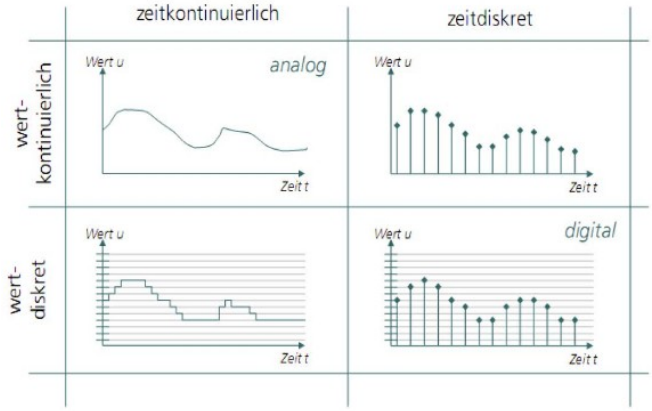
Telematik Zusammenfassung

Einführung Kommunikationsbasiskonzepte

- Signalklassen



- Das Sampling Theorem
Das Samplingtheorem beschreibt die Notwendigkeit der hohen Frequenz der Abtastrate. Diese sollte immer mindestens doppelt so hoch sein wie die Frequenz des abzutastenden Signals.

- Signal-to-Noise Ratio
Das Signal-to-Noise Ratio ist die Störung im Signal. Diese wird durch dB gemessen und ergibt sich aus dem Verhältnis von der Signalspannung und der Störspannung, zum Logarithmus mal 20: $20 \cdot \log(\frac{U_S}{U_N})$

Modelle der Digitalen Kommunikation

- Layer Architecture / model

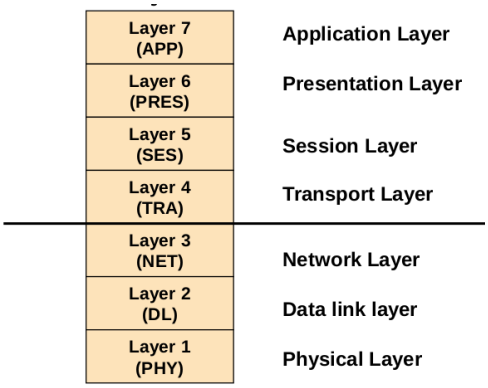
Die Schichtenarchitektur beschreibt eine Art Zwiebelsystem: Die oberen Schichten greifen auf Dienste der unteren Schichten zu, sowie sind Anwendungen, oder Aufgaben, verschiedener Dienste oder Applikationen auf eine festgelegte Schicht begrenzt. Dadurch wird ein komplexes System wartbar.

- Service und Protokolle

1. Service: Abstrakte Funktion, welche für einen Benutzer von außen wie ein eine Art Blackbox aussieht. Meist sind diese „Services“ über mehrere Schichten hinweg implementiert. Beispiel: eMail ist eine Service der mit mehreren Protokollen arbeitet.

2. Protokoll: Ein Protokoll ist nun die Festlegung verschiedener Standards zur Kommunikation, also auch deren Syntax, Semantik und Synchronisation. Meist sind diese Protokolle schon hardwaremäßig implementiert, kann aber auch eine Kombination aus Software und Hardware sein. Auf der untersten Schicht beschreibt ein Protokoll das verhalten der Kommunikationshardware. Einfache Beispiele dafür sind Multiplexing/Demultiplexing, sowie Routing.

- Das OSI-Schichtenmodell



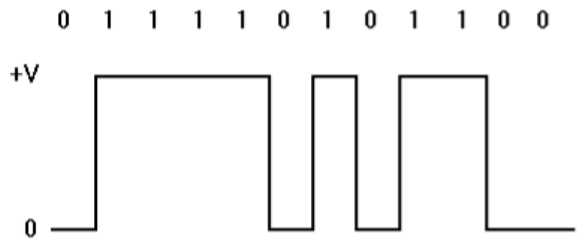
Das OSI-Schichtenmodell wurden 1983 entworfen, um einen Standard für die Kommunikation zu schaffen. Hierbei wurde die Entwicklung des Internets aber noch nicht mit bedacht, wodurch in der heutigen Zeit das OSI-Schichtenmodell, im Bezug auf das Internet, verkleinert werden muss. Es entfällt die Session und Presentation-Schicht. Diese sind direkt in die jeweilige Ebene darüber, oder darunter eingeordnet. Zum Beispiel wird die Transport- und Session-Schicht im Falle von TCP zusammengefasst, da TCP beide Schichten abdeckt. Das Gleiche ist bei der Presentation-Schicht, diese wird meist mit der Applikations-Schicht zusammengelegt.

OSI Model				
Layer		Protocol data unit (PDU)	Function[3]	Examples
Host layers	7. Application	Data	High-level APIs, including resource sharing, remote file access, directory services and virtual terminals	TLS, FTP, HTTP, HTTPS, SMTP, SSH, Telnet
	6. Presentation		Translation of data between a networking service and an application; including character encoding, data compression and encryption/decryption	CSS, GIF, HTML, XML, JSON, S/MIME,
	5. Session		Managing communication sessions, i.e. continuous exchange of information in the form of multiple back-and-forth transmissions between two nodes	RPC, SCP, NFS, PAP,
	4. Transport	Segment (TCP) / Datagram (UDP)	Reliable transmission of data segments between points on a network, including segmentation, acknowledgement and multiplexing	NBF, TCP, UDP
Media layers	3. Network	Packet	Structuring and managing a multi-node network, including addressing, routing and traffic control	AppleTalk, ICMP, IPsec, IPv4, IPv6
	2. Data link	Frame	Reliable transmission of data frames between two nodes connected by a physical layer	IEEE 802.2, L2TP, LLDP, MAC, PPP, ATM, MPLS
	1. Physical	Bit	Transmission and reception of raw bit streams over a physical medium	DOCSIS, DSL, Ethernet physical layer, ISDN, USB

- Codierungen auf der ersten Schicht

Auf der ersten Schicht wird mit mehreren Codierungen gearbeitet, die Häufigsten sind NRZ, NRZI und Manchester.

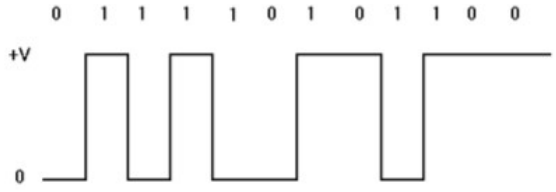
NRZ:



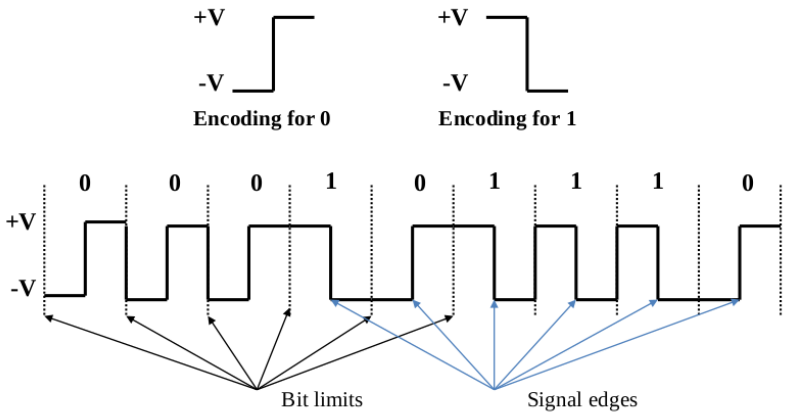
- Einfache Implementierung
- Effiziente Bandbreitennutzung
- Viele folgende Nullen können nicht richtig, oder falsch erkannt werden
- Hohes Gleichstromlevel ½ Vmax

NRZI:

NRZI ist eine Weiterentwicklung von NRZ welches auf das Synchronisationsproblem zielt. Mit ihm kann man nun Ketten von Einsen erkennen, leider aber noch keine Ketten von Nullen. Auch wird hier nur eine Eins erkannt wenn ein Spannungswechsel anliegt, also von 0 → 1 oder 1 → 0.



Manchester Codierung:

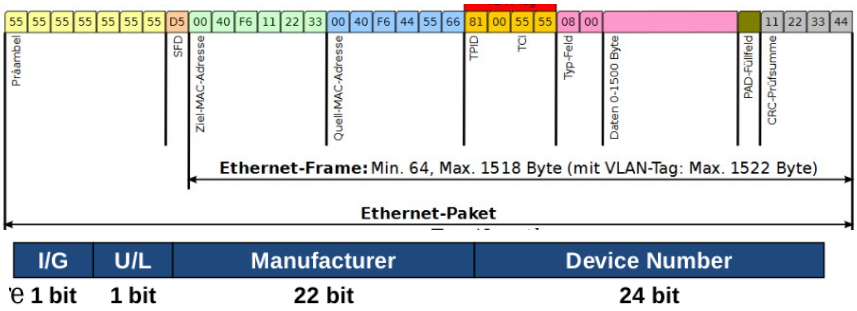


Die Manchester Codierung nun löst das Problem der Synchronisation und somit auch das der Ketten von Einsen und Nullen, jedoch zu lasten der Bandbreite. Diese ist bei Manchester nur halb so groß wie bei den vorherigen Codierungen. Heutzutage wird diese Codierung aber in 10/100 Ethernet benutzt. Bei neueren Standards, wie Ethernet 1000 oder höher, kommen andere Codierungen wie B4/B5 zum Einsatz.

- CSMA/CD

Das Carrier-Sense-Multiple-Access / Collision Detection Protokoll ist nun der Versuch einen geregelte Zugriff auf ein Transportmedium, zum Beispiel das Ethernet, zu gewährleisten. Bei diesem Protokoll hört die Station, welche senden mag, das Medium erst ab, bevor es den Sendevorgang startet. Ist das Medium frei, sendet es sein Paket. Da nun das Paket (Signal) eine gewissen Zeit, durch Ausbreitung des Signals, benötigt, kann es vorkommen das eine zweite Station, welche auch das Medium abhört, gleichzeitig ein Paket verschickt. Dadurch kommt es zu einer Kollision, welche im Grunde nur eine Aufsummierung der Signale nun ist. Erkennt nun eine Station, meist die die zuletzt zu senden angefangen hat, eine solche Kollision, verschickt es direkt ein Jamming-Signal an alle anderen Station, woraufhin alle direkt aufhören zu senden. Nach dem Erhalt dieses Jamming-Signals beginnt jede Station mit dem „Binary Exponential Backoff“ Algorithmus, welche einfach nur aus einer Menge, welche bis zum 16ten Schritt immer weiter vergrößert wird, von Zufallszahlen, aus und multipliziert diese mit 51,2 Mikrosekunden. Woher kommen nun diese 51,2 Mikrosekunde? Diese kommen von der doppelten Round Trip Time der

Signallaufzeit und einer Rechnung der minimalen Ethernet-Framegröße. CSMA/CD funktioniert auf einer Länge von 2500m, wodurch ein Signal ca 13,9 Mikrosekunden braucht, um von einer Station zu der anderen zu gelangen. Jedoch muss auch die Antwortzeit, welche auch wieder 13,9 Mikrosekunden beträgt, bedacht werden. Zusammen ergibt dies dann 27,8 Mikrosekunden, welche nun die Round Trip Time ist. Nimmt man diese nun mal 2, um Fehler auszuschließen, käme man auf 55,6 Mikrosekunden. Da unser Ethernet Frame aber nur eine minimale Größe von 512 Bit (64 Kbytes) hat, wird eine RRT von 51,2 Mikrosekunden, bei 10 Mbits, angenommen. Somit sind Kollisionen, bei dem Übertragen eines Frames, ausgeschlossen, da das Medium die ganze Zeit belegt ist und kein weiteres, neues Ethernet Frame, von einer Station, gesendet werden kann.



Übertragungsmedien, BUS-Topologien und Inter-Networking

- Der Ethernet-Standart IEEE802.3

Der heutige Ethernet-Standart wurde von XEROX in den 1972 Jahren entwickelt. Er beschreibt die Verbindung zweier Kommunikationspartner mit dem Übertragungsmedium dem „Ether“. Der Name Ethernet kam aber erst 1973 durch den Firmengründer von 3Com zustande. Im laufe der Zeit wurde der Standard immer weiter erweitert, anfänglich bei Übertragungsraten von wenigen Mbits (10), bis zu heutigen Gbits (40 und mehr). Dabei muss man beachten das die verschieden Standards nur eine bestimmte Anzahl an Hosts zulassen, wie zum Beispiel bei 10Base5 an dem nur maximal 100 Teilnehmer dran angeschlossen werden können, bei einer Leitungslänge von 500m, und ein 50Ohm Widerstand zur Terminierung gebraucht wird. Beim 10Base2 sind es maximal 30 Teilnehmer und 185m Kabellänge. Die heutigen, gängigen, Standards sind Fast und Gigabit Ethernet.

- Switching und Routing

Ein wichtiger Bestandteil moderner Kommunikationsmedien sind Switching und Routing. Beide unterscheiden sich in der Funktion grundlegend, sind aber von der Aufgabe her gleich. Beide Verfahren stellen eine gewisse Verbindung zwischen zwei Kommunikationspartner her. Das Switching, in unserem Fall betrachten wir nur das Switching beim Ethernet, arbeitet auf der Layer 2 Schicht, der Sicherungsschicht auch genannt. Er ist eine Art „Weiche“, welche entscheidet, an welchen seiner Ports ein Datenpaket weitergeleitet wird. Dies realisiert er durch MAC-Adresstabellen, in der die zugehörigen MAC-Adressen und die zugehörigen Ports stehen. Werden Pakete „geswitched“, spricht man von Paket-Switching. Beim telefonieren kommt das Circuit-Switching zum Einsatz. Dieses stellt eine Punkt-zu-Punkt Verbindung, also ohne Zwischenpunkte wie es beim Paketswitching ist, zwischen zwei Kommunikationspartner her.

Das Ethernet wird dabei immer in einer Star- oder Bustopologie verbunden, wodurch es zu einigen Problemen kommen kann. Jeder Switch, oder Router, stellt eine Art physikalische Trennung zweier Netzteile dar, auch „Collision Domains“ genannt, was dazu führt das man auch einen Ring bauen kann, denn wer weiß bei einem großen Netz noch genau ob nicht schon Pakete von dem einen Netz über eine andere Route kommen können? Eigentlich ist der Ansatz der, der das TCP/IP Protokoll ausmacht, jedoch verursacht dies eine Schleife beim Switchen, wodurch ein Paket immer und immer wieder weitergeleitet wird. Um dieses Problem zu lösen gibt es das Spanning Tree Protocol, auch STP genannt. Es ist eine Art „Lernprotokoll“ zwischen Switchen, welches eine Aushandlung zwischen anderen Switches bereitstellt, so das diese bestimmte Ports, welche zu dem Circuit Switching führen können, abstellt. Diese „abgestellten“ Ports heißen dann „Designated Port (s)“, Ports über die der andere Switch, das andere Netz, am schnellsten erreicht werden kann, wozu auch die Bandbreite hinzugezogen wird, heißt „Root Port (s)“.

Router haben für ihre Aufgaben auch bestimmte, festgelegte, Protokolle:

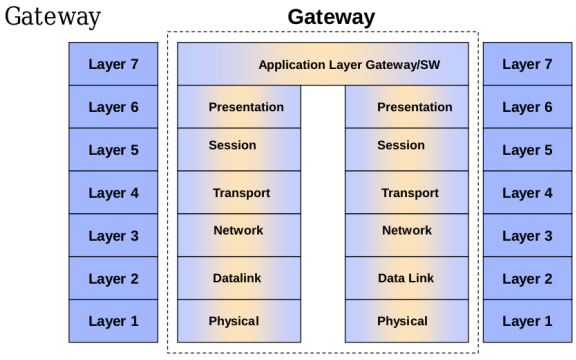
– BGP (Border Gateway Protocol) de-facto standard

– IGRP (Interior Gateway Routing Protocol) by Cisco

– RIP (Routing Information Protocol)

Diese Protokolle beschreiben das Austauschen der angeschlossenen Netzinformationen und der Kosten für bestimmte Routen. Leider haben diese Protokolle bei IPv4 auch einen großen Nachteil, durch sie entstehen sehr große Routing-Tabellen, da jeder Router so viele Informationen über andere Netze sammelt, wie möglich.

Oft werden Router auch als **Gateways** verstanden, was bei heutigen Routern schon oft der Fall ist, jedoch in der Grundlage falsch ist. Gateways sind die Vereinigung aller Schichten, von der Bit-Übertragungsschicht, bis hin zur Applikationensschicht:



Hauptaufgaben eines Gateways sind daher:

– Addressing across network boundaries

– Address mapping

– Protocol conversion

Gerade durch den letzten Punkt, der Protokollkonversation, werden heutige Router als Gateways verstanden.

Internet und IP Security

- Geschichte und Entwicklung des heutigen Internets

Die Geschichte des Internets geht zurück auf das Jahr 1969 mit der Gründung des ARPANET. Es bestand damals aus 4 „Nodes“, also Knoten, nur, welche meist Universitäten waren. Kurze Zeit danach kam schon die eMail-Spezifikation, welche bis heute noch im Einsatz ist. 1974 kam dann das TCP Protokoll, gefolgt von der Teilung in TCP und IP im Jahre 1978. Erst im Jahre 1991 kam dann eine Spezifikation, welche die Welt nachhaltig verändern sollte, das WWW war geboren. Es beschreibt eine Art der Darstellung von Webseiten, wodurch es auch möglich wurde, das weniger Technik visierte das Internet nutzen konnten. Von anfänglichen 130 Seiten 1993, kamen bis 2016 knapp 1 Milliarde Webseiten hinzu. Ebenso wuchs auch der Bedarf an IPv4 Adressen für die jeweiligen Server der Webseiten, sowie für die Clients, welche diese abrufen sollten. Dadurch kam es in den letzten Jahren schon zu einer Verknappung des Adressraumes an verfügbaren IPv4 Adressen. 1998 kam dann, gerade durch die sich schon abzeichnende Entwicklung, die Spezifikation für den IPv4 Nachfolger: IPv6. Heutzutage beanspruchen Netflix und Youtube 50% des gesamten Internettraffics.

- Die Internet Protokoll Familie

Die Internet Protokoll Familie ist eine Sammlung der wichtiges Protokolle für den heutigen Internetverkehr. Es umfasst das (R)ARP, welches für die Adressvermittlung auf der Datenvermittlungsschicht, also dem Layer 2, das IP-Protokoll, welches auf dem Layer 3, dem Routing Layer, operiert, dann dem ICMP (Internet Controll Message Protocol), welche für den Austausch an Kontrollinformation zwischen einzelner Kommunikationspartner ist, sowie das TCP und UDP Protokoll, zwei der bekanntesten Protokoll für den Transport von Daten. Dabei muss man aber beachten, das es gravierende Unterschieden zwischen dem TCP und dem UDP Protokoll gibt. Zum einen ist das TCP-Protokoll Verbindungsorientiert, heißt es arbeitet mit einer Bestätigung der Gegenseite über den Erfolg einer aufgebauten Verbindung. Das UDP-Protokoll hingegen ist Verbindungslos, wodurch es sich besser für Videoübertragungen oder Latenz kritische Anwendungen eignet. Es ist auch deutlich einfacher aufgebaut als das TCP Protokoll.

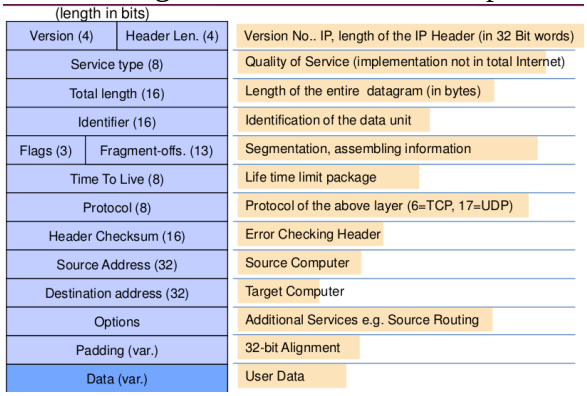
Das IP Protokoll hingegen ist, visuell, eine Ebene unter dem TCP/UDP, auch wenn es auf dem gleichen Layer operiert. Es sorgt für die Adressierung, das Routing und dem aufteilen der Pakete und dessen zusammensetzen der einzelnen Pakete. Sein „Datagramm“ reicht von 576 Bytes, bis hin zu 65535 Bytes und ist auch, wie das UDP-Protokoll, Verbindungslos.

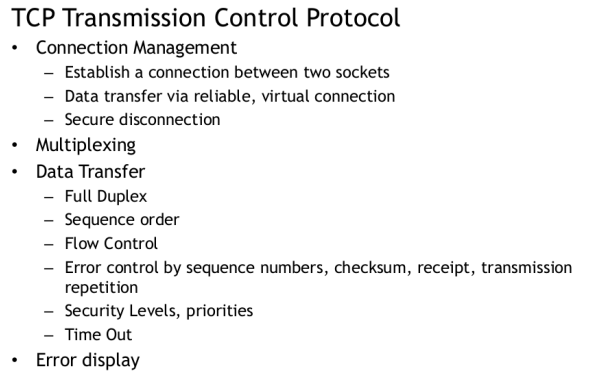
Bei dem IP Protokoll gibt es außerdem, wie oben schon angesprochen, zwei verschiedene Versionen, welche heutzutage zum Einsatz kommen. Einmal V4 und V6. Einer der größten Unterschiede zwischen diesen beiden Versionen ist der verfügbare Adressraum, bei V4 sind es 32 Bit Adresse, wodurch man auf knapp 4 Milliarden adressierbaren Hosts kommt. Bei V6 sind es 128 Bit Adressen, welche es ermögliche mehrere Adressen pro qm² zu verteilen. Da es bei V4 bald schon zu Problemen der Adressierungen kam, hat man schon früh Techniken wie NAT (Network Address Translation) eingeführt sowie die CIDR (Class inter Domain Routing) Notation, um

Klassen von Netzen zu erstellen und diese zu warten. Dabei viel auch der Begriff des Subnetz. Heutzutage gibt es 4 große Hauptklasse, welche sich auf verschiedene Kontinente aufteilen: A, B, C und D. Um nun verschiedene Hosts, oder auch mehrere zu erreichen, hat man schnell sogenannte „Cast“ Adressen eingeführt. Angefangen von der Unicast Adresse, welche nur auf einen Host zielt, dann die Multicast, welche auf mehrere Adressen zielt, den Broadcast, welcher auf alle angeschlossenen Hosts im Netz zielt und am Ende noch das Geocast, welches, wie der Name schon sagt, auf einen oder mehrere Hosts, länderübergreifend, zielt. Anycast hingegen zielt auf irgendeinen, nicht weiter spezifizierten, Host.

Eine weitere Entwicklung von IPv6 ist das direkte implementieren von IPSEC (später), QoS für Video und Audioübertragungen, sowie dem ausbügeln eines gewachsenen Problems bei IPv4, den immer größer werdenden Routing-Tabellen. Mobile IP wurde bei IPv6, dank des großen Adressraums, auch einfacher. Auch ist der Header von V6 viel kompakter und Einfacher, bei gleicher Funktionalität. Viele Erweiterungen müssen bei IPv6 durch sogenannte „Header Expansions“ zu dem eigentlichen Header hinzugefügt werden. Um einen Übergang von IPv4 zu IPv6 zu gewährleisten, gibt es nun verschiedene Ansätze, wie dem Dual-Stack, welches beide Protokolle zur Verfügung stellt und dem IPv4 zu IPv6 Tunnel, bei dem zum Beispiel IPv6 Pakete über einen IPv4 Tunnel transportiert werden.

Der IP-Datagramm Header sowie Eckpunkte von TCP:





- Internet: Security mit Firewalls und Proxys

Beim Internet gibt zwei verschiedene Grundaspekte, einmal die Security und die Safety. Security umfasst dabei den Schutz, oder auch „Sicherheit“, gegen Angriffe von Außen auf das eigene System, wohingegen Safety die „Sicherheit“ gegen den Ausfall einer Komponente, oder eher die Zuverlässigkeit, beschreibt. Weitere Stichworte dabei sind Authentizität, welche den Nachweis der Identität beschreibt, sowie die Integrität, welche die Unveränderlichkeit der einzelnen Daten garantiert/beschreibt. Um diese Security oder Safety zu erreichen, gibt es nun verschiedene Ansätze. Zum einen gibt es Firewalls, welche Pakete anhand ihres Protokoll-Headers filtern, umleiten oder gar blockieren kann. Dabei arbeitet sie mit der Quell- bzw. Zieladresse oder dem Protokoll. Des weiteren gibt es Applikation Proxy Gateways und Proxy Server, welche der Verschleierung oder auch Filterung von Inhalten dienen. Applikation Proxy Gateways sind meist Proxys, welche nur für ein Protokoll, zum Beispiel HTTP, konfiguriert sind. Sie bieten durch den zentralen Zugriff auch eine Möglichkeit der Analyse des Datenverkehrs.

- Technische Sicherheitslösungen

Nun gibt es aber auch technisch umgesetzte Lösungen um die Sicherheit im Internet zu gewährleisten. Darunter zählen die wichtiges der symmetrischen Verschlüsselung, welche auf die Sicherheit der Vertraulichkeit zielt, und der asymmetrischen Verschlüsselung, welche auf die Authentizität, Integrität und Haftbarkeit zielt. Damit gibt es mehrere Ziele für die Kryptographie, darunter zählen die Sicherstellung der Vertraulichkeit, der Sicherstellung der Integrität von Daten, der Authentizität sowie der Nachverfolgbarkeit. Beide Verschlüsselungen arbeiten dabei mit Schlüsseln, die symmetrische mit nur einem Schlüssel sowie die asymmetrische mit zwei oder mehreren Schlüsseln. Dadurch fällt direkt eine Problematik bei der symmetrischen Verschlüsselung auf, das Schlüssel-Verteil-Problem: Jeder Kommunikationspartner muss, für eine sichere Kommunikation, vorher den privaten Schlüssel auf einem „sicheren“ Weg erhalten haben. Bei wenigen Partnern ist dies ohne Probleme möglich, jedoch ist die Wartbarkeit und Inbetriebnahme bei mehreren Partnern fast unmöglich. Jedoch ist die symmetrische Verschlüsselung deutlich schneller als die asymmetrische, da sie auf Bit-Operationen beruht.

Die asymmetrische Verschlüsselung arbeitet mit mindestens zwei oder mehreren Schlüsseln. Es wird ein privater und ein öffentlicher Schlüssel benötigt. Der private wird dann zum Entschlüsselung der Daten herangezogen, sowie der öffentliche, welche die Kommunikationspartner erhalten, zur Verschlüsselung der Daten. Heißt will Partner y mir x etwas sicher schicken, verschlüsselt er die Nachricht mit der öffentlichen Schlüssel und ich entschlüssel die Daten mit meinem Privaten Schlüssel. Der öffentliche wird somit aus dem privaten generiert.

Typische Vertreter für symmetrische Verfahren: DES, 3DES sowie RC4 und RC5.

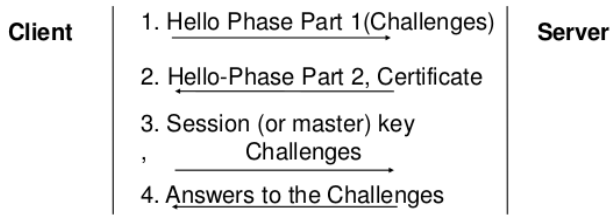
Typische Vertreter für asymmetrische Verfahren: RSA, DSS und EC-DSA.

- Signieren gegenüber Verschlüsselung

Signieren ist im Gegensatz zur Verschlüsselung, was die Verwendung der Schlüssel angeht, genau umgedreht. Signaturen dienen dazu, das der Empfänger zweifelsfrei feststellen kann ob die Nachricht auch von der gewünschten Person verfasst wurde. Dafür verschlüsselt der Autor seine Signatur mit dem Privaten Schlüssel womit die Entschlüsselung mithilfe des öffentlichen Schlüssels geschieht. Oft werden diese Signaturen auch mithilfe von Hashfunktionen für die Integritätsprüfung gehashed. Vertreter dieser Hashfunktionen sind MD5 und zB Wirelpool.

- TLS und SSL

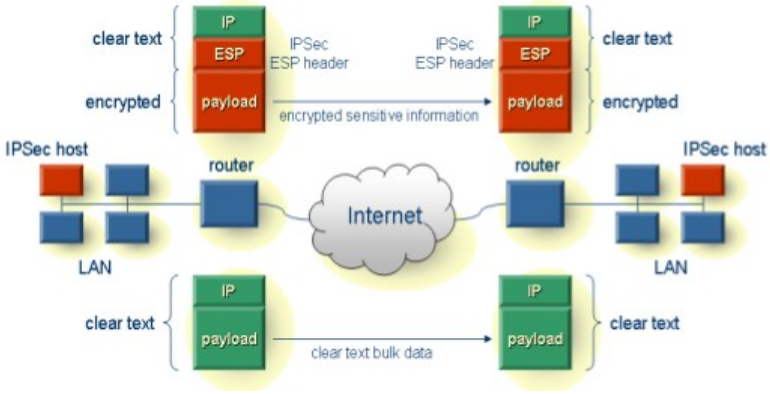
Eine weitere Möglichkeit den Datenstrom im Internet zu sichern, ist die Transport Layer Security und das Secure Socket Layer, kurz TLS und SSL. TLS ist dabei ein hybrides Verfahren beider Verschlüsselungsarten, der symmetrischen und der asymmetrischen. Auf Grund der Schnelligkeit werden die Daten symmetrisch verschlüsselt, sowie die Header asymmetrisch. TLS, oder auch SSL welches auf TLS aufbaut, arbeiten mit einem sogenannten Handshake-Protokoll. Es beschreibt die verschiedenen Phasen vom Aufbau, bis zur weiteren verschlüsselten Kommunikation zweier Partner.



In der ersten Phase nimmt der Client eine Verbindung zum Server auf und sagt ihm welche Verschlüsselungen er kann. Daraufhin sucht der Server eine Verschlüsselung auf und sendet seinen Public Key zum Client zurück. Der Client antwortet daraufhin mit einem Session Key, welchen er vorher mit dem Public Key des Servers verschlüsselt hat, außerdem wird eine, mithilfe des Session Keys verschlüsselte Testnachricht an den Server geschickt. Nun ist der Server, dank der Entschlüsselung des Session Keys, in der Lage, die Testnachricht zu entschlüsseln, welche er dann auch an den Client, zur Authentifizierung, zurückschickt. SSL erweitert diesen Handshake um ein paar weitere Schritte, welche den Austausch von Zertifikaten mit einbeziehen.

- IPSec

IPSec ist eine Verschlüsselung des Datenstrom direkt auf der Transportebene. Es ist in IPv6 fest integriert. Dabei baut es auf zwei weitere IPv6 Header auf, einmal den AH (Authentification Header) sowie den ESP (Encapsulatet Security Payload) Header auf. Beide sind Header Expansions bei IPv6.



Dabei kann IPSec mit einem Internet Key Exchange Protokoll auch mit Schlüsseln arbeiten, um den Datenstrom zu verschlüsseln. Meist werden Algorithmen wie SHA-1 und MD5 zur Verschlüsselung des AH-Headers benutzt, sowie AES oder 3THE für die Verschlüsselung des ESP. Aufgrund dem Benutzen verschiedener Algorithmen, ist IPSec für den Langzeitgebrauch (Long-Term-Use) geeignet.

Mobile System (WLAN, Bluetooth etc…)

- WLAN

In der heutigen Zeit ist WLAN gar nicht mehr weg zu denken. Man findet es mittlerweile in fast jedem Café, Bahnhof oder gar Reisebussen. Es ist spezifiziert nach dem IEEE 802.11 Standard. Meistens arbeitet es als Infrastruktur Netzwerk, kann aber auch als so genannten „distributed Foundation Wireless MAC (kurz DFWMAC) betrieben werden. Bei dem infrastrukturbetrieb kommt ein zentraler Knoten, meist ein WLAN-Router, welcher einen „Access-Point“ mit einer festen SSID (Service Set Identifier) bereitstellt. Dieser verwaltet dann auch die Zugriffssteuerung der einzelnen WLAN-Knoten. Kommt eines der DFWMAC - Verfahren zum Einsatz, zum Beispiel mit DCF, wird wieder auf das CSMA / CA Protokoll gebaut, welches in diesem Fall keine „Collision Detection“ bereitstellt, sondern eine Collision Avoidance hat. Andere Formate, wie DFWMAC mit RTS / CTS arbeiten mit Request to Send und Clear to Send. Dieses System funktioniert aber nur, wenn die Knoten, das Übertragungsmedium, also den Funkbereich, komplett belegen. Zuletzt gibt es das DFWMAC mit PCF, auch Point Coordination Function genannt. Bei ihm übernimmt ein Knoten die Rolle eines Point Coordinators, welcher die Kommunikation durch bestimmte Signale steuert. Der WLAN-Standard wird immer weiter erweitert, jedoch gibt es immer die gleichen Techniken an denen noch verbessert werden kann, dazu zählen:

Better modulation procedure

- BPSK (Binary Phase Shift Keying)

- QPSK (Quad Phase Shift Keying)

- QAM-16, QAM64, QAM 256 (Quadrature Amplitude Modulation with 16/64/256

States)

•

802.11a

- 5 Ghz band

- Data rates up to 54 Mbit/s

802.11b/g

- 2.4 ghz band

- Data rates up to 54 Mbit/s

- Backward Compatible

- High interference potential caused by other services (Bluetooth !)

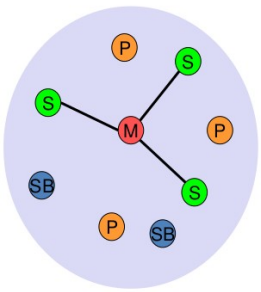
802.11 n

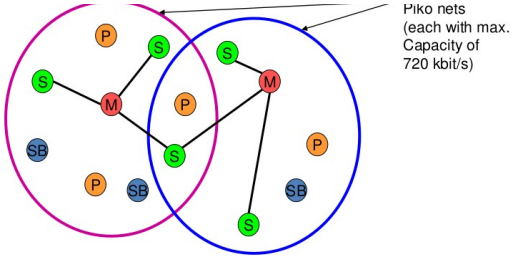
- 2.4 and 5 GHz

- Data rates of up to 600 Mbit/s by multiple-input multiple-output (MIMO)

- Bluetooth

Ein anderes Verfahren um Geräte Kabellos zu verbinden, ist heute Bluetooth. In den 1994er Jahren entwickelt, es es heute das Standardverfahren um zum Beispiel Handys über kurze Strecke zu verbinden. Es arbeitet auch auf dem 2.4 GHz Band, mit jeweils 79 Kanälen. Aber wofür Kanäle? Diese braucht es für die Aushandlung der Netze, denn Bluetooth funktioniert in sogenannten Pico-Netzwerken. Diese sind so aufgebaut, das es eine bestimmte Anzahl an aktiven Knoten, maximal 7 „Slaves“ (adressiert mit 3 Bit) und vielen inaktiven, parked (adressiert mit 8 Bit), Knoten, maximal 255, gibt. Einer dieser Knoten wird der Master, also der Koordinator, des Netzes. Jedoch kann ein Slave oder auch ein Parked Knoten, auch ein Master eines anderen Pico-Netzwerkes sein. Damit sich nun niemand in die Quere kommt, sendet der Master eine bestimmte, zufällige, Frequenz an die Slaves, auf die diese das aktuelle Datenpaket senden sollen. Das ganze nennt man auch Frequencehopping, erfunden durch Hedy Lamarr. Eines der größten Herausforderungen bei Bluetooth ist die Synchronisation der Zeit auf allen Knoten, denn nur dann ist ein sicheres Frequencehopping garantiert. Gibt es keinen Platz mehr in dem Netz, oder ist ein Teilnehmer inaktiv, wird er auf Stand By gestellt.



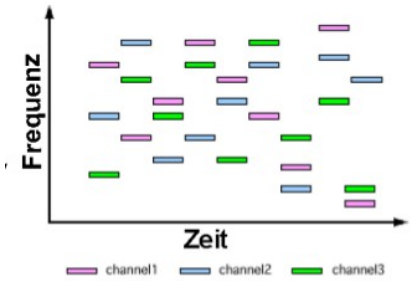


Andere Eckdaten zu Bluetooth: Reichweite < 300m, Datenraten bis 1 Mbits (max 2), 1 – 100 mW Leistungsaufnahme, 433,9 Kbit/s symmetrical or 723,2/57.6 Kbit/s asymmetric packetswitched Datenübertragung.

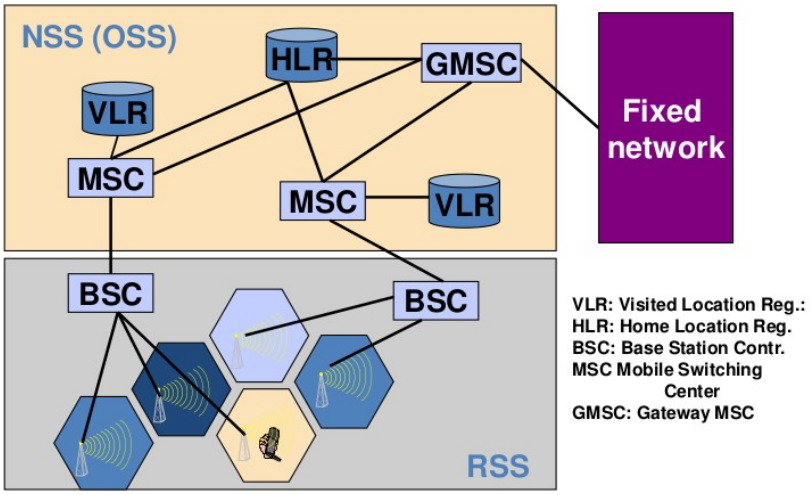
- Mobile Kommunikation UMTS, GSM, usw…

Heutzutage hat fast jeder ein Handy, nahezu 6 Milliarden Nutzer gibt es Weltweit. Dabei muss man sich fragen wie das ganze funktioniert? Die Antwort ist Multiplexing in verschiedenen Formen. Zum einen gibt es das Time Division Multiplexing, das Space Division Multiplexing, das Frequency Division Multiplexing sowie das Code Division Multiplexing. Alle diese Methoden zielen auf die ein oder andere Art auf eine Effiziente Bandbreiten, oder eher Kanalnutzung. GSM, welches heutzutage das am weitesten verbreiteteste Mobilnetz ist, arbeitet dabei auf 890-915Mhz + 935-960Mhz, während das GSM 1800er Netz, auf 1710-1785Mhz + 1805-1880Mhz arbeitet. GSM benutzt aber nicht alle Multiplexing Verfahren, sondern nur das Code+, Frequency+ sowie das Time-Multiplexing. Dies ermöglicht die Benutzung von 124 Frequenzen gleichzeitig, sowie 8 Zeitslots. Alles zusammen kommt man so auf knapp 1000 Verbindungen pro Zelle. Das Code Division Multiple Access kommt bei UMTS oder LTE, wo es um höhere Bandbreiten geht, zum Einsatz. Nicht zu vergessen ist das Spread Spectrum bei GSM, oder eher das Frequency Hopping Spread Spektrum, welches die Ausnutzung des Mediums durch das Frequenzhopping in

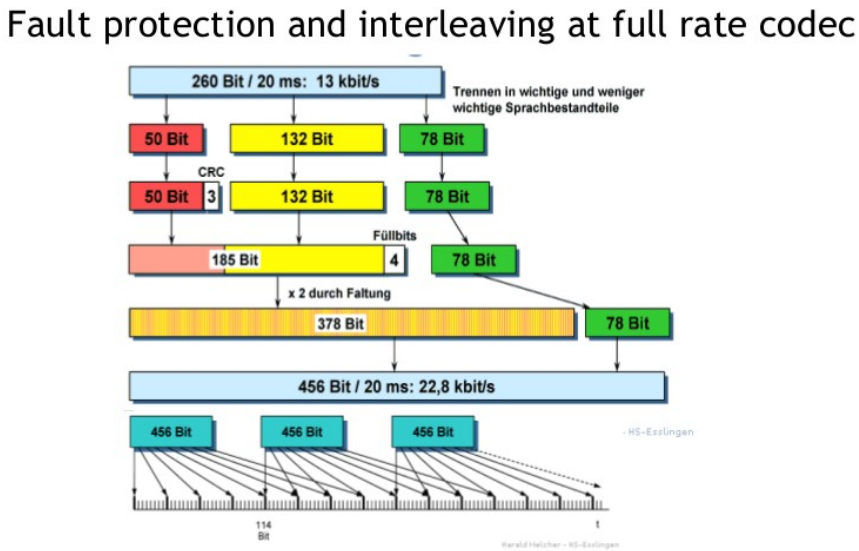
verschiedenen Frequenzen und Kanälen beschreibt.



Die Grundlegende Struktur eines GSM-Netzes sieht wie folgt aus:



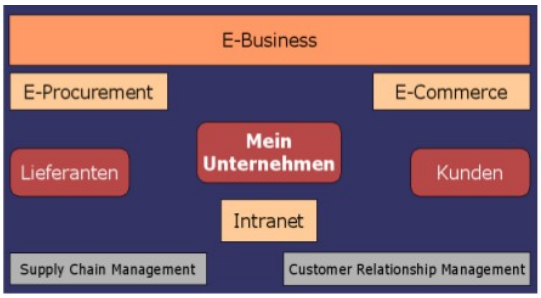
Dabei wird es immer in zwei große Subklassen aufgeteilt, einmal den NSS (OSS) und dem RSS, dem Radio Subsystem. Beide sind eine Sammlung von verschiedenen Stationen im GSM Netz, zum Beispiel beinhaltet das RSS die Basis-Stationen, also die Sendemasten, auch BST genannt, sowie deren zugehörigen Controller, BSC. Es ist also die Schnittstelle zwischen Mobiltelefon, MS, und der Vermittlungsstelle. Dabei wird, wie oben angesprochen, jeder Mobile Station 124 Kanäle im Down, sowie im Upstream bereit gestellt. Alle mit 200 Khz gestaffelt. Die Übertragungsraten, mit Fehlerbehandlung und Interleaving staffeln sich wie folgt:



Das NSS, auch Network Switching System, ist damit die „Vermittlungsstelle“. Sie beherbergt die HLR und VLR, welche beide als Art Datenbank, oder eher Register dienen. Dabei steht im Home Location Register die Basisdaten der einzelnen Mobiltelefone, also Kartennummer, Handynummer usw, während in dem VLR nur temporäre Informationen, über den Mobiltelefonbenutzer im aktuellen RSS, liegen. Wie man aber oben an dem Schaubild der Bandbreiten gut erkennt, sind diese für die heutige Internetzeit kaum noch zu gebrauchen. Daher wurde schon schnell ein neuer, schnellerer Standard verabschiedet: GSM GPRS. Dieses arbeitet nun auf 171,2 Kbits, danach kamen dann die Standards Edge, 3G, UMTS etc. Bei UMTS werden heutzutage sogar Datenraten bis zu 300 Mbits im Downstream, und 75 Mbits im Upstream erreicht. Des weiteren bietet UMTS geringere Latenzen, flexiblere Netzgrößen (bis zu 100 km) sowie durch Techniken wie MIMO, FDMA oder SC, höhere Datenraten. Auch darf man die Modulationen nicht vergessen, wie 4PSK zu 16QAM bis hin zu 64QAM und MIMO. In Planung sind heutzutage die Standards 4G sowie 2020 rum 5G.

E-Commerce

E-Commerce ist das Schlagwort des 21 Jahrhunderts, es umschreibt den neuen, elektronischen, Handel über private, oder auch öffentliche Netzwerke, zum Beispiel das Internet. Dabei spricht man bei eCommerce von dem Verbinden von verschiedenen Techniken, unter anderem „Informations- und Datenbanksysteme“, „Interaktive Kommunikationswege“, sowie der „Multimedia“. Auch umfasst es das elektronische Bezahlen sowie den elektronischen Austausch von Handelsdaten, zum Beispiel von Firmen untereinander oder Daten von RFID Sensoren zum Kunden / Händler.



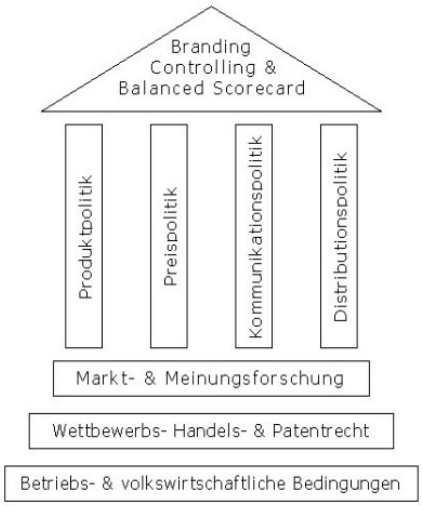
Das E-Business wird auch in Deutschland immer wichtiger, waren es 2012 nur rund 276 Mrd. $, sind es 2016 schon 458 Mrd. $. Somit wächst der Handel stetig.

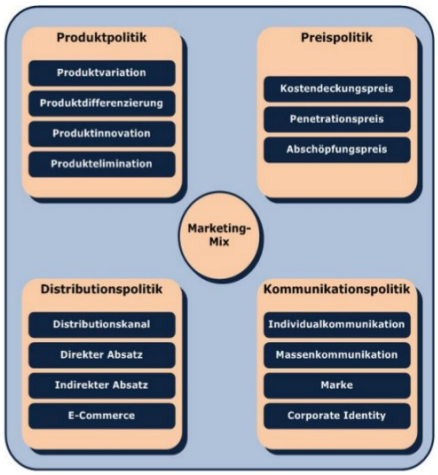
Aber nicht immer erfolgte der E-Commerce über das Internet, Anfang der 1970er kam in England das BTX System heraus, welches aber erst Mitte der 80er Jahre wirklich erfolgreich war. Ab dem Zeitpunkt wurde es sogar von Tankstellen, Autohändlern, Privatpersonen für Homebanking, und vielen anderen benutzt. Am Ende waren es dann knapp 1,2 Millionen Nutzer. Es ab aber auch Konkurrenz zum BTX-System, nämlich das Minitel System, gegründet von der französischen Telekom und IBM. Es hatte Ende der 1980er Jahre schon knapp 6 Millionen Nutzer, obwohl es erst 1982 eingeführt wurde. Aber all diese Benutzerzahlen sind nichts im Vergleich zu der Nutzerzahl im heutigen Internet.

Bis jetzt haben wir nur aus der B2C (Business 2 Costumer) Sicht gesprochen, aber wie funktioniert die B2B (Business 2 Business) Kommunikation? Für diesen Zweck hat man den Standard EDI eingeführt, oder später auch EDIFACT, welches aber nur als Protokoll dient und nicht zur

Datenübertragung. Es wird aber auch häufig für eMails verwendet, um eine interne Kommunikation im Unternehmen zu gewährleisten.

Das eCommerce wird mit 7 Stichpunkten beschrieben, dazu zählen: Economic operators, Economic activities, Business Objects, Transactions, Evaluation, Dating und Localization. Jedoch kann man sich all diese Stichpunkte, wenn man ein wenig in dem „realen“ Marktgeschehen ist, leicht erklären. Ein weiterer Punkt, der beim eCommerce, aber anders ist, ist das Marketing.





Ein Riesen Vorteil beim Marketing im eCommerce, ist das „one-to-one“ Marketing, welches darauf beruht, das man durch einen Kauf, Klick oder nur durch das bloße Ansehen eines Artikels im Internet, eine gewisse Rückmeldung zu dem Artikel oder sein Unternehmen hat. Vorher war dies nur durch Kontaktaufnahme per Telefon oder Post möglich und dauerte sehr lange, vor allem war nicht jeder bereit per Telefon eine Auskunft über gewisse Fragen zu geben. Dabei gibt es die Methode das Log-File des Servers durch Analyse Software auszulesen, auch Log Analyses genannt. Es gibt die sogenannten Page-Impressions, also die Anzahl einzelner HTML-Seitenaufrufe, sowie die Visits, also die wirkliche Besuchszahl, getrennt meist von der IP-Adresse, an. Es gibt aber auch die Möglichkeit eine Auswertung auf Client-Seite zu betreiben, und zwar durch sogenannte Tags und Pixel, oder Cookies. Bei der Pixel Methode wird ein kleines Bild, genau 1 Pixel groß, auf der Webseite eingebettet, um somit einen Besuch eines bestimmten Artikels, oder eines Produktes, zu registrieren. Dabei muss das Bild nicht einmal auf dem gleichen Server wie die Webseite liegen, meist liegt es extern auf einem Server eines Analyse-Dienstleisters. Eine weitere, in den Frühzeiten des Internets meist verhasste Methode, ist die des Cookie-Trackings. Dabei wird, oft auch benötigt, ein Cookie beim Client angelegt, welches zum Beispiel eine Tracking-ID oder Artikel eines Warenkorbs enthält. Durch diese genannten Möglichkeiten, können nun, wenn sie zusammenarbeiten, Webseitenbetreiber eine Analyse, oder Statistik, über das Surfverhalten einzelner Nutzer machen.

Zum Schluss noch die wichtigsten Techniker für das eBusiness:

- N-Tier Architekturen

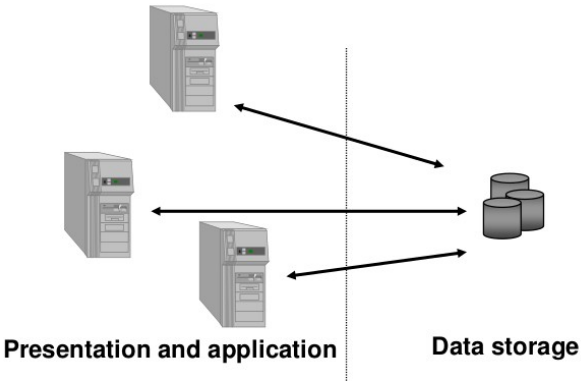
- Thin Clients

- Scalability

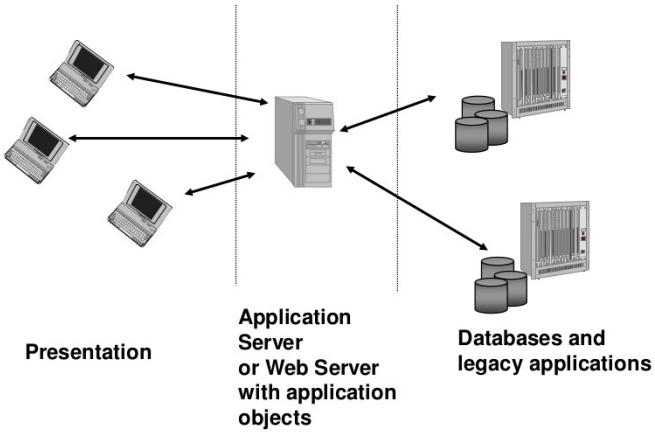
- AJAX

- JAVA

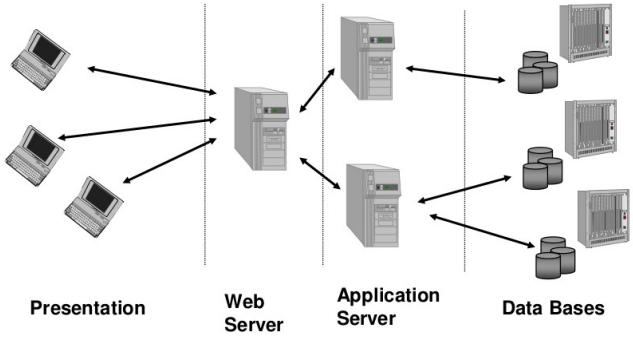
Dabei gibt es bei der N-Tier Architektur verschiedene Modelle, angefangen bei dem 2-Tier Modell, bei dem die Anwendung, also auch Darstellung und Berechnung etc, auf dem Client liegt, die Daten aber aus einer Datenbank kommen.



Des weiteren gibt es die 3-Tier Architektur, welche nun auf den Ansatz baut, mit einem Webserver für die Darstellung und Berechnung der Applikation, welche wiederum auf eine Datenbank im Hintergrund zugreift. Meist heutige Internetseiten wie eBay oder Cloud-Dienste.



Zum Schluss kommt noch die 4-Tier Architektur, sie ist aufgebaut wie die 3-Tier Architektur, wobei nun aber nochmal Darstellung und Berechnung, der Applikation, getrennt ist.



- elektronische Bezahlsysteme

Als nächstes befassen wir uns mit elektronischen Bezahlsystemen, dabei wird zwischen zwei großen Hauptkategorien, oder Schlagworten, unterschieden. Einmal dem „stored account“ und einem dem „stored value“. Beide Unterscheiden sich Grundlegen, bis auf die Tatsachen, das man mit beiden bezahlen kann. Bei „stored account“ findet man Vertreter wie die geläufige Kreditkarte oder das EVL, auch elektronisches Lastschriftverfahren. Es hat den Vorteil, das das Geld niemals die Bank verlässt, heißt der Kunde bezahlt mit seinem „Namen (Account)“ und fordert, oder ermächtigt, den Verkäufer den geforderten Betrag von seinem Konto abzubuchen. Somit wird das Geld von Konto zu Konto übertragen, was heutzutage meist virtuell geschieht. Jedoch muss der Käufer dem Verkäufer soweit vertrauen, das dieser nur den angegebenen Betrag von seinem Konto bezieht. Andersherum muss der Verkäufer, dem Käufer, soweit vertrauen, das dieser der Eigentümer der Karte ist und sie nicht gestohlen oder gesperrt ist. Trotz all dieser Bedenken wächst die Zahl der Kreditkarten Inhaber in Deutschland kontinuierlich, in Amerika hat jeder schon rund 2 Kreditkarten, in Deutschland sind ist derzeit rund 38 Millionen, von rund 82 Millionen, Personen. Die meisten Bezahlungen, in Deutschland, werden mit rund 58% immer noch mit Bargeld betätigt.

Auf der anderen Seite steht das „stored value“. Bei diesem Verfahren findet man die üblichen Geldkarten, wie zB für Amazon, Google Play oder iTunes. Diese haben das Ziel, wie man sich denken kann, den „Namen“ oder den Account des Kunden, oder Käufers, zu schützen. Sie werden meist vor dem Bezahlen mit einem gewissen Betrag aufgeladen, welcher dann bei der Bank eingeholt wird oder als Schuld dort verbucht wird.

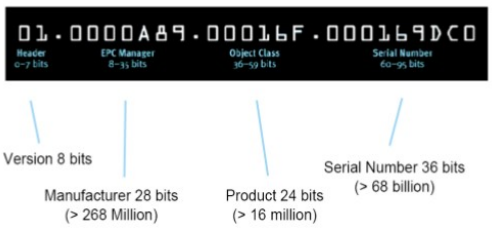
Eine weitere Art der Bezahlung, welche immer wichtiger wird, sind Bitcoins.

- RFIDs

Als nächsten Schwerpunkt betrachten wir RFIDs. Sie ermöglichen es Waren zu kennzeichnen und somit ihren „Lebensweg“ zu verfolgen, gerade im Zeitalter des IoT, kann man so alles nachverfolgen. Dabei beschreiben die RFIDs nur die Kennzeichnung von Produkten mit einem bestimmten Code und gibt, zB, eine Spezifizierung für die Frequenzen zum kommunizieren mit eingebauten elektronischen Tags. Die Hauptprobleme die mit RFID versucht werden aufzufangen sind:

Zerstörung, oder Beschädigung einer Ware, das Out-of-Stock Problem (Lieferanten Problem), der Widerruf von Artikeln, dem Recyclen dieser, das erkennen von Fälschungen, dem auffinden von Unverkaufbaren Artikeln (welche nicht mehr produziert werden müssen), sowie dem Voraussagen von dem wirklich benötigten Warenbestand.

Um nun eine Identifizierung zu ermöglichen, wurden sogenannte Tags entwickelt, wie zum Beispiel der Universal Product Code (1974 in den USA) kurz UPC, oder dem heute geläufigen EPC (Electronic Product Code). Viele kennen aber nur den EAN (European electronic Number) Code, welcher anfänglich auch nur in Europa zum Einsatz kam. Der EAN Code kann aber in einem EPC Code verpackt werden, jedoch nicht umgekehrt. Andere Codes, welche aber nicht so erfolgreich waren, sind: GS1 und GTIN.



Um nun einen Nutzen aus diesen Kennzeichnungen durch Codes zu haben, gibt es eine sogenannte „Physical Markup Language“, welche in einer engen Beziehung zu dem ONS, Object Name Service, welches wie das DNS System im Internet funktioniert, steht. Mit diesen beiden Hilfsmitteln ist es möglich, Produkte und deren Handelsweg (Lebensweg), eindeutig zurückzuverfolgen.

Transporttelematik

Telematik findet man heutzutage auch in jedem Transportwesen, sei es auf der Straße mit Mautsystemen oder Navigationssystemen, oder im Schienenverkehr mit intelligenten Signalen, im Luftverkehr bei Systemen wie dem TCAS sowie in der Schifffahrt, wo man mithilfe der Telematik versucht ein automatisches Schiffsmanagementsystem zu etablieren. Heißt die Telematik greift auch in das Umweltbewusstsein der Menschen ein, indem es manche Sachen effizienter macht oder einfacher zu benutzen. Auch steht der Umweltaspekt immer mehr im Fokus, gerade da sich die Anzahl der PKWs in Deutschland, zwar langsam, aber jährlich immer weiter erhöht. Derzeit sind es rund 43,4 Millionen, angemeldete, Fahrzeuge. Würde man die nicht angemeldeten hinzuzählen, wären es weit mehr. Wie man sich nun vorstellen kann, kommt es bei der immer weitere wachsenden Anzahl an PKWs zu Problemen, wie Staus, auf den Straßen. Hier kann Telematik durch intelligente Verkehrsführung, zum Beispiel durch Anzeigetafeln, helfen. Auch versucht man, durch die Telematik, Maut auf Straßen zu erheben, um zum Beispiel LKWs zu besteuern, und im Endeffekt, die Fracht auf andere, weniger Umweltschädliche Transportmöglichkeiten, wie den Schienenverkehr, zu verlegen. Auch Fahrgemeinschaften versucht man so zu fördern, ein Beispiel dafür ist zB BlaBlaCar. Dieser Wunsch der Entwicklung steht aber leider gegen die alljährliche Autoproduktion, welche mittlerweile fast 1 Milliarde Autos umfasst. Gerade diese gewaltige Anzahl an Autos will „sicher“ auf die Straßen gebracht werden. Das dies gerade durch Telematik, also besserer Technik wie Sensoren, Verkehrsleitsysteme usw, schon gelungen ist, zeigt die Statistik, in der man sieht, das es jedes Jahr weniger Tode bei Autounfällen gibt.

- Navigationssysteme

Eines der bekanntesten, und wohl am größten geschätzte, Entwicklung der Telematik, ist das Navigationssystem. Fast jedes Auto hat heutzutage ein „Navi“ on-board. Dabei sind die Anfänge auf einfache Berechnungen zurückzuführen. Eines der ersten Werkzeuge, wie das Navi heute, war der Sextant. Dieser arbeitet als eine Art „Vergleicher“ der Sonnenstrahlen zum Horizont, mit dessen Hilfe man seinen Standpunkt, geschweige man hatte ein aktuelles „Nautic Year Book“ an Board, bestimmen konnte. In den „Nautic Year Books“ stehen die genauen Winkel, Uhrzeiten und Breitengrade der Sonne. Somit war es möglich, wenn man eine genaue Uhr hatte, sich dadurch zu orientieren. Die „Genauigkeit“ der Uhrzeit war soviel Wert in dieser Zeit, das das englische Parlament sogar einen Wettbewerb veranstaltete, wer die genauste Uhr baut. Das Preisgeld dafür betrug Anfang des 18 Jahrhunderts 20.000 Pfund.

Heutige Navigationssysteme arbeiten aber schon lange nicht mehr so „analog“. Sie bedienen sich den Signalen von Satelliten, welche im Weltall greisen. Angefangen beim Transit-System, welches mit 4 Satelliten arbeitete, bis zum heutigen GPS. Das Transit-System wurde 1967 beim Blitzkrieg Israels benutzt, jedoch musste man bedenken, das man bis zu 110 Minuten auf ein erneutes Signal

warten musste.

Das heutige System, GPS (Global Positioning System) oder ausgeschrieben NAVSTAR GPS (Navigation System Use Time And Ranging-Global Positioning System), ist der Standard für fast alle Navigationssysteme in der Transportwelt. Es basiert auf einer Berechnung der Laufzeit eines Signales zum Empfänger, auch „signal propagation time measurement“ genannt. Dabei senden 24 Satelliten in 6 Orbitalen Positionen stetig ein Signal mit einem Zeitstempel und ihrer Position zur Erde. Gibt es nun einen Empfänger, der mindestens 3 dieser Signale empfängt, kann dieser seine Position auf der Erde bestimmen. Ein vierter Satellit kann noch herangezogen werden, um eine Abweichung der Zeit des Satelliten zu korrigieren. Die Signale werden dabei auf zwei Frequenzen gesendet, einmal 1000 MHz und 2000 MHz. Hat man nun das Signal von 3 Satelliten, kann man anhand des Schnittpunktes der, von den Satelliten aufgespannten Kreise, seine Koordinaten bestimmen. Jedoch gibt es auch störende Faktoren für das System, zum einen sind das atmosphärische Störungen, wie zum Beispiel Ionospherische Fehler, dann gibt es Zeitfehler, wenn zum Beispiel die Uhrzeit eines Satelliten falsch ist, sowie noch den Fehler der Reflektion eines Signals. Dabei wird eine Genauigkeit von knapp 10 – 20 m erzielt, welche für den zivilen Bereich akzeptabel ist, jedoch nicht für den militärischen. Daher hat GPS zwei Systemodis, zum einen das SPS für den zivilen, und das PPS für den militärischen, welcher viel genauer ist als der SPS. Durch weitere Langwellensender und weiteren Satelliten, welche auf für den zivilen Bereich zugänglich sind, ist es möglich seinen Standpunkt auf 1m genau zu bestimmen. Solche Systeme, welche aber nur mit zwei zusätzlichen Satelliten arbeiten, sind WAAS (USA), EGNOS (Europa) und MSAS (Asien). Das System mit den Langwellensendern heißt DGPS.

Weitere, von anderen Ländern entwickelte System sind: GALILEO, GLONASS und Beidou (China).

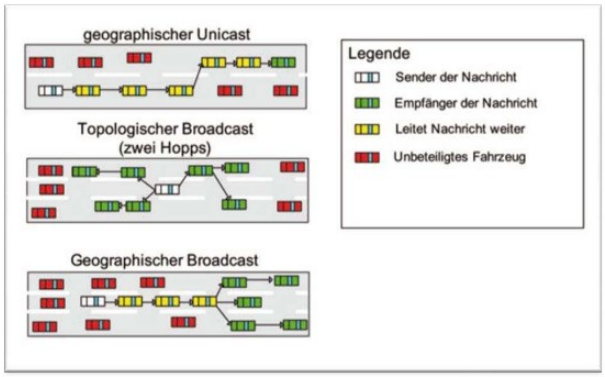
- Elektromobilität

Die Elektromobilität gibt es schon sehr lange, um 1900 rum gab es sogar mehr e-Autos als welche mit Verbrennungsmotor. Dies lag aber an dem noch kleinen Straßennetz, welches sich meist nur auf innerstädtische Verbindungen, bezog. Erst durch den Ausbau, oder generell den Bau, von Fernstraßen, wurde das e-Auto zunehmend, durch die höhere Energiedichte des Verbrennungsmotor, verdrängt. Doch damals gab es das gleiche Problem wie heute: Die Batterien. Die Batterien sind heute noch eines der größten Probleme, sie sind schwer, laden nur langsam (meist über Stunden) und können kaum die Energie, im Verhältnis zu einem vollen Sprittank, aufnehmen. Jedoch kennzeichnet sich eine Trendwende, da immer bessere Techniken entwickelt werden, und vor allem, mehr Firmen in die Produktion von Akkus einsteigen. Wünschenswert wäre eine e-Auto Entwicklung, gerade durch den ökonomischen Aspekt, denn ein e-Auto hätte, bei Erzeugung des Stroms durch fossile Energieträger, knapp 40% Nutzenergie. Im Vergleich ein Dieselauto kommt gerade mal auf 15%, was schon, für Verbrennungsmotoren, effektiv ist.

- Car-2-Car Kommunikation (C2C)

Ein weiterer Fortschritt in der Telematik bei Autos ist die C2C Kommunikation, welche es, analog, schon lange gibt. Jedoch nicht elektrisch, sondern nur durch Hupzeichen, Lichtzeichen und Handzeichen. Die neuen Techniken erlauben es aber, das Autos direkt miteinander kommunizieren können, um zum Beispiel zu erkennen das das Auto vor einem bremst, das hintere Auto warnen das

man bremst, einen Parkplatz zu finden usw. Auch könnten sich die Autos dann über die Ampelschaltzeiten informieren, um so mit einer geeigneten Geschwindigkeit eine grüne Welle zu nutzen oder Platz für einen Krankenwagen zu machen. Um dies zu ermöglichen gibt es zwei Grundlegende Einheiten, einmal die OBU (On Board Unit) und die RSU (Road Side Unit). Beide können untereinander kommuniziere. Die RSU kann des weiteren auch einen Internetzugang bereitstellen oder einen Leitung zu Rettungsdiensten für den sogenannten eCall, welcher ab 2018 in jedem neuen Auto eingebaut sein muss. Für die Kommunikation der Einheiten kann man das alt bekannte WLAN wieder nehmen, jedoch auf anderen Frequenzen als das private zuhause: 5.855 – 5.925 MHz.

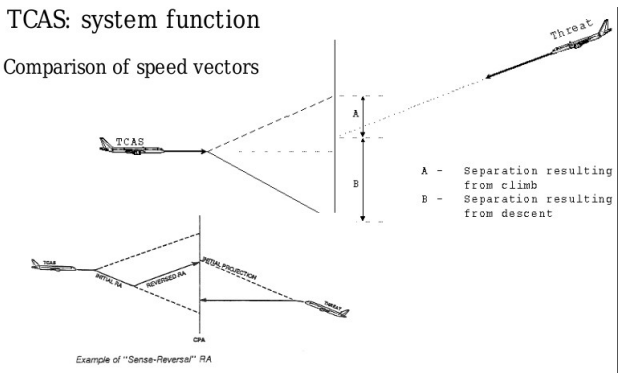


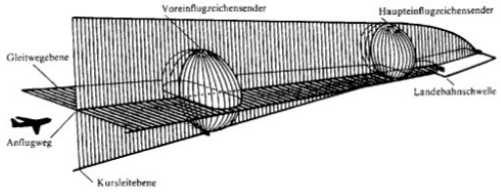
Die innerbetriebliche Kommunikation im Auto, gerade die der wichtigen Systeme, wird durch andere Netzwerke/Techniken realisiert. Darunter zählen: CAN, LIN, FLEXRAY und MOST.

- Telematik im Luft- und Schienenverkehr

Auch im Schienenverkehr und in der Luftfahrt hält die Telematik Einzug, sei es im Schienenverkehr das GSM-R (Rail), welches für die Kommunikation der Lokführer mit der Leitstelle oder untereinander benutzt wird, oder den intelligenten Signalen mit automatischen Bremssystemen falls eine Kollision droht, auch ETCS (European Train Control System) genannt.

In der Luftfahrt hat die Telematik auch den Aspekt der Sicherheit, zum einen durch das Frühwarnsystem einer Kollision TCAS (Traffic alert and collision avoidance System) und dem ILS (Instrumented Landing System). Weiterentwicklung des ILS ist ein GPS gestütztes System, auch SLS genannt, wobei das ILS, welches seit 1942 existiert, ausgereift ist. Ein weiteres, heutiges System ist das ADS-B.





Telemedizin

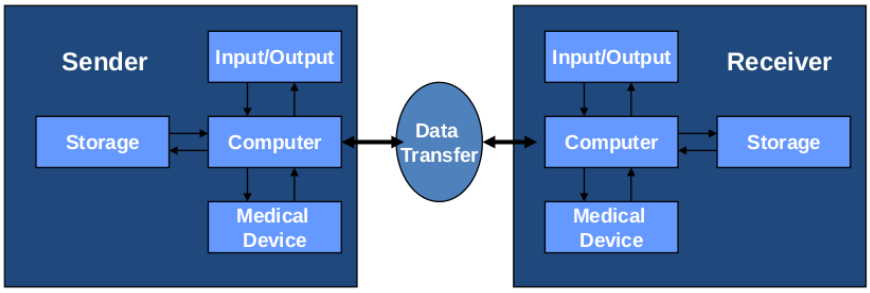
- Definition der Telemedizin

→ Applikationsbasierte Definition

Die Telemedzin ist der Gebrauch von Informations und Telekommunikationstechnologien um das gesundheitliche Wohlbefinden zu fördern falls die zwei Kommunikationspartner geographisch getrennt sind

→ Systembasierte Definition

Telemedizin ist der Überbegriff für technische Informationssysteme, welche der Übertragung und Empfangen von Daten dient, sowie deren Infrastruktur.



Des weiteren befinden wir uns in der nächsten Kondratjew Welle der „Bio Medizin“. Kondratjew hat ein Model verfasst, welches besagt, das die Menschheit alle 30 – 50 Jahre einen evolutionären Sprung durch Basic Erfindungen macht, also Erfindungen für jeden.

In Deutschland werden ca jedes Jahr 315 Milliarden € für die Gesundheit aufgewendet, sei es durch private Krankenkassen, gesetzliche oder berufliche. Darüber hinaus soll die Telematik diese Ausgabe drücken oder sie effizienter ansetzen.

Zu den medizinischen Telematik Komponenten der Infrastruktur gehören: Informations Systeme, Elektronische Gesundheitsdaten, Datenkarten und Netzwerkbasierte Systeme.

Zu den Anwendungen: Öffentliche Gesundheitsinformationen und Telemedizin für das gesundheitliches Wohlbefinden.

Zu den Kosten und Erträgen: Für den Doktor und den Patienten sowie die gesetzlichen Rahmenbedingungen.

Es gibt knapp 123.000 Ärzte in Deutschland, die sich auf 100000 Praxen verteilen, sowie 2000 Krankenhäuser.

Krankenhäuser untereinander kommunizieren dabei mit dem HIS, welches schon 1969 entwickelt wurde und mit dem EDIFACT Standard arbeitet. Es dient gerade bei Röntgenaufnahmen oder Untersuchungsberichten für die Vermittlung der Patienten.

Andere Standards zum Datenaustausch sind: DICOM, HL7, ISO 11073, IHE und OSCB.

- Post und Fernmeldewesen

Das Nachrichtenwesen wurde lange als Herrschaftsinstrument benutzt.

Darüber hinaus stand die Post unter dem Schutz des Kaisers. Somit war die Postzustellung bis zur Liberalisierung Staatsangelegenheit. Erst durch die Globalisierung wurde das Fernmeldewesen geöffnet und Schrittweise liberalisiert. Die erste Stufe dabei erfolgte 1989, sowie die zweite ab 1995 und die dritte am 1996/1998. Erst dadurch wurde das Monopol, welches die deutsche Telekom durch die Liberalisierung bereits hatte, gebrochen. Seit 2008 muss die Telekom die Festnetzanschlüsse zu einem normalen Preis an andere Wettbewerber verkaufen.

Gesteuert und beaufsichtigt wird das ganze durch die Bundesnetzagentur.