aus dem übertragenen Signal. Auf der Senderseite werden die Codeelemente mit einem bestimmten Takt erzeugt, der zur Erkennung der Codeelemente auch auf der Empfängerseite vorhanden sein muss. Anstatt den Takt über eine eigene Leitung separat zu übertragen, kann er auch durch einen geeigneten Leitungscode implizit übertragen werden.

Verschiedenen Leitungscodes und ihre Vorschriften sind:

NRZ-Code (Non Return to Zero): $0 \leftrightarrow U_L,\ 1 \leftrightarrow U_H$. Dieser Code ist nicht gleichstromfrei und ermöglicht keine Taktrückgewinnung.

RZ-Code (Return to Zero): $0 \leftrightarrow U_L,\ 1 \leftrightarrow U_H \rightarrow U_L\ nach\ T/2$. Dieser Code ist nicht gleichstromfrei und nicht selbsttaktend (0-Folgen übertragen den Takt nicht, 1-Folgen wohl).

AMI-Code (Alternate Mark Inversion): $0 \leftrightarrow 0, 1 \leftrightarrow U_H bzw. -U_H alternierend.$ Es gibt also drei Signalzustände für ein binäres Codeelement. Der Code ist gleichstromfrei aber nicht selbsttaktend (0-Folgen übertragen den Takt nicht, 1-Folgen wohl).

Manchester-Code : $0 \leftrightarrow -U_H \rightarrow +U_H nach T/2, 1 \leftrightarrow +U_H \rightarrow -U_H nach T/2.$ Dieser Code ist gleichstromfrei und selbsttaktend. Für die Übertragung ist allerdings die doppelte Bandbreite erforderlich im Bezug zur Schrittgeschwindigkeit, in der Codeelemente übertragen werden. Der Manchester-Code wird für Ethernet verwendet, wobei im CSMA/CD-Verfahren anhand der Pegelwerte bei $0,75T$ und $1,25T$ ermittelt wird, ob der Kanal von einem anderen Teilnehmer belegt ist (dazu später mehr.)

Während Basisbandübertragung die Bandbreite des Übertragungsmediums meist nur geringfügig nutzt, kann die Bandbreite bei der Breitbandübertragung vollständiger genutzt werden. Ein Beispiel ist ein Koaxialkabel mit einer Bandbreite von $450MHz$, bei dem ein TV-Signal mit $6MHz$ Bandbreite genauso von $100 - 106MHz$ wie von $400 - 406MHz$ übertragen werden kann. Durch Breitbandübertragung können also mehrere Kanäle gleichzeitig in verschiedenen Frequenzbereichen übertragen werden. Die Technik der Breitbandübertragung heißt

Modulation; sie wird z.B. zur Übertragung digitaler Informationen über eine Telefonleitung (Twisted Pair) mit Hilfe sog. Modems (Modulator/Demodulator) verwendet.

2.3.3 Modulation

Unter Modulation versteht man die Steuerung von Parametern eines Modulationsträgersignals durch ein Basisbandsignal (Informationssignal). Die Veränderung des Trägersignals kann angepasst auf die physikalische Leitung geschehen, z.B. um einen bestimmten Frequenzbereich zu nutzen. Mathematisch kann die Modulation wie folgt erklärt werden: Das Trägersignal $S(t) = A * \cos(2\pi f t + \varphi)$ wird in der Amplitude A, Frequenz f oder Phase φ verändert. Neben Amplituden-, Frequenz- und Phasenmodulation gibt es Kombinationsverfahren wie die Quadraturamplitudenmodulation (QAM). QAM ist eine Kombination von Amplituden- und Phasenmodulation. Neben Einträgermodulation gibt es auch Mehrträgermodulation, mit der es möglich ist, einen Kanal in mehrere Unterkanäle für die Mehrfachübertragung zu unterteilen. Bei binären Informationssignalen wechseln die Parameter des Trägers zwischen zwei möglichen Werten. Die bekanntesten Modulationsverfahren sind:

Amplitudenmodulation (Amplitude Shift Keying, ASK) auch harte Tastung genannt.

Frequenzmodulation (Frequency Modulation, FM):

Beim Signalwechsel erfolgt kein Phasensprung. Findet der Frequenzwechsel beim Nulldurchgang statt, so spricht man von phasenkohärenter Frequenzmodulation.

Phasenmodulation (Phase Modulation, PM):

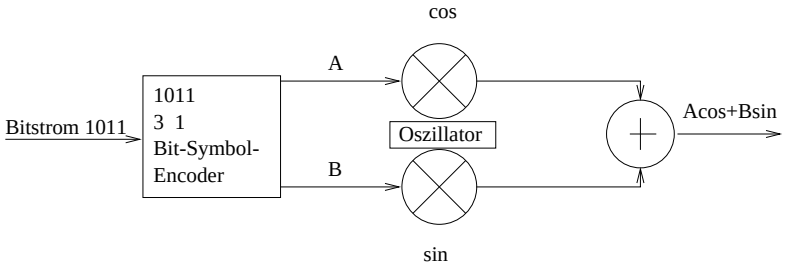
Bei der Phasenmodulation werden zwei phasenverschobene Träger (z.B. 180^0) übertragen.

Quadraturamplitudenmodulation (QAM):

QAM ist ein Verfahren mit hoher Bandbreiteneffizienz und Rauschunempfindlichkeit. Es wird bei Übertragungstechniken wie ATM (Asynchronous Transfer Mode) und ADSL (Asymmetric Digital Subscriber Line) verwendet. Das QAM-Signal kann mehrere Amplitudenwerte übertragen, z.B. 2B1Q (Two Binaries, One Quaternary), wobei mehrere Bits durch einen Amplitudenwert kodiert werden.

Erstes Bit	Zweites Bit	Quaternäres Symbol	Spannung in Volt
1	0	+3	+2,50
1	1	+1	+0,83
0	1	-1	-0,83
0	0	-3	-2,50

Neben der Amplitude wird bei QAM zusätzlich die Phase zur Modulation eingesetzt. Genau genommen, wird ein zweiter um 90^0 versetzter Träger eingerichtet. QAM ist also ein Mehrträgermodulationsverfahren. Wegen des um 90^0 versetzten Trägers wurde der Namenspräfix Quadratur gewählt. Der Kodierer bildet aus dem Eingangsstrom Bitgruppen und verteilt diese Gruppen auf die orthogonalen Träger mit halber Bitgruppenfrequenz. Anschließend werden die modulierten Träger aufsummiert.



Pulscodemodulation (Pulse Code Modulation, PCM):

PCM hat ihren Ursprung in der digitalen Telefonie. Hierbei wird ein wert- und zeitkontinuierliches Signal in eine binäre Impulsfolge umgewandelt, die dann übertragen wird. PCM arbeitet in drei Stufen:

1. Abtastung: Das Quellsignal wird in äquidistanten Zeitabständen abgetastet, d.h. das zeitkontinuierliche Signal wird in ein zeitdiskretes umgewandelt. Das Abtasttheorem von Shannon besagt, dass ein Tiefpasssignal mit Grenzfrequenz f_g nach Abtastung mit einer Rate $r = 1/T \geq 2f_g$ durch einen Tiefpass mit Grenzfrequenz f_g exakt zurückgewonnen werden kann. Die Abtastung entspricht einer Wiederholung des endlichen Signalspektrums im Abstand $r = 1/T$. Real wird leichte Überabtastung gewählt, z.B. wird ein Telefonsignal mit $3,4\ KHz$ Bandbreite mit $8\ KHz$ abgetastet.

2. Quantisierung: Durch Quantisierung wird ein wertkontinuierliches Signal in ein wertdiskretes Signal umgewandelt. Hierbei entsteht ein Quantisierungsfehler, der sog. Quantisierungsrauschen verursacht. Man kann zeigen, dass

das Verhältnis von Nutz- zu Störleistung durch Quantisierung bei 2^k Stufen $k * 6\,dB$ beträgt (Faktor 4): $\frac{S_{Nutz}}{S_{Stoer}} = 2^{2k} = 4^k \longrightarrow 10lg4^k\,dB = k * 6\,dB$. Hinreichend für unser Gehör sind z.B. $7 - 8$ Bit Quantisierung, um das Quantisierungsrauschen nicht mehr wahrzunehmen ($48\,dbS/N - Abstand$). Die Dynamik bei k-Bit-Quantisierung liegt ebenfalls bei $D = k * 6\,dB$ (logarithmisches Verhältnis vom lautesten zum leisesten Ton $D = 20 * lg((2^k * \Delta)/\Delta) \approx k * 6\,dB$). Wird z.B. ein Telefonsignal mit $3,4\,KHz$ Bandbreite mit $8KHZ$ abgetastet und mit 8-Bit quantisiert, so wird für die Übertragung ein Kanal für $64\,KBit/s$ benötigt.

3. Kodierung: Das quantisierte Signal wird für die Übertragung kodiert, z.B. bei ISDN durch die 4BT3-Kodierung.

2.3.4 Übertragungsarten

Die Übertragungsart definiert, wie einzelne Bits oder Bitgruppen von einem Gerät zum anderen transportiert werden. Man unterscheidet:

Serielle und parallele Übertragung:

Bei serieller Übertragung wird nur eine Leitung verwendet. Dies ist besonders bei größeren Entfernungen angebracht. Bei paralleler Übertragung wird eine Bitgruppe gleichzeitig über mehrere Leitungen übertragen. Wegen der höheren Kosten und unterschiedlichen Signallaufzeiten auf den einzelnen Leitungen wird parallele Übertragung nicht bei größeren Entfernungen eingesetzt. Bei Kopplungenmit geringen Entfernungen, z.B. CPU-Speicher (Bus) oder Rechner-Drucker (parallele Schnittstelle) wird meist parallel übertragen. Das HIPPI-LAN (High Performance Parallel Interface) ist ein Beispiel für ein LAN mit paralleler Übertragung.

Synchrone und asynchrone Übertragung:

Bei asynchroner Übertragung arbeiten Sender und Empfänger zeitentkoppelt. Der Sender kann Bits zu beliebigen Zeitpunkten übertragen; der Empfänger weiß nie, wann sie eintreffen. Um keine Informationsbits zu verlieren, wird einer kleinen Gruppe von Bits ein Startbit vorangeschickt, mit dessen Hilfe der Empfänger sich für den Empfang initialisiert. Das Ende einer Bitgruppe wird durch ein Stopbit angezeigt.

Im Gegensatz zur asynchronen Übertragung arbeiten Sender und Empfänger bei der synchronen Übertragung mit einem gemeinsamen Takt. Die Bits werden zu größeren Gruppen, sog. Frames, zusammengefasst. Am Anfrang eines Frames steht ein Synchronisationsfeld SYN ähnlich dem Startbit. Der gemeinsame Takt kann z.B. über das Trägersignal übermittelt werden. Synchrone Übertragung ist i.a. schneller als asynchrone, da der Empfänger nicht für kleine Bitgruppen stoppt.

Simplex-, Halbduplex-, Vollduplex-Übertragung:

Bei Simplex-Übertragung fließt die Information zeitunabhängig in eine Richtung. Bei Halbduplex fließt sie alternierend in beide Richtungen. Bei Vollduplex können Informationen zeitgleich in beide Richtungen fließen. Vollduplex benutzt im Gegensatz zu Halbduplex und Simplex i.d.R. getrennte Medien für beide Übertragungsrichtungen. Vollduplex wird z.B. in LAN's hauptsächlich eingesetzt, Halbduplex z.B. bei Modems über ein 2-Draht-Twisted-Pair.

2.4 Topologien

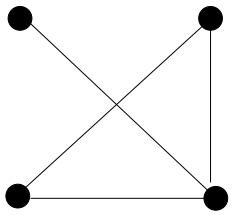
Man unterscheidet zwischen physischer und logischer Topologie. Manche Geräte sind physisch nicht direkt miteinander verbunden; sie müssen logisch jedoch direkt, d.h. transparent über andere Geräte miteinander verbunden werden. Andere Geräte, die unmittelbar oder mittelbar miteinander verbunden sind, dürfen z.B. logisch nur unter bestimmten Bedingungen verbindbar sein. Der Netzmanager muss eine solche Verbindung explizit gestatten und verbieten. Immer wenn Zwischenstationen an einer Sendung beteiligt sind, müssen folgende Arbeiten, die man als Routing bezeichnet, geleistet werden:

- Feststellung des Ziels,
- Ermittlung des Wegs zum Ziel,
- Weiterleitung der Sendung auf dem Weg zum Ziel.

Im Gegensatz zu globalen Netzen weisen lokale Netze eine einfache und regelmäßige Struktur auf. Die wichtigsten lokalen Netze sind:

Punkt-zu-Punkt-Topologien:

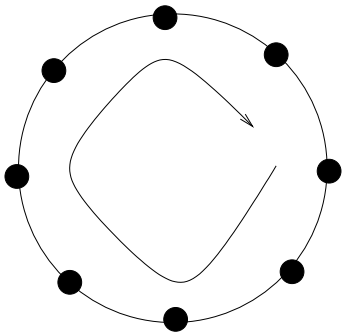
Beim Maschennetz gibt es zwischen je zwei Endpunkten eine direkte Verbindung. Daher ist eine sehr schnelle Kommunikation zwischen Host's möglich. Darüberhinaus können einzelne Verbindungen an betreffende Geräte angepasst werden. Aufgrund der hohen Leitungsanzahl von $N * (N - 1)$ Leitungen bei N Endgeräten wird jedoch meist nur eine teilweise Vermaschung durchgeführt. Nicht direkt verbundene Endgeräte kommunizieren dann über ein Routingverfahren über Zwischenstationen. Bei teilweiser Vermaschung sind also Routing und Verkehrsmanagement erforderlich, wobei es zu keiner Über- und Unterlastung der Betriebsmittel des Netzes kommen soll.



Teilweise vermaschtes Netz

Ring:

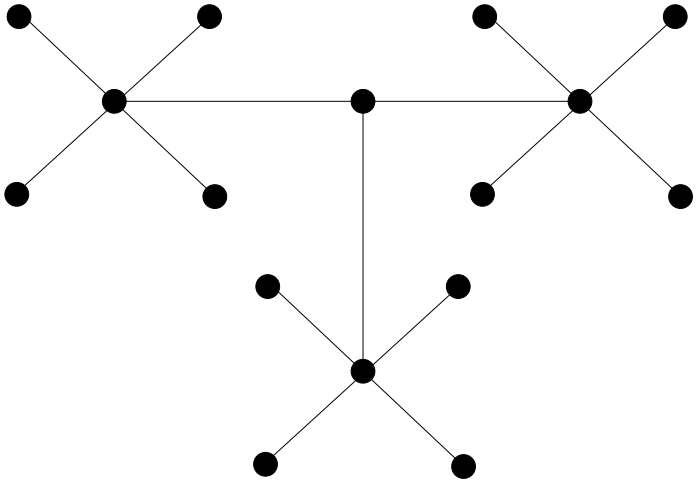
In einem ringförmigen Netz verläuft der Datenaustausch meist nur in einer Richtung. Die Kommunikation geschieht i.d.R. über mehrere Zwischenstationen nach dem Store-and-Forward-Verfahren, d.h. jede Zwischenstation speichert eine empfangene Sendung ab, bevor sie sie weitersendet. Ein Ring kommt mit wenigen Leitungen aus: $N - 1$ bei N Stationen. Andererseits reagiert er bei Störungen, wie dem Ausfall einer Leitung, empfindlich. Ein solcher Ausfall kann den gesamten Ring lahmlegen. Deshalb werden die Leitungen zwischen zwei Stationen häufig doppelt realisiert.



Ring mit Übertragungsrichtung

Stern:

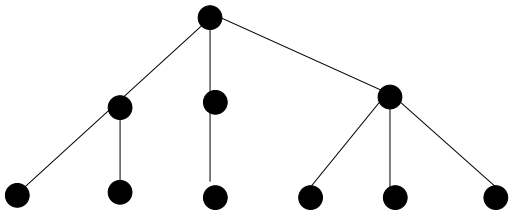
In einem sternförmigen Netz laufen alle auszutauschenden Daten über einen zentralen Schalterknoten, der als einziger Store-and-Forward-Fähigkeit besitzt. Diese Zentrale muss eine hohe Verfügbarkeit aufweisen, da sie das Funktionieren oder auch Nicht-Funktionieren des Netzes bestimmt. In der Praxis werden Sterne oft hierarchisch miteinander verbunden. Der zentrale Vermittlungsknoten eines Bereichs ist dann wiederum sternförmig mit weiteren Zentralen verbunden. Das Telefonnetz ist der bekannteste Vertreter eines Netzes mit Sterntopologie. Der Zentralknoten des Sterns hat eher eine Vermittlungs- als eine Routing-Aufgabe.



Sternnetz

Baum:

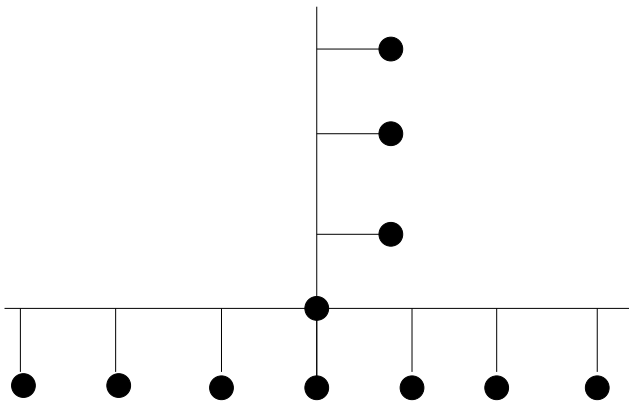
Eine Baumtopologie wird häufig bei Anwendungen eingesetzt, die hierarchisch sind, wie einer Firma mit ihren Abteilungen. Der Ausfall einer Verbindung bewirkt das Abkoppeln eines Teilbaums vom übrigen Netz. Jedoch bleiben der Teilbaum und der restliche Baum funktionsfähig. Die Anzahl der Leitungen eines Baums mit N Endknoten liegt in der Grösenordnung $O(N)$. Da es von jedem Baumknoten zu jedem anderen genau einen Weg gibt, können alle Routing-Informationen in der Adresse eines Knotens verzeichnet sein. Bäume werden bei WAN's und bei LAN's verwendet, die über Brücken (Bridges) miteinander verbunden sind.



Baum

Bus- oder Broadcast-Topologie:

Bei einem Bussystem steht allen Stationen ein gemeinsames globales Übertragungsmedium zur Verfügung. Gesendete Daten können prinzipiell von allen angeschlossenen Stationen empfangen werden. Die Nutzung des Bus muss bei mehreren Sendern durch geeignete Vereinbarungen (Protokolle) geregelt werden. Den Vorteilen der sehr einfachen Erweiterbarkeit und der Unempfindlichkeit gegen den Ausfall von Host's steht der Nachteil des Totalausfalls beim Zusammenbruch des Busmediums gegenüber. Durch Zusammenschaltung mehrerer Busse mit Store-and-Forward-Knoten entstehen sog. T-Netze.



T-Netz mit zwei Bus-Topologien

Physikalisch lassen sich alle Topologien mit verschiedenen Kabeltypen realisieren. Üblicherweise werden mehrere Kanäle über ein physikalisches Medium durch Multiplexer gleichzeitig realisiert. Bekannteste Multiplexverfahren sind das Frequenzmultiplex bei Breitbandnetzen und das Zeitmultiplex bei Basisbandnetzen.

2.5 Multiplexing und Vermittlung

Unter Multiplexing versteht man die Mehrfachausnutzung einer physikalischen Verbindung durch mehrere logische Kanäle. Multiplexing nutzt die Tatsache, dass die benötigte Bandbreite einzelner Dienste kleiner als die des Übertragungsmediums ist. Man unterscheidet folgende wichtige Multiplex-Varianten:

Frequenzmultiplex (Frequency Division Multiplexing, FDM):

Hierbei werden durch unterschiedliche Trägerfrequenzen verschiedene Frequenzbänder aus dem gesamten Übertragungsbereich gebildet. Wegen Nebensprechen

und Rauschen muss ein Frequenzabstand zwischen den Subkanälen eingehalten werden. Hierdurch ist die genutzte Bandbreite kleiner als die zur Verfügung stehende Bandbreite des Mediums.

Zeitmultiplex (Time Division Multiplexing, TDM):

Beim Zeitmultiplex wird jedem Übertragungskanal die gesamte Bandbreite des Mediums zur Verfügung gestellt. Allerdings erhält jeder nur für einige μs das ganze Medium. Man stellt sich vor, dass die Zeitachse in konstante Zeitscheiben, sog. Slots, unterteilt ist. Die Dauer der Bedienung aller Kanäle wird als Cycle oder Frame bezeichnet. Um unterschiedliche Übertragungsraten zu erreichen, können einer Kommunikationsverbindung unterschiedlich viele Kanäle zugeordnet werden. Geschieht diese Zuordnung statisch, d.h. von Anfang bis zum Ende der Verbindung, so ist die Auslastung des Mediums schlechter als bei einer dynamischen Zuordnung der Kanäle, die pro Cycle neu geschieht. Dieses letztere Verfahren wird auch asynchrones TDM oder ATDM genannt. Bei ATDM kann die Übertragungsrate also in festen Einheiten variieren. Als Grundbitrate für TDM und ATDM werden meist $64 KBit/s$ gewählt.

Zeitkompressionsmultiplex (Time Compression Multiplexing, TCM):

Beim Zeitkompressionsmultiplex wird im Halbduplex-Verfahren zeitversetzt in beide Richtungen also bidirektional übertragen. Die Idee des Verfahrens ist hierbei, die Bits auf der Senderseite in einem Puffer zu sammeln und mit höherer Bitrate als vom Sender gefordert stoßweise in sog. Bursts zu übertragen (z.B. mit Faktor 2 bei 2 Kanälen). Die Verbindung erscheint hierdurch genauso schnell wie eine Vollduplex-Verbindung und es kann immer potentiell mit der vollen Bandbreite des Mediums gesendet werden. Für das Umschalten der Übertragungsrichtung und die Laufzeit des Signals wird eine gewisse Zeit benötigt, so dass die Datenrate natürlich hinter der des Mediums zurückbleibt.

Zeitkompressionsmultiplex

Statistisches Multiplex:

Beim statistischen Multiplex wird die Übertragungskapazität erst bei Bedarf den Kanälen zugeteilt. Hierdurch wird eine bessere Auslastung des Mediums als bei den meisten anderen Verfahren möglich. Die Daten aus den zu multiplexenden Kanälen werden an den Eingängen eines Multiplexers sehr kurz gepuffert. Dann fasst der Multiplexer sie zu einem Ausgabestrom zusammen und überträgt sie. Die Bandbreite wird durch die Datenmenge pro Abtastrunde bestimmt. Hierbei überschreitet die Summe der Spitzendatenraten die Übertragungskapazität des Mediums und die Gesamtdurchschnittsrate aller Kanäle ist niedriger als die Übertragungskapazität des Mediums. Wegen des Gesetzes der großen Zahlen, liegt die Summe der Bitraten aller Kanäle bei vielen Kanälen mit einer Wahrscheinlichkeit nahe 1 bei der Gesamtdurchschnittsdatenrate. Mit anderen Worten ist die Wahrscheinlichkeit gering, dass ihre momentane Datenrate die Übertragungskapazität des Mediums übersteigt, wenn die Kanäle zahlreich sind. Den statistischen Multiplex-Gewinn misst man als Verhältnis der Summe der Spitzendatenraten zur Übertragungsrate des Mediums. Das ATM-Verfahren arbeitet z.B. auf der Basis des statistischen Multiplex.

Wenn Informationen über Zwischenstationen in einem Netz zielgerichtet zum Empfänger weitergeleitet werden, so dass nur er die Informationen erhält, spricht man von Vermittlung (im Gegensatz zu Broadcast-Netzen). Traditionell werden drei Vermittlungstechniken eingesetzt:

Leitungsvermittlung (Circuit Switching): Sie hat sich vor allem in den Telefonnetzen etabliert.

Paketvermittlung (Packet Switching): Sie entstand mit der Datenkommunikation.

Nachrichtenvermittlung (Message Switching): Electronic Mail ist ein Beispiel für Nachrichtenvermittlung, wo komplette Nachrichten zwischen Netzknoten im Store-and-Forward-Modus transferiert werden.

Bei der Leitungsvermittlung verläuft die Kommunikation in drei Phasen:

1. Verbindungsaufbau,
2. Informationstransfer,
3. Verbindungsabbau.

Im Verbindungsaufbau wird ein Pfad zwischen Quelle und Ziel bestimmt und auf diesem Pfad die notwendigen Betriebsmittel exklusiv reserviert. Leitungsvermittlung bietet sich für Dienste mit konstanter Datenrate an, während die Effizienz bei variablen Datenraten eher schlecht ist. Beim Multi-Rate Circuit Switching

(MRCS) werden Vielfache einer Basisdatenrate, z.B. von $64\ KBit/s$, beim Verbindungsaufbau spezifiziert und mehrere Kanäle fest zugeteilt.

Bei der Nachrichtenvermittlung gibt es keine dedizierte Verbindung zwischen Sender und Empfänger. Stattdessen findet eine Vermittlung auf dem Store-and-Forward-Prinzip statt. Vorteile sind die gute Auslastung der Netzressourcen und die Zuverlässigkeit der Übertragung, da jeder Transitknoten eine Fehlerprüfung durchführt. Die variable Zwischenspeicherzeit der Nachricht kann sehr lang sein, so dass Nachrichtenvermittlung für den interaktiven Betrieb ungeeignet ist. Die Länge der Nachrichten wird nach oben begrenzt, da die Netzknoten sonst über zu hohe Speicherkapazitäten verfügen müssten.

Die Paketvermittlung wurde als effizienteres Verfahren für die Terminal-Host-Kommunikation als die Leitungsvermittlung entwickelt. Die variablen Datenraten interaktiver Verbindungen konnten von der Paketvermittlung effizienter verwaltet werden. Paketvermittlung ist ein Kompromiss zwischen Nachrichten- und Leitungsvermittlung mit dem Ziel, die Vorteile beider Techniken zu vereinen: kurze Verzögerungszeiten der Leitungsvermittlung und hohe Auslastung der Medien durch die Nachrichtenvermittlung. Die zu übertragende Nachricht wird in kleinere Einheiten segmentiert und mit einem Header und ggfs. einem Trailer versehen. Im Header stehen u.a. die Adressen von Sender und Empfänger und die Folgenummer des Datenpakets innerhalb der Nachricht. Der Trailer enthält meist Angaben zur Fehlerbehandlung. Die Pakete werden von Knoten zu Knoten im Netzwerk weitergereicht. Jedoch ist die Verweilzeit in den Zwischenstationen gering. Ein Paket verweilt nur im Puffer eines Knotens und wird nicht auf einen Sekundärspeicher ausgelagert. Es gibt zwei Formen von Paketvermittlung:

Vermittlung von virtuellen Verbindungen (Virtual Circuit Switching): Hierbei wird ein virtueller Kanal zur Verfügung gestellt, d.h. die Reihenfolge der Pakete und ihre Korrektheit wird garantiert.

Datagrammvermittlung (Datagram Switching): Hierbei wird jedes Paket einzeln über das Netz transferiert. Datagramme können unterschiedliche Pfade im Netz beschreiten. Überholvorgänge zwischen Datagrammen sind möglich. Die Reihenfolge der Datagramme muss also im Empfänger wiederhergestellt werden.

In der digitalen Übertragung dominiert heute die Paketvermittlung gegenüber der Leitungsvermittlung wegen deutlich besserer Effizienz.

Kapitel 3

Lokale Netze (LAN's)

Klassische oder konventionelle Netze basieren heute im LAN-Bereich meist auf Ethernet- oder Token-Ring-Technik. In diesem Abschnitt bewegen wir uns vorwiegend auf der ISO-Ebene 2, der Leitungsebene oder Data Link Layer. Die Leitungsebene wird in zwei Subebenen, die Logical Link Control (LLC) und die Medium Access Control (MAC) unterteilt. Nur die MAC-Ebene ist vom Übertragungsmedium abhängig. Sie stellt Protokolle bereit, durch die Endknoten Zugang zum Medium erhalten. Die anderen Aufgaben der Ebene 2 wie die Behandlung von Übertragungsfehlern, die Formung von Datenblöcken mit Adressierung und die Herstellung der korrekten Reihenfolge der Datenblöcke beim Empfänger übernimmt die Logical Link Control. Wir werden uns nachfolgend auf die Beschreibung von Ethernet- und Token-Ring-Netzen mit einigen Zugangsverfahren beschränken.

3.1 Allgemeine LAN-Architektur

Ethernet- und Token-Ring-Netze unterscheiden sich nur unterhalb der Logical Link Layer, nämlich auf der physikalischen Ebene und der Medium Access Control-Ebene. Die LLC-Ebene kennt drei Diensttypen:

1. Unacknowledged Connectionless Service: Dies ist ein Datagramm-Dienst ohne Fehlerbehandlung und Flusssteuerung.

2. Connection-oriented Service: Dies ist ein verbindungsorientierter Dienst mit Maßnahmen gegen Verlust, Duplizierung und Umordnung von Frames, sowie Regulierung des Datenflusses zwischen Sender und Empfänger.

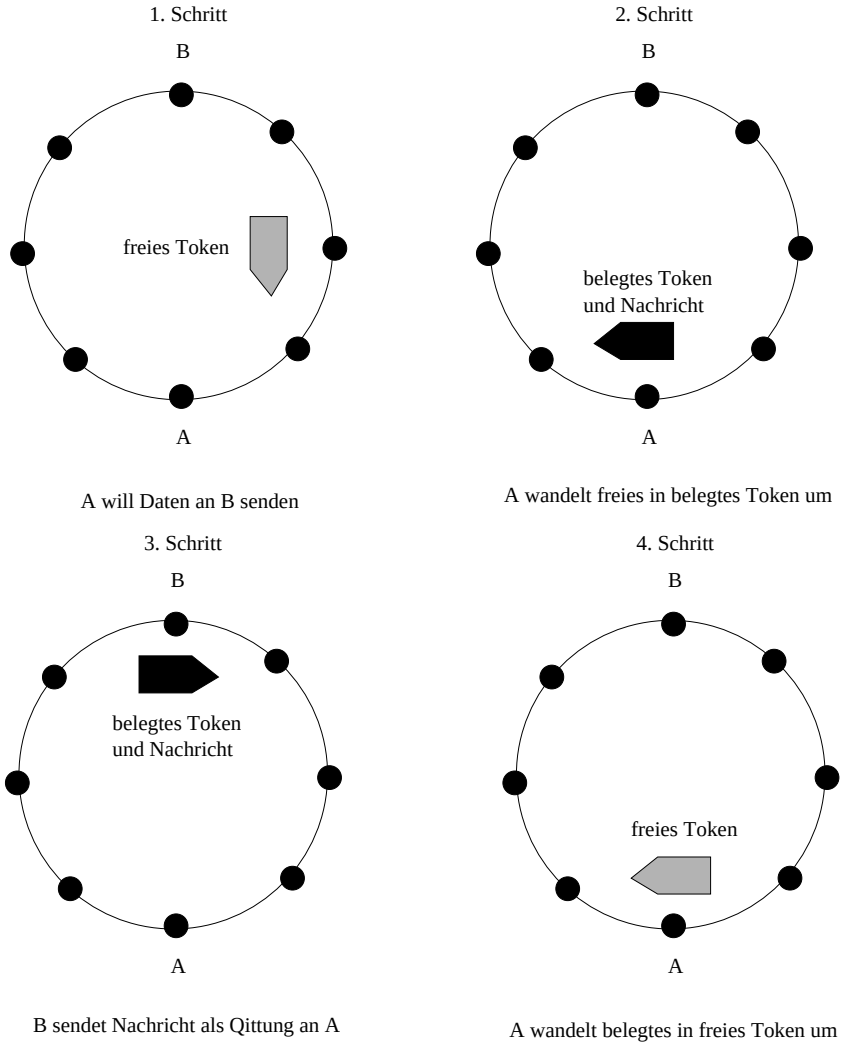
3. Acknowledged Connectionless Service: Dies ist ein Kompromiss zwischen 1 und 2 ohne Flusssteuerung. 3 enthält weniger Steuerdaten als Overhead.

Das Medienzugriffsprotokoll legt fest, wann die angeschlossenen Stationen das gemeinsame Übertragungsmedium erhalten. Man unterscheidet deterministische und stochastische Protokolle. Bei stochastischen Protokollen können mehrere Stationen gleichzeitig versuchen das exklusive Übertragungsmedium zu erhalten. Bei deterministischen Protokollen ist der Zugang so geregelt, dass ein gleichzeitiger Medienzugriff ausgeschlossen ist. Während Ethernet (CSMA/CD) ein stochastisches Wettbewerbsprotokoll (Contention Protocol) benutzt, hat Token Ring (wie auch FDDI) ein deterministisches Zugriffsprotokoll. Die Adressen der Netzstationen sind durch je eine 6 Byte lange Kennung eindeutig bestimmt, wodurch in solchen Shared-Media-LAN's mit Broadcast der Empfänger eindeutig anhand der Kennung bestimmt werden kann.

3.2 Netzzugangsverfahren

Der Token Ring ist eine Punkt-zu-Punkt Topologie. Auf dem Ring kreist ein sog. Token. Dies ist eine spezielle Bitfolge, die von einer sendebereiten Station als Sendeberechtigung interpretiert wird. Die erste sendebereite Station, an der das freie Token vorbei kommt, wandelt das freie Token in ein belegtes Token um und hängt die zu übertragenden Daten an dieses belegte Token an. Nachdem der Empfänger die Nachricht erhalten hat, sendet er sie als Quittung an den Sender zurück. Der Sender vergleicht die Quittung mit der ursprünglich ausgesendeten Nachricht. Bei Ungleichheit wird erneut gesendet; bei Gleichheit wandelt der Sender das belegte Token in ein freies Token um und übergibt dies an die folgende Station im Ring. Hierdurch ist sichergestellt, dass jede Station irgendwann senden kann und keine Station verhungert.

Das Token Ring-Verfahren ist nicht nur auf physikalische Ringe beschränkt; es können auch Sterne oder Busse als logische Ringe verwaltet werden. Die Arbeitsweise eines Token Bus ist analog zum Token Ring. Der wesentliche Unterschied besteht darin, dass hier keine Ordnung der angeschlossenen Stationen durch physikalische Verbindungen a priori vorgegeben ist. Es ist frei wählbar, wer für jede Station logischer Vorgänger oder Nachfolger sein soll. Das Token-Ring-Verfahren auf Bussen gehört zur Gruppe der Auswahltechnik-Verfahren, da nach Beendigung einer Datenübertragung die nächste sendeberechtigte Station ausgewählt wird.



Für Busse ist aber eine andere Verfahrensgruppe typischer: die Reservierungsverfahren oder Random Access-Methoden. Die ältesten Random Access-Methoden sind die sog. Aloha-Verfahren, bei welchen jede an den Bus angeschlossene Station Daten übertragen darf, wann immer sie will. Senden zwei Stationen gleichzeitig, so kommt es zu einer Kollision auf dem gemeinsam genutzten Bus. Diese Kollision muss erkannt und durch geeignete Verfahren behandelt werden. Je nachdem, ob der Netzzugang zu beliebigen Zeitpunkten oder getaktet erfolgt, unterscheidet man Pure Aloha oder Slotted Aloha. Beide Verfahren arbeiten wegen der Kollisionsgefahr jedoch nur zufriedenstellend, solange der Verkehr auf dem Bus gering ist. Aus diesem Grund sind sie für lokale Netze nicht gut geeignet.

Wesentlich verbessert ist der Bus-Durchsatz, d.h. die Anzahl erfolgreicher Übertragungen pro Zeiteinheit, bei Verwendung eines der zahlreichen Varianten

des Carrier Sense Multiple Access-Verfahrens (CSMA). Das Prinzip von CSMA lässt sich treffend mit 'listen before talk' beschreiben. Jede übertragungsbereite Station, prüft vor der Sendung, ob der Bus mit einer anderen Sendung bereits belegt ist; dies nennt man auch Carrier Sensing. Ist der Bus belegt, so wartet die Station, ansonsten kann sie senden.

Leider können aber durch die Laufzeitverzögerungen des Signals trotzdem Kollisionen auf dem Bus entstehen. Wenn zwei oder mehr Stationen den Bus quasi gleichzeitig abhören und ihn als frei ansehen; senden sie. Es kommt zu einer Kollision, die durch ein Collision Detection-Verfahren (CD) erkannt und behandelt werden muss. Die erste Station, die die Kollision anhand einer unzulässigen Signalform auf der Leitung erkennt, sendet dann ein Störsignal (Jam) aus. Daraufhin unterbrechen alle noch aktiven Sender, die das Störsignal empfangen haben, ihre Datenübertragung. Zu einem späteren Zeitpunkt wird versucht, die Daten erneut zu übertragen. Damit sich beim Wiederholen der Sendungen nicht erneut ein Konflikt ergibt, werden Verfahren eingesetzt, die ein zeitversetztes Senden möglichst ohne Kollisionen steuern. Diese Verfahren gehören zur Collision-Avoidence-Gruppe (CA). Das für Ethernet eingesetzte Gesamtzugriffsverfahren nennt man daher auch CSMA/CD.

3.3 Weiterentwicklung von leitungsgebundenen LAN's

Neben der Steigerung der Übertragungsrate von $4\,MBit/s$ auf heute $1\,GBit/s$ sind folgende wichtigste Entwicklungen im leitungsgebundenen LAN-Bereich zu nennen:

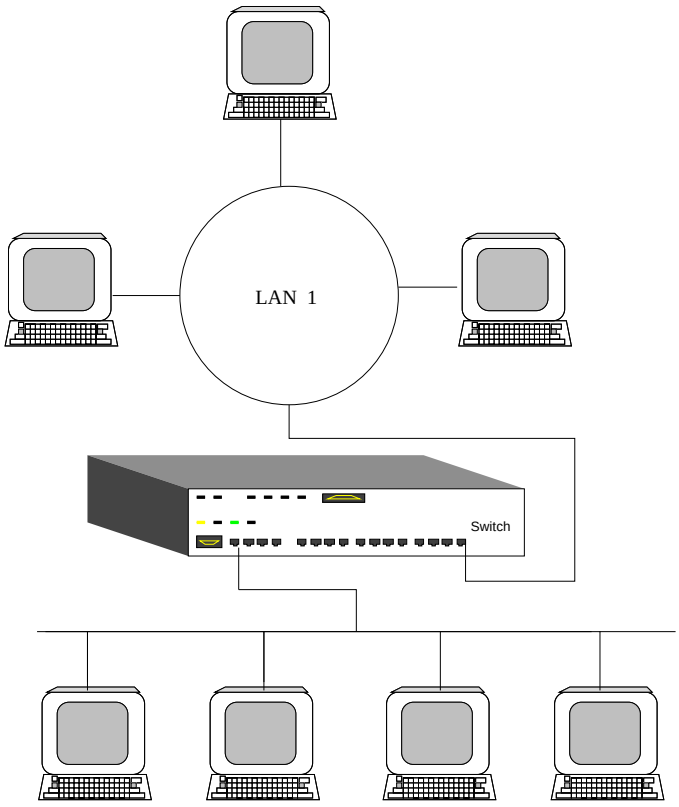
- Standardisierung der Verkabelung,
- Entwicklung von Broadcasting zum Switching, d.h. vom Shared Medium- zum Switched-LAN,
- Virtuelle LAN's.

Wegen der hohen Investionen in Kabeltechnik wurden 4 Kabeltypen standardisiert:

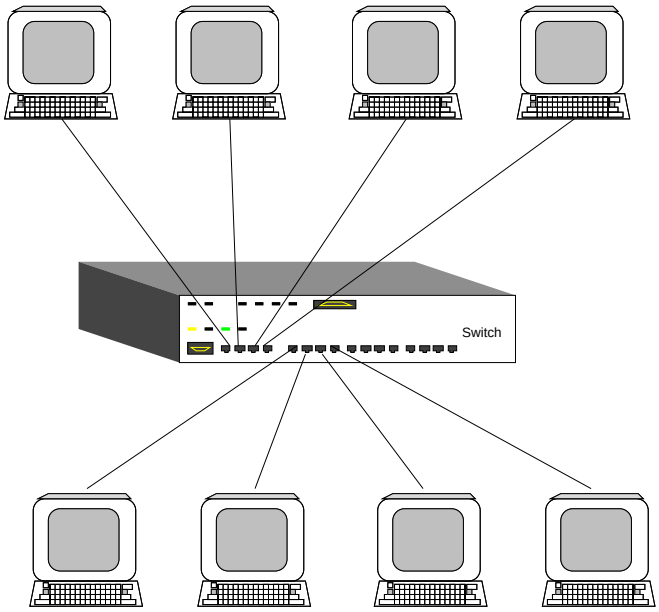
- Unshielded Twisted Pair,
- Shielded Twisted Pair,
- Koaxialkabel,
- Lichtwellenleiter.

Das Switching in LAN's ist eine Entwicklung aus der Bridge Technik. Ein Switch ist eine Multiport-Bridge, die Frames von einem LAN zu einem anderen weiterleiten kann. Dazu unterhält der Switch eine Weiterleitungstabelle mit Ports und angeschlossenen Adressen. Switches, die nur eine Endstation pro Port unterstützen, heißen Workgroup-Switches. Andere Switches lassen mehrere Stationen pro Port zu.

Der entscheidende Vorteil des Switching ist, dass aus einem großen LAN mit hoher Netzbelastung ohne Änderung in der Hard- und Software der Host's mehrere kleinere LAN's mit geringerer Netzbelastung gebildet werden können. Diese kleineren LAN's können bzgl. nicht notwendiger Datenübertragungen durch Broadcast voneinander abgeschottet werden.



Switch zwischen verschiedenen LAN's



Workgroup-Switch in einem LAN

Man unterscheidet zwischen Store-and-Forward- und Cut-Through-Switching. Während beim Store-and-Forward-Switching der gesamte Frame im Switch zwischengespeichert wird, bevor er weitergeleitet wird, beginnt die Übertragung beim Cut-Through-Switching bereits nach dem Empfang der Empfängeradresse im Switch. Cut-Through-Switching ist i.a. wesentlich schneller als Store-and-Forward-Switching. Hingegen fehlt eine Fehlererkennung im Switch, wodurch auch fehlerhafte Frames weitergeleitet werden.

Switching wird nicht nur für Ethernet sondern zunehmend für Token Ring-Netze eingesetzt. Heute werden meist LAN's im Vollduplex-Betrieb und Workgroup-Switching eingesetzt, wodurch der Einfluss des MAC-Protokolls praktisch vernachlässigt werden kann, da es z.B. im Ethernet nur sehr selten zu Kollisionen kommt. In einem GBit-Ethernet (Übertragungsrate von $1\,GBit/s$) können im Vollduplex-Betrieb maximal $2GBit/s$ kollisionsfrei zwischen je zwei Stationen übertragen werden.

Mit dem Switching sind auch die virtuellen LAN's entstanden (sog. VLAN's). Darunter werden dynamisch konfigurierbare Netze verstanden, die nicht physikalisch sondern nur logisch (durch Software) definiert sind. VLAN-Technologie bringt zwei Hauptvorteile:

- VLAN's stellen einen Weg zum Management von Broadcasts in großen Netzen dar.

- Ohne physikalische Änderungen können logische Gruppen von Nutzern und Netzressourcen bei Bedarf umkonfiguriert werden.

Auch der asynchrone Transfer Modus (ATM) wird in LAN's zunehmend realisiert, wobei ATM-LAN's zur Zeit meist aus konventionellen LAN-Umgebungen bestehen, die auf ATM migriert wurden. Hier sind u.a. zu nennen:

- LAN-Emulation (LANE),
- IP über ATM (IPOA),
- Multiprotokoll über ATM (MPOA).

3.4 Nicht leitungsgebundene (Wireless) WLAN's

Wireless LAN ist zunächst ein Sammelbegriff für drahtlose Netze und bezeichnet sowohl Funknetze als auch Infrarot-Datenübertragung. Erste drahtlose lokale Netze existieren etwa seit 1992. WLAN - Technologien aus dieser Zeit hatten durchschnittlich eine Bandbreite, die weit unter 1 Mbit/s lag. Die fehlende Standardisierung der damaligen WLAN - Technologie stellte ein wesentliches Problem dar, so dass nur Produkte eines Typs u.U. vom selben Hersteller kompatibel waren. Mit der Einführung der IEEE 802.11 - Standards wurde dieses Problem weitgehend behoben.

IEEE-Standard	Beschreibung	Übertragungsrate, Frequenzband
802.11	erster Standard, Jahr 1997	2 bis 3 Mbit/s, 2.4 GHz
802.11 b	Nachfolger von 802.11 Jahr 1999	bis 11 Mbit/s, 2.4 GHz
802.11 g	Nachfolger von 802.11b	bis 54 Mbit/s, 2.4 GHz
802.11 a	Nachfolger von 802.11b	bis 54 Mbit/s, 5 GHz

Der Wunsch nach Mobilität führte zu einem Aufschwung der drahtlosen Vernetzung. Mobile Geräte, wie Personal Digital Assistants (PDAs) und Notebooks, sind aus dem Unternehmensalltag nicht mehr wegzudenken. Die Sendeleistung der LAN-Cards liegt weit unter der von Handys, teilweise sogar unter der von Microwellen. Aufgrunddessen kommen WLANs auch verstärkt in Krankenhäusern zum Einsatz. Das Übertragungsmedium kann sogar von mehreren, unabhängigen Netzwerken gleichzeitig verwendet werden. Das übliche Einsatzgebiet eines WLANs ist ein Bürogebäude, in dem strategisch Zugangsstationen (Access Points) verteilt werden. Über Kupferkabel oder Glasfaser stehen diese Access Points (auch über längere Strecken) miteinander in Verbindung. Damit ist eine Verbindung mit mobilen Geräten über ihre Funkreichweite hinaus möglich.

Einerseits zeichnen sich Funknetze durch eine bessere Flexibilität und auch oftmals durch Kostenersparnis gegenüber kabelgebundenen Netzen aus, geben dabei aber auch die alleinige Kontrolle über das Übertragungsmedium aus der Hand. Nicht nur die Klienten, denen vom Betreiber ein physikalischer Zugang zum Netzwerk in Form eines Anschlusses an das Übertragungsmedium gewährt wurde, sondern alle Klienten, die in den Empfangsbereich eines Access Points gelangen, können Daten in das Netz einspeisen und mithören. Umgekehrt kann es in öffentlichen Bereichen wie Flughäfen, Bahnhöfen, Hotels oder Messen ferner wünschenswert sein, dass ein Accesspoint sich bei einem mobilen Teilnehmer legitimiert.

3.4.1 Komponenten und Betriebsarten

Damit zwei oder mehr mobile Stationen innerhalb eines WLAN kommunizieren können, müssen sie mit einer WLAN-Netzwerkkarte ausgestattet sein. Diese Karten werden als Steckkarten oder als USB-Version vertrieben. Grundsätzlich werden zwei mögliche Betriebsarten eines WLAN unterschieden:

Pear-to-Pear- oder Ad Hoc-Modus: Eine Pear-to-Pear-Verbindung , ist die einfachste Möglichkeit ein WLAN aufzubauen. In Manets (Mobile Ad Hoc Networks) betreiben mehrere moblie WLAN-Stationen ein Ad Hoc-Netzwerk.

Infrastructure-Modus: Sollen mehrere Stationen über eine zentrale Stelle im WLAN miteinander kommunizieren, so wird ein sogenannter Access Point benötigt. Dies ist ein zentraler Funkknoten, der für ein bestimmtes Gebiet die Versorgung mehrer moblier Stationen übernimmt. Mit Hilfe von Access Points kann sowohl der Datendurchsatz als auch die Reichweite eines WLANs gebenüber dem Ad Hoc-Betrieb stark erhöht werden. Die Reichweite eines Access Points bei einer Sichtverbindung im Freien kann die im Standard 802.11b vorgegebenen 400 Meter deutlich übersteigen. In den eigentlichen Einsatzgebeiten der Access Points, in Räumen und ohne freien Sichtkontakt (Rigipswände, Mauern, Glas mit Metallbeschichtung, usw.), kann die Reichweite allerdings deutlich unter 100m liegen. Das komplexere WLAN mit Access Points, das i.d.R. auch in ein bestehendes Kabel-LAN eingebunden ist, wird als Infrastructure bezeichnet. Nach der Postierung der Access Points muss das Signal, wenn sich die mobile Station bewegt, automatisch zwischen den Access Points weitergereicht werden. Dies nennt man Roaming. Die Sende- und Empfangsgebiete zweier Access Points sollten sich daher überschneiden.

3.4.2 Übertragungstechnik

Die meisten WLAN's arbeiten mit der Spread Spectrum Technologie (SST). SST wurde ursprünglich vom amerikanischen Militär entwickelt. Sie ist eine Breitband-Radio-Technologie, die eine höhere Bandbreite als die Narrowband-Technologie (z.B. für digitale Telefonie nach dem DECT-Standard) nutzt. Der Empfänger und der Sender müssen aber auch hier auf ein Spektrum festgelegt werden. Durch Frequenzsprünge (frequency hopping) ist es möglich, die verschiedenen Teilfrequenzen unter allen Anwendern aufzuteilen, Störungen (z.B. durch Mikrowellen-Grills) zu vermeiden und die Übertragung sicherer gegen Abhören zu machen.

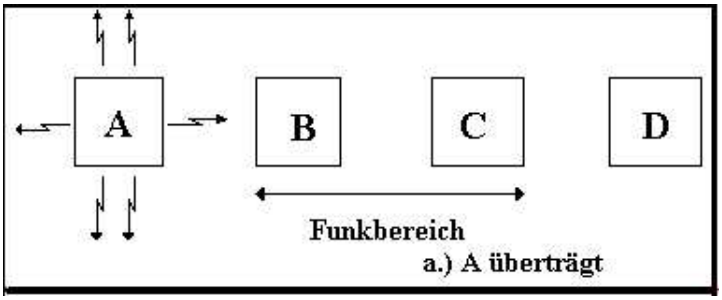
WLAN, nach dem Standard 802.11g, arbeitet im 2,4-GHz-Band und überträgt Daten mit bis zu 54 MBit/s. Der Frequenzbereich von Bluetooth zum Beispiel beginnt bei 2,402 und endet bei 2,480 GHz. Innerhalb dieses Bands sind 79 Frequenzsprünge mit je 1 MHz Abstand festgelegt, wobei 1.600 Sprünge in der Sekunde stattfinden.

3.4.3 Übertragungsprotokolle

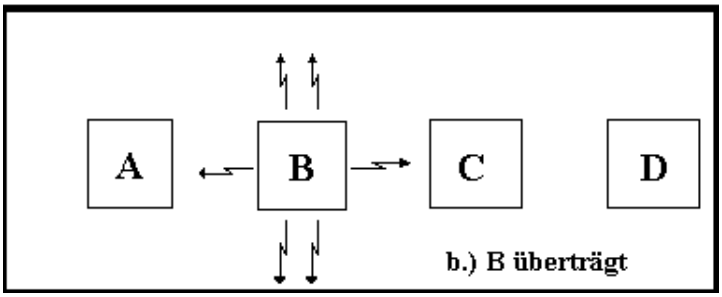
Bei der Datenübertragung in WLAN's gibt es andere Probleme und Lösungen als bei LANs. Das grösste Problem wird durch funktechnisch verborgene Stationen verursacht. Das aus dem Ethernet-Protokoll bekannte CSMA mit dem Prinzip "Listen before Talk" reicht nämlich hierbei nicht aus, da nicht jede Station alle anderen Stationen empfangen kann.

Zur Verdeutlichung dienen 4 drahtlose Stationen. Hierbei spielt es keine Rolle, welche der Stationen die Basisstation mit Access Point ist bzw. welche Stationen die mobilen Einheiten darstellen. Der Funkbereich sei wie folgt definiert : A und B befinden sich innerhalb der Reichweite voneinander und können sich gegenseitig stören. C kann auch B und D, nicht aber A stören.

Fall a: Was passiert nun, wenn, während A Daten an B überträgt, C ebenfalls Daten an B senden will? C ist nicht in Reichweite von A und kann deswegen nicht feststellen, dass A an B sendet. Beginnt C nun mit der Datenübertragung, stört sie die Kommunikation zwischen A und B. Diese Schwierigkeit einer Station (hier C), einen potentiellen Mitbewerber (hier A) um das Medium nicht zu erkennen, bezeichnet man als Hidden Station Problem. A ist also eine Hidden Station in Bezug auf C (und umgekehrt).



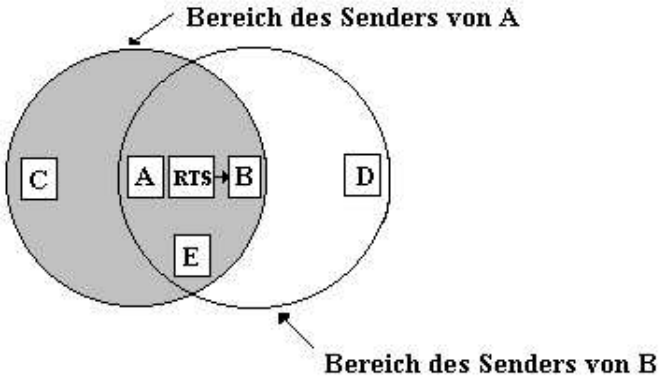
Fall b: Was passiert nun, wenn, während B Daten an A überträgt, C Daten an D senden will? C tastet den Sendebereich von B ab, erkennt eine laufende Übertragung und folgert, dass sie nicht an D senden darf, obwohl die erkannte Übertragung nur in der Zone zwischen B und C einen schlechteren Empfang verursachen würde. Diese Schwierigkeit nennt man Exposed Station Problem: B ist also der Strahlung von C zwar ausgesetzt; jedoch wird der Empfang in A hierdurch nicht gestört, da A nicht in Reichweite von C ist. B ist als Exposed Station der Strahlung von C ausgesetzt.



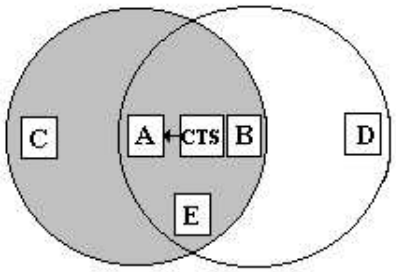
Vorteil und Problem eines WLAN gegenüber einem LAN: Bei einem Kabel verteilen sich alle Signale an alle Stationen. Es kann jeweils nur eine Übertragung im System stattfinden. Bei Radiokurzwellen können unter Berücksichtigung, dass die Ziele nicht innerhalb gleicher Bereiche liegen, gleichzeitig mehrere Übertragungen statfinden. Durch das Übertragungsprotokoll des WLAN muss also erkennbar sein, ob gleichzeitige Sendungen Kollisionen verursachen.

Die Grundlage für den IEEE-Standard 802.11 für WLAN's bildet das Protokoll MACA (Multiple Access with Collision Avoidance). Hierbei regt der Sender den potentiellen Empfänger zur Ausgabe eines kurzen Rahmens an, so dass im Bereich des Empfängers gelegene Stationen die anstehende Übertragung erkennen können und für die Dauer der Übertragung des bevorstehenden Datenrahmens nichts senden.

A will einen Rahmen an B senden. A beginnt durch Aussenden eines RTS-Rahmens (Request to send) an B. Dieser kurze Rahmen (30 Byte) enthält die Länge des nachfolgenden Datenrahmens.



B antwortet seinerseits mit einem CTS-Rahmen (Clear to send). Der CTS-Rahmen enthält die aus dem RTS-Rahmen kopierte Datenlänge. Nach Empfang des CTS-Rahmens beginnt A mit der Übertragung.



Stationen, die einen dieser Rahmen erkennen, reagieren wie folgt: Stationen, die RTS empfangen (C und E), befinden sich in der Nähe von A und müssen so lange (also eine feste Zeit) warten, bis CTS an A konfliktfrei zurückgesendet werden kann. Stationen, die CTS empfangen, befinden sich in der Nähe von B und müssen während der folgenden Datenübertragung, deren Länge durch Einsicht des CTS-Rahmens ermittelt wird, passiv bleiben.

C befindet sich innerhalb des Sendebereiches von A, nicht aber in dem von B. Deshalb hört sie RTS von A, aber nicht CTS von B. Solange sie das CTS nicht stört, kann sie gleichzeitig senden, während der Datenrahmen von A an B übertragen wird. Hierbei wird davon ausgegangen, dass der Sendebereich und der Empfangsbereich einer Antenne gleich ist. D.h. wenn C das CTS von B nicht empfangen kann, kann C die Station B auch nicht mit Sendungen erreichen und eine Sendung von A z.B. stören.

Demgegenüber liegt D nicht im Sendebereich von A, sondern in dem von B. Auch hier wird angenommen das D auch nicht im Empfangsbereich von A liegt.

Dann kann D auch nicht die Sendung des CTS-Rahmens von B an A stören. D empfängt also nur CTS, nicht aber RTS. Sie folgert aus diesem CTS, dass sie sich auch ihr Sendebereich in der Nähe einer Station befindet, die jeden Augenblick einen Rahmen empfangen muss, deshalb hält sie sich vom Senden zurück, bis der Rahmen fertig übertragen wurde.

Station E hört beide Steuernachrichten und muss wie C warten bisB den CTS-Rahmen an A geschickt hat und weiter wie D warten, bis der Datenrahmen von A an B fertig übertragen wurde.

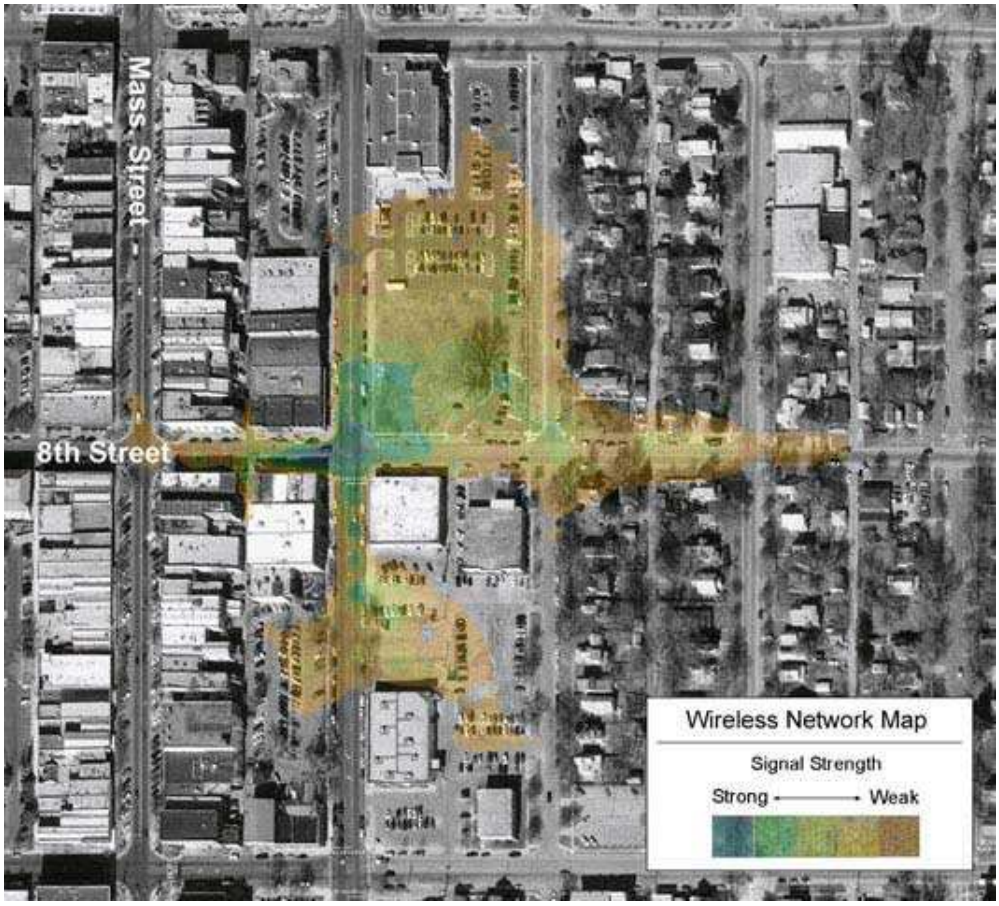
Trotz dieses Protokolls sind Kollisionen nicht ausgeschlossen. Es könnten B und C gleichzeitig RTS-Rahmen an A senden. Diese kollidieren und mindestens einer geht verloren. Im Falle einer Kollision wartet der erfolglose Sender, also derjenige, der innerhalb des Zeitintervalls CTS nicht hört, eine zufallsgesteuerte Zeitspanne und versucht es später erneut.

3.4.4 Sicherheitsprobleme und Gegenmassnahmen

Ein WLAN zu installieren ist nicht schwer. Die zentrale Funkstation, der Access Point, wird an das Stromnetz und an das bereits existierende lokale Netz angeschlossen. Im mobilen Rechner wird dann nur noch die Funknetz-Karte und die Software installiert. Dann ist das WLAN im Prinzip funktionsfähig.

Ungenaue Reichweite

Anwender, die ihr WLAN so oder ähnlich installieren und ohne weitere Vorkehrungen an die Arbeit machen, gehen geradeheraus fahrlässig mit ihren Daten um. Das Netz steht für Hacker-Angriffe weit offen. Denn während im LAN die Daten über ein Kabel von der Quelle zum Ziel transportiert werden, sendet ein WLAN die Informationen durch den Äther. Wo zum Einbruch ins lokale Netz eine physikalische Verbindung notwendig ist, reicht beim WLAN eine Antenne und die Nähe zum Access Point. Die Gefahr durch Funksignale eines Access Points lässt sich mit dem folgenden Bild belegen:



Aufgrund der starken Sendeleistung des Access Point und der fehlenden Technik zur Begrenzung seiner Reichweite, sind die Daten nicht auf den Empfang z.B. innerhalb einer Firma beschränkt sondern können weit über die Firmengrenzen hinaus abgehört werden. Die genauen Reichweiten von Access Points können nicht allgemeingültig angegeben werden. Umso ungehinderter Access Points senden können, desto weiter ist die ihre Reichweite. Ein Access Point in einer oberen Etage eines Hochhauses kann z.B. über 100m Reichweite Daten senden.

Service Set Identifier (SSID)

Der Netzwerkname SSID dient der Identifizierung eines drahtlosen Netzwerkes. Eine mobile Station kann einerseits nach einem Access Point mit einer bestimmten SSID suchen; dies nennt man aktives Scanning. Andererseits kann ein Access Point seine SSID allen mobilen Stationen zur Verfügung stellen; dies nennt man passives Scanning.

Bei den meisten Access Points kann die SSID durch Abschalten des passiven Scanning versteckt werden. Dann können nur solche Stationen am WLAN

teilnehmen, denen der Name des Netzwerkes (SSID) bekannt ist. Aus Unwissenheit wählen viele Benutzer einen ungünstigen Namen (z.B. Familiennamen als SSID). Eine Solche SSID, die mit dem Benutzer in Verbindung gebracht werden kann, ist ein leichtes Spiel für Angriffe auf das WLAN. Auch weisen Anbieter die Kunden oftmals nicht darauf hin, den Netzwerknamen von dem vorgegebenen Standardwert zu ändern, um Netzangriffe zu erschweren. Leider wird durch Sniffer-Programme, wie Netstumbler, in einigen Access Point trotz sogenanntem Hidden Mode die SSID sichtbar.

Dynamic Host Configuration Protocol (DHCP)

Vor allem der Einsatz des Dynamic Host Configuration Protocol (DHCP) ohne weitere Sicherheitsvorkehrungen stellt ein Sicherheitsproblem dar. DHCP weist einer mobilen WLAN-Station automatisch eine im Netz gültige IP-Adresse zu. Fast alle Access Points bieten hierzu einen integrierten DHCP-Server an oder sind in der Lage, DHCP-Anfragen an einen zentralen Server im LAN weiterzuleiten. Wenn eine dieser Funktionen aktiviert ist und der Zugang zum WLAN nicht zusätzlich gesichert ist, kann ein Eindringling nicht nur den Datenverkehr im WLAN belauschen, sondern erhält automatisch eine gültige IP-Adresse im lokalen Netz. WLAN-Clients erhalten damit Zugang zu lokalen Rechnern und Internet-Anbindungen. Alle eventuell vorhandenen Sicherheitsvorkehrungen, wie etwa eine Firewall, die zur Abwehr von Eindringlingen aus dem Internet installiert wurde, sind dann nutzlos. Der Hacker-Rechner ist als vollwertige Station im internen Netz integriert, kann sich dort umsehen und z.B. noch vorhandenen Schutzmechanismen wie Firewalls für das Festnetz angreifen.

Bei der Konfiguration eines Access Points ist es am einfachsten, IP-Adressen aus einem festen Bereich zur Verfügung zu stellen. Jede Station, die nach ihrem Start den Access Point kontaktiert, bekommt eine freie Adresse aus diesem Pool zugewiesen. Hierbei entsteht die obige Gefahrensituation, unberechtigen Stationen eine IP-Adresse zuzuweisen. Weiterhin hat eine Station nicht nach jedem Start zwingend dieselbe IP-Adresse. Dies kann von Nachteil sein, da Server-Prozesse i.d.R. unter einer festen IP-Adresse angesprochen werden. Weiterhin wird die Auswertung von Logdateien erschwert.

Aus diesen Gründen ist es möglich, jeder mobilen Station in Abhängigkeit der MAC-Adresse der Netzwerkkarte per DHCP immer dieselbe IP-Adresse zu geben. Auf diese Weise erhalten nur Teilnehmer mit eingetragener MAC-Adresse eine IP-Adresse per DHCP. Dies ist eine weitere Sicherheit, sofern eine Station nicht eine falsche MAC-Adresse vortäuscht.

Leider sind viele neuere Netzwerkkartentreiber in der Lage, beliebige MAC-Adressen auszugeben. Sinn: Nach einem Tausch einer defekten Netzwerkkarte kann dann weitergearbeitet werden, ohne dass der DHCP-Server umkonfiguriert

werden muss. Weiterhin lassen sich die MAC-Adressen aktiver Stationen durch Sniffer-Software ausspionieren. Insgesamt kann eine im Access Point als erlaubt eingetragene MAC-Adresse von einer Hacker-Station also vorgetäuscht werden. Die in Access Point eingebauten MAC-Adressen-Filter, die verhindern sollen, dass sich unbekannte Endgeräte unerlaubterweise Zugang (evtl. sogar mit IP-Adresse) zu einem Funknetzwerk verschaffen, sind also überwindbar.

Wired Equivalent Privacy (WEP)

Der wichtigste optionale Sicherheitsmechanismus in drahtlosen Netzwerken nennt sich Wired Equivalent Privacy (WEP). Um drahtlose Netze sicherer zu machen und eine dem Kabel vergleichbare Sicherheit zu schaffen, entwickelte man die WEP-Verschlüsselung und integrierte sie in den Standard IEEE 802.11.

WEP verwendet eine Verschlüsselung mach dem symmetrischen Verschlüsselungsalgorithmus RC4, der von Ron Rivest 1987 entwickelt wurde. Symmetrisch bedeutet, dass Sender und Empfänger einer verschlüsselten Nachricht denselben Schlüssel zur Kodierung bzw. Dekodierung der Nachricht nutzen. RC4 ist ein Stromchiffrierer, der den Klartext in WEP byteweise verschlüsselt. (Im Gegensatz zu Blockchiffrierern, die jeweils einen Block von z.B. 64 Bit verschlüsseln.)

Der symmetrische Schlüssel muss in WEP manuell in allen Stationen konfiguriert werden. Um den Schlüssel ohne Umkonfiguration trotzdem häufiger zu wechseln und damit Angriffe auf das Protokoll zu erschweren, wird in WEP ein Teil des Schlüssels in Form eines Initialisierungsvektors vor jeder Datenübertragung vom Sender neu berechnet und an den Empfänger mit den verschlüsselten Daten übertragen. Der wahlweise 64 bzw. 128 Bit lange symmetrische RC4-Schlüssel in WEP setzt sich also aus dem berechneten, 24 Bit umfassenden Initialisierungsvektor (IV) sowie dem eigentlichen geheimen Schlüssel von 40 bzw. 104 Bit zusammen.

In RC4 dreht sich alles um Permutationen. Permutiert wird die Zahlenliste von 0 bis $N-1 = 2^n-1$, wobei $n = 8$ bei einer byteweisen Chiffrierung und $N = 256$ ist. RC4 besteht aus zwei Teilen, dem Key Scheduling Algorithm (KSA) und dem Pseudo Random Generator Algorithm (PRGA). Wie sich anhand dieser Namen vermuten lässt, kann RC4 als Pseudo-Zufallszahlengenerator betrachtet werden: Der ausgegebene Schlüsselstrom, mit dem die Klartextdaten byteweise mit exklusivem Oder verknüpft werden, sollte von wirklichen Zufallszahlen möglichst wenig unterscheidbar sein.

Der KSA dient zur Erzeugung einer ersten pseudo-zufälligen Permutation aus dem geheimen Schlüssel, der PRGA benutzt diese Permutation zur Generierung des Schlüsselstroms. Während des Verlaufs des PRGA ändert sich die Permutation ständig. Selbstverständlich führt der gleiche geheime Schlüssel (z.B. in Sender und Empfänger) immer zu dem gleichen pseudo-zufälligen Schlüsselstrom. Wenn

man RC4 also als Zufallszahlengenerator betrachtet, übernimmt der Schlüssel die Rolle eines Random Seed.

Für die Erzeugung der anfänglichen Permutation ist der KSA zuständig. Er beginnt mit der trivialen Permutation $0, 1, ..., N-1$ und verändert sie durch Vertauschungen. Der KSA läuft in N Runden ab. Jede dieser Runden endet mit der Vertauschung des Inhalts zweier Zellen, d.h. zwei Zahlen in der Permutation tauschen die Plätze.

Zuvor werden in jeder Runde die Indizes der zu vertauschenden Zellen bestimmt. Diese Indizes sind i und j. i ist sehr leicht zu bestimmen. In der ersten Runde ist es 0 und wird dann Runde für Runde inkrementiert, so dass mit dem Abschluss des Algorithmus jede Zelle mindestens einmal vertauscht worden ist (möglicherweise mit sich selbst). Bei j liegt der Fall etwas komplizierter. j wird vor der ersten Runde mit 0 initialisiert. In jeder Runde wird dann vor der Vertauschung folgendes auf j addiert:

- der Inhalt der i. Zelle
- das erste noch nicht verwendete Schlüsselbyte. Wenn alle Schlüsselbytes verwendet worden sind, beginnt man im Schlüssel wieder von vorne.

Diese Additionen werden $mod\ N$ ausgeführt.

In C-ähnlichem Pseudocode sieht der KSA wie folgt aus:

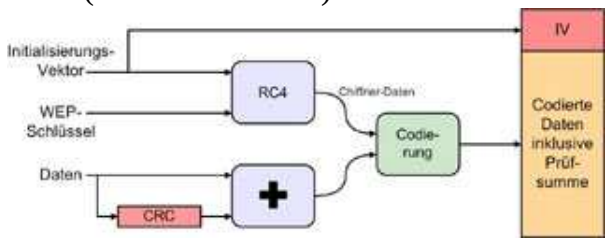
```
for (i=0; i < N; i++) S[i]=i;
for (i=0, j=0; i < N; i++) {
  j=(j+S[i]+K[i mod length(K)]) mod N
  Swap(S[i], S[j]);
}
```

Der PRGA ist dem KSA sehr ähnlich. Die Unterschiede sind im Wesentlichen:

- Der Inhalt derjenigen Zelle, deren Index die Summe der Inahlte der Zellen ist, auf die i und j zeigen, wird als Ausgabe verwendet.
- Der ursprüngliche Schlüssel wird nicht weiter benutzt.
- i beginnt auf 1, da es vor der ersten Verwendung erhöht wird.

```
i=0; j=0;
while (true) {
   i++;
   j=(j+S[i]) mod N;
   Swap(S[i], S[j]);
   Output(S[S[i]+S[j] mod N]);
}
```

Um ein Datenpaket zu übertragen, wird zunächst eine Prüfsumme nach dem CRC 32-Verfahren (Cyclic Redundancy Check) gebildet, um zu verhindern, dass ein Angreifer die Daten während des Versands unerkannt manipulieren kann. Danach wird aus dem geheimen WEP-Schlüssel und dem Initialisierungsvektor nach dem RC4-Verfahren ein Schlüsselstrom gebildet, der mittels der logischen XOR-Funktion (exklusives ODER) mit dem Klartext verknüpft wird.



Der Empfänger der Daten muss aus dem Initialisierungsvektor und dem ihm bekannten WEP-Schlüssel wieder den RC4-Schlüsselstrom erzeugen, um mit der XOR-Funktion die Daten wieder zu entschlüsseln. Danach macht er den Integritätscheck nach dem CRC 32-Verfahren gemacht, um die Integrität der Daten zu überprüfen.

Angriffe auf WEP

Mit nur einem mitgeschnittenen Teil des Chiffrats mit Initialisierungsvektor von 24 Bit kann bei einer geheimen Schlüssellänge von 40 Bit in überschaubarer Zeit mit sämtlichen Schlüsselkandidaten die Dekodierung versucht werden, um den korrekten Schlüssel zu errechnen (Brute Force-Attacke). Sobald ein Angreifer den korrekten Schlüssel gefunden hat, ist dieser in der Lage, den gesamten Netzwerkverkehr des drahtlosen Netzwerkes mitzulesen, bis der Schlüssel durch den Betreiber des Funknetzes gewechselt wird, sofern dies überhaupt geschieht.

Aufgrund seiner Kürze von 24 Bit wiederholt sich ein Initialisierungsvektor und damit der gesamte Schlüssel relativ häufig (im Mittel alle 4000 Datenpakete, spätestens nach 16.7 Millionen Datenpaketen). Die Datenübertragung gilt jedoch nur dann als sicher, wenn der generierte Bitstrom für je zwei gleiche Datenpakete unterschiedlich ist.

Mit 104 Bit Datenlänge ist der geheime Schlüsselanteil zwar schwerer zu bestimmen; jedoch gibt es bekannte Schwächen im RC4 Algorithmus, mit denen es z.B. bei ungünstiger Wahl des Initialisierungsvektors trotzdem gelingen kann, das Verfahren zu kompromittieren.

Die beste Abwehr von Angriffen auf WEP ist ein häufiger Schlüsselwechsel, der aber durch die nicht automatisierte Schlüsselverteilung aufwendig ist.

Extensible Authentication Protocol

EAP bietet die Möglichkeit, dass sich Client und Server gegenseitig ihrer Identität vergewissern. Somit ist auch der Client gegen Angriffe von wilden Access Points geschützt. Dazu werden zwei verschiedene Authentifizierungsverfahren verwendet. Bei EAP-TLS tauschen Client und Server Zertifikate aus. Bei EAP-TTLS liefert nur der Server ein Zertifikat; der Client muss sich über Benutzernamen und Passwort identifizieren. Bei EAP-TLS wird zwischen Client und Server ein gesicherter Tunnel aufgebaut. Über diesen Tunnel wird ein Sitzungsschlüssel transferiert, der von einem sogenannten RADIUS-Server bestimmt wird. Besonders am EAP-Verfahren ist, dass der Access Point über den Tunnel regelmässig die WEP-Schlüssel wechselt.

Wireless Fidelity Protected Access (WPA)

WPA ist vor der Veröffentlichung des Standards IEEE 802.11i erschienen und bildet dessen Grundlage. Die gröbsten Sicherheitsmängel von WEP wurden hiermit beseitigt, z.B. die mangelhafte Authentisierung und die Gefahr durch einen gemeinsamen Schlüssel aller Stationen, der selten gewechselt wird.

Bei WPA erfolgt die Netzwerkauthentifizierung nach EAP. Es bietet zusätzlichen Schutz durch Schlüssel, die auf dem Temporal Key Integrity Protocol (TKIP) basieren. Gegenüber WEP besteht die erhöhte Sicherheit auch darin, dass der ursprüngliche Schlüssel nur bei der Initialisierung verwendet wird und anschliessend ein Session-Key zum Einsatz kommt. Bei der Schlüsselverwaltung gibt es zwei Möglichkeiten: den Managed Key ■ d.h. die Zugangskennungen werden auf einem zentralen Server verwaltet ■ oder Pre-Shared Keys. Hierbei melden sich alle Nutzer eines Netzes mit demselben Passwort an. Seit vergangenem Jahr gibt es den WPA2, der anstatt der o.a. RC4-Verschlüsselung den Advanced Encryption Standard (AES) benutzt.

Grundlegende Konfiguration eines Access Point

Beim Kauf eines Access Points liefern die Hersteller ein Plug-and-Play-Vergnügen, das unter Sicherheitsaspekten als sehr kritisch einzustufen ist, denn die Werkseinstellungen bezüglich Sicherheit sind allesamt offen. Deswegen sollten folgende Einstellungen eines Access Points verändert werden:

- IP-Adresse und Passwort des Accesspoint zu seiner Administration
- Deaktivieren des passiven Scanning der SSID
- Filtern der MAC-Adressen und Zuordnung fester IP-Adressen mit DHCP

- Einschalten der 128 Bit WEP-Verschlüsselung
- Verwenden einer zusätzlichen Verschlüsselungs-Software (z.B. IPSec) zwischen Clients und Server.

Kapitel 4

Weitverkehrsnetze (WAN's)

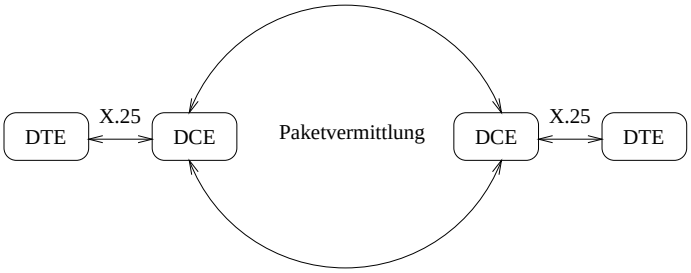
Die Datenkommunikation begann ursprünglich im WAN-Bereich als Daten an entfernte Rechner geschickt werden mussten. Jedoch ist die Entwicklung von WAN's gegenüber der Entwicklung von LAN's deutlich zurückgeblieben. Gründe dafür sind die hohen Kosten und das Monopol staatlicher Telefongesellschaften für WAN's bis zum Anfang der 90'er Jahre.

Klassische WAN's für das Internetworking zwischen LAN's sind Mietleitungen und X.25-Dienste. Mietleitungen sind Standverbindungen, die den Mietern permanent zur Verfügung stehen. Der Netzbetreiber schaltet eine Verbindung in einem öffentlichen Netz durch, das sonst Wähldienste anbietet. Die Kosten für Mietleitungen sind fest, so dass die Verbindungen nur bei hoher Auslastung lohnen.

4.1 X.25

X.25 ist ein internationaler Standard zum Zugang zu öffentlichen Datennetzen, der 1976 von CCITT (heute Nachfolger ITU-T) verabschiedet wurde und bis heute mehrfach überarbeitet wurde. X.25 ist weit verbreitet und wird deshalb auch in näherer Zukunft eine wichtige Rolle spielen. Da X.25 für unzuverlässige analoge Übertragungen entwickelt wurde, enthält es aufwendige Fehlerbehandlungsverfahren. Daher ist X.25 für ein störsicheres Netz nicht gut geeignet.

X.25 spezifiziert in den unteren drei ISO-Schichten die Schnittstelle zwischen einer Datenendeinrichtung (Data Terminal Equipment, DTE) und einer Datenübertragungseinrichtung (Data Circuit-Terminating Equipment, DCE). Ein DTE kann ein Terminal oder Rechner sein; ein DCE kann ein Modem sein. Die DTE's müssen bei X.25 im Paket-Modus arbeiten, ggfs. müssen sie dazu mit einem sogenannten PAD (Packet Assembler/Disassembler) ausgestattet werden.



Kommunizierende X.25-Stationen

X.25-ISO-Schicht 3:

Schicht 3 stellt eine Ende-zu-Ende-Verbindung zwischen zwei DTE's über beliebig viele Zwischenstationen zur Verfügung, ohne dass die Betriebsmittel dediziert zugeteilt werden. Die Nutzerdaten werden hier in X.25 Pakete umgewandelt. Es gibt zwei Typen virtueller Verbindungen:

Permanent Virtual Circuit (PVC): Die Verbindung wird einmal eingerichtet und steht dann ständig zur Verfügung.

Switched Virtual Circuit (SVC): Hierbei muss die Verbindung vor jeder Kommunikation neu aufgebaut werden.

In Schicht 3 gibt es drei Prozeduren für virtuelle Verbindungen:

- Call Setup für den Verbindungsaufbau,
- Data Transfer für die Datenübertragung,
- Call Clearing für den Verbindungsabbau.

X.25-ISO-Schicht 2:

Schicht 2 verwendet das Datensicherungsprotokoll LAPB (Link Access Procedure Balanced). Mit LAPB kann sowohl ein DTE als auch ein DCE Kommunikation initiieren, wobei die Datenpakete fehlerfrei und in der richtigen Reihenfolge empfangen werden. Die maximale Länge des Datenfeldes innerhalb eines Pakets wird zwischen Netzbetreiber und Teilnehmer festgelegt.

X.25-ISO-Schicht 1:

Die physikalische Schicht arbeitet nach der X.21-Empfehlung mit Übertragungsraten bis $19,2\ KBit/s$. X.21 gestattet als Zwischenlösung sogar V-Modems als Anschlüsse an das Paketnetz.

4.2 Telefonnetz

Mit Hilfe von Modems (Modulator und Demodulator) kann das analoge Telefonnetz digital genutzt werden. Hierbei ist eine bidirektionale Kommunikation möglich. Neben den Hauptfunktionen Modulation und Demodulation verfügen heutige Modems über eine Reihe von zusätzlichen Funktionen z.B. zur Datenkompression, Fehlerbehandlung und Faxunterstützung. Modems werden über eine RS 232-Schnittstelle oder als Steckkarten an PC's angeschlossen. Es gibt ITU-T-Standards der V-Serie für Modems, wobei V.34-Modems über viele Funktionen verfügen, die insbesondere in Unternehmensnetzen von Bedeutung sind:

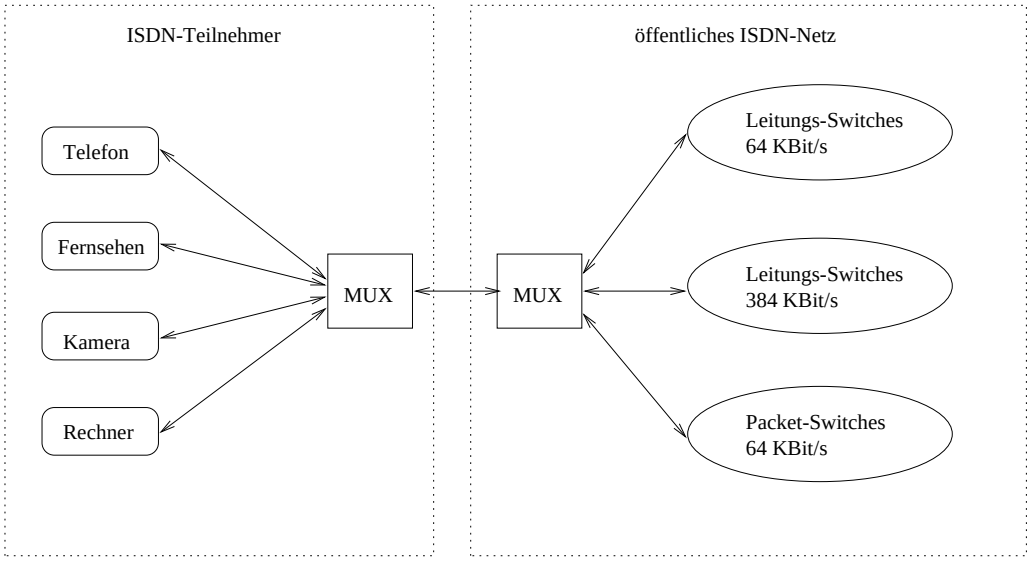
Standard	Bitrate
V.32	$4800 - 9600\ Bit/s$
V.32bis	$14400\ Bit/s$
V.34	$28800\ Bit/s$

Es gibt Modems, die asynchron und solche die synchron Daten übertragen. Bei asynchroner Übertragung werden die Daten zeichenweise mit einem Start- und zwei Stop-Bits übertragen. Die synchrone Übertragung erfolgt als Bitstrom, wobei die Synchronisation der Modems über eine separate Leitung erfolgt. Die Fehlerkorrektur wird mit dem Protokoll MNP (Microscan Networking Protocol) betrieben. Die Empfehlung V.42 umfasst die älteren Normen MNP 3 und 4. Für die Datenkompression gibt es die Standards MNP 7 und V42.bis, die die Datenmenge bis auf ca. 25% reduzieren können.

4.3 ISDN

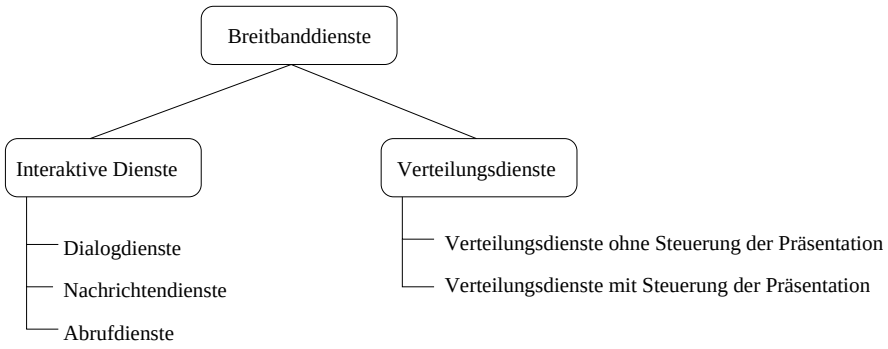
Die Idee des ISDN (Integrated Services Digital Network) stammt aus der Mitte der 70'er Jahre, als man mit dem Public Switched Telephone Network (PSTD) begann verschiedene Kommunikationsdienste in einem digitalen Netz zu vereinen. Allerdings enthält ISDN eine schwache Seite, da verschiedene Geräte über einen gemeinsamen Multiplexer an eine gemeinsame Leitung angeschlossen sind. Dies nennt man einen integrierten Zugang. Die Übertragung ist digital und die Leitung über Zeitmultiplex in verschiedene Kanäle unterteilt.

Der Nachteil dieses Konzepts wird im Netz sichtbar, wo die Dienste nach Vermittlungsart und Datenrate getrennt vermittelt werden. Das ist dadurch begründet, dass es Anfang der 80'er Jahre keine Kombination von Leitungs- und Paketvermittlung gab. Für einen Dienst mit anderer Übertragungsrate muss also immer ein Netz neuer Switches zur Vermittlung installiert werden. Dies macht ISDN sehr kostspielig.



Zunächst entwickelte sich nur ein leitungsvermitteltes Netz, das Schmalband- oder Narrowband-ISDN (N-ISDN). Der Betrieb von N-ISDN begann Anfang der 90'er Jahre mit 2 Anschlussmöglichkeiten für Teilnehmer: $144 KBit/s$ bzw. $2,048 MBit/s$ für Basis- bzw. Primärmultiplexanschluss. Mitte der 80'er Jahre begann man mit einer Erweiterung von ISDN unter dem Namen Breitband- oder Broadband-ISDN (B-ISDN). B-ISDN soll die echte Integration von Diensten auf allen Ebenen - Zugang, Vermittlung und Transport - und die benötigte Bandbreite für neue Anwendungen bieten.

B-ISDN arbeitet auf ATM-Transfertechnik. Hierbei wird die Multiplex-Vermittlung und die Unterteilung in $64\ KBit/s$ überwunden. Die Breitbanddienste des B-ISDN haben zwei Hauptkategorien: interaktive Dienste und Verteilungsdienste. Diese unterteilen sich wie folgt:



Dialogdienste:

Hier wird Echtzeit-Datentransfer realisiert, wobei die bidirektionale Kommunikation symmetrisch oder asymmetrisch sein kann. Beispiele sind Videotelefonie, Videokonferenzen, Hochgeschwindigkeits-Datenübertragung, Videoüberwachung (asymmetrisch fast unidirektional).

Nachrichtendienste:

Im Gegensatz zu der direkten Kommunikation der Dialogdienste arbeiten Nachrichtendienste im Store-and-Forward-Modus also mit Zwischenspeicherung. Beispiele sind EMail, Mail für Bewegtbilder und Sprache sowie Hochauflösungsbilder.

Abrufdienste:

Abrufdienste werden genutzt, um öffentlich zugängliche Informationen beim Endbenutzer darzustellen. Beispiele sind WWW, Filme und Audioinformationen, die in Breitbandnetzen übertragen werden.

Verteildienste ohne Steuerungsmöglichkeit durch den Nutzer:

Hierzu zählen Boadcast-Dienste wie das Fernsehen, wobei der Nutzer keine Steuerungsmöglichkeit z.B. bzgl. Start und Reihenfolge der Sendungen hat.

Verteildienste mit Steuerungsmöglichkeit durch den Nutzer:

Hier werden die Informationen ebenfalls von einer zentralen Quelle bereitgestellt, jedoch hier in einer Aufeinanderfolge von Informationseinheiten, die zyklisch wiederholt werden. Der Nutzer kann also die ausgewählte Informationseinheit jederzeit von Beginn an wiedergeben. Dies entspricht dem Videotext-Dienst der Fernsehanstalten.

4.4 ATM

Der asynchrone Transfermodus (Asynchronous Transfer Mode, ATM) ist die Kommunikationstechnologie, die als Basis für zukünftige Weitverkehrsnetze betrachtet wird. In ATM werden Vorzüge der Paketvermittlung, wie Bandbreiteneffizienz, und der Leitungsvermittlung, wie Bandbreitengarantie und kurze Verzögerungszeiten (Latenzzeiten) vereinigt. Jeder Datenverkehr wird durch einen Strom kleiner Datenpakete von 53 Byte Länge realisiert. Diese Datenpakete heißen ATM-Zellen. Sowohl der Bitstrom der Telefonie als auch der Strom von Datenpaketen bei einer Datenübertragung müssen hierbei in ATM-Zellen umgewandelt werden. ATM ist von $1\,MBit/s$ bis zu mehreren $GBit/s$ skalierbar. Außerdem wirkt ATM in folgenden Punkten integrierend:

- gleiche Infrastruktur für unterschiedliche Dienste,
- gleiche Technologie für LAN und WAN,
- gleiche Technologie für private und öffentliche Netze.

Die 53 Byte Länge einer ATM-Zelle sind als Kompromiss zwischen Herstellern von Endgeräten zur Datenkommunikation (USA) mit 64 Byte Längenforderung und den Telefongesellschaften (Europa) mit 32 Byte Längenforderung zustande gekommen: $(64 + 32)/2 = 48$ Byte-Information und 5 Byte-Header. Kleinere Zellen eignen sich besser für isochrone Dienste, da die Transferverzögerung kurz ist. Größere Zellen nutzen die Bandbreite des Netzes für die Datenübertragung besser.

Der Header einer ATM-Zelle enthält folgende Informationen:

- Weginformation für die Vermittlung,
- Typ der Daten,
- Flusssteuerungs-Informationen,
- Fehlerbehandlungs-Informationen.

ATM ist verbindungsorientiert; eine ATM-Verbindung heißt virtuelle Kanalverbindung (Virtual Channel Connection, VCC). Mehrere Teilverbindungen zwischen ATM-Switches sog. virtuelle Kanäle (Virtual Channel, VC) bilden eine solche VCC. VC's mit dem gleichen Ziel werden zu virtuellen Pfaden (Virtual Path, VP) vereinigt und von ATM als Einheit transparent vermittelt. Die virtuellen Entitäten (VP, VC, VCC) müssen über physikalische Übertragungsmedien (Twisted Pair, LWL...) realisiert werden. ATM-Verbindungen können dauerhaft oder nur für die Dauer einer Kommunikation aufgebaut werden. Man unterscheidet:

- permanente virtuelle Verbindungen (Permanent Virtual Connection, PVC),
- vermittelte virtuelle Verbindungen (Switched Virtual Connection, SVC).

PVC's werden i.a. manuell durch das Netzmanagement konfiguriert. Konfiguration bedeutet hierbei Buchung erforderlicher Ressourcen in einer Reihe von ATM-Switches zwischen den Endgeräten. SVC's werden mit Hilfe der ATM-Signalisierung aufgebaut.

Die Anforderungen der Anwendungen an ATM sind sehr verschieden:

- asynchroner bzw. synchroner Transfer,

- verbindungsloser bzw. verbindungsorientierter Transfer,
- konstante bzw. variable Bitrate,
- strukturierter bzw. unstrukturierter Bitstrom.

Die Gegensätze zwischen der Einheitlichkeit des Transportdienstes und der Verschiedenartigkeit der Anwendungen müssen durch die ATM-Anpassungsschicht (ATM-Adaption Layer, AAL) überbrückt werden. Allerdings hat man wegen der starken Unterschiede der Anforderungen mehrere Klassen verschiedener Anpassungsschichten definiert:

Klasse A: Emulation der Leitungsvermittlung mit konstanter Bitrate und Synchronisation, z.B. für Multimedia-Anwendungen.

Klasse B: Emulation verbindungsorientierter Leitungsvermittlung (wie Klasse A) aber mit variabler Bitrate, z.B. für Video- und Audio-Anwendungen, die synchrone Datenübertragung benötigen.

Klasse C: Emulation verbindungsorientierter Leitungsvermittlung mit variabler Bitrate, wobei die Datenübertragung asynchron ist, z.B. für High-Speed-Datenkommunikation aber auch für X.25.

Klasse D: Emulation eines verbindungslosen Dienstes mit variabler Bitrate ohne Timing zwischen Quelle und Ziel, z.B. für konventionelle LAN's und Switched Multimegabit Data Service (SMDS).

Kapitel 5

Internetworking

Internetworking befasst sich mit der Kopplung mehrerer Netze. Der größte und bekannteste Netzverbund ist das Internet. Im Zusammenhang des Internetworking müssen folgende Aufgaben gelöst werden:

Adressierung: Eindeutige hierarchisch-strukturierte Adressen sind zur Vereinfachung des Routings und der Skalierbarkeit der Netze erforderlich.

Routing/Relaying: Bestimmung des Pfades (Routing) und Weiterleiten des Datenverkehrs (Relaying).

Flusssteuerung: Regulierung des Datenflusses zwischen Netzen mit unterschiedlicher Leistung und Auslastung, um Überlast und Verstopfung zu verhindern.

Quality of Service (QOS): Zeitkritische Dienste, wie Multimedia-Anwendungen, müssen netzübergreifend in ihrer Qualität unterstützt werden.

Überwindung von Heterogenität: Unterschiede zwischen direkt zu verbindenden LAN's, z.B. Ethernet und Token-Ring, und zwischen LAN's und Transitnetzen des WAN müssen überbrückt werden.

5.1 Koppelelemente

Koppelelemente verbinden Netze unterschiedlicher oder auch gleichartiger Architektur. Für das Internetworking bieten sich Bridges, Router und Gateways an.

Gateway:

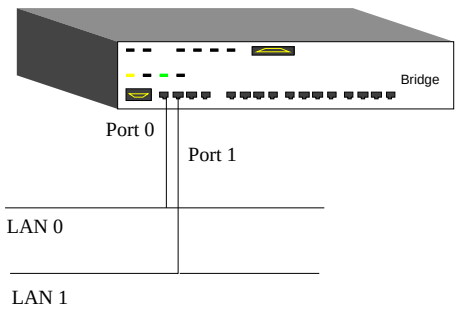
Ein Gateway ist ein dedizierter Rechner zur Kopplung von Netzen unterschiedlichen Typs, z.B. SNA und DECnet. Der Gateway konvertiert die verschiedenen Netzwerkprotokolle und verbindet die Anwendungen miteinander. Er arbeitet also auf der Anwendungsschicht.

Bridge:

Bridges verbinden verschiedene LAN's auf der ISO-Ebene 2 in der MAC-Subschicht. Deswegen werden Bridges auch MAC-Bridges genannt. Dabei können die LAN's direkt oder über ein WAN miteinander verbunden werden. Man spricht dann von local bzw. remote Bridges. Bei remote Bridges wird dem Sender jedes Frame bestätigt, bevor es durch die Bridge weitergeleitet wird. Weiterhin erkennt eine remote Bridge, wenn zu große Zeitabstände zwischen Frames auf einer Leitung entstehen und kann dann zwischenzeitlich die Verbindung abbauen. Diese Eigenschaft gehört zum Bereich des Leitungsmanagement einer Bridge.

Alle Bridges arbeiten auf der Basis einer Store-and-Forward-Technik: Eine Bridge hört alle Datenpakete auf den angeschlossenen LAN's mit. Dabei wird ein Datenpaket z.B. vom Ethernet-Controller einer Bridge eingelesen und in einen Zwischenspeicher kopiert. Anschließend überprüft die Bridge die Zieladresse des Frame und trifft dann die Entscheidung, ob es sich um lokalen Datenverkehr des LAN handelt oder ob das Frame an ein anderes LAN weitergeleitet werden muss. Diese Entscheidung wird anhand von gespeicherten Adresslisten getroffen, die die Bridge mit Hilfe der Adressen in den Sendepaketen aufbaut. Hierbei werden die Adressen den Ports der Bridge zugeordnet.

MAC-Adressen an Port 0	MAC-Adressen an Port 1
00AA0006C1BC	10BA119ADFAB
76543210ABCD	ABCDEFFFFFFF
...	...



Den Mechanismus des automatischen Aufbaus von Adresstabellen einer Bridge bezeichnet man auch als Learning. Den Vorgang ein Datenpaket, das für einen Empfänger auf ein- und demselben LAN bestimmt ist, nicht weiterzuleiten, nennt man Filtering. Wird ein Datenpaket an ein anderes Zielnetz weitergeleitet, so heißt dies Forwarding.

Die Zieladresse kann allerdings auch in keiner Tabelle der Bridge verzeichnet sein. In diesem Fall wird das Datenpaket an alle angeschlossenen LAN's weitergeleitet. Diesen Vorgang nennt man Broadcast. Wird die Zielstation erreicht, so sendet sie i.d.R. ein Bestätigungspaket, durch das die Bridge die Adresstabelle vervollständigen kann.

Damit die Adresslisten aktuell bleiben, d.h. keine Adressleichen oder falsche Einträge z.B. nach Umkonfigurationen enthalten, wird ein Aging-Verfahren angewendet. Hierbei werden Adressen, die länger als z.B. 10 Minuten nicht mehr angesprochen wurden aus der Adressliste gelöscht.

Der Store-and-Forward-Mechanismus der Bridges stellt für Protokolle, die Bestätigungspakete des Empfängers versenden, z.B. TCP oder IPX, ein zeitliches Problem dar, da für die Zwischenspeicherung der Daten relativ viel Zeit benötigt wird. Im interaktiven Betrieb ist die Latenzzeit entscheidend. Dies ist die Zeit, die vergeht, bis das erste Bit eines Datenpakets von Eingangsport der Bridge zum Ausgangsport transferiert ist. Sie beträgt zwischen $150\,ms$ und $300\,ms$. Bei einem Novell-Client, der über IPX mit einem Novell-Server verbunden ist, kann über 5 Bridges mit je $200\ ms$ Latenzzeit eine Übertragungszeit von $2\ s$ pro Datenpaket entstehen. Dies ist aber in vielen interaktiven Anwendungen, z.B. Multimedia-Applikationen, nicht mehr tragbar.

Switch:

Switches sind historisch aus Bridges hervorgegangen. Ihr Einsatzgebiet ist aber von dem von Bridges verschieden. Bridges arbeiten i.a. von der Annahme ausgehend, dass ca. 80% des Datenverkehrs innerhalb der angeschlossenen LAN's lokal ist und nur ca. 20% an ein anderes Netz geleitet werden müssen. Über einem Switch läuft i.d.R. der gesamte Datenverkehr, d.h. auch der zwischen den Stationen innerhalb ein- und desselben LAN. Im Extremfall eines sog. Workgroup-Switch existiert für jeden angeschlossenen Rechner ein separater Port im Switch. Switches haben also i.d.R. wesentlich mehr Ports als Bridges, z.B. 16 oder 128 statt 2 oder 4.

Man unterscheidet Software-Switches und Hardware-Switches. Während Software-Switches meist mit programmierten Standard-Risc-Prozessoren arbeiten, verfügen Hardware-Switches über ASIC's (Application Specific Integrated Circuit), bei denen Programme in Hardware umgesetzt sind. Daher sind Hardware-Switches wesentlich schneller als Software-Switches. Außerdem verfügen Software-Switches über weniger Ports als Hardware-Switches.

Weiterhin unterscheidet man Cut-Through-Switches und Store-and-Forward-Switches. Während die Übertragung eines Datenpakets bei Cut-Through-Switches nach dem Empfang der Zieladresse (6 Byte) bereits beginnt, wird das Datenpaket beim Store-and-Forward-Switch zwischengespeichert, bevor es weitergesendet wird. Cut-Through-Switches haben eine Latenzzeit von $15 - 60\,\mu s$, bei Store-and-Forward-Switches beträgt die Latenzzeit typischerweise zwischen $50\ \mu s$ für 64 Byte große Pakete und $1,2\ ms$ bei 1518 Byte großen Paketen. Der Store-and-Forward-Switch, den man auch als Multiport-Bridge bezeichnet, bietet jedoch gegenüber einem Cut-Through-Switch die Fehlererkennung übertragener Datenpakete. Cut-Through-Switches eignen sich hingegen durch die geringere Latenzzeit in fehlerarmen Netzen und für Echtzeit-Anwendungen.

Router:

Der Broadcast-Verkehr innerhalb eines LAN's kann zu dessen Überlastung führen. Deswegen wurden LAN's bis zum Ende der 80'er Jahre überwiegend durch Bridges in kleinere LAN's aufgeteilt. Beim Ethernet besteht im übrigen eine Höchstgrenze von 1024 Stationen; beim Token-Ring von 256 Stationen. Seit Anfang der 90'er Jahre entstanden durch den Einsatz von Routern große flächendeckende LAN/WAN-Netze mit einer Vielzahl unterschiedlicher Protokolle. Im Unterschied zu einer Bridge arbeitet ein Router auf der Netzwerkebene (ISO-Schicht 3). Seine Hauptaufgabe ist die Wegfindung (Routing) zwischen unterschiedlichen Netzen. Außerdem eignen sich Router zum Verbinden verschiedener Netzwerktopologien wie Ethernet, Token-Ring und FDDI, da sie auf der Netzwerkebene arbeiten. Wichtig ist allerdings, welche Protokolle ein Router unterstützt, da nur diese weitergeleitet werden können. Außerdem sind nicht alle Protokolle routbar:

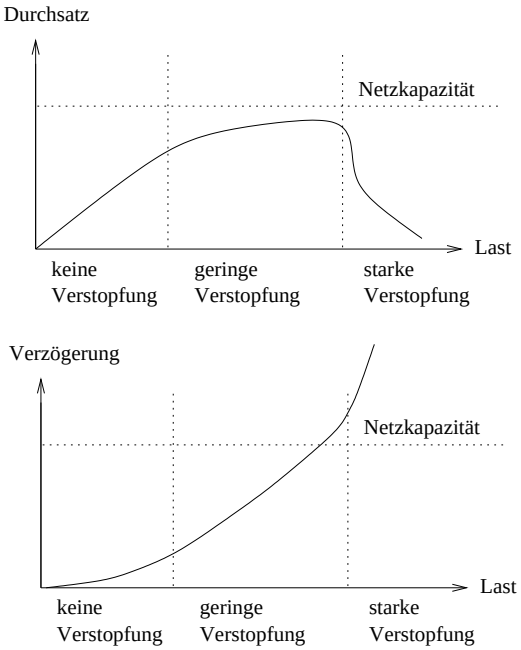
Routbare Protokolle	Nicht-routbare Protokolle
DECnet	LAT
OSI/ISO	SNA
TCP/IP	NetBIOS
XNS	LANManager
IPX	Xodiac
XTP	ARP/RARP

Zur Bestimmung eines möglichst optimalen Weges tauschen Router ihre Informationen über Routing-Protokolle aus. In der TCP/IP-Welt werden hierarchische Routing-Domänen gebildet, wobei die Router innerhalb einer Domäne über ein Interior-Gateway-Protocol (IGP), wie das Routing-Information-Protocol (RIP)

oder Open-Shortest-Path-First (OSPF), Informationen austauschen. Router unterschiedlicher Domänen kommunizieren hingegen über ein Exterior-Gateway-Protocol (EGP), wie EGP oder das Boarder-Gateway-Protocol (BGP). Durch die hierarchische Aufteilung in Domänen reduziert sich der Kommunikationsaufwand zum Austausch der Routing-Informationen erheblich.

5.2 Verstopfung und Flusssteuerung

Da Übertragungskanal und Pufferspeicher immer eine endliche Kapazität haben, kann es bei starker Last zu einer Verstopfung des Netzes kommen. Quantitativ stellt sich dies typischerweise wie folgt dar:



Liegt keine Verstopfung vor, so wächst der Durchsatz nahezu linear mit der Last. Bei geringer Verstopfung wachsen die Verzögerungszeiten dramatisch an. Bei starker Verstopfung fällt sogar der Durchsatz stark ab. Um Verstopfung zu vermeiden, wird die Flusssteuerung eingesetzt. Sie ermöglicht eine Begrenzung der Last und verhindert, dass ein Empfänger durch den Sender überlastet wird.

Die meist benutzte Flusssteuerungstechnik ist das Automatic-Repeat-Request (ARQ). Hierbei kann der Empfänger bei Überlastung oder Datenverlust den Sender zu einer Drosselung der Datenrate auffordern. Es gibt drei ARQ-Versionen:

Stop-and-Wait-Verfahren:

Dies ist das einfachste ARQ-Verfahren. Der Sender überträgt ein Datenpaket und wartet auf eine positive oder negative Bestätigung durch den Empfänger. Negative Bestätigungen werden vom Empfänger bei Fehlern im Datenpaket oder bei Erreichen einer Zeitschranke (Timeout) z.B. bei Verstopfung verschickt. Der Sender überträgt das Datenpaket erneut oder er sendet das nächste Datenpaket. Dieses Verfahren ist für hohe Datenraten und hohe Signallaufzeiten (z.B. Satellitenstrecken) ungeeignet.

Go-Back-N-Verfahren:

Dieses Verfahren wird häufig eingesetzt (z.B. HDLC). Der Sender wartet hier nicht nach jedem Datenpaket auf eine Bestätigung, sondern es dürfen bis zu N Pakete hintereinander ohne Bestätigung verschickt werden. Das (k+N)-te Paket kann allerdings nur gesendet werden, wenn eine positive Bestätigung für das k-te Paket erhalten wurde. Wird eine negative Bestätigung im Sender erhalten, so werden alle Pakete ab dem fehlerhaften erneut versendet. Dies können maximal N sein. Daher stammt der Name des Verfahrens.

Selectiv-Repeat-Verfahren:

Dieses Verfahren ist eine Verbesserung von Go-Back-N bzgl. des erreichbaren Durchsatzes. Hier werden nur die Pakete wiederholt übertragen, deren Bestätigung negativ ist oder für die der Timer im Sender abgelaufen ist. Allerdings entsteht zusätzlicher Aufwand bei Selective-Repeat durch den erforderlichen Pufferspeicher für Datenpakete, die während des Wartens auf das wiederholte Datenpaket ankommen. Außerdem muss der Empfänger die Reihenfolge der Datenpakete wiederherstellen.

Nun kann die eigentliche Validierung auf dem Server erfolgen, z.B. durch Abbildung der übermittelten UserID auf einen Nutzernamen in der Datei passwd und Vergleich mit einer Liste zugelassener Nutzer. Eine Funktion zur Nutzervalidierung könnte z.B. wie folgt aussehen:

Kapitel 6

Netzwerk-Sicherheit

6.1 Einführung

Die drei Hauptziele der Netzwerk-Sicherheit sind:

- Wahrung der Vertraulichkeit von Daten: Schutz von Daten vor unberechtigtem Lesen und Abhören
- Wahrung der Integrität von Daten: Sicherung des Originalzustands der Daten mit Schutz gegen Änderungen und Fälschungen
- Überprüfbarkeit der Authentizität von Daten: Nachweis des Ursprungs der Daten

Bei Kenntnis des TCP/IP-Protokolls ist es insbesondere im Internet leicht nachvollziehbar, dass Daten abgehört, Empfänger- und Senderadressen gefälscht, Paketinhalte verändert und gefälschte Pakete ins Internet eingespeist werden können. Diese Angriffe können potentiell in jeder Zwischenstation ausgeführt werden. Neben kryptografischen Verfahren verwendet man standardmäßig Firewalls, um die oben angegebenen Ziele zu erreichen.

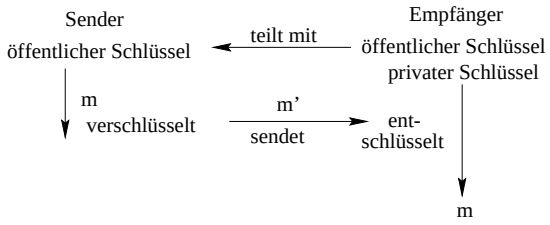
6.2 Kryptografi sche Verfahren

Kryptografische Verfahren werden eingesetzt, um die Vertraulichkeit von Kommunikationsdaten zu wahren und um deren Integrität und Authentizität zu überprüfen. Die Vertraulichkeit wird durch Verschlüsselung der Daten erreicht.

Man unterscheidet zwischen symmetrischen und asymmetrischen Verschlüsselungsverfahren:

Bei symmetrischen Verfahren benutzen Sender und Empfänger den selben Schlüssel zur Ver- und Entschlüsselung der Daten. Die Schlüssel müssen bei den symmetrischen Verfahren also geheim bleiben, d.h. sie dürfen nicht in die Hände dritter gelangen. Hierdurch stellt sich insbesondere das Problem der Schlüsselverteilung und -verwaltung. Das Verfahren DES (Data Encryption Standard) ist ein Beispiel für ein symmetrisches Verschlüsselungsverfahren.

Bei asymmetrischen Verfahren benutzt der Sender zur Verschlüsselung einen anderen Schlüssel als der Empfänger zur Entschlüsselung. Hierbei wird dem Sender der Sendeschlüssel vom Empfänger mitgeteilt. Er ist nicht geheim und wird daher als öffentlicher Schlüssel bezeichnet. Der Empfangsschlüssel zur Entschlüsselung darf nur dem Empfänger der Nachricht bekannt sein und wird daher als privater Schlüssel bezeichnet. Die Sicherheit der asymmetrischen Verfahren beruhen darauf, dass es nahezu unmöglich ist, aus einem bekannten öffentlichen Schlüssel den zugehörigen privaten Schlüssel zu ermitteln, d.h. dies ist nur mit extrem hohem Rechenaufwand möglich. Das Verfahren RSA (benannt nach den Entwicklern Rivest, Shamir und Adleman) ist ein Beispiel für ein asymmetrisches Verschlüsselungsverfahren.



Verschlüsselung spielt im Internet eine große Rolle. Wenn z.B. mehrere Firmenstandorte über das Internet miteinander verbunden sind, ist es unumgänglich, die Daten zu verschlüsseln, um Vertraulichkeit zu erreichen. In diesem Zusammenhang spricht man von einem Virtual Private Network (VPN). Weiterhin sind asymmetrische Verschlüsselungsverfahren die Grundlage für die Authentifizierung von Kommunikationspartnern. Hierbei wird eine Nachricht (Zertifikat s.u.) - umgekehrt wie im bisher geschilderten - mit dem privaten Schlüssel verschlüsselt und mit dem öffentlichen Schlüssel entschlüsselt.

Die Integrität der übermittelten Daten wird i.d.R. durch den Einsatz von Hashfunktionen überprüft. Eine Hashfunktion ermittelt aus einer Kette von Eingabezeichen variabler Länge einen Ausgabewert fester Länge. Der Hashwert stellt so etwas wie einen Fingerabdruck der Nachricht dar. Im Sender wird nun ein Hashwert aus der zu sendenden Nachricht berechnet und mit der Nachricht an den Empfänger übermittelt. Im Empfänger wird dann wieder aus der empfangenen Nachricht ein Hashwert ermittelt und mit dem übermittelten Hashwert des Senders verglichen. Sind die beiden Hashwerte gleich, so stimmen die empfangene Nachricht

und die gesendete Nachricht mit hoher Wahrscheinlichkeit überein. Ansonsten ist die Nachricht sicher verfälscht. Ein häufig verwendeter Hash-Algorithmus ist z.B. MD5 (Message Digest 5).

Zur Überprüfung der Authentizität einer Nachricht werden häufig Hashfunktionen in Kombination mit asymmetrischen Verschlüsselungsverfahren verwendet (z.B. bei den Protokollen SSL und TLS). Hierbei werden sogenannte Zertifikate verwendet, durch die ein Sender einer Nachricht identifiziert werden kann.

Der Public-Key-Algorithmus RSA

Als Beispiel für einen Public-Key-Algorithmus soll RSA betrachtet werden.

- Zunächst wählt man zwei beliebige aber große Primzahlen $p \neq q$ und berechnet $n = p * q$.
- Dann berechnet man zwei Zahlen e, d mit $e * d = 1\, mod\, ((p-1) * (q-1))$. (Hierfür gibt es einen effizienten Algorithmus.) Also gilt $e * d = k * (p - 1) * (q - 1) + 1$.
- Man kann nun zeigen, dass für $0 \leq m \leq n - 1$ gilt $m^{e*d} = m\ mod\ n$.
- Nun wird m als die zu übermittelnde Nachricht aufgefasst. Der öffentliche Schlüssel kann aus dem Zahlenpaar e, n und der geheime Schlüssel aus der Zahl d gebildet werden.
- Die Verschlüsselungsfunktion lautet: $m^{'} = m^e\ mod\ n$.
- Die Entschlüsselungsfunktion lautet: $m = (m^{'})^d\ mod\ n$.

Die Sicherheit dieses Verfahrens liegt in der Schwierigkeit, die Faktorisierung von n als Produkt zweier Primzahlen zu bestimmen. Dies ist allerdings nur für große n bzw. p, q genügend sicher. p, q sollten mindestens in der Größenordnung von 10^{100} liegen.

Bei erfolgreicher Faktorisierung von $n = p * q$ kann ein Angriff auf das RSA-Verfahren wie folgt gestartet werden. Der Sender kann aus dem öffentlichen Schlüssel e, n den geheimen Schlüssel d bestimmen, indem er $n = p * q$ faktorisiert und dann $(p - 1) * (q - 1)$ errechnet. Mit Hilfe von e und der Gleichung $e * d = 1$ mod $((p - 1) * (q - 1))$ kann er dann den geheimen Schlüssel d bestimmen.

Übrigens muss d groß gewählt werden, denn sonst kann d durch Einsetzen von Zahlen t in die Gleichung $m^{e*t} = m\ mod\ n$ erraten werden.

Wir wollen das RSA-Verfahren einmal an einem Beispiel durchspielen. Da es hierbei nur auf das Rechenprinzip ankommt, wählen wir zwei kleine Primzahlen p, q, damit die Rechnung besser nachvollzogen werden kann:

- $n = 33 = 3 * 11 = p * q$
- $(p-1) * (q-1) = 2 * 10 = 20$
- Nun wird d bestimmt, wobei es kein Teiler von $(p-1) * (q-1)$ sein darf. Jede Primzahl, die größer als p und q ist erfüllt diese Forderung: $d = p^{'} > max(p,q)$. Wir wählen z.B. $d = 13$.
- Nun wird e bestimmt aus $e * 13 = x * 20 + 1$. Wir wählen z.B. $e = 17$ bei $x = 11$.
- $e = 17,\ n = 33$ ist nun öffentlicher Schlüssel.
- $d = 13$ ist nun privater Schlüssel.
- Jede Nachricht $0 \leq m \leq 32$ kann nun verschlüsselt und entschlüsselt werden. Wir wählen z.B. $m = 2$. Dann gilt:
  - $m^{'} = 29 = 2^{17}\ mod\ 33$
  - $m = 2 = 29^{13}\ mod\ 33$

Wenn die zu übermittelnden Nachrichten mehr als $n-1$ unterschiedliche Werte annehmen können, werden sie in kleinere Mengen aufgeteilt, die weniger als $n-1$ unterschiedliche Werte annehmen und mehrfach versendet.

6.3 Kryptografi sche Protokolle

Kryptografische Protokolle implementieren die kryptografischen Algorithmen auf verschiedenen Ebenen des Protokollstapels; so gibt es z.B. anwendungsbezogene und anwendungsunabhängige kryptografische Protokolle.

6.3.1 Secure Socket Layer (SSL)

SSL wurde von Netscape ursprünglich für den sicheren Datenaustausch zwischen einem Browser und einem Web-Server entwickelt. Es handelt sich bei SSL jedoch nicht um ein anwendungsspezifisches Verfahren wie z.B. Pretty Good Privacy (PGP), d.h. SSL kann für verschiedene Dienste eingesetzt werden. SSL setzt direkt auf der TCP-Ebene von TCP/IP auf.

Bei SSL können verschiedene kryptografische Verfahren (z.B. Hash-Funktionen SHA, MD5 und symmetrische und asymmetrische Verschlüsselung DES, RC4, RSA, DSS) eingesetzt werden. Die einzusetztenden Verfahren handeln Client und

Server vor der Datenübertragung in einem Protokoll dynamisch miteinander aus. Zur Überprüfung der Integrität werden Hash-Funktionen eingesetzt.

SSL verwendet immer eine Kombination eines asymmetrischen und eines symmetrischen Verschlüsselungsverfahrens. Mit Hilfe des asymmetrischen Verfahrens wird ein Schlüssel ausgetauscht, der dann zur symmetrischen Verschlüsselung der zu übertragenden Daten verwendet wird. Daten werden symmetrisch verschlüsselt, da dies wesentlich Laufzeit-effizienter ist als bei asymmetrischer Verschlüsselung.

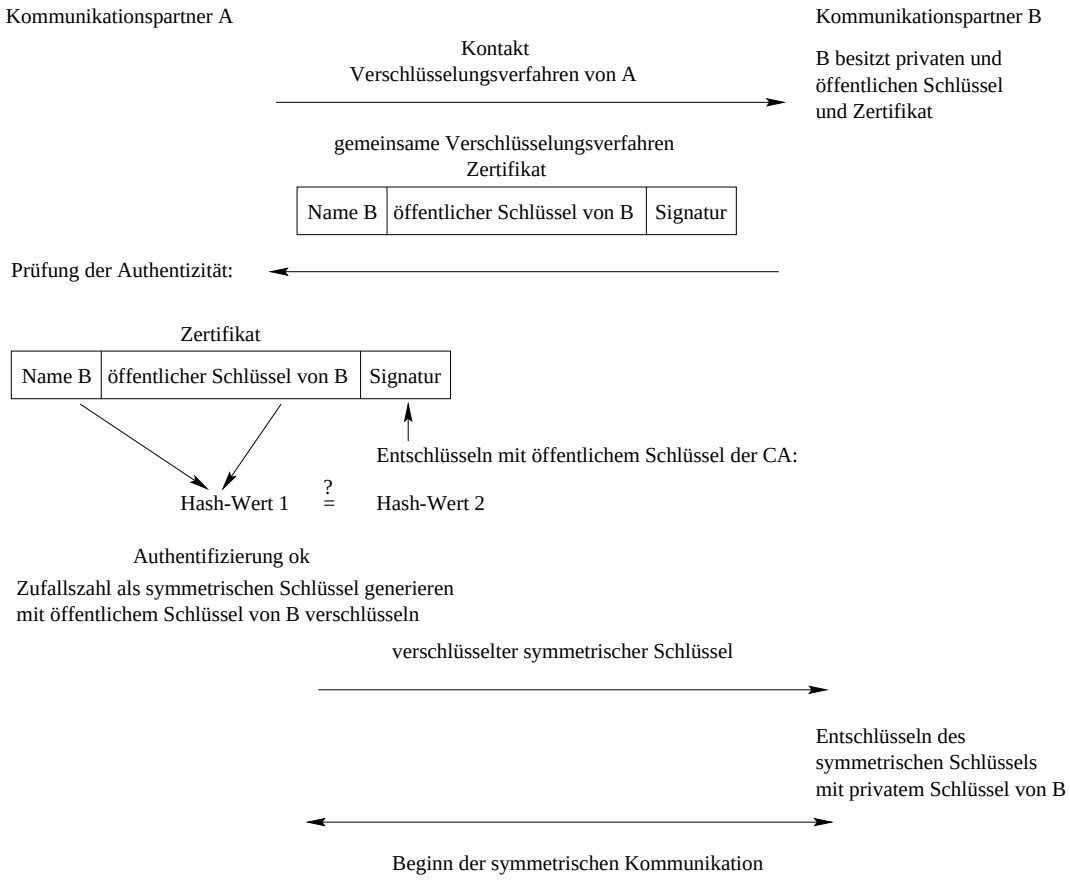
Zur Authentifizierung des Gegenübers, d.h. sowohl des Servers durch den Client als auch des Clients durch den Server, kann ein Zertifizierungsverfahren eingesetzt werden. Meistens wird heute die Authentifizierung des Servers durch den Client praktiziert, aber auch Clients werden zunehmend mit Zertifikaten zur Authentifizierung ausgestattet.

Mit Hilfe eines Zertifikats kann eindeutig festgestellt werden, ob ein öffentlicher Schlüssel von einem bestimmten Kommunikationspartner stammt. Ein Zertifikat besteht aus dem Namen des Teilnehmers und seinem öffentlichen Schlüssel. Es wird auf Anfrage von einer Zertifizierungsstelle (Certificate Authority oder Trust Center) ausgestellt. Dabei beglaubigt die Zertifizierungsstelle das Zertifikat mit ihrer elektronischen Unterschrift. Dies geht wie folgt: Aus dem öffentlichen Schlüssel und dem Namen des Kommunikationspartners wird ein Hash-Wert berechnet. Dieser Hash-Wert wird mit dem privaten Schlüssel der Zertifizierungsstelle verschlüsselt. Das Ergebnis dieser Verschlüsselung nennt man Signatur oder Unterschrift. Diese Signatur wird an Namen und öffentlichen Schlüssel angehangen, wodurch das ganze Dokument zu einem Zertifikat wird.

Die Prüfung der Authentitzität eines Kommunikationspartners geschieht nun wie folgt: Der Partner sendet das Zertifikat mit seinem öffentlichen Schlüssel. Nun soll festgestellt werden, ob das Zertifikat echt ist, d.h. ob der öffentliche Schlüssel zu dem angegebenen Partner gehört. Dazu wird aus dem Namen und dem öffentlichen Schlüssel mit dem gleichen Algorithmus wie bei der Zertifizierungsstelle wieder der Hash-Wert berechnet. Anschließend wir die Signatur mit dem öffentlichen Schlüssel der Zertifizierungsstelle entschlüsselt. Stimmt das Ergebnis dieser Entschlüsselung mit dem errechneten Hash-Wert überein, so ist der Kommunikationspartner authentifiziert; ansonsten ist er nicht authentifiziert. Der öffentliche Schlüssel der Zertifizierungsstelle muss dem Authentifizierer also bekannt sein. Im Netscape-Browser sind z.B. bereits die öffentlichen Schlüssel der am häufigsten genutzten Zertifizierungsstellen fest verzeichnet.

Das folgende Bild zeigt den Aufbau einer Verbindung mit SSL: A sendet beim Kontakt mit B seine verfügbaren symmetrischen Verschlüsselungsverfahren. B wählt aus diesen Verfahren eins aus und sendet es zusammen mit dem Zertifikat an A. A prüft wie oben beschrieben die Authentizität von B. Schlägt die Überprüfung der Authentizität fehl, so wird die Verbindung abgebrochen. Nur wenn

diese Überprüfung erfolgreich verläuft, generiert A eine Zufallszahl, die mit dem öffentlichen Schlüssel aus dem Zertifikat verschlüsselt und an B gesendet wird. Diese Zufallszahl wird dann von B mit seinem privaten Schlüssel entschlüsselt, so dass beide Partner im Besitz einer geheimen Zufallszahl sind, die den Schlüssel zur symmetrischen Verschlüsselung darstellt.



B kann mit A also nur dann kommunizieren, wenn B im Besitz des privaten Schlüssels zu dem im Zertifikat gespeicherten öffentlichen Schlüssel ist und wenn das Zertifikat bei einer Zertifizierungsstelle beglaubigt wurde.

6.3.2 Pretty Good Privacy (PGP)

PGP dient zur sicheren Übertragung von Electronic Mail. Es handelt sich also um ein anwendungsspezifisches Protokoll. Zur Schlüsselverwaltung verwendet PGP

das RSA-Verfahren. Zur Verschlüsselung der Daten wird der symmetrische IDEA-Algorithmus verwendet. Zum Erstellen eines Fingerabdrucks eines öffentlichen RSA-Schlüssels wird das Hash-Verfahren MD5 verwendet.

Die Vorarbeiten für eine sichere Verbindung über Electronic Mail sehen für zwei Benutzer wie folgt aus:

- Beide Benutzer generieren öffentliche und private RSA-Schlüssel durch den Befehl:

  ```
  pgp -kg
  ```

- Beide Benutzer extrahieren ihren öffentlichen RSA-Schlüssel in eine ASCII-Datei, z.B. mit dem Namen pubkey.asc:

  ```
  pgp -kxa <EMail-Empfängername> pubkey.asc
  ```

- Beide Benutzer senden sich den öffentlichen Schlüssel des jeweils anderen Benutzers zu:

  ```
  mail <EMail-Empfängername> -s “PGP-Schlüssel” < pubkey.asc
  ```

- Beide Benutzer fügen den öffentlichen Schlüssel des anderen ihrem Schlüsselbund öffentlicher Schlüssel hinzu:

  ```
  pgp -ka pubkey.asc
  ```

- Beide Benutzer lassen sich einen Fingerabdruck des öffentlichen Schlüssels ausgeben und verifizieren ihn auf Richtigkeit z.B. durch gegenseitige Bestätigung per Telefon:

  ```
  pgp -kvc <EMail-Empfängername>
  ```

- Nach der Bestätigung des Fingerabdrucks unterschreiben beide Benutzer den öffentlichen Schlüssel des anderen mit ihrem privaten Schlüssel. Nur ein unterschriebener öffentlicher Schlüssel kann zur Sendung verwendet werden:

  ```
  pgp -ks <EMail-Empfängername>
  ```

- Ab jetzt können sich die Benutzer verschlüsselte und ggfs. unterschriebene Mails zusenden. Die folgende Anweisung erzeugt z.B. aus der Datei mit dem Namen Brief eine mit dem privaten Schlüssel des Senders unterschriebene und mit dem öffentlichen Schlüssel des Empfängers verschlüsselte Datei mit dem Namen Brief.asc:

```
pgp -esa Brief <EMail-Empfängername>
```

- Mit folgender Anweisung wird die Datei Brief.asc übertragen:

```
mail <EMail-Empfängername> -s “Brief.asc” < Brief.asc
```

- Beim Empfänger wird die Unterschrift des Senders authentifiziert und die Mail mit dem privaten Schlüssel des Empfängers durch folgenden Befehl entschlüsselt. Die unverschlüsselte Mail steht in einer Datei mit dem Namen Brief.

```
pgp Brief.asc
```

Neben der direkten Handhabung mit dem Kommando pgp wird Pretty Good Privacy auch von Mail-Clients wie kmail von KDE unterstützt. Im Gegensatz zu SSL gibt es bei PGP keine zentralen Instanzen zur Zertifizierung von Schlüsseln, sondern die Benutzer unterzeichnen ihre öffentlichen Schlüssel gegenseitig und schaffen so eine Gemeinschaft von vertrauenswürdigen Benutzern:

So kann der Benutzer C z.B. das Zertifikat des Benutzers B anerkennen, wenn es vom Benutzer A unterschrieben ist, ohne dass Benutzer C und B sich direkt kennen. Benutzer C vertraut dann der von ihm mit Hilfe des öffentlichen Schlüssels von A verifizierten Unterschrift von A im Zertifikat von B. Es ergibt sich eine Transitivität im Vertrauensgeflecht (Web of Trust).

6.3.3 Secure Shell (SSH)

Die Secure Shell (SSH) ist ein weiteres Beispiel für ein anwendungsspezifisches Protokoll. SSH ist als Verbesserung des telnet-Terminalprotokolls entstanden, da telnet alle Daten also auch Passworte unverschlüsselt über den Kommunikationskanal sendet. SSH ist auf UNIX- und Linux-Systemen weit verbreitet.

SSH arbeitet mit dem Public-Key-Verfahren RSA ähnlich wie PGP. Jeder Server, d.h. Rechner auf dem ein sshd-Dämonprozess läuft, besitzt ein RSA-Schlüsselpaar aus öffentlichem und privatem Schlüssel, durch den der Rechner identifiziert wird. Weiterhin wird bei jedem Start des sshd-Dämons ein dämonspezifisches Schlüsselpaar generiert.

Wenn ein ssh-Clientprozess sich mit dem sshd-Serverprozess verbinden möchte, sendet sshd den öffentlichen Rechner- und Dämon-Schlüssel an den Client ssh. Jeder Client besitzt eine Datenbank mit den öffentlichen Schlüsseln der Rechner, mit denen er bereits Kontakt hatte. ssh sucht den empfangenen Rechner-Schlüssel mit der Datenbank. Falls er nicht gefunden wird, muss die Aufnahme des Schlüssels in die Datenbank vom Benutzer bestätigt werden, um mit dem Rechner in

Kontakt treten zu können. Dann generiert der ssh-Client eine Zufallszahl, die er als Sitzungsschlüssel mit den öffentlichen Rechner- und Dämon-Schlüsseln verschlüsselt und an den sshd-Server sendet. Der sshd-Server entschlüsselt den Sitzungsschlüssel mit seinen privaten Rechner- und Dämon-Schlüsseln. Die weitere Kommunikation findet nun mit Hilfe dieses Sitzungsschlüssels mit einem symmetrischen Verschlüsselungsverfahren statt.

Nach dem Aufbau der symmetrisch verschlüsselten Verbindung zwischen ssh-Client und sshd-Server findet die Authentifizierung des ssh-Client durch den sshd-Server statt. Hier kann die normale Passwort-Abfrage oder eine Authentifizierung über ein RSA-Verfahren gewählt werden. Ein Vorteil der Authentifizierung mit RSA ist, dass die Eingabe eines Passwortes entfallen kann.

Zur Authentifizierung mit RSA generiert der Benutzer einmalig auf dem Client-Rechner einen privaten und öffentlichen RSA-Schlüssel und kopiert den öffentlichen RSA-Schlüssel in das Heimat-Verzeichnis auf dem Server-Rechner. Die Authentifizierung verläuft wie folgt: Der ssh-Client sendet seinen öffentlichen Schlüssel an den sshd-Server. Wenn dieser Schlüssel auf dem Server-Rechner verzeichnet ist, sendet der sshd-Server eine Zufallszahl an den ssh-Client zurück, die er mit dem öffentlichen Schlüssel verschlüsselt. Der ssh-Client entschlüsselt diese Zufallszahl mit seinem privaten Schlüssel und berechnet mit dem MD5 Hash-Verfahren einen Fingerabdruck der Zufallszahl, die er an den sshd-Server wieder zurücksendet. Der sshd-Server berechnet ebenfalls mit dem MD5 Verfahren den Fingerabdruck der Zufallszahl und vergleicht ihn mit dem empfangenen Fingerabdruck. Wenn beide übereinstimmen ist der Benutzer authentifiziert und erhält Zugang zum Server-Rechner.

Es wird ein Fingerabdruck der Zufallszahl anstatt der Zufallszahl selber verschickt, um Angriffen vorzubeugen. Sonst wäre es möglich aufgrund der Kenntnis (z.B. durch Abhören) der Zufallszahl, die zu einer verschlüsselten Zufallszahl gehört, und Senden dieser Zufallszahl Zugang zum Rechner zu bekommen (chosen-plaintext attack).

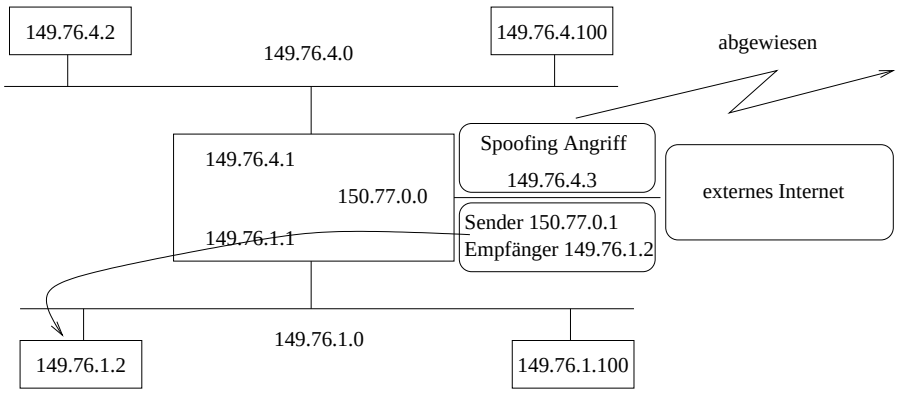
6.4 Firewalls

Neben den Verschlüsselungsverfahren werden Firewalls bestehend aus Paketfiltern (Router) und Applikationsfiltern (Proxies) eingesetzt.

Paketfilter sind die bekannteste Form einer Firewall. Sie greifen auf der Netzwerkschicht ein und untersuchen IP-Pakete auf Sende- und Empfangs-IP-Adressen sowie Portnummern. Dabei werden IP-Datagramme herausgefiltert, die nicht weitergeleitet werden dürfen.

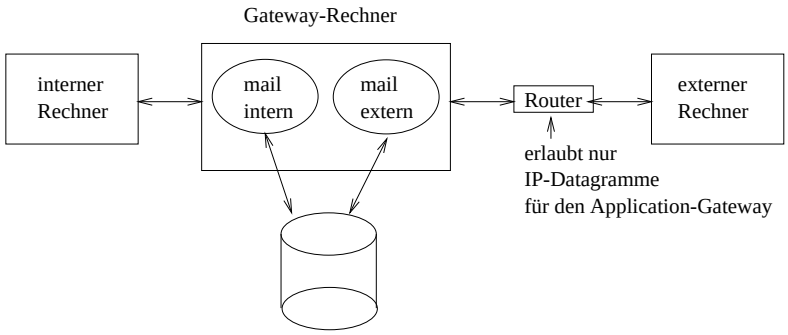
Der Router kann z.B. IP-Datagramme nicht in das interne Netz hinein lassen, wenn sie z.B. eine interne Netzadresse aus dem externen Internet vortäuschen.

Es werden also sogenannte Spoofing-Angriffe abgefangen. Weiterhin kann der Router z.B. bestimmte externe IP-Datagramme in ein bestimmtes internes Netzsegment hinein lassen.



Application-Gateways werden durch Proxy-Prozesse realisiert, die einen direkten Zugriff auf oder aus dem Internet vom internen Netz verhindern. Sie fungieren dabei als eine Art Relaisstation, die den Zugriff auf das Internet oder interne Netz für den Benutzer übernimmt. Weit verbreitet sind hierbei, z.B. Mail-Gateways und Webserver-Proxies.

In Kombination mit Paketfiltern lässt sich ein internes Netz vom Internet abschotten, indem der Router nur Pakete in das interne Netz hinein lässt, die auf einen Application-Gateway-Rechner gerichtet sind.



Literaturverzeichnis

[1] Tanenbaum, Andrew S.: Computernetzwerke; 4.Aufl.;Pearson Studium; 2003

[2] Comer, Douglas E.; Computernetzwerke und Internets mit Internet-Anwendungen; Pearson Studium; 2001

[3] Schneier, Bruce; Angewandte Kryptographie; Addison Wesley; 1996

[4] W.R. Stevens; UNIX network programming; Prentice Hall, Englewood Cliffs, 1990