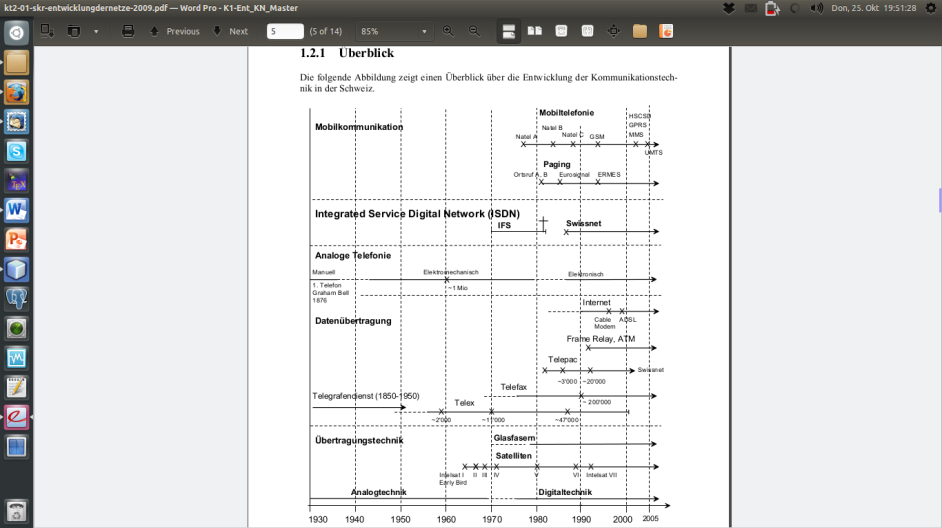
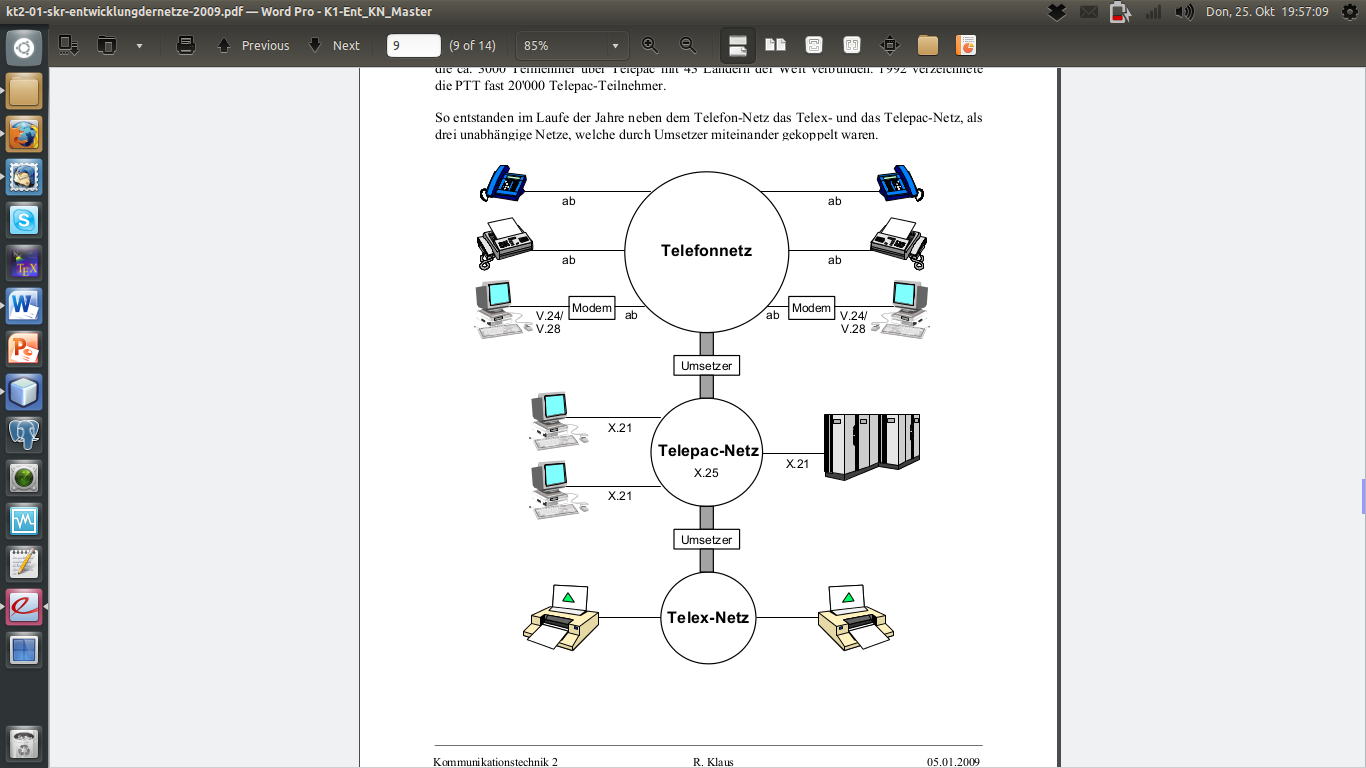
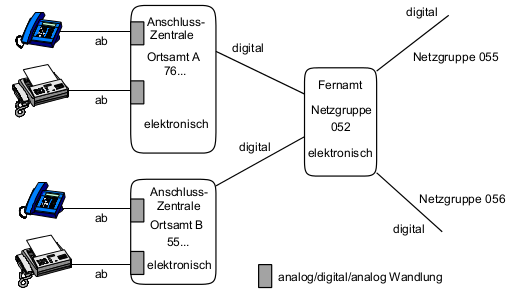
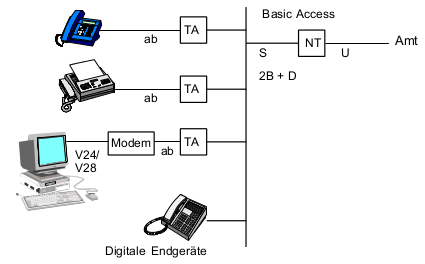
**KT2 SEP HS2012/RB**







PCM30 ab 1970



ISDN-Basis-Anschluss: 2 B-Kanäle mit 64Kb/s, 1 D-Kanal mit 16Kb/s, 1 Sync Kanal mit 48 Kb/s  
Netto = 144 Kb/s, Brutto = 192 Kb/s

ISDN-Primäranschluss: 30 B-Kanäle mit 64 Kb/s, und 1 Sync mit 64 Kb/s

# Pulse Code Modulation

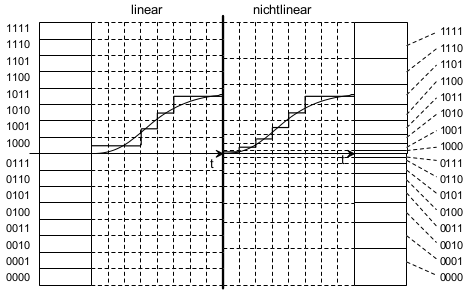
Analog -> PCM:

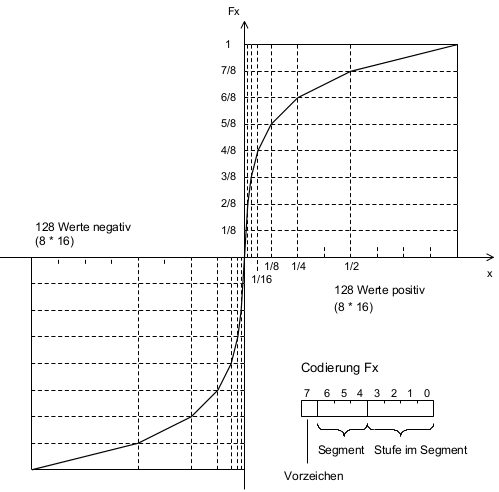
1. Filterung: 300...3400 Hz
2. Abtastung: Freq. doppelt so hoch wie Bandbreite (Abtasttheorem von Shannon)   
   => 8 kHz, d.h. alle 125 μs
3. Quantisierung: gibt Quantierungsfehler. Dass diese möglichst klein bleiben, wird nicht linear abgetastet. Europa = A-Law, USA = μ-Law.
4. Jedem Pt wird ein Wert aus 8 Bit zugeordnet. Bei 8 kHz gibt es 64kb/s.

PCM->analog:

1. Dekodierung: Codes zu Amplitudenwerte umwandeln.
2. Halten: bei 64kb/s 125us den Wert halten.
3. Glätten: Mit Tiefpassfilter die hohen Freq. entfernen und das Signal glätten.

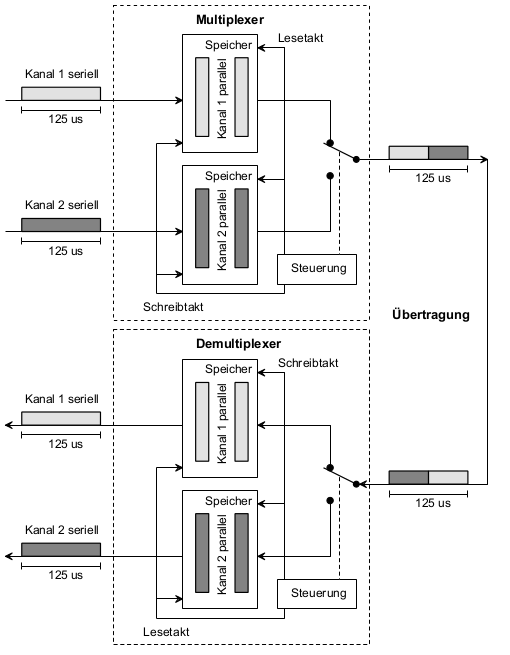
Nichtlineare Quantisierung: Man ordnet kleinen Amplitunden kleine Werte zu => Quantisierungsfehler werden kleiner. A-Law (Europa) und u-Law (USA) von G.711 macht das. Bsp mit 4 Bits:





Kleine Werte werden viel stärker abgetastet als grosse.

# Zeitmultiplexing



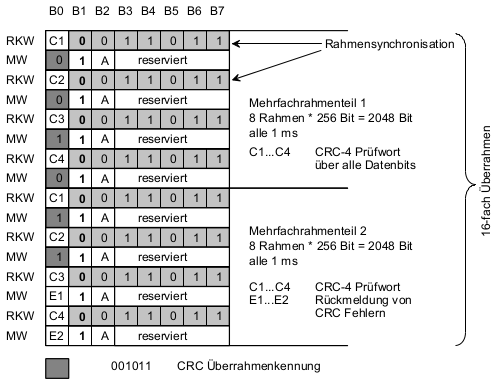
Bsp mit 8 Eingangskanälen:

1. Einschreiben: Die Eingänge schreiben mit f in die ersten Puffer.
2. Speichern: Wenn der Puffer voll ist, wird das in den 2. Speicher kopiert und der Puffer wieder freigegeben.
3. Senden: Der Controller greift zum richtigen Zeitpunkt auf den Speicher zu und sendet die Daten. Bei 8 Kanälen mit mindestens 8\*f, da 8mal mehr Daten übertragt werden müssen.

Auslesen gleich, einfach andere Richtung.

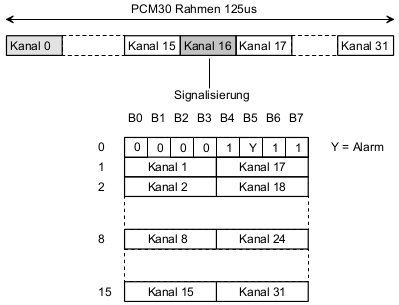


Hier bei **PCM30, die Rahmenstruktur**: K0 für Rahmen- und Fehlererkennung, K16 für Signalisierung. **30 Basiskanäle**, + K0 und K16.



Rahmen mit CRC.

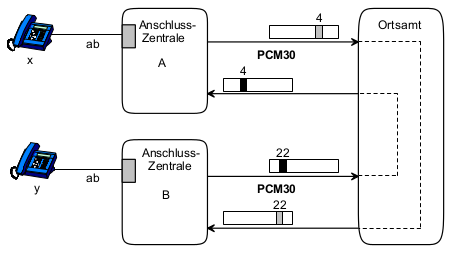
# Signalisierung bei PCM in K16

**Channel Associated Signalling (CAS):**Jedem Datenkanal wird ein Teil des Signalisierungskanals durch feste Bitpositionen zugeordnet. Jeder der so erhaltenen Signalisierungskanäle besteht aus 4 Bit alle 16 Rahmen und hat somit eine Kapazität von 2 KBit/s. ****

**Common Channel Signalling (CCS):**Keine feste Zuordnung zwischen Kanal-Nummer und Signalisierungskanal. **Neuere System arbeiten mehrheitlich mit diesem Verfahren, da der Signalisierungskanal wesentlich besser ausgenutzt werden kann**. Im ISDN-Anschlussbereich wird im Signalisierungskanal das sogenannte D-Kanal Protokoll übertragen, zwischen Amtszentralen wird das Signalisierungsprotokoll Nr. 7 eingesetzt.

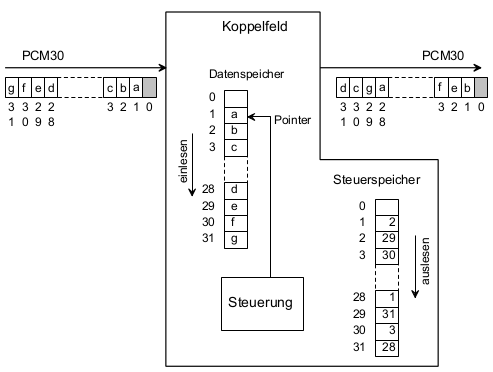
# Digitale Vermittlung

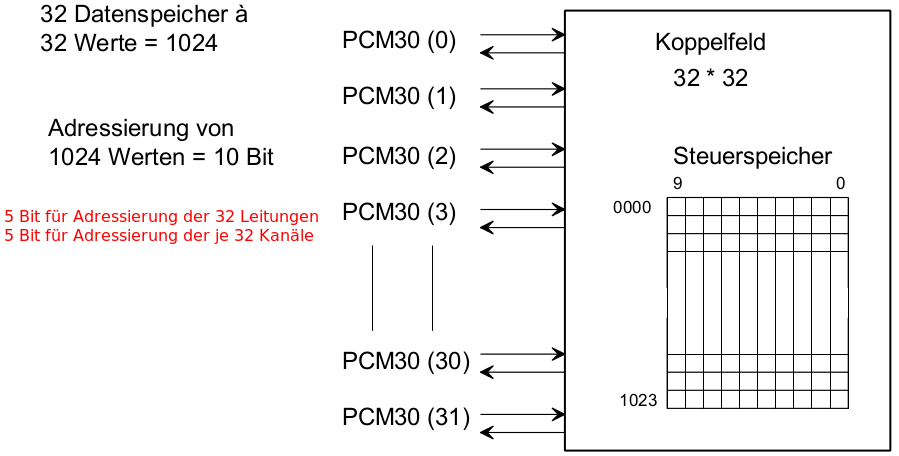
Die Übertragung auf PCM ist immer richtungsgetrennt!



X auf Slot 4 von Zentrale A wird vom Ortsamt auf Slot 22 von Zentrale B gemapped.

**Koppelfeld** verbindet die Eingänge mit den Ausgängen. Takt muss bekannt sein. Im **Steuerspeicher** ist die **Zuordnung der Eingangs- zu den Ausgangszeitschlitzen**. Die **Steuerung** mappt die Daten.   
Der Index des Steuersp. ist Time Slot des Ausgangssignals und der Wert im Steuersp. ist die Nummer des zu sendenden Wertes aus dem Datenspeicher:

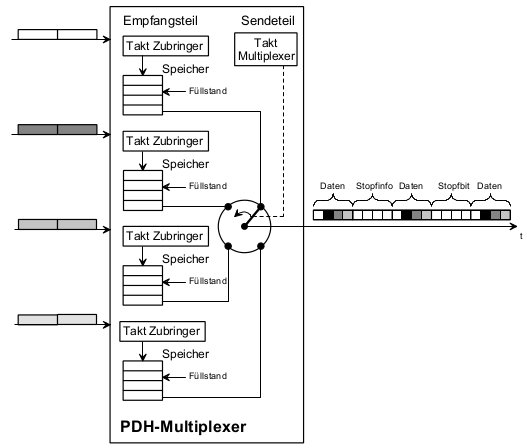


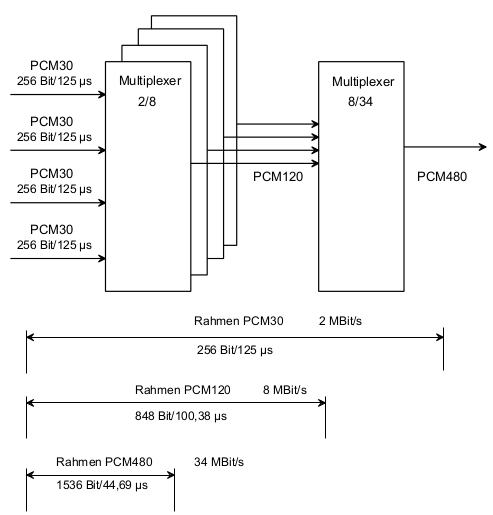


# Plesiochrone Digitale Hierachie (PDH)

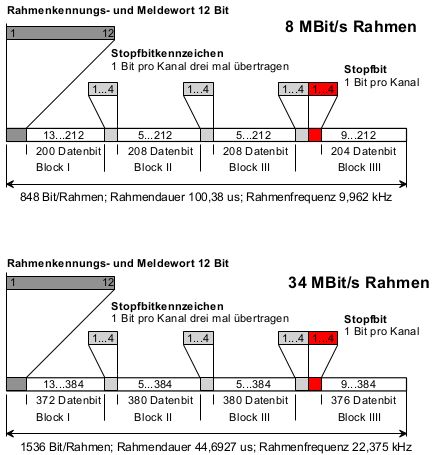


Die Daten werden ab E1 bitweise multiplexed. Da es keinen einheitlichen Takt gibt, werden ist die Freq immer etwas grösser als das xFache (zB bei Eingang 8kHz => 34 statt 32 kHz). Der Rest wird mit Stopfbits gefüllt. Wenn gestopft wird, wird dies durch ein Info-Bit angezeigt. Dann kann der empfangende Multiplexer/Demultiplexer die Bits wieder entfernen.



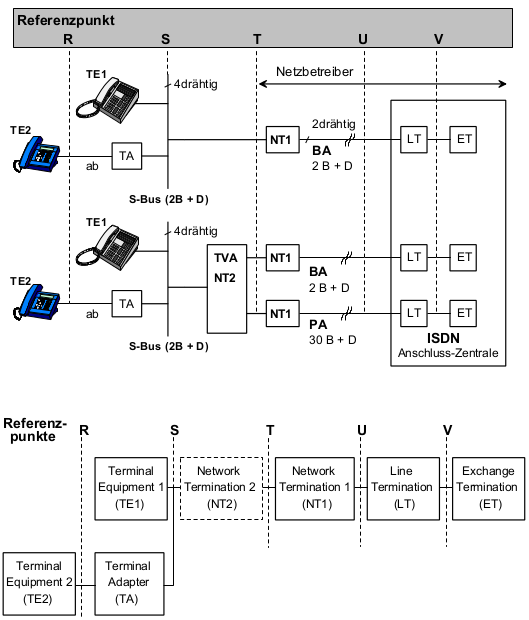


Die Rahmen sind untereinander völlig unabhängig und werden immer individuell behandelt!

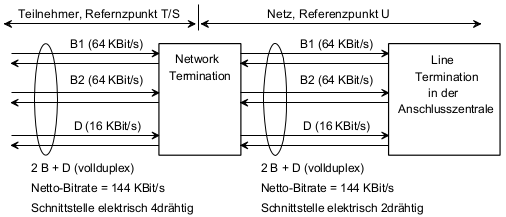


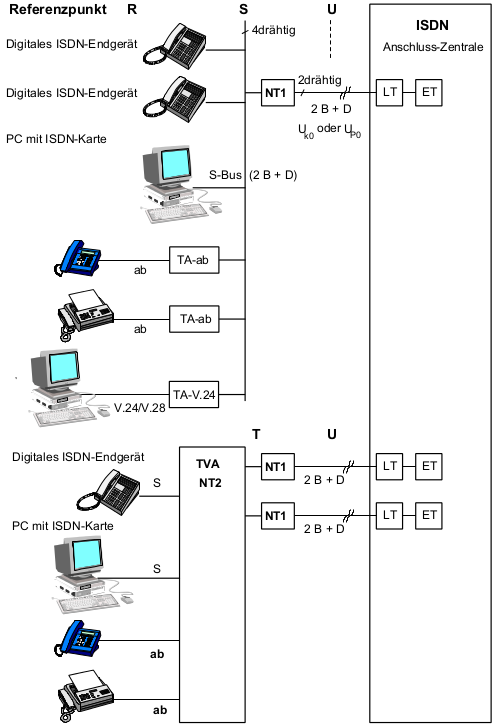
# ISDN

* Alles digital mit 64kb/s.
* Mit 2 oder 30 B-Kanälen verfügbar.
* 2adriger Anschluss.
* Analoger TA möglich => Kompatibilität.



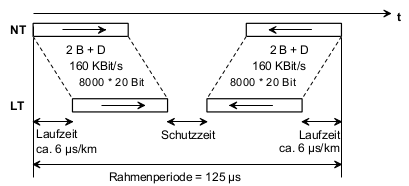
Basisanschluss:



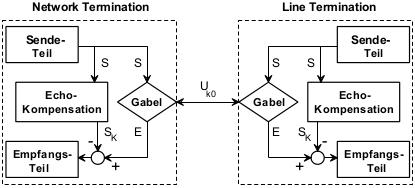


**U-Schnittstelle**: B/D-Kanäle sind zeitmultiplexed.

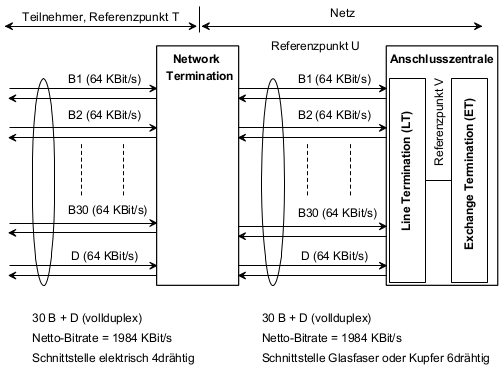
**UP0:** Leitung welchselt Senderichtung ab. Nur noch im TVA-Bereich verwendet.



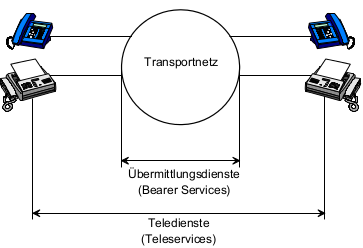
**UK0**: Beide Richtungen werden gleichzeitig übertragen. Via Gableschaltung wird auf jeder Seite das eigene Signal abgezogen und so das andere extrahiert:



Primäranschluss:



# ISDN-Dienste



Gruppen: Übermittlungs-, Tele-, Zusatzdienste.

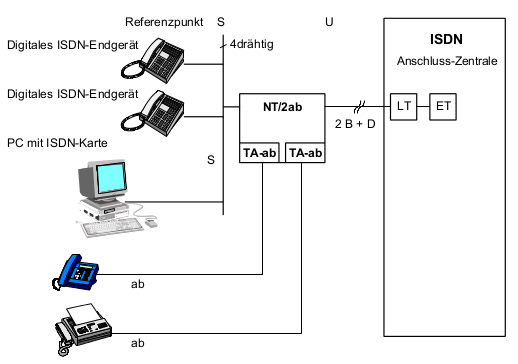
Übermittlungsdienste:

* Unrestricted Digital Information (UDI) on demand/permanent => transparente 64Kb/s-Verbindung.
* Leitungsvermittelte Verbindung für Sprachinformation (Speech) => 3.1kHz Gesprächsverbindung.
* Leitungsvermittelte Verbindung für Audio (3.1 kHz) => Analog
* Paketvermittelte Verbindung im B- oder D-Kanal => Paketdaten auf Basis von X.25.

Teledienste:

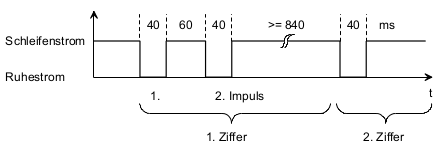
* Telefonie 3.1 kHz
* Telefax Gruppe 4
* Telefonie 7 kHz auf 50-7kHz, 1 B-Kanal
* Videotelefonie auf 2 B-Kanäle

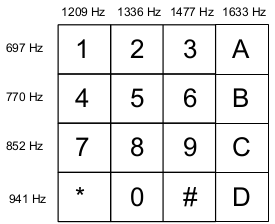
# ISDN in CH

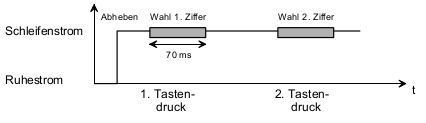


# ab-Schnittstelle

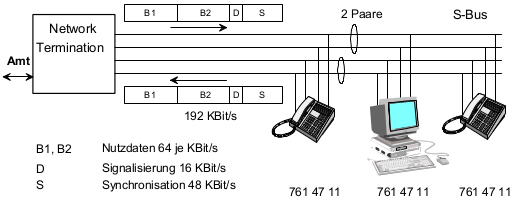
48VDC Speisung, 70VAC (25Hz) Ruf überlagert. Gebührenimpuls bei 12kHz alle 10Rp.

IWV:

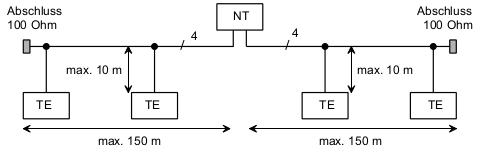
MFV:

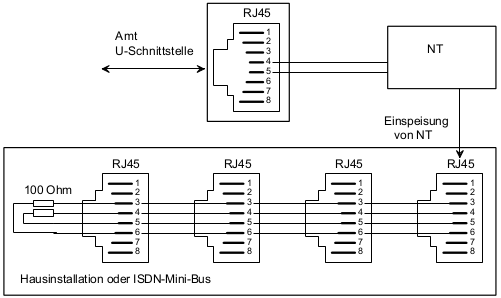


# S-Bus



**Multiple Subscriber Number** für Nummernzuweisung.





# S-Bus-Signalisierung

Digital Subscriber Signalling System No. 1 (DSS1).

* Der Signalisierungskanal (D-Kanal) umfasst die Layer 1...3, wobei die NT1 nur die Umformung der U-Schnittstelle in die S-Schnittstelle auf Stufe Layer 1 vornimmt.
* Ist ein Endgerät (oder ein Terminal Adapter) über eine NT1 angeschlossen, so kommuniziert es auf Layer 2 und 3 direkt mit der Anschlusszentrale.
* Ist ein Endgerät (oder ein Terminal Adapter) über eine TVA angeschlossen, so übernimmt diese die Funktionen der Layer 2 und 3.

In Europa EDSS1, es gibt einige Unterschiede in Layer 3.

# Signalisierung-Layer 2 (Normen Q.920, Q.921)

* Informationsübertragung quittiert oder unquittiert
* Fehlererkennung und Fehlerkorrektur
* Verwaltung der Kanäle
* Adressierung der Geräte

Das verwendete Protokoll basiert auf dem High Level Data Link Contol-Protokoll (HDLC), wird Link Access Procedure on the D-Channel (LAPD) genannt und hat folgenden Aufbau:



TEI am S-Bus: ID des Endgerätes: Wenn fest eingestellt zw. 0…63, wenn dynamisch zw. 64…127.

Wichtigste Layer-2-Abläufe:

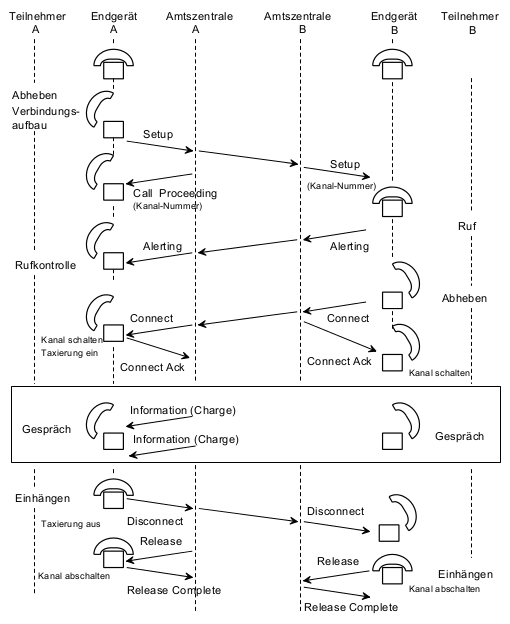
* Das Endgerät fordert mit der TEI-Broadcast-Adresse (127) und dem SAPI Management-Funktionen (63) bei der Anschlusszentrale eine TEI an. Im Informationsfeld steht der Befehl für die TEI-Anforderung und eine Zufallszahl, mit welcher TEI-Anforderungen von mehreren Geräten unterschieden werden.
* Die Anschlusszentrale meldet die TEI mit der zugehörigen Zufallszahl.

# Signalisierung-Layer 3 (Normen Q.930, Q.931)

* Verbindungsauf- und Abbau
* Steuerung der Dienstmerkmale (z.B. Umleitung)
* Fehlerbehandlung

Wichtige Felder:

* Protokolldiskriminator: Unterscheidet ISDN-Protokolle.
* Call Reference: Unterschiedet die Layer-3-Verbindungen, die auf einer Layer-2-Verbindung basieren können.
* Message Type
* Information Element: Gebührendaten, Rufnummern, etc.



Siflu

# VOIP

## Geschichte

**Traditionelle Telefonie:** leitungsvermittelt, zeitmultiplex => konstante Bitraten, exklusiver Datenkanal während Session, kleine kostante Delays

**Paketvermittelte Telefonie:** best effort, paketverluste, grosse unkonstante Delays => in lokalen Netzen beherrschbar, im Internet nicht

## Motivation aus heutiger Sicht

Zusammenlegung der Sprachnetze mit den Datennetzen (Ökonomie) Voip lässt sich in IT umbebung integrieren => call-center, help desk, home office,...

Neue Geschäftsmodelle: cablecom, econophone, sipcall,...

Flexibilität: Auswahl codecs, bitrate, qualität, signalisierung,...

## Unified Communications

Kombination verschiedener Nachrichtenformate und Endgeräte auf einheitlicher Umgebung => Alle Kommunikationskanäle standortunabhängig und jederzeit verfügbar

## Funktionsebenen von Telefonsystemen

bei voip lose gekoppelt, durch offene Schnittstellen

### Media Stream (duplex Audioübertragung im Sprachband)

Bei Voip über Paketstrom realisiert, basiert auf Realtime Transport Protocol (RTP)

(=B-Kanal) != streaming wegen Kollisionen, Buffer

### Signalisierung von Anrufen = Sessions

Aufbau, Unterhalt und Abbau von Verbindungen sowie für Informationsaustausch

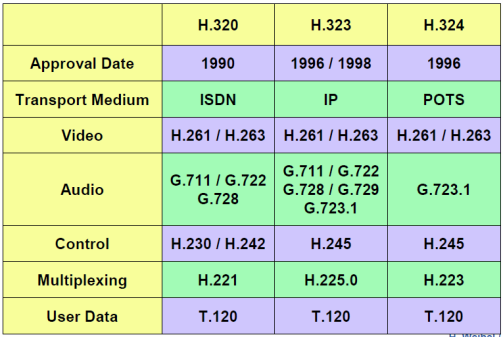
zuständig

Protokolle: H.323, SIP, SCCP (cisco), Skype

### Steuerung der Anwendung => Dienstelogik

Zusatzdienste (Weiterverbinden, Halten, Anklopfen...) werden von Endsystemen selbst oder durch spezielle Server gesteuert.

## Architektur von H323 und von SIP



## H32x Protokollfamilie (ITU standard)

Protokollfamilie umfasst Codierungs Standards für Sprache, Bild, Streams, steuerung

und Signalisierung

H324: Multimedia über POTS

H320: Multimedia über ISDN

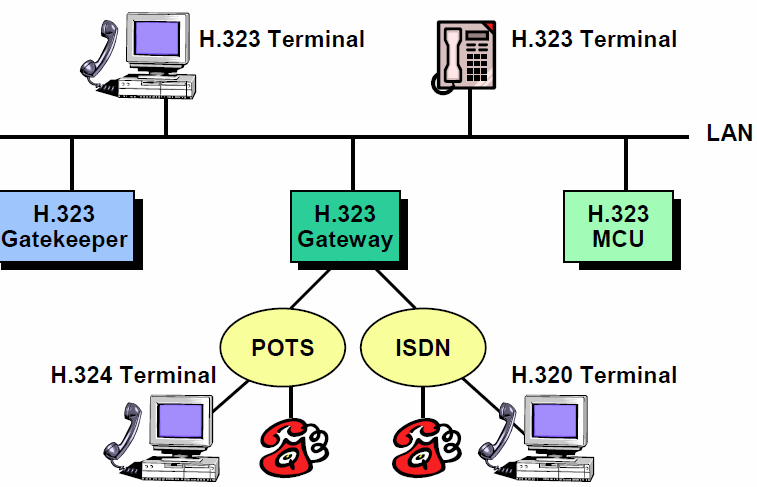
H.323 Netzwerkelemente:

**Gateway** Übergang in andere Netze

**Gatekeeper**: Zone, Teilnehmer dieser Zone müssen sich bei ihm registrieren, Bandbreitenmanagement, Umsetung Telnr – IP

**Endgerät**: bei Freigabe kann es eine Verbindung aufnehmen (Handshaking H.245 => teilt Fähigkeiten mit, Sprache einziger Standard)

**Multipoint control Unit:** Konferenzschaltung Audio / Video kombinieren

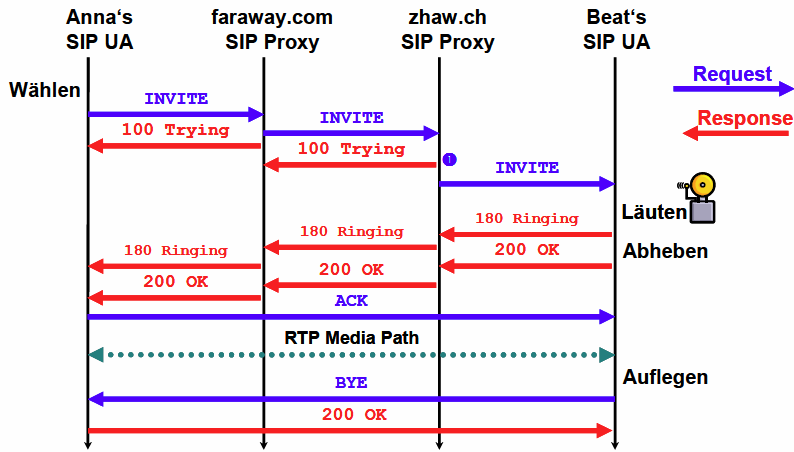


## SIP (IETF)

Näher an paradigmen des Internet, ursprünglich Aufbau von Videokonferenzen, ver-

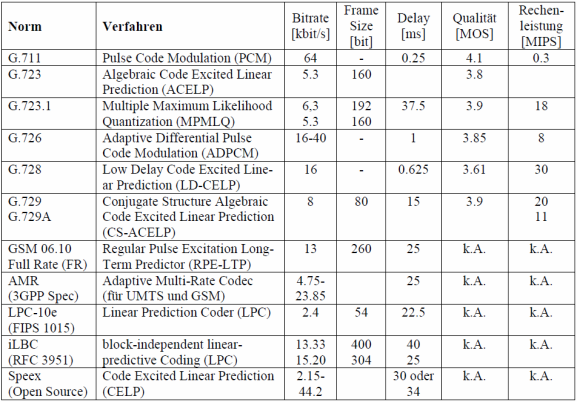
teilung von Multimediainhalten im internet => umfasst nur die Signalisierung von

Session, session wird in Session Deskription Protokoll (SDP) gehandelt



# Sprachcodecs

Kompression durch Ausnutzung von Signalcharakteristika | fehlende Pakete: Interpolation, extrapolation oder replay | Sprechpausenunterdrückung: da kein Duplexkanal => comfort noise anstelle absoluter Stille

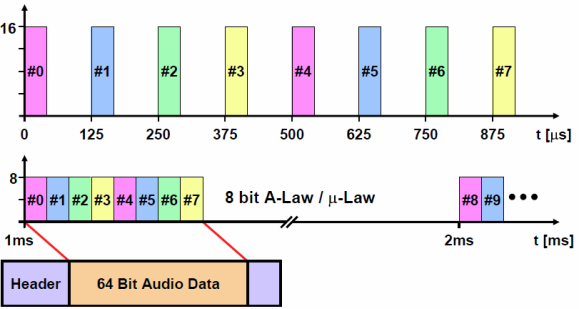


## Arten von Sprachcodecs

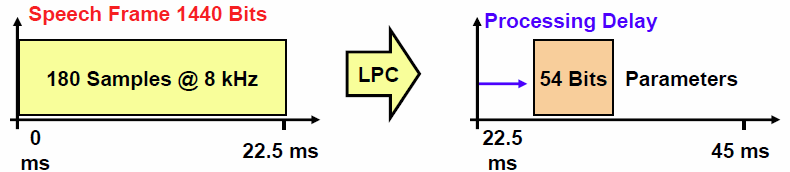
### Waveform – Codec (PCM, ADPCM [ISDN])

Codierung des Zeitlichen Signal-Verlauf => hohe Bitrate, geringer Rechenaufwand,

kleine Verzögerung, andere Töne



### Source – Codec (LPC)



Parameter eines Modells werden ermittelt und übertragen => geringe Bitrate, hoher

Rechenaufwand, grosse Verzögerung, nur Sprache

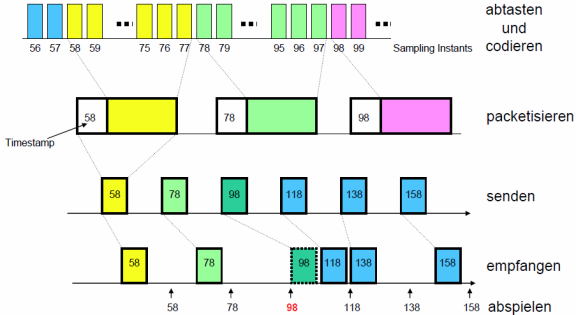
### Hybrid – Codec

Kombination, meiste Voip Codecs gehören dazu (!G.711)

# Media Streams und das Real-time Transport Protocol (RTP)

TCP nicht geeignet (retransmission, verzögerungen) => UDP, RTP

## Arbeitsweise von RTP

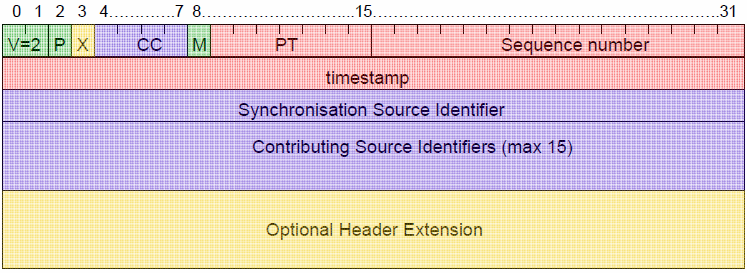


Paket füllen: 20\*125ys = 2.5ms => timestamp

## Format von RTP-Paketen

Setzt auf UDP auf, Port 5004, | für jede Mediastream Richtung eine RTP session |

grosser Overhead (L2/IP/UDP/RTP) wegen kurzen delay, kompression, qualität



P: Padding => Ende des Pakets hat Padding oktets die nicht zur Payload gehören

(Anzahl im letzetn Oktett) | bei nicht beliebig wählbarer Blockgrösse (schlüsselung)

X: Header Extension activ

CC: CSRC Count: Anzahl Contributing source Identifier

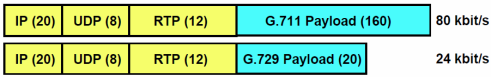
M: durch Profil definiert => Frame – Grenze

PT: Payload: angabe welche Applikation payload interpretieren muss

SSRC / CSRC: Signalquellen => identifikation / synchronisation

## Compressed RTP (cRTP)

Header Kompression => kleiner overhead (Header oft gleich, nur 1feld anders)



## Das Real-time Transport Control Protocol (RTCP)

Monitoring: Empfänger misst delayvariation (jitter), Empfänger führt statistik über

verlorene pakete. Wichtig bei Multicast

## Secure RTP/RTCP (SRTP/SRTCP) RFC 3711

Verschiedene Verfahren, standard: AES 128bit | Header nicht verschlüsselt (kompr)

# Sprachqualität (ITU-T P.800)

MOS: 5: excellent, 4: good (bei payment erwartet) 3:fair, 2: poor, 1: unsatisfactory

## Einflussfaktoren

Delay (<150ms) | Verlustlücken < 200ms | Echo (Echokompensator im Endgerät) |

Codec (robustheit bei verlust => überbrücken) fidelity(X): gesendet = X \* empfangen

# Signalisierung mittels SIP

Textorientiert (HTML, SMTP,..) URI anstelle Telnr, setzt auf TCP / UDP auf | User-

location | user availability | user capability | session setup | session management

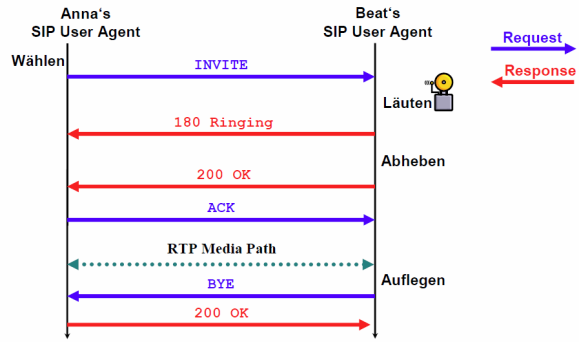
## Ablauf von Verbindungsauf - und Abbau

### Ohne Proxy

Direkter Verbindungsaufbau, ausser: URI von gerufener Person unbekannt | gerufene

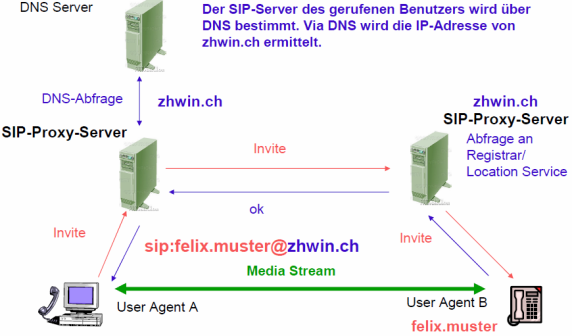
Person nicht an selbem Terminal erreichbar | Terminal IP ändert | gerufene versteht

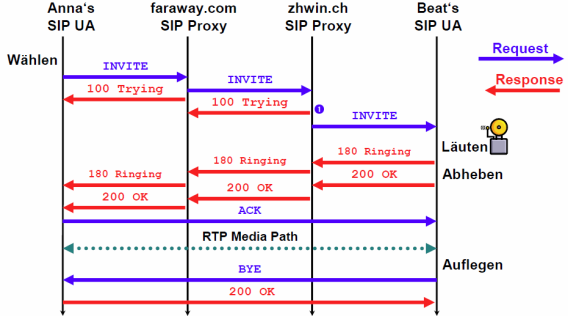
kein SIP (Telefon, GSM-Handy, ...)



### Mit Proxy (statisch oder DHCP)

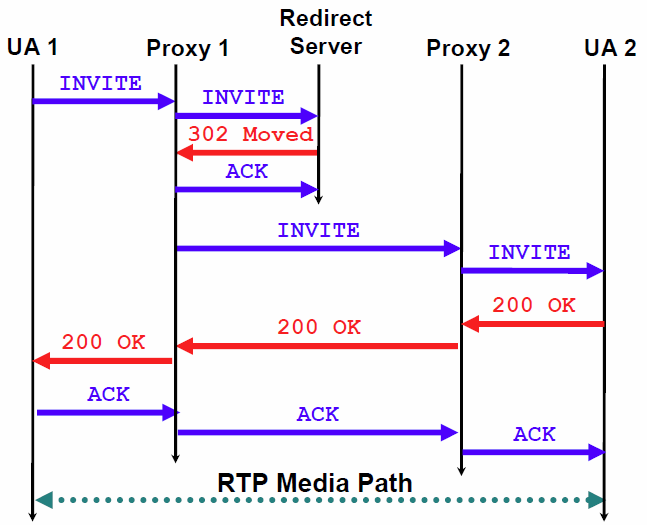
SIP-Proxy handelt alle Anfragen für seine User Agents





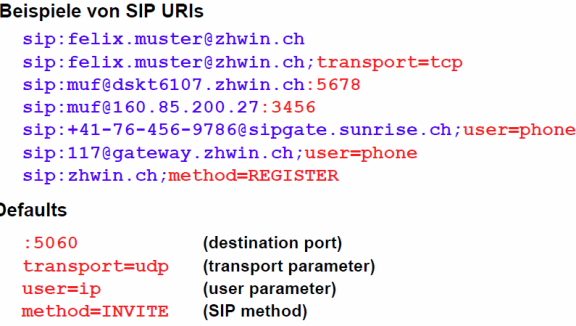
### Proxy, Registrar, Redirect Server

Ein Proxy-Server kann einen kommenden Anruf weiterleiten, oder ihn an den Sender zurückgeben (Redirect)

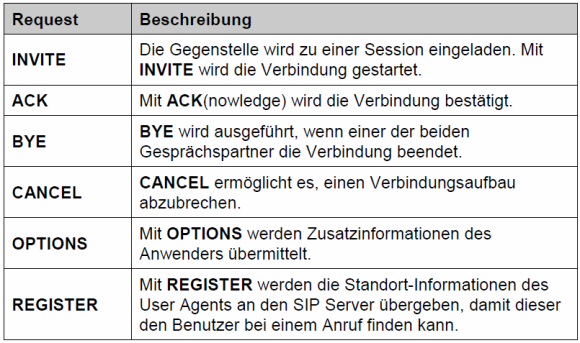


## Uniform Resource Identifier (URI)

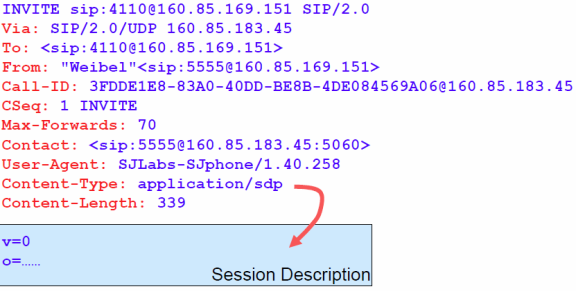
Identifiziert SIP – Instanzen, form: <sip:user@domain>



## SIP-Methoden



## Die INVITE-Methode im Detail



**Via**: bei jedem Hop ein neues feld, branch identifiziert Transaktion, beginnt immer

mit „z9hG4bK“ (bei RFC 3261)

**Call-ID**: haben alle Meldungen des Dialogs, verwendung von IP verhindert, dass ein

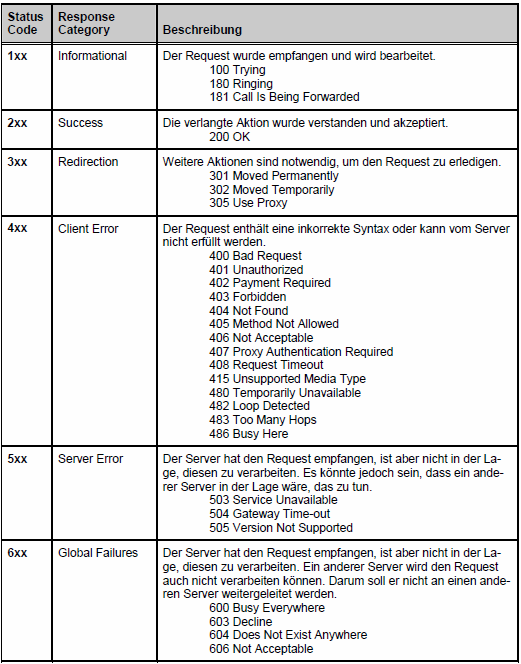
anderer user zufällig dieselbe ID wählt | To, From, Call-ID identifizieren peer-to-peer

SIP beziehung vollständig

**CSeq**: Sequenznummer: Meldungen ordnen, verluste feststellen, wird bei jedem Request um 1 erhöht besteht aus nummer + Methode

## SIP-Antwortcodes

Wie bei http / SMTP

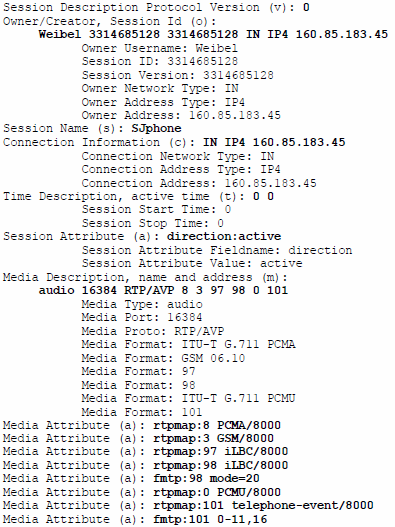


## Sicherung von SIP

Kann nicht end-to-end verschlüsselt werden (Knoten müssen Meldungen ändern können), daher TLS zwischen SIP servern

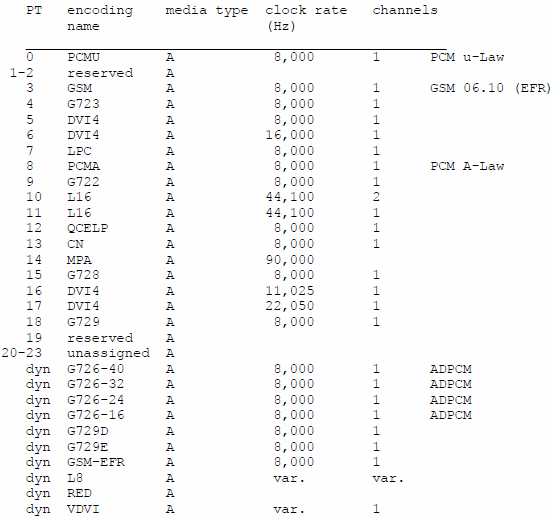
# Session Description Protocol (SDP) (RFC 2327)

Beschreibung einer Session anhand Inhalt (Body) von INVITE Requests / Responses

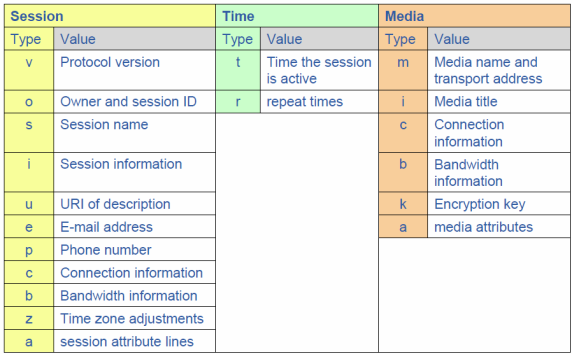


m=: medium | RTP/AVP sind druch RFC 3551 beschrieben | Media Formate RTP

Payload Types (PT) für Mediatype (A) Audio:



## SDP-Parameter



# VoIP-Endgeräte

## IP Phone

Normales Telefon mit IP schnittstelle | anschlussorientiert | sinnvoll wo kein pc da-

neben ist | meist mit Switch | power over ethernet

## Soft Phone

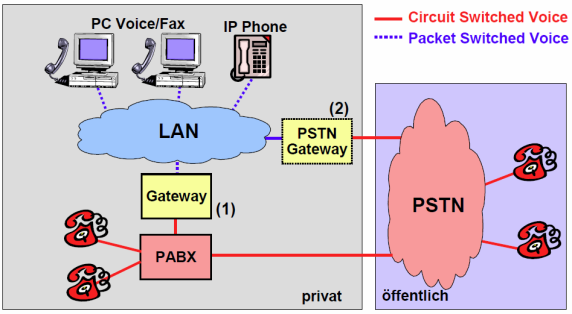
Apps, die Telefonieren ermöglichen, nicht anschlussbezogen, dort wo Benutzer ist

## Analog Telephone Adapter

Adapter, verfügen über ähnlichen Funktionsumfang wie IP-Phone

# Einsatzgebiete von VoIP

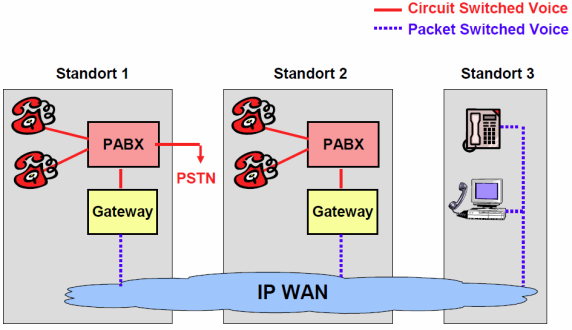
## PABX – Ersatz (Teilnehmervermittlungsanlagen)



## PABX-Trunking

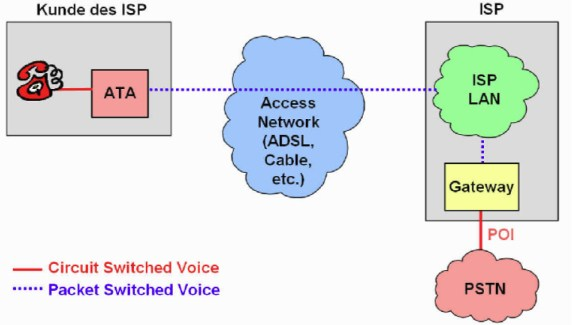
Mehrere PABX über IP vernetzen, grosses einsparungspotenzial im Vergleich zu

mietleitungen | alternativ: **Circuit Emulation over Packet (CEP):** transportiert ein TDM-Signal (z.B PCM30) als ganzes in IP-Paketen



## Telephony Internet Service Provider

ISP wird zu Fernmeldedienstanbieter und braucht daher eine konzession und wird meldepflichtig gemäss FMG



POI: Piont of Interconnection => Schnittstelle PSTN – ISP

# KT2 Kapitel 7 Datenübertragung

## Zugang zum Internet

ISDN [analoge ab-Schnittstelle mit modem; digitale ISDN schnittstelle mit ISDN

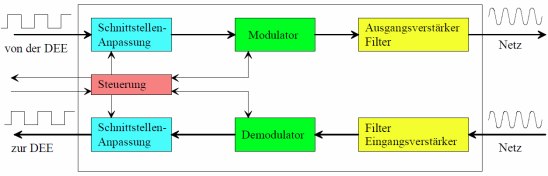
adapter; ADSL] | TV – Kabelnetze | Strom – Netze (Powerline) | Public WLAN |

Wireless Local Loop | Mobile (GSM, HSPDA, GPRS, UMTS)

## Modem [MO]dulator – [DEM]odulator

wandelt digitale Signale in Signale im Sprachfrequenzbereich (0.5 – 3.4 kHz) um

## Funktionsprinzip



ITU legt Werte für Übertragungsgeschwindigkeit, Betriebsverfahren, Wahlverfahren

fest | Simplex, Halbduples, Vollduplex Verbindungen

## Realisierung von Vollduplex – Verbindungen

Problem: 2 Draht Leitungen Lösung: pro Richtung 1 Leitung (teuer) | 2 Kanäle in

verschiedenen Frequenzbändern auf selber Leitung => Echokompensation (gesendetes Signal vom empfangenen subtrahieren)

## Modulationsarten (auf 0,3 – 3,4 kHz)

**Amplitudenmodulation (AM):** Frequenz fest; Information in Amplitude codiert.

**Frequenzmodulation** **(FM oder FSK = Frequency Shift Keying)** Amplitude fest;

Information ist in Frequenz codiert.

**Phasenmodulation** **(PM oder PSK = Phase Shift Keying):** Amplitude und Frequenz

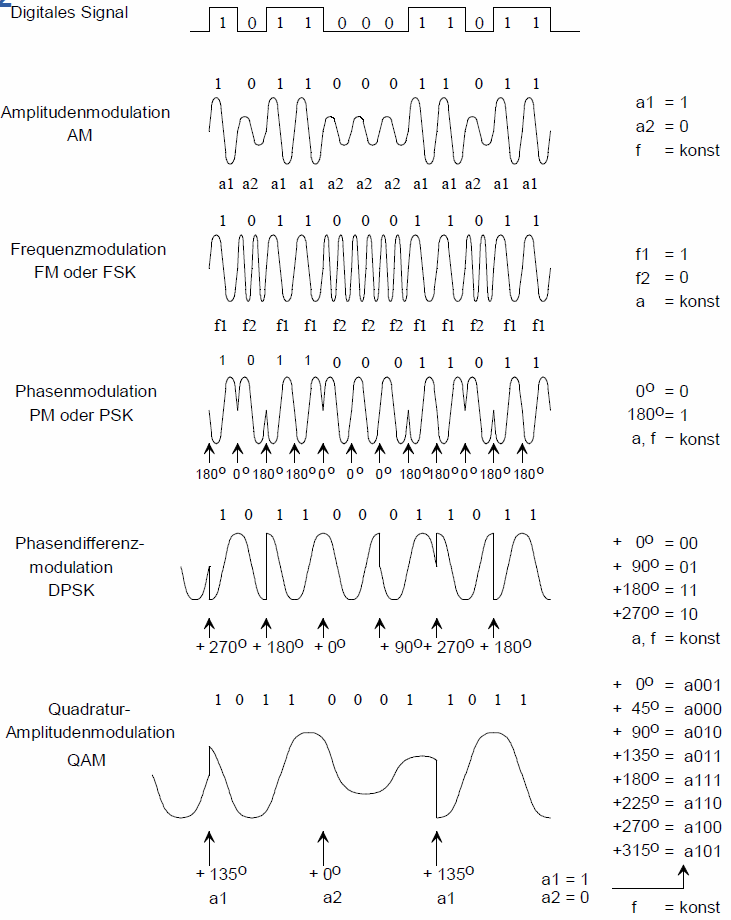
fest, Information in Phasenlage codiert.

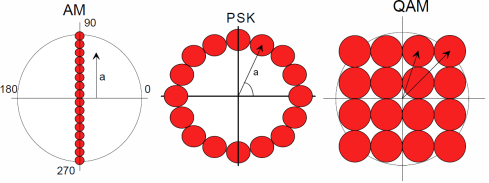
**Phasendifferenzmodulation (DPSK):** Amplitude und Frequenz fest; Information in Phasendifferenz codiert.

**Quadratur-Amplitudenmodulation (QAM)** Kombination vom Amplitudenmodulation und Phasendifferenzmodulation.

=> max. mögliche Schrittgeschwindigkeit (Baud) ist durch Bandbreite limitiert => Übertragung von mehreren Bits pro Schritt (DPSK, QAM)

## Die Wichtigsten Modulationsarten





Grösse der Kreise: max. Abweichung; => QAM hat grösste Übertragungsrate bei konstanter Fehlerrate

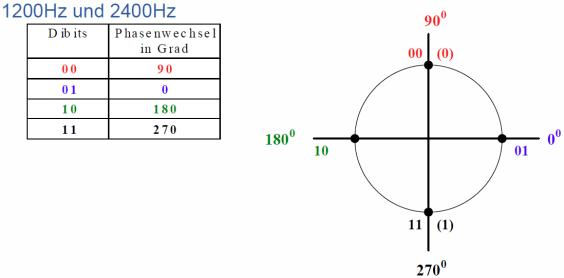
## Modems nach ITU Empfehlungen

### Modem nach V.21 (300 Bit/s Duplex | öffentliches Wählnetz)

**Frequency Shift Keying** (unterschiedliche Trägerfreq. für Senden / Empfangen)

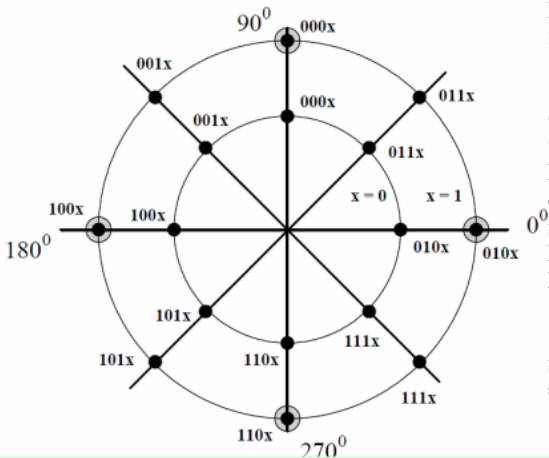


### Modem nach V.22 (1200 Bit/s Duplex | öffentliches Wählnetz | 600Bd)



**Phasendifferenzmodulation** (1200 Hz, 2400Hz) | 4 Phasen, 2Bits / Takt (Dibits) => 600Bd \* 2 Bit = 1200Bit/s | schaltet bei schlechter Leitung in 2 Zustand Modus zurück (=600Bit/s)

### Modem nach V.22bis (2400 Bit/s Duplex | öffentliches Wählnetz | 600Bd)



Erweiterung von V.22 auf 2400Bit/s mittels Quadbits => **höchstwertige 2 Bit (3,2)** Phasenwechsel des Quadranten gegenüber der vorherigen Phase; **Bit 1** definiert zusätzlichen Phasenwechsel innerhalb Quadrant; **Bit 0**: Amplitude **Baudrate**: 600Bd (600Bd \* 4Bit = 2400Bit/s); bei schlechter Leitung: nur noch 4 Zustände (= V.22 = 1200Bit/s)

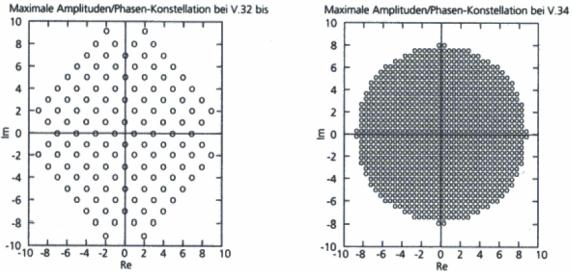
### Modem nach V.32 (9600 Bit/s, Vollduplex, 2400Bd)

**Echokompensation** | beide Kanäle 1800Hz | 5 Bits / Schritt; 1 Redundanzbit => 4 Nutzbit (4Bit \* 2400Bd = 9600Bit/s)

### Modem nach V.32bis (14400 Bit/s, 2400Bd)

Wie V.32 jedoch 7Bits / Schritt, 1 Redundanzbit = 6 nutzBit

### Modem nach V.34 / V.34+ (V.Fast) (28800 Bit/s | 33600 Bit/s [V.34+], 2400 / 3000 / 3200 Bd [je nach Leitung])

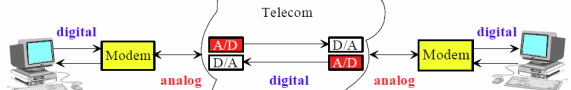


### V.42 – Datensicherung und V. 42bis Datenkompression

Erhöhung der Übertragungsrate durch Datensicherung und Kompression (bis 4 zu 1)

### Modem Technik X2 (V.90) Up: 28800 Bit/s (V.34 | V.34+), Down: 56Kbit/s

A/D – Wandlung beschränkt Ü-rate auf ca 35Kbit/s (Quantisierungsrauschen) **Upstream** mit **28.8 Kbit/s** (V.34)



**Downstream**: theor: 64Kbit/s (8000/s 8 Bit => 256 Zustände), wegen nichtlinearer

Quantisierung aber nur 128 Zustände möglich = 7Bit \* 8000/s = **56Kbit/s**; Falls Strecke zusätzliche AD-Wandlungen enthält => in beide Richtungen V.34 => X2 wird nur angewandt, wenn keine AD-Wandlung nötig ist, sonst V.34



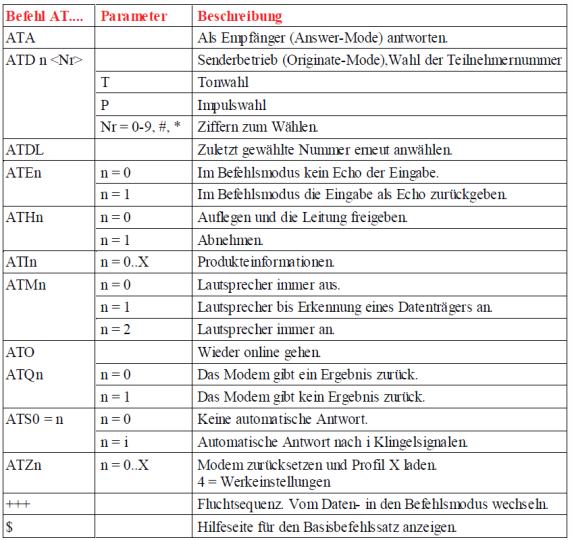
## Leistungsmerkmale Telefax

V.27ter: 2400/4800 | V.29: 7200/9600 | V.17: 7200/9600/12000/14400 Bit/s

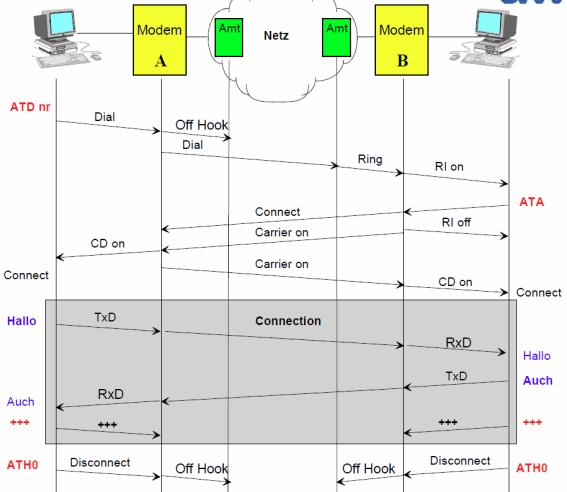
## Programmierung (AT - Befehlssatz)

**Interne Modem**: Herstellerspezifische Software **| Externe Modem**: Hayes oder

AT-Befehlssatz:

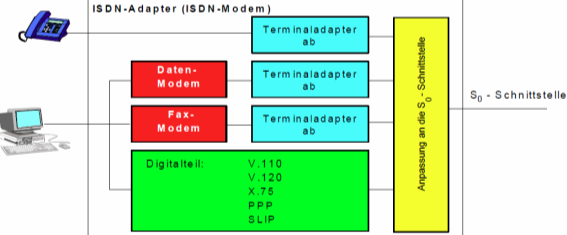


Modem hat 2 Zustände: Befehl / Datentransfermode | nach Einschalten im Befehlmode => Connection aufbauen „CONNECT“, geht automatisch in transfermode über | Übergang Transfer-Befehlmode: Unterbruch / Abbruch der Verbindung oder Escape-Befehl „+++“, davor und danach 1sek Pause, +++ während 1sek eingeben |



# ISDN – Adapter | ISDN Modem

Adaper: ISDN – Modem (Bild, ohne Modem / TA)



**V.110 (CCITT):** Umsetzung des seriellen Datenstromes der Datenendeinrichtung auf 64 Kbit/s Strom von ISDN | Daten werden ohne Datensicherung mit **Leerbits** in

64 Kbit/s ISDN - Kanal verpackt.

**V.120 (CCITT):** Verpacken / Übertragen mit HDLC (High Level Data Link Control)

**X.75 (Protokoll):** Ursprung: öffentliche Paketvermittelte Datennetze, heute im ISDN

**SLIP (Serial Line IP Protokoll)(RFC 1055):** Layer 2 Übertragung von TCP/IP

**PPP (Point to Point Protokoll) (RFC 1547):** nachvolger von SLIP

# Digital Subscriber Line (DSL) [KP=Kupferpaar]

**HDSL (High Bit Rate DSL):** 776Kbit/s 1KP, 1160Kbit/s 2KP, 2312Kbit/s 3KP => 2 Mbit/S E1 PDH – Signal über 3 Kupferpaare

**SHDSL (Symmetric High – Speed DSL):** 2312 Kbit/s 1KP, 4624 Kbit/s 2KP => 2 Mbit/s E1 PDH – Signal über 1 Kupferpaar

**ADSL**: unten | VDSL (Very High Bitrate DSL): Up 6, Down 55 Mbit/s (dist)

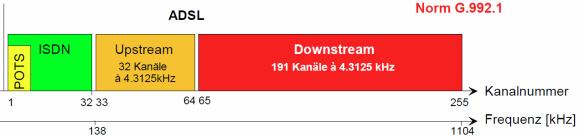
## DSL Grundpinzip

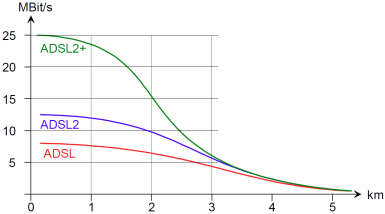
Nutzt grösseren Frequenzbereich aus als ISDN |HDSL und SHDSL erlauben keinen parllelen Telefon Betrieb (POTS oder ISDN) => möglich bei ADSL, VDSL

## Asymetric Digital Subsriber Line (ADSL)

Bei ADSL werden Daten und Sprachinformationen beim Teilnehmer und der Zentrale durch Splitter getrennt und über verschiedene Wege geleitet | ADSL over POTS (Plain Old Telefon System) [ITU G.922.1 Annex A] | ADSL over ISDN [ITU G.922.1 Annex B]

Übertragung: DCT (Discrete Multi Tone ) => teilt Frequenzbereich in 4,3125 kHz grosse Frequenzbänder auf => QAM (4kBd), leitungsparameter bestimmen wieviele Zustände (z.B: 256 Zustände = 8Bit / Takt => 32kBit/s/Kanal) => Daten parallelisieren, über max 256 Bänder versendet

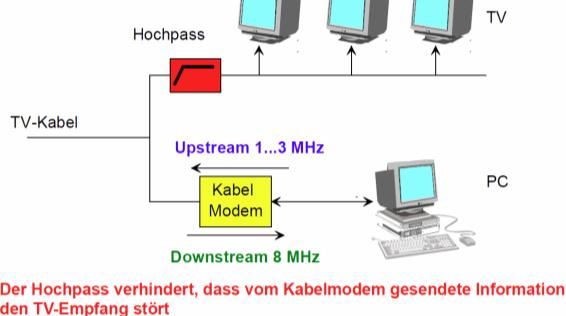




ADSL2+: zusätzlicher Frequenzbereich (bis 2200kHz anstelle 1104kHz)

# TV – Kabelnetze

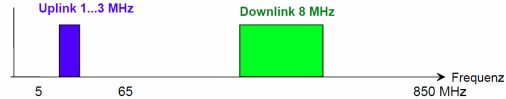
Konventionell: reines Verteilnetz | Programme: Frequenzmultiplex in 8 MHz Bänder; bis 850Mhz, ca. 80prog | für Datenverkehr: Verstärker bidirektional; TV / Datenkanal entkoppelt, tiefe Freq: Up, hohe: Down



## Übertragungstechnik (DOCSIS)Data Over Cable Service Interface Specification (ITU)

Down: QAM 64 zustände (6Bits) =41Mbit/s oder 256 Zustände (8Bits) = 55Mbit/s

Up: QuadPSK (2Bits) = 3Mbit/s oder QAM 16 Zustände (4Bits) = 7Mbit/s



## Funktionsweise

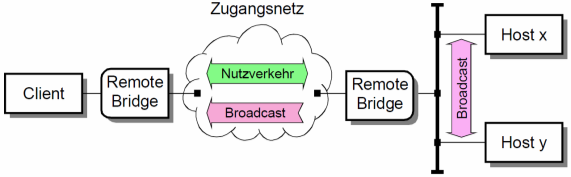
**Down**: 802.3 vergleichbares Protokoll; nur Kopfstation sendet, keine Kollisionen; Dabelmodems werden über 24Bit MAC-Adresse angesprochen; Modem = Bridge; ca 500 Teilnehmer/Segment (10% Teilnehmer mit 1Mbit/s aktiv)

**Up**: Media Access (Uplink wird per Zeitmultiplex in Timeslots geteilt, werden dynamisch den Modems zugeteilt); innerhalb 1timeslot sendet nur 1 Modem; 1gemeinsamer Timeslot (für anmelden beim Einschalten)

# KT2 Kap8 Remote Client integration

# Grundkonfigurationen und Leistungsmerkmale

## Grundkonfigurationen und Leistungsmerkmale

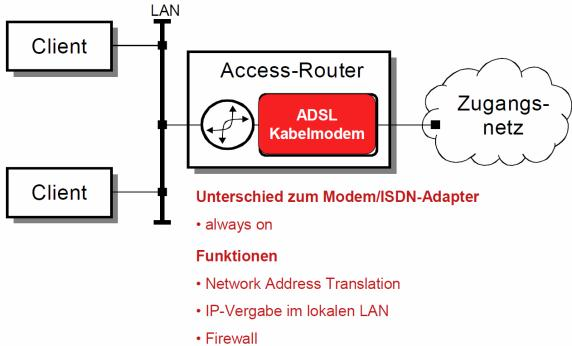


Anstelle von Remote Bridge Router verwenden um Broadcast Verkehr zu sperren, Filterung von Paketen

## RoutingKonfigurationen

**Einzelner Client**: Modem/ISDN-Adapter, IP-Software-Modul im Client-Knoten

**Mehrere Clients**: auf Rechner mit phys. Netzzugang routing-fähige Software **(IP-Forwarding)** oder Access Router (meist proprietäre Protokolle)



## Dial on Demand

Automatischer Verbindungsaufbau bei Bedarf | Abbau bei Nichtbenutzung (Timeout) | Bandbreitenabhängiges Zu/wegschalten von Kanälen (Channel Bundling) | schwierige Kostenoptimierung

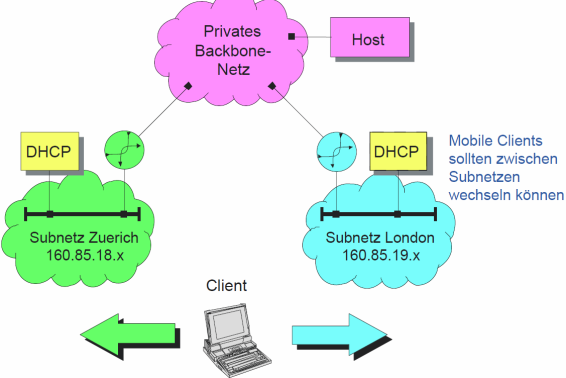
## Firewall

Erlaubt gezielt Pakete auszufiltern / übertragen

## Rückruf (Callback)

Remote Client ruft zentralen Server und authentisiert sich, der Server bricht die Verbindung ab ruft den Remote Client zurück. | Gründe: reduziert die Kosten des Clients / Sicherheit |

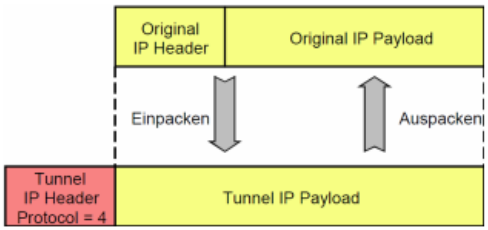
## Dynamische Vergabe von IPAdressen



**DHCP (Dynamic Host configuration Protocol):** flexiblere Variante von BOOTP | dynamische Vergabe von IP’s in best. Beriech | Address Leasing oder fixe Adressen | routbar => zentraler DHCP server oder separate pro Subnetz

## IP Tunneling IETF (RFC 3344)

Feste Adresse für Mobile Node => IETF protokoll **Mobile IP** | Routing Protokolle sinnlos, da die vorteile des hierarchischen Adressraums verloren gingen, enorme Menge an Routingeinträgen, Sicheheit | IP-Tunneling: Datagramm wird als Protokoll Payload eines gleichhochen oder höheren OSI-Layers transportiert | **Ablauf**: Sender (Tunneleingang) fügt äusseren Header hinzu (Protocol = 4); Router routet anhand äusserer IP; Empfänger (Tunnelausgang) entfernt äusseren Header, leitet ursprüngliches Datagramm weiter



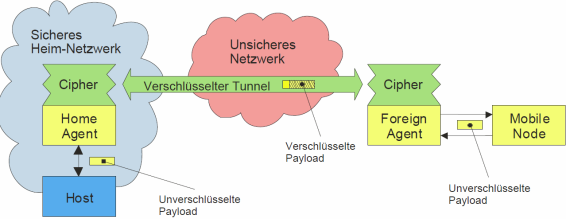
Probleme: MTU überschreitung => Fragmentierung => weniger Durchsatz; Fehler-Behandlung / Signalisierung (ICMP) schwierig, da 2 IP level

**Home Address**: innere IP, IP des mobile Node in seinem Home Network, ändert nie

**Care-of Address**: äussere IP, temporär (DHCP) von remote Netz adressraum

**Home Agent**: Router im home Network, kennt zusätzlich position des mobile nodes; Tunnelanfang

**Foreign Agent**: im selben Subnetz wie mobile Node, logische Komponente (Router oder auf selbem Knoten wie mobile Node); Tunnelende



### Mobile IP startup [Mobile Client = MC]

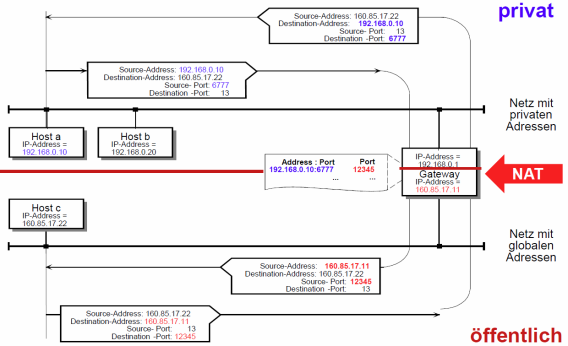
MC bezieht in fremden Netz IP => MC muss foreign Agent finden => MC gibt Foreign Agent seine Link-Layer-Adresse (MAC), Care-of Adresse und Home Address mit Security Infos => foreign Agent registriert MC bei dessen Home Agent: Care-of-Adresse mit Security Informationen => Home Agent prüft Angaben, führt DB nach, schickt Bestätigung an Foreign Agent

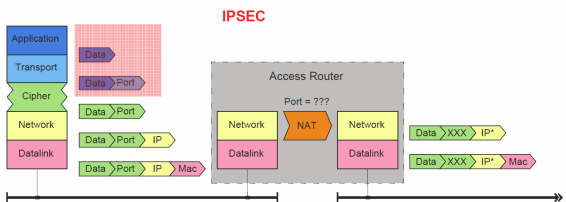
### Mobile IP Betrieb [Mobile Client = MC]

Meldung Host an MC, wird von Home Agent abgefangen => Home Agent weiss wo MC ist (kennt IP von Foreign Agent) => Home Agent tunnelt Meldung an Foreign-Agent => Foreign Agent entpackt Meldung, leitet sie an MC weiter => MC sendet Antwort direkt oder vie Tunnel

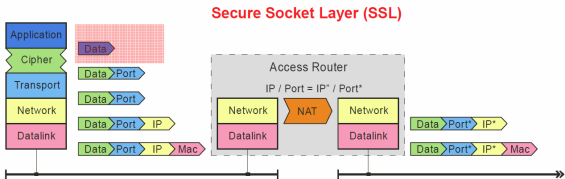
## Network Address Translation | IP Masquerade | Port/Adress Translation

Erlaubt, IP-Netz hinter einer offiziellen IP-Adresse zu verstecken | spart IP adressen | fixe Adressen in lokalem Netz, auch wenn Operator nur dynamische zulässt | versteckte Rechner | Probleme mit Layer ≤ 4 verschlüsselten Verbindungen, da Ports nicht im Klartext

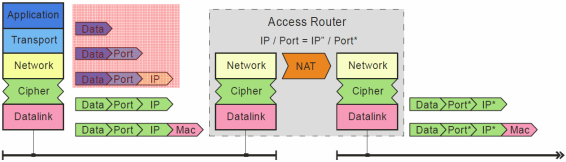














# Link - Layer – Protokolle



Verbindung zwischen 2 Routern über Mietleitung / Wählverbindung zwischen Host / Router benötigt ein Punkt-zu-Punkt Protokoll auf dem Link-Layer (PPP / SLIP)

## Serial Line Internet Protocol (SLIP)

Entwickler: R.Adams (1984) | enthält rohe IP-Pakete mit Flagbyte (0xC0) am Ende des Frames | Nachteile: keine Fehlererkennung/korrektur, nur IP, keine dynamische IP-Adressierung, keine Authentifizierung, kein zugelassener Internet Standard

## Point – to – Point Protocol (PPP) RFC 1661 (1662,1663,1618)

Kapselungsprotokoll für übertragung von Datagrammen über Punkt-zu-Punkt Verbindungen (≠Ethernet, benötigt keine MAC - Adresse) für verschiedene Protokolle

Standard für:

• asynchrone (Start/Stop-Bit) und bit-orientierte synchrone Übertragungsstrecken

• Netzwerk-Protokoll-Multiplexing (verschiedene Netzwerk-Protokolle möglich)

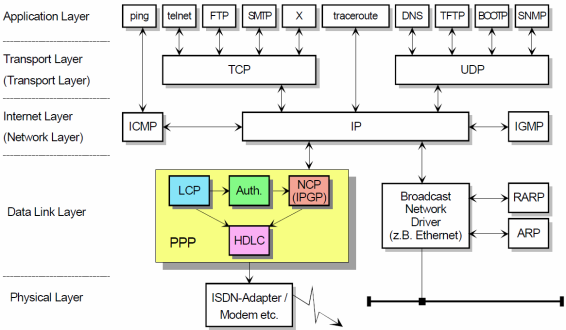
• dynamische Zuordnung/Verwaltung von IP-Adressen

• Verbindungskonfiguration

• Testen der Verbindungsqualität

• Fehlererkennung

• Aushandeln von Optionen



### Hauptkomponenten

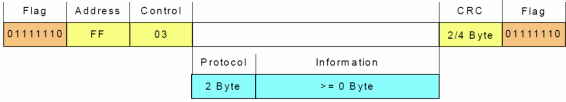
**Link Control Protocol (LCP):** Aufbau, Konfiguration, Test von Datenverbindungen auf Layer2

**PAP, CHAP**: Authentifizierung

**Network Control Protocol (NCP):** Konfiguration der unterschiedlichen Protokolle des Network-Layers (für IP: IP Control Protocol [IPCP])

**Kapselung von Datagrammen:** auf Basis von HDLC

### PPP Frame – Format



**Flag**: Anfang/Ende des Frames (Layer1) (gehört nicht zum PPP - Frame)

**Address**: 11111111 => Standard-Broadcast-Adresse (127) PPP weist keine individuellen Adressen zu Control: 00000011 (unnumbered Frame), da keine Flowcontrol / Fehlerkorrektur

**Protocol**: Protokolle in RFC 1700 definiert | Network-Layer Protokolle: MSB=0; MSB=1: Management Protokolle (LCP, NCP) | 2 Byte, ausser über LCP 1Byte

**PPP-Information**: Datagramm des in Protocol spez. Protokolls | länge: 1500Byte, ausser in LCP anders festgelegt

**FCS (Frame Check Sequence):** 16-Bit CRC, spezielle Fälle: 32Bit CRC

### Aufbau einer PPP verbindung

**Link Establishment Phase**: Verbindungsaufbau / konfiguration (LCP) | Optional: Verbindungsqualität ermitteln | Verbindungsqualität testen (übertragung networklayer-protokolle)

**Authentication Phase**: berechtigung für Verbindungsaufbau (auth: PAP od CHAP)

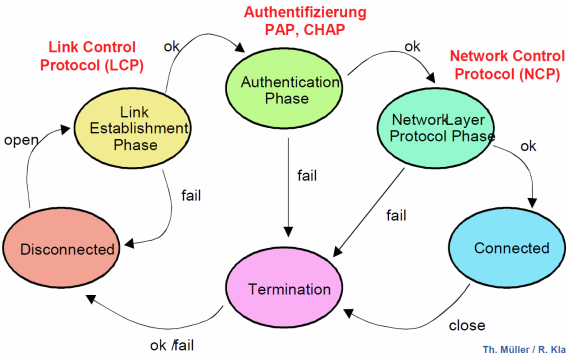
**Network Layer Protocol Phase** festlegen der Netzwerkprotokolle für jedes ver-

wendete Netzwerkprotokoll ein NCP

**Connected**: Es besteht eine Verbindung zwischen beiden Rechnern.

**Termination**: senden von LCP-Frames / Verlust des Trägersignals / Timerüberlauf

**Disconnected**: Verbindung zwischen beiden Rechnern ist nicht mehr vorhanden.



## Link Control Protocol (LCP)

Verbindungssteuerungsprotokoll von PPP |Aufbau, Konfiguration, Verwaltung, Beendigung von p2p verbindungen | 3Frameklassen: Aufbau, Beendigungs, Verwaltungs –Frames | 4Meldungen zum aushandeln der Layer2 Parameter:

**Configure-Request**: Optionen, die das den Request sendende System gerne hätte.

**Configure-Acknowledge**: Optionen, aus einen Configure-Request welche akzeptiert wurden und nun zur Verfügung stehen.

**Configure-Nak** Optionen, aus einen Configure-Request, die (in dieser Form) nicht akzeptiert wurden und nun mit allenfalls anderen Werten (Hints) als Gegenvorschlag zurückgeschickt werden.

**Configure-Reject** Optionen, die Empfänger unbekannt sind => müssen von diesem entfernt werden.

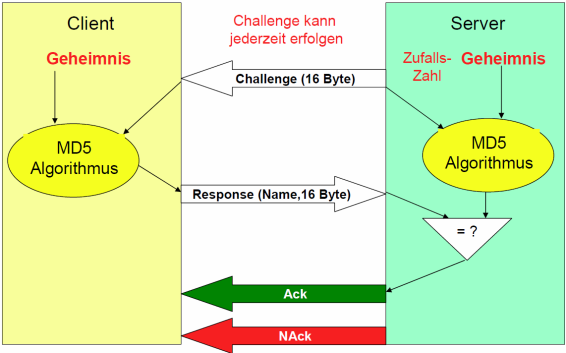
Verbindung wird abgebrochen, wenn ein Partner die zurückgewiesenen Anforderungen nicht akzeptieren kann.

## Authentication Protocols

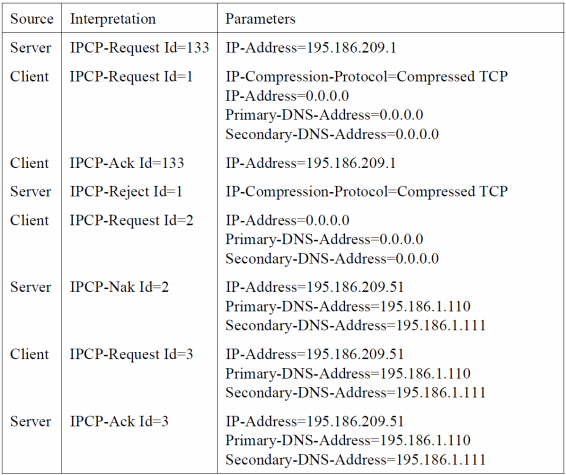
### PAP – Password Autentication Protocol (RFC 1334)

PPP-Frames mit Username/Passwort => Server überprüft angaben => negativ: Verbindung wird unterbrochen => timeout: wiederholung | UNVERSCHLÜSSELT

### CHAP – Challenge-Handshake Authenticatoin Protocol (RFC 1994)



## Network Control Protocol (NCP)



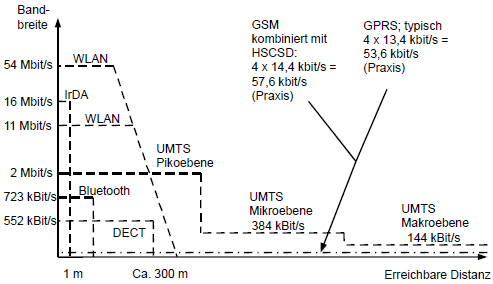
# KT2 Kp 9 Grundlagen Funkkommunikation

# Einführung

Frequenzspektrum: 15kHz – 300GHz | begrenzte Bandbreite | Wartungs- und Verschleissfrei, schmutzige Umgebung, uneingeschränkte Mobilität

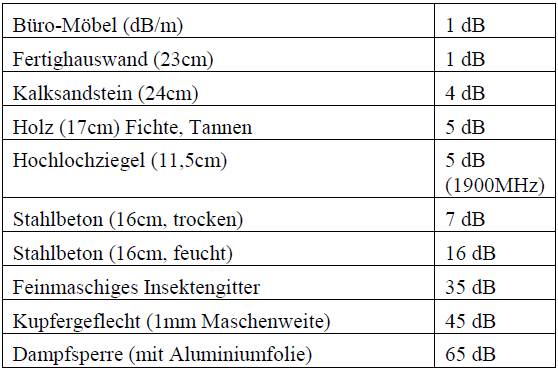
# Die Ausbreitung von Funkwellen

Bitrate und Reichweite entscheidend



## Dämpfungen auf dem Übertragungsweg

Empfangene Leistung nimmt quadratisch mit der Distanz ab Pdb = 10\*log(P/P0): typische Werte bei 800 MHz:



## Mehrwegausbreitung

Schwund (fading): teilweise Auslöschung des direkten Signals durch Signalanteil des Reflektierten Pfads.

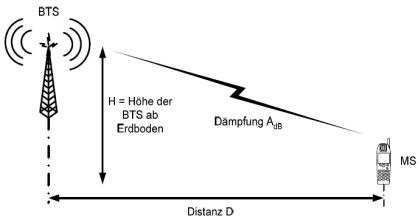
Ausgleich der Phasenlage durch Senden eines bekannten Musters. (Bei PSK) P = P0 / r^x (freiraum: x=2; 2 Wege x=4; n Wege x zwischen 2 und 5)

# Relevanz von Dämpfung und Mehrwegausbreitung

20cm Betonwand entspricht Verdoppelung des Abstands.

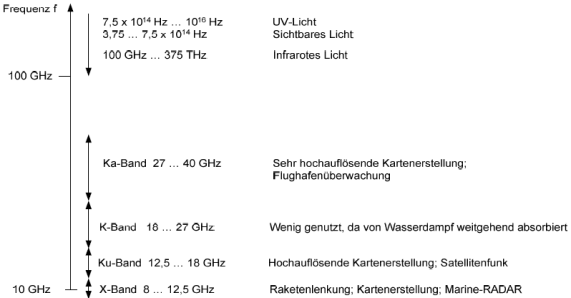
Mehrwegsituation hat den stärksten Einfluss auf die Empfangsleistung

## Das Okumura-Hata-Modell



Adb = 69.55 + 26.16 log(F) – 13.82 log(H) + [44.9 – 6.55 log(H)] x log (D) + C (F = Trägerfrequenz in MHz; H = Höhe der BTS-Sendeantenne über Erdboden in m; D = Distanz zwischen Sende- und Empfangsantenne in km; C = Umweltkorrekturfaktor: Grosstadt: 0 dB, städtisches Gebiet: -5 dB, Vorstädtische Gebiet: -10 dB, Landgebiet: -17 dB)

# Frequenzspektrum

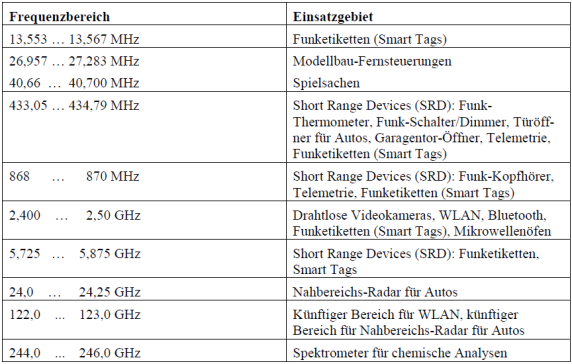




## Regulatorisches

International von ITU-T geregelt

ISM-Bänder (Industrial, Scientific, Medical) frei verwendbar (Leistung begrenzt)



# Kanalzugriffsverfahren

## Frequency Division Multiple Access (FDMA)

Einem Kanal wird eine bestimmte Frequenz zugeordnet. (Verschwendung während Sendepause) Bei DECT und GSM sowohl TDMA wie auch FDMA

## Time Division Multiple Access (TDMA)

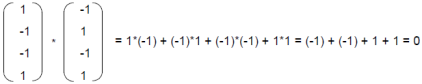
Steuersignale und Synchronisationsverfahren notwendig. Schutzzeit gegen Schwankungen.

Bei GSM reicht Schutzzeit nicht -> Distanz ermitteln und evtl. zu früh senden.

## Code Division Multiple Access (CDMA)

Anstatt 0 oder 1, wird ein Chip gesendet. (Praxis 256-1024 Bitfolge)(UMTS:512).

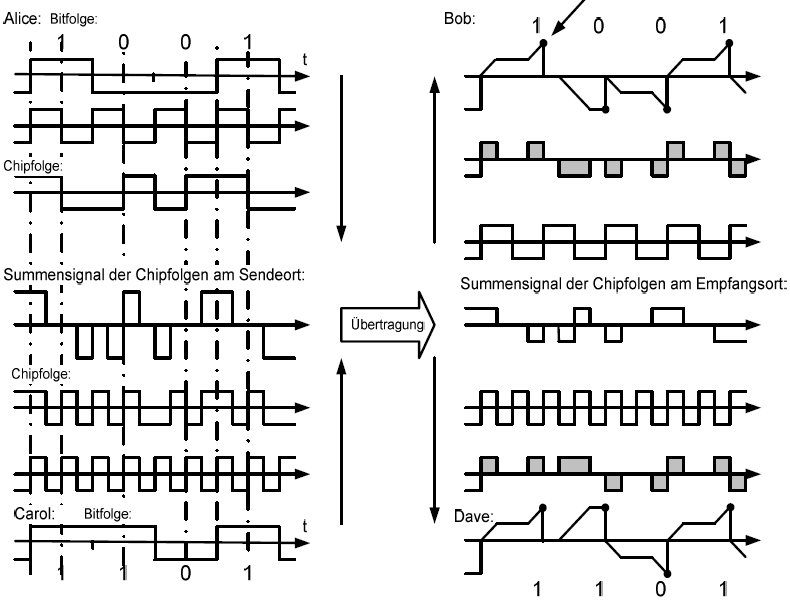
Chipfolgen unterschiedlicher Kommunikationen sind orthogonal.



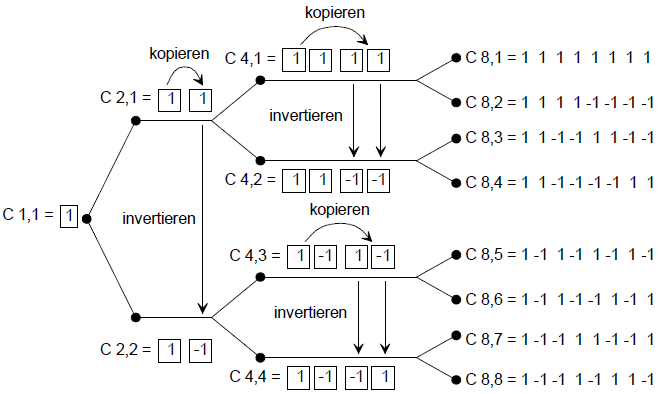
Nutzsignal + 4 Chip Code -> Bandspeizung mit Speizfaktor 4 (da Frequenz \* 4) Übertragungsbandbreite = Nutzsignalbandbreite \* Spreizfaktor

Auch Spread Spectrum Systems genannt.

Beispiel:



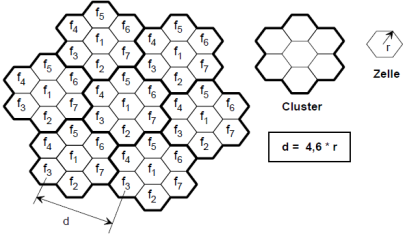
Erzeugung von orthogonalen Codes:



In der Praxis Pseudozufallssequenzen. Orthogonalität meist genügend, nicht perfekt

## Zellulare Netze mit Space Division Multiple Access (SDMA)

Begrenzung der Funkzonen durch geringe Sendeleistung (Pro Zelle eine Sende/Empfangsstation). Gruppen von n Zellen werden zu Clustern zusammengefasst.



Bei 19 Frequenzen d = 13\*r;

Bei 7 Frequenzen d = 4.6 r

Mobilteilnehmer bewegt sich -> Handover-Algorithmus (Seamless Handover)

1 Gespräch braucht 2 Kanäle. (Kreisfläche = Pi\*r^2; 6EckFläche = sqrt(27)/2\*r^2)

# Bandspreizverfahren

## Abgrenzung: CDMA als Kanalzugriffsverfahren und als Bandspreizverfahren

Für Militär entwickelt -> schwierig Abzuhören und Robust gegen Störrsender

## Direct Sequence Spread Spectrum (DSSS)

Entspricht ungefähr CDMA (Chipfolge = Spreizcode)

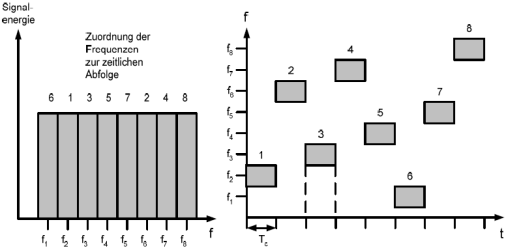
Frequenzspektrum wird durch Chipfolge gespreizt (ausgeweitet) -> Bandspreizverfahren

## Frequency Hopping Spread Spectrum (FHSS)

Sender und Empfänger müssen genau abgestimmt sein bezüglich Hopping-Rate und Hopping-Pattern. (Patterns so ausgelegt, dass Wahrscheinlichkeit, dass 2 Sender den gleichen Kanal wollen gering) Wenn Fehler, dann ARQ (Automatic Repeat Request)

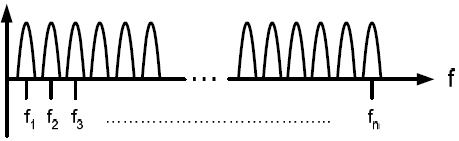
WLAN: (2.40-2.4835 GHz) 79 Subkanäle 2.5 Hopps/s

Bluetooth: 1600 Hopps/s



# Orthogonal Frequency Division Multiplexing (OFDM)

OFDM ist ein Verfahren, bei dem mehrere zueinander orthogonale Subträger f1...fn verwendet werden (siehe Abb. 9.34). Das OFDM-Verfahren wird auch DMT (Discrete Multi Tone)- Verfahren genannt. Das Prinzip ist ein Multiträgermodulations-Verfahren



Einsatz: ADSL

Rechenintensive Signalverarbeitung , unempfindlich gegenüber Fading.

Resultierende Verbindung weniger durch Echo und Reflexion beeinträchtigt.

# Duplexverfahren

## Frequency Division Duplex (FDD)

Hin- und Rückkanal mit FDMA realisiert.

Anwendung: GSM (je 124 Up und Down Kanäle um 900 MHz)

(höhere Trägerfrequenz hat kleinere Reichweite) -> Uplink tiefere F

## Time Division Duplex (TDD)

Zeitmultiplex verfahren. -> Schutzzeit nötig

Anwendung: DECT

# Zwei Anwendungsbeispiele der Funktechnik

## Digital Enhanced Cordless Telecommunications (DECT)

Überbrückung von kurzen Distanzen von Engerät zu Basisstation

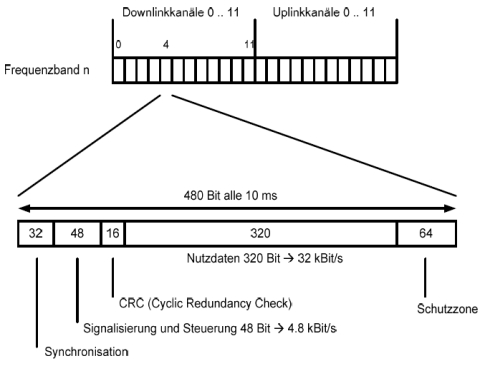
Zugangstechnologie (keine Beschreibung des Netzwerk)

10 Kanäle mit je 12 Up- und 12 Downlinkkanäle

Kanäle können für Datenübertragung gebündelt werden.

Frequenzband (1880-1900MHz) Kanal 1: 1897.344 ; Differenz immer 1.728 MHz

DCS (Dynamic Channel Selection) Wahl aus 120 Kanälen



Zeitschlitz für einen der 24 Kanäle dauert rund 416,7 Mikrosekunden

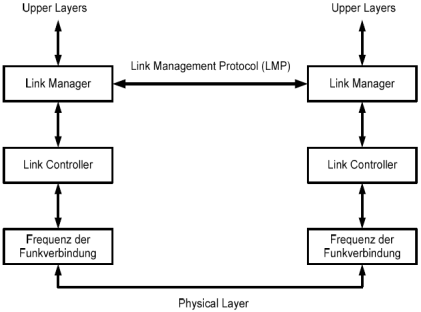
## Bluetooth

Verwendet ISM Band

Standardreichweite: 10m

LMP: Verbindungsaufbau mit Verbindungscodes, Authentifizierung, Verschlüsselung, Aushandlung Basisband-Packetgrösse

Frametyp: ACL (Asynchr. Connection Less) oder SCO (Synchr. Conn. Orientated)



Symmetric ACL: 433.9 kBit/s ; Asymmetric ACL : 723.2 kBit/s 57.6 kBit/s

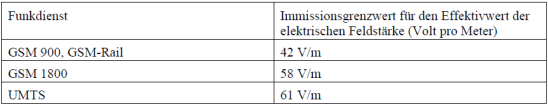
Klasse1: 100mW (Industrie) ; Klasse2: 5mW;

Klasse3: 1mW (Handy)

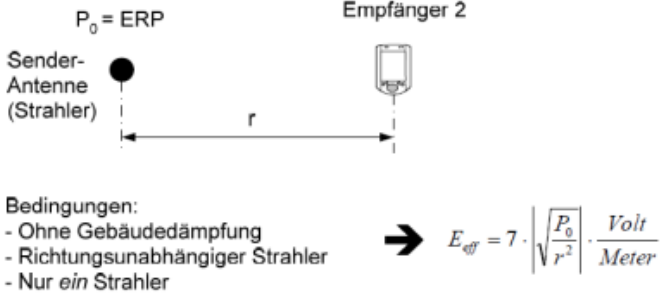
# Elektrosmog, Umweltverträglichkeit

## NIS-Verordnung

Schutz vor nichtionisierender Strahlung



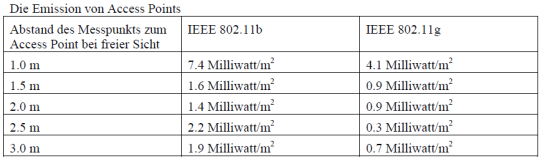
## Zahlenbeispiel für GSM



BUWAL:

Physikalisch hergeleitet: Konstante = 5.48, nicht 7

## Praxis: Emittierte Strahlungsleistungen von WLAN



# KT2 - GSM und Weiterentwicklungen

- GSM: Weltweit verbreitet, wichtigstes Mobilkommunikations-Standard

## Global System for Mobile Communication

- Ursprünglich für 900 MHz entwickelt

- Heute: zusätzliche Systeme mit 1800 MHz und 1900 Mhz

### Merkmale

- Vollständig digitales System

- Internationaler Standard (> 60 Länder)

- Zellulare Netzstruktur mit Zellen zw. 1 und ca. 70km Durchmesser

- Hohe Teilnehmerkapazität

- Verschlüsselung der Nutzdaten

### Dienste im GSM

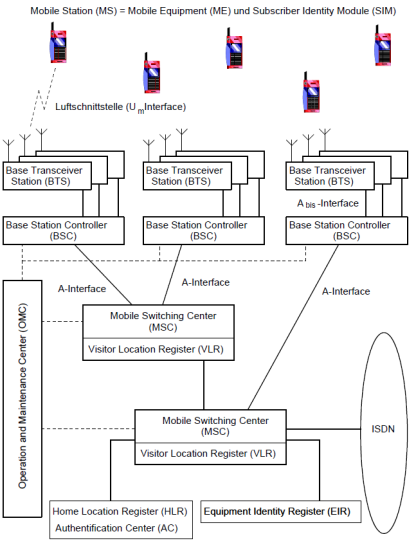
- **Telefondienst**: Telefonie mit Übergang ins Festnetz

- **Notruf**: Europaweit 112. Einziger Dienst, der ohne SIM funktion.

- **Leitungsvermittelte Datenübertragung**: Synchrone und asynchrone Datenübertragung mit bis zu 9600 Bit/s

- **Short Message Service (SMS)**: erlaubt Versenden von alphanumerischen Meldungen bis zu 160 Zeichen. Können von Mobilstation oder von PC über einen Server abgeschickt werden

### Funktionsprinzip und Aufbau



**- Mobile Station (MS**): Besteht aus Mobile Equipment (ME) und Subscriber Identity Module (SIM)

- **Base Transceiver Station (BTS)** und **Base Station Controller (BSC)**

BTS für Umwandlung der Luftschnittstelle in Abis-Interface zuständig, über welches sie mit einem BSC verbunden ist. BSC steuert mehrere BTS und ist für Management d. Funkverb. und lokales Handover zuständig.

BSC ist über A-Interface an Mobile Switching Center (MSC) angeschlos-

sen

- **Mobile Switching Center (MSC)**: GSM-Verbindungsstelle. Über A-Interface mit angeschlossenen BSC und anderen MSC verbunden.

Aufgaben: Schalten von GSM-internen Verb. / Interworking mit Telefonnetz und ISDN / Mobilitätsmanagement

- **Operation and Maintenance Center (OMC)**: Teilnehmeradministration, Gebührenverwaltung, Wartung und Netzoptimierung

- Typisches Netz Schweiz: 9 MSC mit je 10 BSC à je 10 BTS => 900 Zellen

### *Funktionsweise*

- Beim Verlassen d. Herstellers enthält ME 15stellige Nummer (International Mobile Equipment Identity (**IMEI**) => weltweit eindeutige Identifikation eines ME

- An ein MSC in jedem Netz ist das Equipement Identity Register (**EIR**)

angeschlossen => registriert & sperrt gestohlene / fehlerhafte Geräte (weisse, graue und schwarze Liste)

- SIM enthält 15stellige Nummer (International Mobile Subscriber

Identity (**IMSI**)) und Schlüssel d. Teilnehmers

=> weltweit eindeutige Identifikation der SIM

=> SIM = 3 Ziffern Landeskennzeichnung, 2 Z. Netzauswahl, 10 Z.

Teilnehmernummer

- An **MSC** in jedem Netz ist Home Location Register (**HLR**) angeschlossen, das folgende Daten speichert:

- International Mobile Subscriber Identity (IMSI)

- Mobile Subscriber ISDN Number (MSISDN)

- Authentifikations-Schlüssel

- Daten des aktuellen Standortes des Teilnehmers

- Jedes MSC enthält ein Visitor Location Register (VLR), speichert:

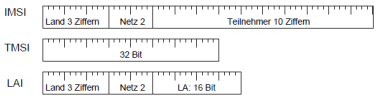
- International Mobile Subscriber Identity (IMSI)

- Temporary Mobile Subscriber Identity (TMSI) (32 Bit)

- Mobile Subscriber ISDN Number (MSISDN)

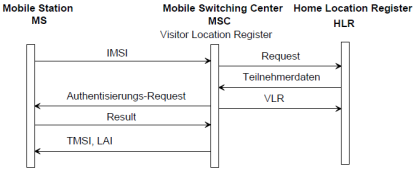
- Authentifikations-Schlüssel

- Location Area Identifier (LAI)



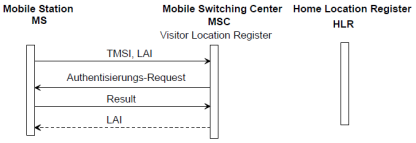
### Die wichtigsten Abläufe

1. Beim ersten Einschalten: IMSI wird vom SIM zum nächsten MSC übertragen
2. MSC lädt mithilfe IMSI die Teilnehmerdaten aus HLR ins VLR und speichert Identifikation des VLR im HLR
3. TMSI wird generiert und mit LAI an die MS geschickt
4. Mit TMSI ordnet MSC der MS dynamisch ein eindeutiges Kennzeichen für ihren Bereich zu
5. LAI gibt aktuellen Standort



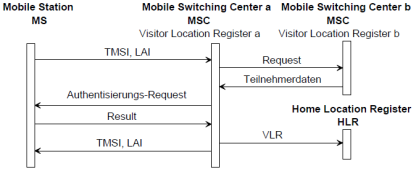
- Beim Einschalten sendet MS die TMSI und LAI an das MSC

- MSC überprüft aufgrund LAI, ob Teilnehmer zuletzt an diesem MSC angemeldet war, wenn ja, ob LA verändert wurde (wenn LA verändert, aber gleicher MSC => LAI korrigieren)



- Wenn TN anderen MSC hat => Teilnehmerdaten von altem VLR ins neue verschieben und mit neuem TMSI und aktuellem LAI aktualisieren

- Neue TMSI und LAI werden an MS geschickt und zusätzlich wird im HLR das für Teilnehmer neu zuständige VLR eingetragen



- Bewegt sich TN mit seiner MS im Netz, muss Standort laufend nachgeführt werden

- LA umfasst 1..n Zellen eines bestimmten MSC

- Signalisierungsaufwand klein halten: Position einer MS nur bzgl. LA (nicht zellengenau) verwaltet

### Keine Verbindung geschaltet:

- Falls neue LA zum gleichen MSC gehört, muss neue LAI im VLR und in der MS aktualisiert werden

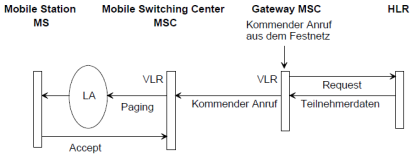
- Falls neue LA zu anderem MSC gehört, müssen Teilnehmerdaten vom alten VLR ins neue kopiert und mit einem neuen TMSI und aktuellem LAI aktualisiert werden. TMSI und LAI werden zusätzlich an MS geschickt

### Anrufe aus Festnetz

- Kommende Anrufe aus Festnetz werden über Gateway-MSC geleitet:

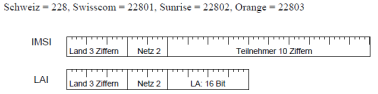
- Gateway-MSC fragt im HLR an, in welchem VLR die gesuchte MS momentan ist

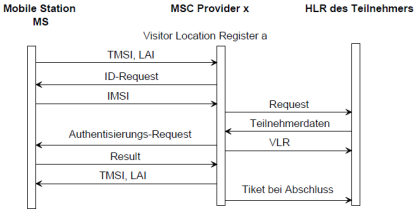
- Das dem VLR zugeordnete MSC sendet Suchauftrag für dieses MS an alle BTS (Zellen), die zur LA gehören, indem sich die MS befindet (Paging)



- Eigenschaft von GSM: MS kann automatisch weltweit lokalisiert werden, falls mit einem GSM-Netz verbunden

- **Roaming**: Wechsel zw. zwei VLR mit permanenter Verfügbarkeit aller grundlegenden Dienste





### Authentisierung

- Schutz vorunzulässigem Netzzugang

- Jeder Teilnehmer wird vom Netz immer authentifiziert, wenn er sich an ein Mobile Switching Center anschaltet

- MSC generiert 128 Bit Zufallszahl und sendet diese an MS

- **Signed Response (SRES):** Per Zufallszahl und teilnehmerspez. Authentifikationsschlüssel wird in der MS und im MSC mit dem Algorithmus A3 die 32 Bit grosse SRES gebildet

- MS schickt ihre SRES an MSC, das beide Werte vergleicht und entscheidet, ob TN an das Netz zugelassen wird => TN zugelassen: Mit Schlüssel des TN, dem SRES und dem Algorithmus A8: generierung eines 114 Bit langem Übertragungs-Schlüssels, mit dem ab diesem Zeitpunkt alle zu übertragenden Daten verschlüsselt werden

### Anmeldevorgang

- MS sendet LAI und TMSI (das erste Mal IMSI) an das MSC

- Sind TNdaten nicht im VLR des MSC gespeichert, so werden diese aufgrund von LAI und TMSI beim alten VLR oder beim ersten Mal aufgrund vom IMSI beim HLR angefordert

- Mit teilnehmerspez. Schlüssel und d. 128 Bit grossen Zufallszahl wird Teilnehmer authentifiziert

### Handover

- Durch Messung d. Signalqualität stellt MS fest, dass die des Einflussbereich einer Zelle verlässt

- Wird Signalqualität während Verbindung schlechter => Handover

- **Intracell-Handover**: wird durchgeführt, wenn während Verb., durch die Bewegung d.TN, die Qualität des geschalteten Kanals nicht mehr genügend ist. Es ändert sich nur Frequenz d. Funkübertr.kanals. Aktivitäten werden durch den BSC gesteuert.

- **Intercell-Handover**: wird durchgeführt, wenn TN während Verb. in eine andere Zelle d. gleichen MSC bewegt. Die neue Zelle kann zum gleichen oder einem anderen BSC gehören. Hat das BSC eine Koppelfunktion, kann die Verb. im BSC geschaltet werden. Sonst: neue Verbindung über das MSC aufbauen.

- **Inter-MSC-Handover:**

- Bewegt sich der TN in eine Zelle, welche einem anderen MSC angehört, muss neuer Web für Verb. über das neue MSC geschaltet werden.

- Teilnehmerdaten müssen vom alten VLR ins neue kopiert und mit neuen TMSI und aktuellen LAI aktualisiert werden

- TMSI und LAI werden an MS geschickt

**Handover-Funktionen sind aufwändig und zeitkritisch, da der Teilnehmer vom Umschalten nichts merken soll!**

### Subscriber Identity Module (SIM)

- Chipkarte mit Mikrokontroller, RAM, ROM, nichtflüchtigem Speicher

- Nach Einschalten:

- Prüfen ob TN Berechtigung besitzt, SIM zu benützen => Personal Identification Number (PIN)

- 3x falsch => Karte gesperrt

- entsperren mit PIN Unblocking Key (PUK)

- 10x falsch => endgültig gesperrt & unbrauchbar

- Nichtflüchtiger Speicher enthält folgende Daten:

- Personal Identification Number (PIN)

- PIN Unblocking Key (PUK)

- International Mobile Subscriber Identity (IMSI / TMSI & LAI)

- Authentifizierungs-Schlüssel

- Das persönliche Rufnummernverzeichnis des Teilnehmers

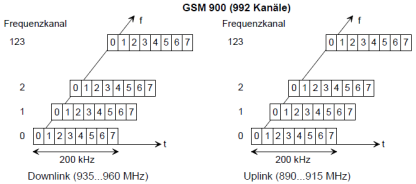
- Die SMS-Nachrichten

### Die Luftschnittstelle des GSM 900

- Daten von Uplink und Downlink werden in zwei Frequenzbändern übertragen

- Frequenzmultiplex: jedes Band nochmals in 124 Bänder à 200 kHz mit je 8 Time Slots aufteilen

=> Total 992 Duplex-Übertragungskanäle



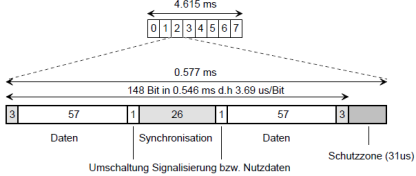
- Jeder Time Slot: 0.577ms

- Darin wird ein Burst von 148 Bit à 3.69us übertragen, die wie folgt verwendet werden:

- 34 Bit (Synchronisation)

-2 Bits (Anweisung, ob Datenbits = Signalisierung/Nutzdaten)

-114 Bits (Nutzdaten / Signalisierung, max. 24.7 kBit/s)



- Schutzzone: Überlappen von Zeitschlitzen verhindern

- Kanäle werden immer paarweise verwendet

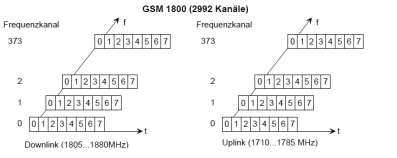
- Up- und Downlink-Kanäle sind fix gekoppelt (Uplink gegenüber Downlink um 3 Time Slots verschoben) => Vereinfachung im Endgerät, da nicht gleichzeitig gesendet und empfangen werden muss.

### Die Luftschnittstelle des GSM 1800

- Mobilfunknetz DCS 1800 von ETSI als Ergänzung zu GSM 900 spez.

-Frequenzbereiche: 1710..1785 MHz Uplink und 1805..1880 MHz Downlink

- 374 Frequenzbänder => Total 2992 Duplex-Übertragungskanäle



- kleinere Sendeleistungen (max. 1 W) gegenüber GSM 900 (max. 2 W)

- Stadtbereich: Zellen mit Radius ca. 1km

- Ländliche Gegenden mit wenig Verkehr: Makrozellen (8km Radius)

- Bereiche mit sehr viel Verkehr: Mikrozellen (150m..1km Radius) oder Picozellen (< 150m Radius)

- Vorteil kleine Zellen: grosse Verkehrsdichten aber: hohe Investitionen

- Geräte mit Frequenzbereich 900/1800 MHz => **Dual Band Handy**

- Geräte mit zusätzlich 1900 MHz (USA) => **Triple Band Handy**

### Logische Kanäle

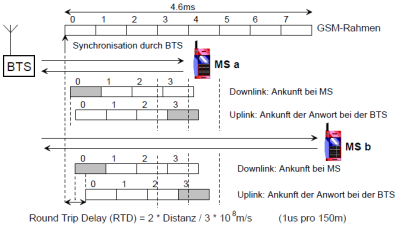
- Logische Kanäle für Sprache, Daten, versch. Arten von Signalisierung, die auf unterschiedliche Weise in Zeitschlitze gemappt werden.

### Time Advance

- Beim Zeitmultiplexverfahren: Endgeräte dürfen nur zu bestimmten Zeiten senden (im abgemachten Timeslot) => müssen mit Basis Station durch Zeitsignal synchronisiert werden => Basis Station sendet regelmässig ein Signal, das den Rahmenanfang kennzeichnet => Basis Station kennt Rahmenanfang und kann im richtigen Timeslot senden

- **Problem**: Signale von Mobil Stationen, die sich nahe an Basisstation befinden, sind früher bei Basis Station, als Signale von Mobil Stationen, die weiter entfernt sind

- **Behebung des Problems durch Schutzzonen**

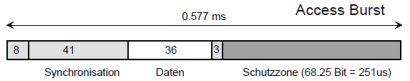


- Durch Distanz bedingte Laufzeit: 300m /us

- Round Trip Delay: 1us pro 150m Distanz

- Ist Mobilstation 35km von Basisstation entfernt, benötigt Signal 234us Laufzeit für Hin- und Rückweg

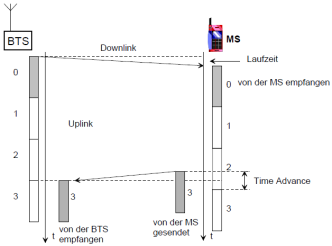
- Meldet sich Mobilstation zum ersten Mal => Access Burst mit 251 us Schutzzone => limitiert die max. mögliche Distanz zw. Basis- und Mobil Station und damit die Grösse einer GSM-Zelle



- Wäre bei Rahmenlänge von 577us die Schutzzone generell so gross, könnte Timeslot nur zu ca. 50% ausgenutzt werden

=> BTS ermittelt laufend Round Trip Delay und ermittelt daraus ca. alle 500ms einen Time Advance Wert und sendet diesen an Mobile Station

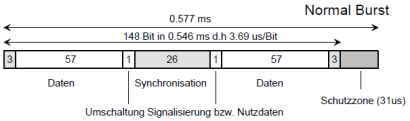
- Mobile Station sendet Daten jeweils um diesen Wert vorverschoben



- Für Time Advance Wert ist Abstufung in 64 Werte (0..63) vorgesehen, wobei eine Stufe einer Bitlänge, also 3.69us oder ca. 550m Distanz entspricht

=> Schutzzone kann in normalem Burst massiv reduziert werden

=> Zellengrösse dadurch auf 35km Radius begrenzt (64\*550m = 35km)



# ZF KT2 - IPv6

## Chronologie

- 90er Jahre: Internet Engin. Task Force (IETF) beginnt

Nachfolger für IPv4 zu entw. Motivation: knapper Adressraum

### Angestrebte Verbesserungen

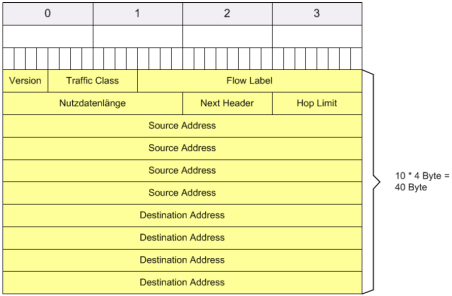
- Erw. Adr.raum / Verbess. d. Protokollheaders / Flow Label /Verbess. Routing (Routing Header) / Verb. d. Sicherheitsmechanismen / Ermittl. MTU durch Endgerät => keine Fragm. durch Router

### Erweiterung des Adressraums

- 16Byte (128Bit) => 3.4\*10exp(38) Adr.

- 340 Billionen Quadrillionen Adr.

### Verbesserung d. Protokollheaders



- Version (0110)/TrafficClass (00000000)

Flow Label: Komm.-Paar (S&E) identifiz. Nutzdatenlänge: max. 65535 Byte (mit Jumbo Payload Option => grössere Datagramme)

### Flow Label

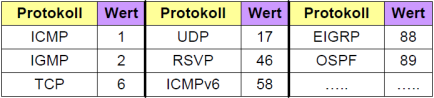
- S weist FL zu / zufäll gener.hex.Z. 00000..FFFFF

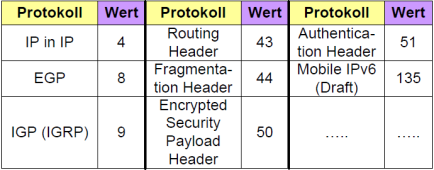
- Default (00000)

- Vorteile: Datenflüsse auf einfache Weise klassifizieren => spez. Abarb. d. bez. Datenpak. für Übermittlung. / Ziel: effiz. Datenfluss/ Ohne Flows muss Router R-Tabellen konsult. für Bestimmung des Output-Port

- Flow = Seq. v. Pak., gesendet von Quelle zu Ziel: Unicast /Anycast / Multicast IPv6 Adr.

### NextHeader





### Format Routing Header



### Hop Limit (8 Bits)

- Entspricht TTL bei IPv4

### Source Address (128 Bits)

- komplette IPv6 Quelladresse

### Destination Address (128 Bits)

- komplette IPv6 Zieladresse

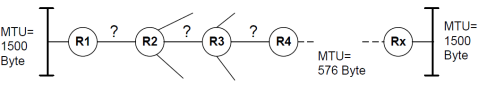
### Verbesserung d. Sicherheitsmechanismen

- IPv4: keine Sicherheitsmechanismen

- Neuerungen: grösserer Adr.raum / onzept "NextHeader" /Tunneling-Mechanismen / Autoconfiguration => erlauben neue Arten von Angriffen

### Ermittlung MTU

- Keine Frag. durch Router aber: Ermittl. mittels Path MTU Discovery (Pfad bis zum E bzgl. kleinsten vorkommenden MTU untersuchen)



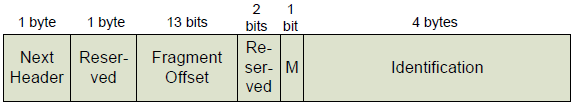
- Kleinste MTU bei IPv6: 1280 Byte

- Nur S darf Fragm. vornehmen

- Ist zu versend. Paket grösser als kleinste vorkommende MTU ->S fragm. Paket

- Reassembly (zusammensetzen d. Fragm.) bei E

### Format des Fragment Headers



- NextHeader (1. Typ d. fragmentierbar. Teils d. urspr. IPv6 Pakets (NextHeader = TCP(6)))

- Reserved: ungenutzt (null)

- Fragment Offset: Versatz in Mengen v. 8 Bytes

- M-Flag (more fragments): 1, falls mehr Fragm.

- Identification (ID): Alle Fragm. eines Pakets haben dieselbe ID

## Adressierung bei IPv6

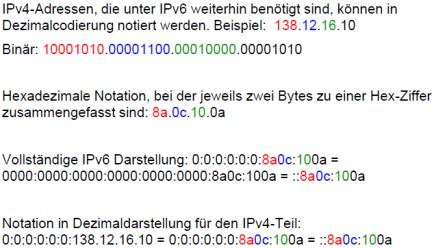
### Darstellung / Notation

2001:0620:0000:0004:0A00:20FF:FE9C:7E4A

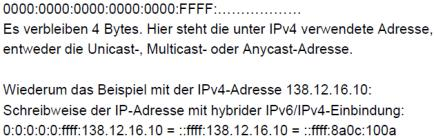
= 2001:620:0:4:A00:20FF:FE9C:7E4A

1023:0000:0000:0000:1736:a673:88a0:a620=

1023::1736:a673:88a0:a620



### Notation für Hosts mit hybrider IPv6/IPv4-Einbindung



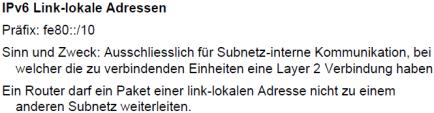
### Adressstruktur von IPv6

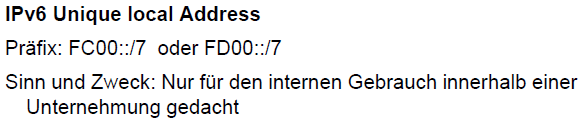
Subnetz-Präfix (64 Bits) + Hostteil (64 Bits)

- IPv6 Global Unicast Adress: 64-n Bits: Globaler Routing Präfix / N Bits: Subnetz-ID / 64 Bits: Schnittstellen-ID

- Real World-Struktur der IPv6 Unicast-Adress: 48 Bits: Globaler

Routing Präfix/ 16 Bits: Subnetz-ID / 64 Bits: Schnittstellen-ID





## Autokonfiguration

### Stateless Adress Autoconfiguration

- Motivation: vereinfachte, teilw. autom. Zuteilung einer. IPv6-Adr

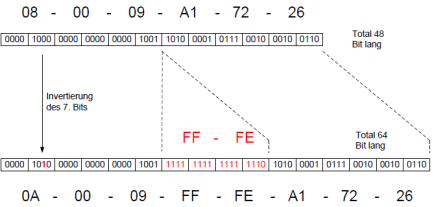
- Weshalb: Zukunft viele Devices mit IPv6 Adr.

- Wie: leicht modifiz. MAC Adr. wird beigezogen, um letzte 64Bits der 128 Bit langen IPv6 Adr. zu erzeugen:

- Modifiziert: Bit Nr. 7 ist im Fokus:

"0" => link-lokale Adresse

"1" => globale Adresse



- Weltweit eindeutig, falls MAC-Adr im gleichen Subnetz nicht nochmals vorkommt

**Nachteil:**

- Verfolgbarkeit d. Rechners / d. Aktivitäten weil immer dieselbe Adr. erhalten wird.

**Beheben**:

Pro Schnittst. mehrere ID verw. / Fixe EUI-64 nur für ankomm. Verb. nutzen / für abgehende Verb. IDs durch Zufall erzeugen.

### Dynamic Host Configuration Protocol v6 (DHCPv6)

Neu mit „Stateless Address Autoconfiguration“ => Host kann seine IPv6 auf Basis d. MAC-Adr. beziehen. (brauch deshalb kein DHCP).

Bei „**Stateful** Address Autoconfiguration“ **DHCP nötig**.

Stateless und Stateful: Adressbezig erfolgt stateless und zusätzlich KonfigInformationen via DHCP.

Pro Schnittstelle mehrere IP-Adressen.

## Domain Name System (DNS) für IPv6

**Record AAAA („Quad-A“):** speichert die 128 bit lange IPv6-Adr. und enthält die Abbildung auf den Hostnamen

**Bsp**:

larbor.zhaw.ch IN AAAA 2001:620:190:fff1::1 =

2001:620:190:fff1:0000:0000:0000:0001

Zugehöriger Reverse Lookup Domain Name:

1.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.1.f.f.f.0.9.1.0.0.2.6.0.1.0.0.2.IP6.AR

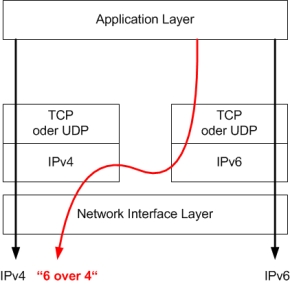
PA

DNS Support für IPv6 ab Version 9 von BIND vorhanden.

**DNS Resolver**: stellt Anfrage nach AAAA-Request, 2 Anfragen v4 (A-Record) und v6 (AAAA-Record). Als Response kann beides oder eines zurückkommen.

## Migration von IPv4 zu IPv6

### Dual Stack



Beide Protokolle im Betrieb | typisch ist Router | wichtig Zugang zu IPv6 DNS Server | Endgeräte meist nur IPv4 oder v6

### Tunnel Broker

IPv6 Pakete werden in Pakete eines andern Protokolls gepackt | häufig IPv6 als Nutzlast von IPv4 Paketen | administrative Aufwand für Konfig sehr gross | deswegen Tunner Broker als Server, die Benutzeranfragen für Tunnels automatisch bearbeiten und Tunnels aufsetzen.



**Tunnel Broker**: Via IPv4 erreichbar, Benutzer wählt sich ein um Tunnel zu registrieren. Broker setzt und schliesst Tunnel.

**Tunnel Server**: Dienen der Skalierbarkeit: Gesamtlast der Tunnelendpunkte kann aufgeteilt werden. Typischerweise Router im Dual-Stack-Betrieb.

**Client**: Ein Dual-Stack Rechner, der ans IPv4-Netz geht. Teilt Broker seine Identität evt. mit Passwort mit. Borker prüft und erteilt Berechtigung

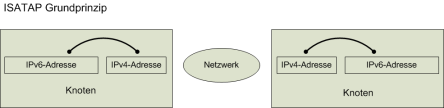
**Ablauf**: Server wird ausgewählt | Wahl der IPv6 Adr. für Client | Festlegung der Laufzeit für Tunnel | im DNS registrieren (muss globale IPv6-Adr. sein) | Konfig des Servers

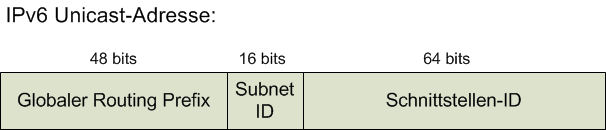
### Tunnelverfahren 6in4

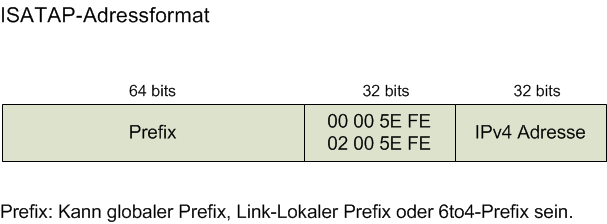
Pack IPv6 Paket direkt in IPv4. Im IPv4-Header: Protocol Type ist 41 für IPv6 | „proto-41 static“ als anderer Name | meist manuell konfiguriert oder automatisierte Konfig. mit TIC Server

### Tunnelverfahren ISATAP

ISATAP: Intra-Site Automatic Tunnel Addressing Protocol Zählt zu den automatischen Tunnelverfahren | für Endgeräte via IPv6 aber Routernetz mit IPv4 | ISATAP Adresse: IPv4 Adresse ist in der Schnittellen-ID der IPv6 eingefügt.







**00** 05 5E: private Adresse | **02** 00 5E: offizielle Adresse | **FE**: IPv6 Adresse mit eingebetteter IPv4 Adresse

### Translation mit 6to4

Um IPv6 Standorte über IPv4 Routernetz zu verbinden ohne Tunnel | IPv4 dient als Punkt-zu-Punkt-Link und Router werden als 6to4-Gateways bezeichnet | offizielle IPv4 Unicastadr. Benötigt | Translation aufwändiger als Tunnerling | gut bei Migration über längeren Zeitraum

Präfix von IANA: 2002::/16 = Präfix 2002 ist 16 Bits lang

=> 2002:<IPv4-Adr.>/48, Präfix inkl. Interface ID und SLA ID (Site Level Aggregator), SLA ist 16 Bit lang => 655536 Subnetze)

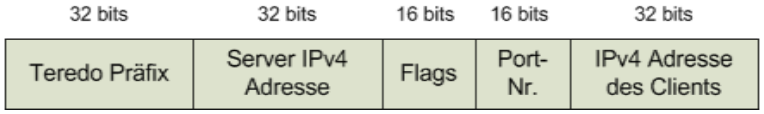


### Translation mit Teredo (NAT-T)

Falls IPv6 Geräte über öffentl. IPv4 Netz kommunizieren wollen und NAT (Network Address Translation) verwenden sollen.

Teredo: Tunnelrealisation, ermöglicht den IPv6-Hosts die sich hinter IPv4-NAT befinden, mit anderen Geräten zu kommunizieren. IPv6 Pakete werden in UDP getunnelt.

Format der Teredo-Adresse:



**Teredo-Präfix: 2001:00000:/32**

**Server**: Teredo Server

**Flags**: Addresstyp von NAT-Typ

**Portnummer**: mapped UDP-Port des Teredo-Dienstes auf Client, Mapped = jedes Bit invertiert

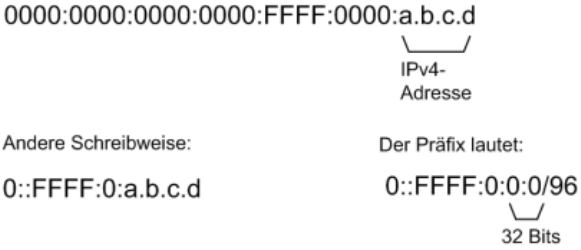
**IPv4 Client**: mapped IPv4 Adresse des Clients

**IPv4 Teredo Client**: Recher mit privaten IPv4 Adresse

### Translation mit StatelessIP-ICMP Translation (SIIT)

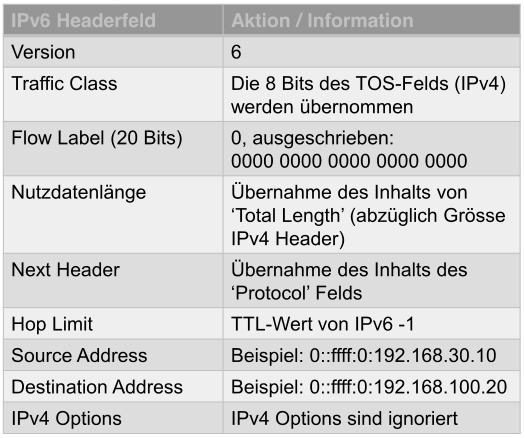
Jeder „Translator“ muss IP-Header und ICMP-Header übersetzen

können. Deshalb Adresstyp **„IPv4-translatable address“**



Translator hat Adresspool und IPv6-Rechner holt dort eine IPv4 Adresse | Translator = meist Router | kennt IPv4 Adressen vom Pool | entfernt den IPv4 Header und setzt IPv6 Header.

Übersetzung der Header-Felder: IPv4 => IPv6



Übersetzung von IPv6 in IPv4:



## Internet Control Message Potocol v6 (ICMPv6) RFC 4443

- Aufgaben:-Router auf Pfad S => E muss S Mitteilung zrü. senden

- E muss S Mitteilung zurücksenden

- Falls NextHeader-Feld = 58 => Payload hat ICMPv6 Paket



- Type: ident. Typ d. Nachricht (bestim. Format nachfolg. Meldu.)

- Code: detaillierte Info zu einem Type

- Checksum: mit Hilfe "Pseudoheader". (Quelle / Ziel / Nutzdatenlänge / NextHeader. Prüfsumme bezieht Header inkl. Pseudohead.

- Message Body: eigentliche Meldung (Fehler- / Infomeld.)

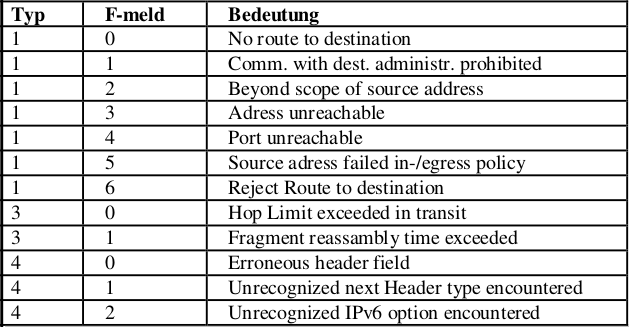
### Regeln für die Verarbeitung v. ICMPv6-Paketen

1. ICMP-Fehlermeld. mit unbek. Typ  an Layer 4-7 leiten
2. Infomeld. mit unbek. Typ  Meldung verwerfen
3. Fehlermeld.: möglichst viele Daten d. problembehaft. Paket aber: MTU nicht mehr als 1280 Bytes
4. Falls Meldung an Layer 4-7: Protokolltyp aus Originalpaket herauslesen (Datenfeld). Falls Protokolltyp nicht eruierbar => verw.

### Wann darf keine ICMPv6-Fehlermeldung erfolgen?

- Fehlermeldung darf keine Fehlermeldung erzeugen / Redirect Meldung (Typ 137) darf keine Fehlerm. erzeugen / Als Folge e. Pakets, das an IPv6 Multicast-Adr. gesendet darf keine erzeugen / Als Folge e. Pakets, das Layer2 Multicast enthält => keine erzeug./ Als Folge e. Pakets, dessen S nicht eindeutig einer einz. Schnittst zugeordnet werden kann => keine Fehlermeldung erstellen





### Neighbour Discovery

- kombiniert ARP, ICMP Router Discovery und Redirect

- wird genutzt: Zur Detekt. d. erreichb. Nachbarn / Autokonfig. v. IPv6 Adr. / Ermittl. v. Netzwerk-Präfixes / Ermittlung v. Routen / Detektion v. IPv6-Adressduplikaten / Auflösung v. MAC-Adr v. Rechnern am gleichen Ethernet LAN / Bemerken v. ändernden MAC-Adressen

