

Kapitel 1

Mobilkommunikation

1.1 Einführung

Wireless vs. Mobile (0, stat. Rechner, 1 Notebook Hotel, 2 Funk LANs, 3 PDA) PDA Personal Digital Assistant Anwendungen in Fahrzeugen, (GSM, GPS, lokales Netz mit Umgebung) oder bei Notfällen, Einsatz in Krisengebieten), als Ersatz eines Festnetzes (z.B. nach Erdbeben), zur Vernetzung historischer Gebäude, Internet im Grünen, Ad-Hoc Netzwerke.

Ortsabhängige Dienste: Umgebungsbewusstsein, Nachfolgedienste, Informationsdienste, Nachfolge der Unterstützungsdienste, Privatheit.

Leistung: Sensoren, Pager, PDA, Palmtops, Laptops.

- Auswirkungen der Endgeräteportabilität
- Drahtlose Netzwerke vs. Festnetze

DECT Digital Enhanced Cordless Telecommunications

1.2 Technische Grundlagen

- Frequenzen:
 - GSM 890-915MHz
 - IEEE 802.11 2400-2483MHz

UHF Ultra High Frequency (300MHz - 30 GHz) (Unterer Frequenzbereich)

SHF Super High Frequency (300MHz - 30 GHz) (Oberer Frequenzbereich)

ISM-Band Industry Science Medicine Antennen: Idealer isotroper Punktstrahler
(Richtdiagramme) Klassifikation:

- Punktstrahler
- einfache Diploe
- gerichtet und mit Sektoren

Bereiche:

- Übertragungsbereich (kleinster Radius)

- Erkennungsbereich (mittlerer Radius)
- Interferenzbereich (größter Radius)

Die Empfangsleistung nimmt mit $\frac{1}{d^2}$ ab (d = Entfernung: Sender, Empfänger).

- Freiraumdämpfung
- Abschattung (Hindernisse)
- Reflektion (große Flächen)
- Streuung (kleine Flächen)
- Beugung (an scharfen Kanten)
- Mehrwegeausbreitung (direkte und phasenverschobene Signale werden empfangen)
- Auswirkungen der Mobilität (schnelles Fading, langsames Fading)

Multiplexing, Modulation, Demodulation siehe Telematik 1

AM Amplitudenmodulation (auch ASK)

FM Frequenzmodulation (auch FSK)

PM Phasenmodulation (auch PSK)

MSK Minimum Shift Keying

PSK frotschritt:

QPSK Quaternary PSK (2 Bits in 1 Symbol (= phasenverschobenes Sinussig.))

BPSK Binary PSK (0: sinusförmiges Signal, 1: negatives Sinussig.)

- Spreizspektrumtechnik: (Problem: frequenzabhängiges Fading löscht schmalbandige Signale manchmal aus. Lösung: Signal mittels Codefolge auf breitere Frequenzen spreizen) (Abb. Folie 2.16.1)
- Auswirkungen von Spreizen und Interferenz (2.36.1)
- Spreizen und frequenzselektives Fading (Folie 2.37.1)

DSSS Direct Sequence Spread Spectrum (XOR der Signals mit Pseudozufallszahl) (chipping sequence) Beim Empfang: Nach Demodulator: Tiefpassfilter und Integrator und dann Entscheider.

FHSS Frequency Hopping Spread Spectrum (Direkte Wechsel der Trägerfrequenz) (2 versionen: fast hopping (mehrere Frequenzen pro Nutzdatenbit), slow hopping (mehrere Nutzdatenbits pro Frequenz)) (Mod, Mod mit Freq.Synthi ... Dem mit Freq.Synthi, Dem)

- Zellenstruktur (Realisierung des Raummultiplex) Vorteile: Mehr Kapazitäten, weniger Sendeleistung notwendig, robuster, überschaubarere Ausbreitungsbedingungen; Nachteile: Netzwerk zum Verbinden der Basisstationen, Handover, Störungen anderer Zellen, Konzentration in best. Bereichen
- Zellgröße von 500m - 35km bei GSM
- Frequenzplanung (keine gleiche ind benachbarten Zellen, ausreichender Abstand bei Freq.-Wiederverwendung, feste Kanaluordnung (Problem: Wechsel in Belastung der Zelle), dynamische Kanaluordnung (Kanäle nach bereits zugeordneten Kanälen der benachbarten Zelle ausgesucht, mehr Kapazität bei höherer Nachfrage, Zuordnung aufgrund Interferenzmessung möglich)
- 3 Zellen Cluster, 7 Zellen Cluster, 3 Zellencluster + 3 Sektoren pro Zelle

1.3 Medienzuteilung

- Versteckte und “ausgelieferte” Geräte
- Nahe und ferne Geräte

Multiplexverfahren zur Steuerung des Medienzugriffs:

SDMA Space Division Multiple Access

FDMA Frequency Division Multiple Access (FDD: Frequency Division Duplex): Beispiele: GSM (niedrige Frequenz für Hinweg zu Basisstation, hoher Frequenzbereich für Antwort)

TDMA Time Division Multiple Access (TDD: Time Division Duplex) Beispiele: DECT (uplink, downlink (jeweils eigener Zeitbereich))

DAMA Demand Assigned Multiple Access (Explizite Reservierung: Verbesserung von ALOHA durch Reservierung der Zeitschlitz)

PRMA Packet Reservation MA, (Implizite Reservierung)

Reservation-TDMA: (N Minizeitschlitz, jede Station kann in eigenem Minizeitschlitz bis zu k Datenzeitschlitz reservieren ($N \cdot k$). Im Datenteil können nicht benutzte Zeitschlitz nach Round-Robin von anderen Stationen mitverwendet werden).

MACA Multiple Access with Collision Avoidance (RTS: Request to send; CTS: clear to send (Bestätigung für RTS)) [DFWMAC: Distributed Foundation Wireless MAC] Signalisierungspakete: SA, DA, Paketgröße. Vermeidet versteckte und “ausgelieferte” Endgeräte. (Automat auf 3.5.2 kennen)

Polling Nacheinander Abfragen von Endgeräten durch eine Station

ISMA Inhibit Sense Multiple Access (Besetztton, Wenn frei, Bestätigungspakete bei Wiederbelegung/Kollision, Besetztton; Verwendung bei CDPD)

CDMA Code Division Multiple Access (XOR mit Pseudozufallszahl (Schlüssel)) Danach Addition, Aufschlüsseln mit jeweiligem Schlüssel, wenn Ergebnis > 0 , dann “1”, wenn Ergebnis < 0 , dann “0”.

SAMA Spread Aloha Multiple Access (Spreizspektrumstechnik mit nur einem Code nach ALOHA-Prinzip)

Folie 3.24.2 können!

1.4 Drahtlose Telekommunikationssysteme

GSM Global System for Mobile Communication

Leistungsmerkmale

- Kommunikation: (Sprach-, Datendienste, SMS)
- Totale Mobilität
- Erreichbarkeit: (grenzübergreifend, Netz übernimmt Lokalisierungsaufgaben)
- Hohe Kapazität: (Bessere Frequenznutzung)
- Übertragungsqualität: (hoch und zuverlässig)
- Sicherheitsmaßnahmen: Zugangskontrolle durch Chipkarte und PIN

Nachteile von GSM:

- keine End-to-End Chiffrierung der Nutzkanäle

- Netzzugriff nur über “reduzierten” B-Kanal (keine Verlängerung des 64kbit/s Trägerdienstes!)
- Beeinträchtigung der Konzentration (beim Autofahren)
- elektromagnetische Verträglichkeit
- Missbrauch
- Möglichkeit zur gezielten Kontrolle, Überwachung
- hohe Komplexität
- Kompatibilitätsprobleme (bzgl. Signalisierung) im Netz innerhalb GSM-Standard

Dienste:

- Trägerdienste (Bearer Services):
 - TK-Dienste: Daten zwischen Benutzer-Netz-Schnittstellen (APs)
 - Spez. nach OSI-1-3
 - Für Datendienste andere Übertragungsraten als für Sprache: Datendienste leitungsvermittelt: synchron (bis 9,6kbit/s), asynchron (300 bis 1200Bit/s), paketvermittelt: synchron (bis 9,6kbit/s), asynchron (300 - 9600Bit/s)
- Teleservices (Telematic Services):
 - TK-Dienste, Mobilfunk, Benutzerkommunikation
 - Aspekte wie zellulare Operationen berücksichtigen (alle Basisdienste) auch Sicherheitsmaßnahmen
 - Dienste: Mobilfunk-Telefonie (Gespräche mit 3,1kHz Bandbreite (300 - 3400 Hz)), Notruf (Priorität, Verdrängung, wenn Zelle voll), Multinumbering (mehrere Nummern pro Teilnehmer)
 - Non-Voice Teleservices: Fax-Gruppe 3, Telefax, Videotext, Teletex, Voice Mailbox, Elektronische Post, SMS
- Zusatzdienste:
 - Entsprechen bis auf geringere Übertragungsraten denen des ISDNs
 - Können sich je nach Land leicht unterscheiden
 - Dienste: Identifikation, ID-Unterdrückung, automatischer Rückruf, Anklopfen, Konferenzverbindung, Sperren

ETSI European Telecommunications Standardisation Institute
 PLMN Public Land Mobile Network
 PAD Packet Assembler/Disassembler
 Bearer Services (Trägerdienste), Telematic Services (Teleservices) und Supplementary Services (Zusatzdienste)

Komponenten von GSM:

MS Mobile Station
 BS Basisstation
 MSC Mobile Switching Center (Mobilvermittlungseinrichtung)

LRs Location Register

Subsysteme:

RSS Radio Subsystem

NSS Network Subsystem

OSS Office Subsystem (Betriebs- und Wartungs-Subsystem)

Bei GSM verwendete Abkürzungen:

AT Authentikation Triplets

AUC Authentication Centre

BSS Base Station System

BSC Base Station Controller

BTS Base Transceiver Station

EEPROM Electrically Erasable Programmable Read Only Memory

EIR Equipment Identity Register

GMSC Gateway MSC

GSM Global System for Mobile Communications

HLR Home Location Register

IMEI International Mobile Station Equipment Identity

IMSI International Mobile Subscriber Identity

ISC International Switching Center

ISDN Integrated Services Digital Network

Kc Cipher Key

Ki Subscriber Authentikation Key

LAI Location Area Identifier

MCC Mobile Country Code

ME Mobile Equipment

MNC Mobile Network Code

MS Mobile Station

MSC Mobile Switching Centre

MSIN Mobile Subscriber Identifikation Number

MSISDN Mobile Subscriber ISDN Number

MSRN Mobile Station Roaming Number

NVM Non Volatile Memory

OMC Operation and Maintenance Centre

PIN Personal Identification Number

PLMN Public Land Mobile Network

PSTN Public Switched Telephon Network

PUK Personal Unblocking Key

RAM Random Access Memory

ROM Read Only Memory

SIM Subscriber Identity Module

SMS Short Message Service

SRES Signed Response

TDMA Time Division Multiple Access

TMSI Temporary Mobile Subscriber Identity

VLR Visitor Location Register

Aufbau eines GSM-Systems: (Folie 4.11.2 können!!) (MS, BS, BSC, MSC, GMSC, HLR, VLR, RSS, NSS, OSS)

Bei Schnittstelle BSC zu MSC Transcodierung: kein(!) PCM! Netz: ZZK-7 (Verbindung der MSCs und EIR, HLR und VLR. (Netzwerk-Subsystem) (Systemarchitekturen kennen)

Funk-Subsystem: RSS

- BSS = BSC + Summe(BTS) + Übertragungssysteme
- MS

Prinzip zellularer Netze ($r < 35\text{km}$, hexagonal (idealisiert), Handover)

Funktionen: BTS (funktechnische Funktionen) und BSC (Funkkanal-Vermittlungseinrichtung)

- Beide: Frequenzspringen
- Beide: Chiffrieren /Dechiffrieren
- Beide: Paging
- Beide: Messungen (BTS: Uplink, BSC: Traffic)
- BTS: Kanalcodierung/-decodierung, Ratenanpassung
- BSC: Management Funkkanäle, Mobility Management (Authentifizierung, Location Registration/Update), Handover

Mobilstation besteht aus:

- MT (mobile Terminal) (entspricht NT bei ISDN)
- TA (Terminal Adapter)
- TE (Term. Equipment) (keine GSM-spez. Funktionen)
- SIM (Subscriber Identity Module)
- Aufbau: TE -(R) - TA - (S) - MT -o U_m .

Netzwerk-Subsystem:

- Hauptbestandteil des öffentlichen mobilen Funknetzes. Übernimmt vermittlungstechnische Aufgaben, Mobility Management, Systemkontrolle, kann andere Netze anbinden
- Komponenten:
 - MSC (Verbindungssteuerung über Koppelnetz. An 1 MSC können etliche BSCs angeschlossen sein)
 - Datenbankeinrichtungen: HLR (zentrale Master-DB: semiperm. und temp. Daten aller Teilnehmer, die auf Dauer einem HL-Bereich zugeordnet sind), VLR (lokale DB für Teilmenge der Benutzerdaten incl Aufenthaltsort)

MSC:

- Zentrale Stellung:
 - Vermittlungsfunktion
 - Zusatzfunktionen (Unterstützung der Teilnehmermobilität)
 - Verwaltung von Netzwerkressourcen
 - Anbindung an andere Netzwerke (GMSC)
 - Integration verschiedener Datenbanken

- Funktionen:
 - Rufspezifische Funktionen
 - Abschluss und Bearbeitung der Zeichengabe (ZZK-7)
 - Management der spez. Signalisierungsabläufe
 - LR
 - Fax, Data Calls
 - SMS
 - Vergebungsdaten

Betriebs- und Wartungssystem (OSS):

- zur Instandhaltung
- Komponenten:
 - AUC (teilnehmerspez. Berechtigungsparameter aus VLR auf Anfrage, Sicherheit und Geheimhaltung der Teilnehmerinformationen)
 - EIR (Registrierung, bei Diebstahl → Sperren des Gerätes)
 - OMC (Kontroll- und Bedienstellen) (aufwendigster Teil)

Zeit-Vielfachzugriff: FDD (Downlink 935-960MHz (124 Kanäle a 200kHz), Uplink 890-915MHz), GSM TDMA Frame (1-8 in 4,6ms), GSM Timeslot (mit Guardspace wegen Δ wegen Mobilität. Aufbau des Timeslots: Guardspace, Tail (3 Bit), Nutzdaten (57Bit), S (1 Bit), Training (26Bits), S, Nutzdaten, Tail, Guardspace. Alles in 577 μ s.

GSM-Rahmenhierarchie:

- hyperframe (3h 28min): (0 - 2047) mal:
- superframe (6,12 s): 0-50 (A) oder 0-25 (B) mal:
- multiframe (A: 120ms, B:235ms): (A) 0-25 mal oder (B) 0-50 mal:
- frame (577 μ s): 0-7 slots (bursts)

Mobile Terminated Call (Folie 4.43.1 können!)(Doppelspitze = Antwort): rufend → PSTN → GM-SC → HLR → VLR (Wo?) → HLR (!) → GMSC → MSC (bei mir?) → VLR → MSC → BSS → MS (ID) → BSS → MSC → VLR (Authentifizierung) → MSC → BSS (Aufbau) → MS

4 Arten des Handover (Folie 4.46.1) Handover-Entscheidung (Schwellwert der Intensitäten) Sicherheit in GSM:

- Zugangskontrolle / Authentifikation: SIM
- Vertraulichkeit: verschlüsselte Übertragung
- Anonymität: TMSI, bei jedem LUP (Location Update) neu vergeben, verschlüsselt übertragen.

3 Algorithmen in GSM spez.:

- A3: Authentisierung ("geheim", Schnittstelle offen gelegt) (Folie 4.50.1)
- A5: Verschlüsselung (für Datentransfer) (Folie 4.51.1)

- A8: Schlüsselberechnung (“geheim”, Schnittstelle offen gelegt) (Folie 4.51.1)

Datendienste in GSM:

- Übertragung 9,6kbit/s (fortgeschrittene Kanalkodierung erlaubt 14,4kbit/s), zu wenig für Internet
- HSCSD High-Speed Circuit Switched Data (4,8kbit/s * 1,2,3,4; 9,6kbit/s * 1,2,3,4; 14,4kbit/s * 1,2,3,4)
- GPRS: paketorientierte Vermittlung, Belegung der Zeitschlitze nur bei Bedarf; +: Schritt in Richtung UMTS, flexibler. -: teurer
- GPRS-Netzelemente: GSN (GGSN + SGSN), GGSN, SGSN, GR

AIUR	Air Interface User Rate
GPRS	General Packet Radio Service
GSN	GGPRS Support Nodes
GGSN	Gateway GSN (Umsetzung GPRS - PDN (Packet Data Network))
SGSN	Serving GSN (Unterstützung der MS)
GR	GPRS Register (Benutzeradressen)
GPRS Dienstgüte: Reliability Class (3 Klassen (1 = beste)), Delay Class (4 Klassen (1 = beste, 4 = unspecified)).	
UMTS	Universal Mobile Telecommunications System
UTRA	UMTS Terrestrial Radio Access
EDGE	Enhanced Data rates for GSM Evolution
CAMEL	Customized Application for Mobile Enhanced Logic
VHE	Virtual Home Environment UMTS:

- UTRA
- Erweiterungen von GSM: EDGE, CAMEL, VHE
- Anforderungen: min 144kbit/s (Land), min 384kbit/s (Vorstadt), bis 2Mbit/s (Stadt)
- UMTS FDD Rahmenstruktur
 - superframe (0-71) mal:
 - frame (0-15) mal:
 - slot: 2 Kanäle uplink, 1 Kanal downlink. Uplink DPCCH (Dedicated Physical Control Channel) mit pilot, TPC (transmit Power Control) und TFI (Transport Format Identifier), Uplink DPDCH (Dedicated Physical Data Channel) mit data; Downlink DPCH (Dedicated Physical Channel) mit (DPCCH, DPDCH). 1 Slot = 625 μ s.
- UMTS TDD Rahmenstruktur
 - frame a 10ms (0-15) mal:
 - slot (625 μ s) mit: data, midamble, data, Guard Period

Zukunft Mobilfunknetze: (Folie 4.37.1): UMTS (schnell, 10kbit/s), MBS (schnell, 150MBit/s), SAMBA (langsam, bis 20MBit/s), ISDN (fest, mit B-ISDN bis 150MBit/s), WAND, MEDIAN (portabel, 10kbit/s - 150MBit/s (MEDIAN))

1.5 Satellitensysteme

Siehe ZF Telematik 1.

Ergänzung zu zellularen Mobilfunksystemen. Aufbau: (Folie 5.9.1). ISL, MUL, GWL. ISL Inter Satellite Link

MUL Mobile User Link

GWL Gateway Link

Stabile Umlaufbahn: $r = \sqrt[3]{\frac{gR^2}{(2\pi f)^2}}$ mit: R = Erdradius, r = Radius (Erdmittelpunkt, Satellit), f = Umlauffrequenz.

Synchrondistanz: 35786km.

- Inklination: Neigung des Orbits gegenüber Äquator
- Elevation: Erhebungswinkel des Satelliten über Horizont. (Höhere Elevation besser, da weniger Abschattung)
- meist getrennte Frequenzbereiche für Uplink und Downlink
- transparente Transponder: nur Frequenzumsetzung
- regenerative Transponder: zusätzlich Signalaufbereitung

Minimale Elevation: kleinste E., bevor neuer Satellit des Systems sichtbar wird.

Dämpfung beeinflusst durch:

- Sendeleistung
- Antennengewinn (Sender)
- Abstand von Sender und Empfänger
- Antennengewinn (Empfänger)

Loss L: $L = \left(\frac{4\pi rf}{c}\right)^2$ mit: f = carrier frequency

Probleme: schwankende Signalstärke (Mehrwegeausbreitung), Signalunterbrechung (durch Abschattung (kein LOS)).

mögliche Lösung: Schwankungen durch Leistungsreserven ausgleichen, Einsatz mehrerer gleichzeitig sichtbarer Satelliten.

LOS Line of Sight

Wichtige Einflussfaktoren auf Absorption: Regen, Nebel

GEO geostationärer Orbit (ca. 36000km) (synchron zur Erdrotation, versorgt großes Gebiet, daher Frequenz schlecht wiederverwendbar, schlechte Elevation in Breitengraden über 60°, große Entfernung → lange Laufzeit (275ms), ungeeignet für flächendeckende Mobilfunkversorgung, meist Rundfunk, Fernseh)

LEO Low Earth Orbit (700 - 2000km) (Sichtbarkeitsdauer 10-40min, globale Versorgung möglich, Laufzeit ca 5-10ms, kleinere Ausleuchtungsgebiete, bessere Frequenznutzung, Handover benötigt, viele Satelliten nötig, Doppler-Effekt! (Iridium, Globalstar))

MEO Medium Earth Orbit (6000 - 20000km) (auch: ICO: Intermediate Circular Orbit) Vergleich mit LEO: (Geschwindigkeit langsamer, weniger Satelliten, geringerer Doppler-Effekt, meist kein Handover benötigt, längere Laufzeit (70 - 80ms), höhere Sendeleistung benötigt, größere (stärker bündelnde) Antennen für kleine Ausleuchtungsgebiete benötigt)

HEO Highly Elliptical Orbit

Van-Allen-Gürtel (innerer und äußerer): kein Satellitenbetrieb möglich (wegen ionisierten Teilchen). Routing:

- durch: ISL
- weniger erforderliche Gateways
- Gespräche so weit wie möglich über Satelliten (dadurch terrestrisch billiger)
- nur ein Uplink und ein Downlink benötigt
- Probleme:
 - präzise Ausrichtung der Antennen komplex
 - Eigenbewegung der Satelliten
 - höherer Treibstoffverbrauch
 - kürzere Lebensdauer

SUMR Satellite User Mapping Register Lokalisieren von Mobilstationen:

- ähnlich wie bei GSM. In Bodenstationen oder Gateways abgelegt: (HLR (Stammdaten), VLR (wo zuletzt?), SUMR (zuständiger Satellit, Positionen aller Satelliten))
- Anmeldung einer Mobilstation: (Feststellung der Position durch Satelliten, Anforderung Benutzerdaten HLR, Neuordnung von VLR und SUMR)
- Anrufen einer Mobilstation: (Feststellung Position MS über Register, Verbindungsaufbau über zuständigen Satelliten)

Handover in Satellitensystemen:

- Intra-Satelliten-Handover (von einem Spotbeam zum nächsten)
- Inter-Satelliten-Handover (von einem Satelliten zum nächsten)
- Gateway-Handover (noch im Footprint, aber Gateway nicht mehr in diesem Footprint)
- Inter-System-Handover (zwischen Satellitennetz und terrestrischem Mobilfunknetz (wegen Kosten, oder Erreichbarkeit))

Zugriffsmethode meist FDMA/TDMA (nur bei Globalstar CDMA).

1.6 Broadcast-Systeme

Unidirektionale Verteilmedien

- asymmetrische Kommunikationsumgebung (durch Bandbreitenbeschränkung, Art der Informationen oder Einsatzgebiet (Pager, SMS, Drahtlose Netzwerke))
- Extremfall: Unidirektionale Verteilmedien (hohe Bandbreite Server → Client (downstream), aber KEIN upstream). Probleme des Rundsendemesiums: Information kann nur für eine einzige virtuelle Benutzergruppe; Hilfsmittel benötigt, die eine angemessene Berücksichtigung des individuellen Zugriffsverhaltens erlauben.

Strukturierungskonzept:

- Sendeseite: zyklische Wiederholung der Daten. Verschiedene Sendefolgen: flat disk (ABCABC...), skewed disk (AABCAA...), multi-disk (ABACAB...)

- Empfängerseite: Caching-Algorithmen (kostenbasierte Strategie (welche Wartezeit, wenn Objekt gefordert und NICHT im Cache?), Cache benötigt Wissen über Art der übertragenen Datenobjekte und Zugriffsprofil des Nutzers).

COFDM Coded Orthogonal Frequency Division Multiplex DAB (Digital Audio Broadcast) Spezifikation:

- Ausstrahlungsverfahren: COFDM; 192 - 1536 Teilbänder innerhalb eines 1,5MHz Frequenzblocks
- Frequenzen: erste Bedeckung 1 von 32 Blöcken im Bereich der Fernsehkanäle 5-12, zweite Bedeckung, 1 von 9 Blöcken im L-Band (um 1450MHz)
- Datenrate: 2,304 MBit/s (netto 1,2 bis 1,536 MBit/s)
- Modulation: Differentielle QPSK
- Audioprogramme, Digitale Dienste

MSC Main Service Channel

FIC Fast Information Channel

CIF Common Interleaved Frame

CU Capacity Unit

FIB Fast Information Block DAB-Transportmechanismen:

- MSC (überträgt Nutzdaten (Audio, Multimedia...), besteht aus mehrere CIFs, jeder CIF 55296bit groß und wird alle 24ms übertragen (je nach Übertragungsmodus), CIF enthält CU von 64bit Größe)
- FIC (überträgt alle Steuerdaten, besteht aus FIB (256bit groß inkl. 16bit Prüfsumme), beschreibt Konfiguration und Inhalt des MSC)
- Stream-Modus (transparente Übertragung mit **fester** Datenrate)
- Paket-Modus: einzeln adressierbare Datenpakete

Übertragungsrahmen:

- Im Rahmen mehrere Schritte (Schutzzeit + Symbol).
- (Nutzsymbol, Referenzsymbol) SC (Synchronization Channel), (x Datensymbole) FIC, (Y Datensymbole) MSC

DAB Signalerzeugung:

- Sender
 - (Audio-Encoder, Packet Mux) jeweils an Channel Coder
 - alle Channel Coder an MSC-MUX
 - MSC-MUX mit FIC (Service- und Multiplex-Information) an Transmission-MUX
 - OFDM → Transmitter (radio frequency)
- Empfänger
 - Tuner → OFDM-Demodulator → Channeldecoder (alles mit Control-Bus verbunden)

- entweder an Audio-Dec oder Packet-Demux
- Audiocodierung (ala mp3, Schutzbits zur Fehlererkennung und Korrektur, häufig Bündelfehler → Signal nach festem Schema verwürfeln → beim Empfänger dann korrigierbare Einzelfehler, geringe Schrittgeschwindigkeit, großer Symbolvorrat)
- Bitratenmanagement: Unterschiedliche Ansprüche an Ü-qualität und Datenrate; Standard: dynamische Rekonfiguration, Datenraten variabel, passiert im MUX. (Beispiel Rekonfiguration: Folie 6.20.1)

MOT Multimedia Object Transfer Protocol:

- Problem: Empfangsgeräte mit stark unterschiedlichen Leistungsmerkmalen sollen alle Arten von programmbegleitenden wie programmunabhängigen Datendiensten verarbeiten oder erkennen können
- Lösung: Einheitlicher Standard (Definition des MOT (z.B. bei Online-Diensten, oder CD-ROM verwendet)
- MOT-Struktur: Formate (alles mögliche (MPEG, HTML, Jpeg, HTTP, BMP, GIF...)), Header-core (Länge von Header UND Body, Inhaltsformat), Header-extension (Abstand von Wiederholungen, Segmentierung, Priorität etc.), Body (beliebige Nutzdaten): 7byte Header-core, Header-extension, body

DVB:

- DVB überträgt MPEG-2 Container
- DVB Service Information: NIT (Network Information Table)(Dienste eines Providers:...), SDT (Service Description Table)(Name und Parameter für Dienst x in MPEG-MUX-Kanal x...), EIT (Event Information Table)(Statusinformation aktuelle Übertragung), TDT (Time and Date Table)(Updateinfo für Set-Top-Box)

1.7 Drahtloses LAN

Charakteristika:

- Vorteile:
 - räumlich flexibel
 - Ad-Hoc Netzwerke machbar
 - unanfälliger gegen Katastrophen
- Nachteile:
 - niedrige Übertragungsraten
 - proprietäre Lösungen (noch kein leistungsfähiger Standard)
 - viele nationale Restriktionen (globale Regelung erst langsam (IMT-2000))

Infrarot (- Abschattung..., +: billig...) vs. Funktechnik (-: Abschirmung, +: Durchdringung von Wänden ...)

Infrastrukturnetzwerke (Notebooks über Funk oder IR über AP (Access Point) an Festnetz) vs. Ad-Hoc Notebooks oder PDAs über Funk oder IR untereinander). Architektur Infrastrukturnetz:

- STA (Station: mit Zugriff auf Funkmedium und AP)
- AP
- Portal (zu anderen LANs)
- BSS (Basic Service Set)(Gruppe von Stationen, die die gleiche Frequenz nutzen)
- ESS (Extzended Service Set) Verbindungen verscheidener Zellen (Distribution System)

Architektur Ad-Hoc Netzwerk

- STA
- BSS

Eigene Schichten: PHY und MAC

PLCP Physical Layer Convergence Protocol

PMD Physical Medium Dependent

Schichten und Funktionen

- (PMD (Modulation, Codierung), PLCP (Physical Layer Convergence Protocol)(Carrier Sense)) PHY
- MAC (Zugriffsmechanismus, Fragmentierung, Verschlüsselung)
- PHY-Management (Kanalwahl, MIB)
- MAC-Manegement (Synchronisierung, Roaming, MIB, Power)
- orthogonal dazu: Station Management (Koordination der Manegement-Funktionen)

GFSK Gaussian Filtered Frequency Shift Keying

DBPSK Differential Binary Phase Shift Keying

DQPSK Differential Quadrature Phase Shift Keying 802.11 - Physikalische Schicht:

- 3 Varianten: 2 Funk, 1 IR
- FHSS (2-stufige GFSK nur 1Mbit/s)
- DSSS (DBPSK für 1Mbit/s, DQPSK für 2Mbit/s)
- IR

FHSS PHY Paketformat:

- PLCP Präambel: (Synchronisation (80bit), SFD (Start Frame Delimiter)(16)), PLCP-Paketkopf: (PLW (PLCP-PDU Length Word) (12), PSF (P. Signalling Field) (4), HEC (Header Error Check (CRC: 16,12,5,1)) (16)), Nutzlast

DSSS PHY Paketformat:

- PLCP-Präambel: (wie oben, nur: (128, 16)), PLCP-Paketkopf: (signal (Datenrate Nutzlast (1 oder 2 Mbit/s))(8), service (reserviert oder gemäß 802.11)(8), length (16), HEC(16)), Nutzlast

PCF Point Coordination Function (für zeitbegrenzte Dienste (Verkehrsart der MAC Schicht))
 DFWMAC-DCF CSMA/CA Distributed Foundation Wireless MAC mit Distributed Coordination Function und Carrier Sense Multiple Acces und Collision Avoidance (Prioritätenvergabe oder "backoff"-Algorithmus)
 DFWMAC-PCF DFWMAC mit Point Coordination Function (Pollingverf. mit Liste im Access Point)
 IFS Inter Frame Space Mac-Schicht:

- Verkehrsarten: asynchroner Datendienst (standard) (best-effort-Basis, unterstützt Broadcast und Multicast), zeitbegrenzte Dienste (opt) (über PCF implementier)
- Zugriffsarten:
 - DFWMAC-DCF CSMA/CA (Empfangsbestätigung durch ACK (nicht bei Broadcast!))
 - DFWMAC-DCF mit RTS/CTS (Request to send / Clear to send) (vermeidet versteckte Endgeräte)
 - DFWMAC-PCF (optional) (Pollingverfahren mit Liste im AP)
- Prioritäten:
 - durch Staffelung der Zeitpunkte
 - keine garantierten Prioritäten
 - SIFS (Short Inter Frame Space) (höchste Prio.)
 - PIFS (PCF IFS) (mittlere Prio.)
 - DIFS (DCF IFS) (niedrigste Prio.)
- Schema: DIFS → direkter Zugriff (weil frei), Medium belegt → SIFS, PIFS, DIFS, Wettbewerb → nächster Rahmen

CSMA basierend auf CCA Clear Channel Assessment (Carrier Sense) (Backoff-Mechanismus mit n-Slot-Zeiten im Wettbewerbsfenster. Backoff-Timer bleibt solange stehen, wenn während Zufallszeit (nach erstem freiem IFS, dann wartend) Medium belegt) (Problem, bei zwei gleichzeitig startenden, identischen Wartezeiten zweier Stationen)

- CSMA/CA bei Sendn von Unicast-Paketen: (Sender DIFS, Daten → Empfänger: SIFS ACK → Rest: DIFS Wettbewerb)
- DFWMAC: Unicast-Pakete: (wie bei CSMA/CA, nur vorher noch S: DIFS RTS; E: SIFS CTS; S: SIFS Data...) nach Abschluss von RTS und CTS bei Rest: NAV (Network Allocation Vector) (RTS/CTS)
- Fragmentierung: (Am Anfang DIFS, sonst immer SIFS dazwischen) RTS → CTS → frag1 → ACK1 bei Rest: NAV(RTS), NAV(CTS), NAV(frag1), NAV(ACK1)....
- DFWMAC-PCF (Superframe: wettbewerbsfreie Periode, Wettbewerb): PIFS D1, SIFS U1, SIFS D2, D3 PIFS D4, SIFS U4, SIFS CF(end), Wettbewerb

802.11 Rahmenformat:

- Frame Control (2 Byte) (Version, Typ(steuer-, Management-, Datenrahmen), Frag., Sicherheit ...)

- Duration ID (2)
- Address 1 - 3 (jeweils (6))
- Sequence Control (2) (wichtig für Duplikate)
- Address 4 (6)
- Data (0-2312)
- CRC (4)

Adressen hängen von Paketart ab. (z.B. Destination, Source, BSSID, -; (Ad-Hoc) oder im Distr. Sys.: Receiver, Transmitter (phys.), Dest., Source).

MAC-Management:

- Synchronisation (LAN finden, versuchen, in LAN zu bleiben)
- Power Management (Schlafmodus, ohne Nachricht zu verpassen, period. Schlafen, Rahmenpufferung, Verkehrszustandsmessung)
- Assoziation/Reassoziaton (Eingliederung in Netz, Roaming, Scanning (nach Netz))
- MIB (verwalten, schreiben, lesen)

Synchronisation mit "Leuchtfener":

- Infrastruktur: period. Funksignal (beacon) mit Zeitstempel (Anfang beacon) am AP. Nur gesendet, wenn zu Taktbeginn (der Periode) Medium frei, sonst schnellstmöglich.
- Ad-Hoc: zu Taktbeginn zufällige Verzögerung, dann jede Station beacon(i), wenn Medium frei und kein anderes beacon..

Steuerung der Leistungsaufnahme:

TSF	Timing Synchronisation Function
TIM	Traffic Indication Map (unicast Liste Empfänger) (Infrastr.)
DTIM	Delivery TIM (broadcast/multicast Liste) (Infrastr.)
ATIM	Ad-hoc TIM

Energiesparen mit Wachmustern (infra: wach immer kurz vor TIM, DTIM Intervallanfang; Ad-Hoc: ATIm-Fenster (=1/2 beacon Intervall), Wach immer zu Anfang beacon-interv. und solange, wie nötig)

Roaming: Keine oder schlechte Verbindung? → Scanning, Reassoziaton REQ (an AP), Reasso. RSP, neuer Ap akzept. Reasso. REQ.

WPAN	Wireless Personal Area Network (z.B. Bluetooth)
EY-NPMA	Elimination Yield Nonpreemptive Priority Multiple Access
MIB	Management Information Base
RIB	Route Information Base
NIB	Neighbor Information Base
HIB	Hello Information Base (Status des Ziels (über nächsten Knoten))
AIB	Alias Information Base
SMRIB	Source Multipoint RELAY Information Base
TIB	Topology Information Base
DDIB	Duplicate Detection Information Base
SCO	Synchronous Connection-Oriented link (Bluetooth, MAC-Schicht) (leitungsverm.)
ACL	Asynchronous Connectionless Link (packetverm.) ETSI-HIPERLAN:

- HIPERLAN Schichten: Physical Layer, CAC (Channel Access Control) Layer, MAC
- 4 ursprüngliche HIPERLANs (1-4 (2-4 ATM basiert))
- Datenübertragung immer verbindungslos
- Dienste: Asynchron, zeitbegrenzt mit hierarchisch unabh. Prios
- Topologie: Infrastr., Ad-Hoc (Reichweite: "forwarding" kann im Knoten integriert sein)
- Sonstige Mechanismen: Energiesparmodi, Verschlüsselung, Prüfsummenbildung
- CAC-Dienst (Definition Kommunikationsdienst "über geteiltes Medium, Abstraktion von Mediencharakteristika) MAC-Protokoll (nutzt HIPERLAN CAC), CAC-Protokoll (stellt CAC-Dienst zur Verfügung)Physical-Protokoll (Kanalzugriff)
- Schichten, Dienste, Protokolle: H(HIPERLAN)P/C/M-entities (in Schichten) verschiedene SAPs pro Schicht eigene PDU (innerhalb) zwischen Schichten SDUs
- Physikalische Schicht: Mod., Demod., Vorwärtskorrektur, Messung Signalstärke, carrier Sense. 3 verpflichtende Kanäle (2 optional) (alle um 5,17-5,27GHz)
- Rahmencharakteristik (PHY): Rahmenstruktur: LBR-Kopf (low Bit Rate 1,4Mbit/s), Synch, Daten0, ... Daten m-1
- CAC (Sicherstellen: Zugriff nur auf erlaubte Kanäle, Prioritätsschema (über Paketlebenszeit), Zugriff über EY-NPMA)
- EY-NPMA (Elimination Yield Nonpreemptive Priority Multiple Access): 3 Phasen: Prioritätsfindung, Wettbewerb (Elimination Burst (Burstdauer tricky)), Übertragung
- DT-HCPDU/AK-HCPDU (LBR: Hashed Destination HCSAP-Address, HDA-Checksum, Block Length Indicator, BLIR-Checksum; HBR: Type Ind., BLI, HIPERLAN Id, DA, SA, UD, PAD, CS / Bitmuster, HI (High Bit Rate-part Indicator), AID (Ack Id.), AID-Checksum)
- MAC-Schicht: Paketweiterleitung (gezielt Punkt-zu-Punkt, oder broadcast), Verschlüsselungsmechanismen (KEINE Schlüsselverwaltung), Energiesparmechanismen (Wachmuster, ! Stores müssen existieren (für schlafende Knoten)).
- DT-HMPDU: LI (length Ind.), TI (Type), RL (residual Lifetime), PSN (Seq.Num.), DA, SA, ADA (Alias DA), ASA, Up (prio.), ML (MSDU Lifetime), KID (Key ID.), IV (init. Vector), UD, SC (Sanity Check). Länge: 40 - 2422 Bytes.
- Information Bases (IBs): RIB (Route(wie kann erreicht werden?)), NIB (Neighbour (status)), HIB (Hello (Status Ziel)), AIB (Alias (Adr. Knoten außerhalb Netz)), SMRIB (Source Multipoint Relay (MP Status jetzt?)), TIB (Topology), DDIB (Duplicate Detection ([source, sequence])).
- Ad-Hoc Netzwerke mit HIPERLAN: Normales Notebook (Funkrechner) RNHADd-IB, Forwarder zusätzlich: SmrT-IB (also alle)

Bluetooth:

- Anbindung von Peripheriegeräten, Verbindung von Netzwerken (z.B. GSM über Handy, Bluetooth, Laptop)

- Zustände (PHY-Schicht): STANDBY; Inquiry, Page; connected, transmit; PARK, HOLD, SNIFF
- MAC-Schicht: SCO (synchronous Connection-Oriented Link: leitungsvermittelt, symmetrisch, Punkt-zu-Punkt), ACL (Asynchronous Connectionless Link: Punkt-zu-Mehrpunkt, paketvermittelt, Master fragt Stationen ab (Polling)), Zugangscodes (einzigartig pro Kanal), Paketformat (Access Code, Paket Header (MAC Address(3), type(4Bit), flow, ARQN (Alternating Bit ARQ/SEQ), SEQN(Number, jeweils 1 Bit), HEC (8))), payload

Scatternets:

- Piconets, jedes hat 1 Master und bis zu 7 weitere Knoten, Teilnahme: Synchro auf richtige Hopping-Sequence, Kommunikation zw. Piconetzen (Knoten, die hin- und herspringen)

1.8 Drahtloses ATM

Problem: Hohe Komplexität des Systems. OAM (Operation and Maintenance (Zelle bei ATM, auch um Rahmen zu bilden))

Erkennen von Zellgrenzen notwendig, wenn kein synchroner Rahmen

CS Convergence Sublayer

CPCS Common Part Convergence Sublayer

SSCS Service Specific Convergence Sublayer

B-ISDN Protokollreferenzmodell: Siehe Tele1: AAL (in CS und SAR), PHY (in TC und PMD)

Protokolle:

- PHY: Kodierung, Synchronisation, Übertragung, Erzeugung und Prüfen HEC, Zellausrichtung
- ATM-Layer: Mux/Demux, VPI/VCI remapping, Erzeugung Zell-Header, GFC (Generic Flow Control)
- AAL: 4 Dienstklassen (A-D) basierend auf: Bitrate, Zeitbeziehung Sender - Empfänger, Verbindungsmodus.

RAL Radio Access Layer (für WATM (Wireless ATM), Handover)

WMT Wireless Mobile ATM Terminal

RT Radio Transceiver

AP Access Point

EMAS-E End-user Mobility-supporting ATM Switch - Edge

EMAS-N End-user Mobility-supporting ATM Switch - Network

APCP Access Point Control Protocol

UNI+M User-to-Network Interface with Mobility Support

NNI+M Network-to-Network Interface with Mobility Support

Referenzmodell: WMTs an (jeweils einem) RT, RTs (2) an (1) AP, (2) APs an (1) EMAS-E, EMAS-E an mehrere EMAS-N ...

Protokollschicht Benutzerebene: Bei WATM Ral statt PHY bei Funkstrecke, Rest: User proc., AAL, ATM, PHY

Protokollschicht Kontrollebene: Bei Radioschnittstelle schichtübergreifend W-CTRL, sonst SIG, UNI, (NNI(+M), APCP, UNI+M); SAAL; ATM; PHY

Erweiterte Funktionen:

- Mobile Connection Management Protocol (spezifiziert benötigte QoS, steuert Zuweisung und Freigabe von VCIs, unterstützt Aufbau neuer Pfade während Handover)

- Mobile Handover Management Protocol
- Mobile Location Management Protocol
- Mobile Routing Protocol (Dynamische Topologien, Routing muss drahtlos und verkabelt unterstützen)
- Mobile Media Access Control Protocol (hat Wissen über Auslastung der verfügbaren Bandbreite)
- Mobile Data-Link Control Protocol (Rahmensynchro und -wdh, Übertragung und Bestätigung von Rahmen, Flusskontrolle)

MMF	Mobility Management Function
CCF	Call control and Connection control Function
IMF	Identity Management Function
MTSA	Mobile Terminal Security Agent
RTR	Radio Transmission and Reception
RRC	Radio Resource Control Function
ACF	Association Control Function
ATMC	ATM Connection Function (Standarddienste: CBR, ABR, VBR, UBR)
Funktionsblöcke: Übergang WMT - SP (über ACF und RRC und RTR (parallel)), Übergang AP - EMAS-E (über APCF und ATMC)	
Netzwerkseite:	
APCF	Access Point Control Function
NSA	Network Security Agent
SCF	Service Control Function RAL Anforderungen:

- Anforderung PHY: Definition der Funkzelle-Eigenschaften
- Anforderung PHY: Bitrate, Modulation, Trägerfrequenz, Datenformat, Kodierung, Trainingssequenzen
- Anford. MAC: logischer Zugriff (zeitgl. Zugriff mehrerer Systeme auf den Funkkanal), Dienstklassen (ABR etc.), Mobilitätsunterstützung, Schnittstelle zur PHY und DLC Schicht
- Anf. LLC: Def. von LLC-Protokoll und -Syntax (wie bei MAC Anf.), Behebung spez. Probl. der Funkübertragung (zw. ATM- und MAC/PHY-Schicht), Error Control, Forward EC. Ziel: verpflichtend ARQ, optional: FEC für Echtzeitdienste, Metasignalisierung zur Handoverunterstützung

BRAN ETSI Broadband Radio Access Network (Schichten: BRAN-PHY1, PRAN-PHY2 ...; BRAN-DLC; Network Convergence Layer; core network ATM oder core network IP ...)

Handover:

- Unterstützung Handover-Domain (einheitliches Handover-Protokoll, gemeinsame Strategie, administrativer Bereich (beinh. alle Zugangspunkte und Switches))
- Anforderungen: multiple connection handover, point-to-point, point-to-multipoint, Qos. data integrity and security, signaling, routing, high performance, low complexity
- Unterstützte Varianten:
 - hard handover (Verbind. nur zu 1 Zugangspunkt gleichzeitig)

- Terminal initiated (z.B. wegen Signalqualität)
- Network initiated (z.B. wegen Auslastung)
- Network initiated, terminal assisted (WMT stellt Daten über Empfang zur Verfügung)
- Network controlled (Entscheidung stets beim Netzwerk)
- Backward Handover: (!! Standard, WMT initiiert, alles wird VORbereitet (VOR Handover) (bei mehreren APs in Bereich: BW-HO-REQ, ACPC-Enquiry REQ (an alle APs des Bereichs), RES von allen, HO-REQUEST-QUERY an anderen EMAS-E, dort APCP-Enquiry-REQ an alle APs, nach RSP HO-REQUEST-RESPONSE an 1. EMAS-E, dort BW-HO-RESPONSE an WMT), dann von altem AP APCP-DisassocREQ an EMAS-E, CNF, neuer AP: APCP-AssocREQ an neuen EMAS-E, CNF, von WMT CONN-ACTIVATE (an EMAS-E), von EMAS-E an WMT: CONN-ACTIVE. Bei Inter-EMAS-E/Inter-AP EMAS-E durch COS (Cross Over Switch) verbunden.
- Forward Handover: WMT verbindet sich unvorhergesehen mit anderem AP (Start mit APCP-DisassocREQ, dann Assoc-REQ, dann FW-HO-REQUEST, Enquiry (REQ, RSP), FW-HO-RESPONSE) Bei Inter EMAS-E/Inter-AP: nach Assoc-REQ/RSP HO-NOTIFY an alten EMAS-E, nach FW-HO-RESPONSE SETUP an COS (Antwort von COS: CONNECT), an WMT: CONN-ACTIVE, von EMAS-E(alt) RELEASE (an COS; Antwort: RELEASE-COMPLETE).

Location Management: (über Home EMAS und dortige Auth-REQ/REQ-REPLY: Loc-Update-LS (Location Server))

Verbindungsaufbau, eingehender Ruf, WMT im Fremdnetz:

- Telefon Festnetz → EMAS-E(heimat) → LS(heimat) → EMAS-E(heimat) → EMAS(fremd-Conn) → LS(fremd-Conn) → EMAS(fremd-Conn) → EMAS-E(fremd) → WMT

Adressierung:

AESA ATM Endsystemadresse

Nutzung einer ortsunabhängigen permanenten Adresse, Unterstützung einer temp. routbaren Adresse

M-QoS (wired QoS, wireless QoS, Handover QoS, hard handover, soft handover) (Hauptunterschied zu z.B. Mobile IP !!!)(Hauptgrund für hohe Komplexität)

APCP: (Schnittstelle zwischen funkabhängigen und funkunabhängigen Teil des ATM-Netzwerkes)

CAC Connection admission Control (im EMAS-E)

RRM Radio Resource Management (im AP)

Referenzmodell für weitere Zugriffsarten: (Folie 8.52.1, 8.53.1)

1.9 Mobile IP

- Wegewahl
- Spezifisches Routen zum Endgerät
- Wechslen der IP-Adresse

Anforderungen an Mobile IP:

- Transparenz (mobile Endgeräte behalten IP, Anschlusspunkt an Netzwerk kann gewechselt werden)
- Kompatibilität (mobil - fest)

- Sicherheit (alle Registrierungsrichten müssen authentifiziert werden!)
- Effizienz und Skalierbarkeit (mögl. wenig zusätzl. Daten, große Anzahl mob. Endger. soll weltweit unterstützt werden)

Terminologie: MN Mobile Node
 HA Home Agent (tunnelt IP Datagramme zur COA)
 FA Foreign Agent
 COA Care-of Address (Adresse des akt. gültigen Tunnelendpunktes, kann via DHCP (dynamic Host Configuration Protocol) gewählt werden)
 CN Correspondent Node
 Tunnel HA zu COA (bei Folie 9.5.2 FA) Netzintegration:

- Agent Advertisement (Format: (bytes:1,1,2)type, code, checksum, (1,1,2) Number of addresses, addr.size, lifetime, (4) router address1, (4) preference level 1, ..., Block mit type, length, sequence number, registration lifetime, ..., COA1, COA2...) HA und FA sendenn periodisch spez. Nachrichten über ihre Existenz → MN weiss, ob im Heimatnetz oder in Fremdnetz, MN kann COA aus Nachricht ablesen.
- Registrierung: MN meldet via FA seinem HA die COA, dieser bestätigt via FA an MN (durch Authentifikation abgesichern!) (Format: type, ..., lifetime, home address (4), home agent (4), COA (4), identification (2*4), extensions ...)
- Bekanntmachung: HA macht IP des MN bekannt und benachrichtigt andere Router, das MN über ihn erreichbar. Pakete an MN nun an HA. Änderungen an COA und FA haben darauf keinen Einfluss!

Kapselung:

- (-(originaler IP-Kopf),(originale Nutzdaten)-)
- (neuer IP-Kopf,(-neue Nutzdaten-))
- (äußerer Kopf,(-innerer Kopf, originale Nutzdaten-))
- Ip-in-IP-Kapselung: Tunnel: 1.Header: (Ver, IHL, TOS, Gesamtlänge, IP-Id, Flags, Fragment Offset, TTL, IP-in-IP, IP checksum, IP HA, COA), gekapselter Header: (... , TTL, Lay4 Protoc., IP-checksum, originale IP Sender, IP MN, TCP/UDP/...Nutzlast)
- Minimale Kapselung: Vermeidung redundanter Felder. Nur bei unfragmentierten Paketen (!!), da kein Platz mehr für Fragmentkennung.

GRE Generic Record (Routing) Encapsulation (äußerer Kopf,(-GRE Kopf, originaler Kopf, originale Daten-)) Optimierung des Datenpfades:

- Triangular Routing (Sender alle Pakete via HA zu MN, -: unnötige Verzögerung und Netzlast)
- Lösungsansätze: akt. Aufenthaltsort lernen (Sender), direktes Tunneln dorthin, HA kann Sender über Ort(MN) benachrichtigen. Große Sicherheitsprobleme
- Wechsel des FA: Pakete "im Flug" gehen während des Wechsels verloren, Vermeidung: Benachrichtigung neuer FA an alten. Alter leitet restlichen Pakete an neuen weiter.

- Ablauf: Data (HA) → HA Update an Sender → ACK von Sender an HA → Data (FAalt) → Data an MN → MN wechselt FA → MN Registration FAneu → FAneu Update FAalt → FAalt ACK FAneu → S Data (FAalt) → Data (FAneu) → Data (MN) → FAalt Warning Sender → S Request FAalt → FAalt update S → S ACK FAalt → S Data (FAneu) → Data (MN)...

Reverse Tunneling:

- von MN ausgehend
- Prinzip: MN an FA; FA kapselt und tunnelt an HA; HA über normalen (Internet) Weg an Empfänger.
- Eigenschaften von Mobile IP bei Reverse Tunneling
 - Router akzeptieren oft nur “topologisch korrekte” Adressen (durch Kapselung des FA gewährleistet), TTL-Problematik (und Multicast) gelöst (TTL nun im Heimatnetz richtig, aber u.U. zu weit vom Ziel)
 - Reverse Tunneling löst NICHT: firewall-Problematik (umgekehrte Tunnel zu firewall hijacking missbrauchbar), Optimierung der Wege (Pakete normalerweise zu HA (über Tunnel))
- neuer Standard ist rückwärtskompatibel

Mobile IP und IPv6:

- Sicherheit ist integriert, Authentifikation aller Aktionen
- COA kann über Autokonfiguration erhalten werden
- FA nicht mehr benötigt (da alle Router das Router Advertisement beherrschen (nun anstelle des Agent Advertisement))
- MN kann automatisch Sender über COA benachrichtigen (Senden über HA entfällt (automatische Wegoptimierung))
- “sanfte” Wechsel (ohne Paketverluste) zwischen verschiedenen Subnetzen (MN → COAneu an ROUTERalt → ROUTERalt kapselt restliche Pakete und forwarded zu COAneu)

Probleme mit Mobile IP:

- Sicherheit (Auth. mit FA problematisch, (u.U. nicht unter eigener Kontrolle), kein Schlüsselverwaltungsprotokoll standardisiert, Patent- u. Exportproblematik.)
- Firewalls (verhindert typischerweise Mobile IP, spez. Konfiguration (z.B. für Reverse Tunneling) nötig)
- QoS (Tunneln verhindert das Erkennen eines gesondert zu behandelnden Datenstroms; häufige erneute Reservierungen bei Verwendung von RSVP (Reservation Setup Protocol))

Sicherheit Mobile IP:

- Sicherheitsanforderungen:
 - Integrität (keine unbemerkte Veränderung)
 - Authentizität (Absender = Sender, empfangene Daten = gesendete Daten)

- Vertraulichkeit
- Nicht-Zurückweisbarkeit
- Verkehrsflussanalyse
- Rückspielsicherung (abgefangene gültige Registrierung → wenn erneut gesendet → als ungültig erkannt)
- Sicherheitsarchitektur:
 - Alle Partner: gleiche Verfahren und Parameter (Security Association)
 - zwei Header: Authentication Header (sichert: Integrität, Authentizität; bei asymmetrischem Verschlüsselungsverfahren auch: Nicht Zurückweisbarkeit) Aufbau: (IP Header, Authentication Header, UDP/TCP Packet)
 - Encapsulation Security Payload (schützt Vertraulichkeit): v=verschlüsselt, u=un-v: (IP Header(u), ESP Header (1. Teil u, 2. Teil v), verschlüsselte Daten (v))
 - Sicherung von Registrierungen: Mobile Security Association (MN, HA, FA)
 - Erweiterung der IP-Sicherheitsarchitektur: Authentication-Erweiterung (Auth(HA,FA), Auth(HA,MH)) (MH = Mobile Host), Verhindern Wiederholte Rücksenden von Registrierungen: Zeitstempel (32bit timestamp + 32bit random), nonces (32bit random(MH) + 32bit random(HA))
- Schlüsselvergabe durch HA

DHCP:

- Anwendung: Vereinfachung der Installation und Verwaltung, liefert Rechnern notwendige Information über IP, DNS, Subnetzmasken, etc., damit weitgehend automatische Integration des Rechners in das Netz
- Client/Server Modell (Client broadcast Anfrage → DHCP-Server (u.U. über DHCP-Relay)) (Prinzip: DHCPDISCOVER, Antw: DHCPOFFER, Auswahl Konfiguration, DHCPREQUEST (reject oder Optionen), gewählter Server: DHCPACK, Initialisierung komplett: Client: DHCPRELEASE)
- Charakteristika:
 - Server (mehrere können konfiguriert werden)
 - Erneuerung der Konfiguration (IP-Adressen müssen regelmässig neu angefordert werden)
 - Optionen (verfügbar für Router, Netzmaske, NTP, ...)

Ad-Hoc-Netzwerke:

- Mobile IP braucht Infrastruktur (bei Ad-Hoc oft nicht vorhanden)
- Hauptproblem: Wegewahl (kein Standardrouter, potentiell muss jeder Knoten weiterleiten können)

Routing:

- Traditionelle Routing Algorithmen:

- Distance Vector (period. Austausch mit Partnern (wer wie weit?), Wahl des kürzesten Weges)
- Link State (period. Benachr. aller Router über Zustand aller physikalischen Verbindungen (Router haben somit vollständiges Bild))
- Probleme: Dynamik der Topologie, begrenzte Leistung der mobilen Geräte (period. Aktualisierung braucht viel Energie, sowieso begr. Bandbreite, dann auch noch Routinginformationen; asymmetrische Verbindungen (richtungsabhängige Qualitäten)); Protokolle für Festnetz entworfen.
- DSDV: Erweiterung von Dist. Vector Routing (Sequenznummern, Dämpfung und Änderung (nur, wenn gespeicherte Zeit (zw. 1. und besten Ankündigung) passt))
- Dynamic Source Routing:
 - Trennung in: Auffinden und Aufrechterhalten
 - Auffinden: (nur wenn wirklich benötigt und noch kein Weg vorhanden) (Aussenden broadcast Paket(DA, Kennung); Empfänger: Falls Empfänger → Antwort; Falls schonmal bekommen → Verwerfen; Sonst → eigene Adresse anhängen und als broadcast weiter)
 - Optimierung: Begrenzung durch “maximale Ausdehnung” (falls bekannt), Caching der Weginformationen mit Hilfe von vorbeikommenden Paketen.
 - Aufrechterhalten: (nur während aktueller Benutzung) (nach Senden: Warten auf Quittung (Schicht 2, falls vorhanden); Mithören, ob weitergeleitet; Anforderung einer expliziten Bestätigung) Bei Problemen: neuen Weg suchen (wenn erforderlich).
- Interferenz-basiertes Routing:
 - LIR: (basiert auf: Anzahl der Empfänger, die eine Sendung hören können)
 - MMRCR: (basiert auf: Wahrscheinlichkeitsfunktion von erfolgreichen Übertragungen und Interferenzen)
 - LRR: (basiert auf: Interferenz, bestehend aus Informationen über Störung, Jamming und andere Übertragungen)

DSDV	Destination Sequenced Distance Vector (Routing Algorithmus)
LIR	Least Interference Routing (Wieviele Nachbarn in Hörweite sind)
MMRCR	Max-Min Residual Capacity Routing (Wahrscheinlichkeitsfunktion, Interferenzen)
LRR	Least Resistance Routing (Interferenz)

1.10 Mobile TCP

- Fast Transmit/Fast Recovery (mehrere Bestätigungen für ein Paket → kein Verlust → Weitermachen mit aktuellem Fenster)

Auswirkungen der Mobilität auf TCP-Mechanismen:

- Bei Paketverlust geht TCP von Stau aus (slow start etc.) (hier meist falsch) → Leistung eines unveränderten TCP bricht katastrophal ein.

Indirektes TCP:

- Keine Änderung am TCP-Protokoll für Rechner im Festnetz.
- optimiertes Protokoll für Mobilrechner
- Auftrennung der Verbindung z.B. am FA in 2 Teilverbindungen (KEINE “echte” Ende-zu-Ende-Semantik mehr!!!)
- Rechner im Festnetz bemerken nix.
- Vorteile:
 - keine Änderungen im Festnetz
 - keine Fehlerfortpflanzung: drahtlose Strecke in Festnetz
 - relativ einfach beherrschbar
 - sehr schnelle Übertragungswiederholung (meist 1 hop von FA zu MN und Verzögerungszeit auf der Mobilstrecke bekannt)
- Nachteile:
 - Verlust der TCP-Semantik (ACK an Sender heißt nun nicht mehr, dass Empfänger wirklich was bekommen hat), was, wenn FA offline?, Konsistenz der Schichten?
 - vergrößerte Latenzzeiten durch Pufferung der Daten im FA

Snooping TCP:

- “Transparente” Erweiterung von TCP im FA
- Puffern Daten zum MN im FA, lokale Übertragungswiederholung: FA hört Datenverkehr ab und erkennt Bestätigungen in beide Richtungen. Erweiterung des TCP NUR im FA.
- Datentransfer zum Mobilrechner: FA puffert bis ACK von MN, erkennt Paketverluste durch duplizierte ACK oder time-out, lokale Ü-wdh
- Datentransfer vom Mobilrechner: FA erkennt Paketverluste anhand Sequenznummer und sendet darauf NACK zum MN; MN überträgt nun schnell erneut.
- Integration der MAC-Schicht: oft ähnliche Mechanismen wie TCP, dort können schon Paketverluste durch Wdh erkannt und verworfen werden
- Probleme: Snooping TCP isoliert drahtlose Verbindung nicht so gut: je nach Verschlüsselungsverfahren ist snooping TCP nutzlos.

1.11 Mobilitätsunterstützung

Dateisysteme:

- Ziel: effizienter und transparenter Zugriff auf geteilte Daten unter Konsistenzwahrung
- Problem: beschränkte Ressourcen, teilweise totale Abkopplung, hochgradige Heterogenität der Komponenten, Standarddateisysteme versagen.
- Ideen: (Vervielfachung, Kopieren, Caching), (pre-fetching, Hoarding)
- Konsistenz:

- Hauptproblem bei lose gekoppelten Systemen: Alle Sichten gleich? Welche Änderungen an welche Teilnehmer propagieren?
- Schwache Konsistenz: Ungültig Erklären von Daten durch Server problematisch, zeitweise Inkonsistenzen in Kauf genommen, nachfolgende Konfliktauflösung.
- Konflikterkennungen: inhaltsunabhängig (Versionsnummer, Zeitstempel), inhaltsabhängig (Abhängigkeitsgraphen)
- Dateisysteme für eingeschränkte Ankopplung:
 - Symmetrie: Client/Server-Beziehung (oder Peer-to-Peer), Unterstützung auf Festnetz- und/oder Mobilseite, einziges oder mehrere Dateisysteme, durchgängiger Namensraum
 - Transparenz: Verbergen der Mobilitätsunterstützung, Verbergen der Mechanismen gegenüber Benutzern
 - Konsistenzmodell: optimistisch oder pessimistisch
 - Caching und Pre-Fetching: einzelne Daten, Verzeichnisse, Unterbäume, Partitionen ...; permanent oder nur zu gewissen Zeitpunkten
 - Datenhaltung: Verwaltung (gepufferte Daten, Kopien), Anforderung an Erneuerung, Gültigkeit, Erkennung von Änderungen an Datenbeständen
 - Konfliktbehandlung: anwendungsspezifisch oder allgemein, Fehlerfälle
 - experimentelle Systeme (Coda, Little Work)
- Coda:
 - Anwendungstransparente Erweiterungen von Client und Server
 - Änderungen im Cache Manager des Client, Anwendungen arbeiten auf Cache-Replikaten, Hoarding
 - Konsistenz: Änderungen mitprotokolliert, bei Wiederankopplung Vergleich, wenn Vergleich negativ: manuelle Reintegration, optimistischer Ansatz, grobgranular (Dateigröße)
 - Hoarding: Benutzer kann Dateiliste (incl. Prio.) vorgeben, Cache-Inhalt bestimmt durch LRU, explizites pre-fetching möglich, periodische Aktualisierung
 - Datenabgleich: asynchron, im Hintergrund; Abwägen (refresh-rate, Netzlast)
 - Cache-Misses: Modellierung der “Benutzergeduld”, Funktion von Größe und Bandbreite
 - Client-Zustände: Hoarding (strong connection), Write Disconnected (connection, weak connection), Emulating (disconnection)
- Little Work
 - Lediglich Änderungen am Cache-Verwalter des Client:
 - Connected (normal; kont., hohe Bandbreite), Partially Connected (verzögertes Schreiben zum Server; kontin.), Fetch only (optim. Replik. von Dateien; anforderungsgest.), Disconnected (Abbruch bei Cache-Miss; -)

WWW und Mobilität:

- Protokoll nicht für mobile Anwendungen entworfen
- Web ist kein Dateisystem (dynamische Inhalte, push-Strategien) Ein Klick auf eine Datei kann große Konsequenzen haben.

- HTTP 1.0 und Mobilität:
 - Eigenschaften: zustandslos, Client/Server, Anfrage/Antwort, erfordert verbindungsorientiertes Protokoll (1 Verbindung pro Anfrage), primitive Caching- und Sicherheitsmodelle
 - Probleme: große und redundante Protokollköpfe, unkomprimierte Übertragung, mit TCP: großer Overhead durch 3-Wege-Handshake, slow-start-Problematik, DNS-lookup durch Client erzeugt zusätzlichen Verkehr.
 - Caching: oftmals verhindert (wegen Statistiken), Problem dynamischer Objekte (können nicht im Cache abgelegt werden), Mobilität macht Caches oft unmöglich, Sicherheitsproblematik (wie bei SSL mit Proxies?)
 - POST: (Senden zum Server): kann i.A. nicht gepuffert werden.

HTML und mobile Endgeräte:

- entworfen für hohe Leistung, Optimierung der "Ästhetik" (nicht des Kommunikationsaufwandes!)
- mobile Endgeräte: kleine Anzeige, eingeschränkte Eingabemöglichkeiten
- weitere Features: animierte GIFs, Java AWT, Frames, Active X, Shockwave ...
- → Heterogenität der Endgeräte wird weitgehend ignoriert.

Ansätze:

- Anwendungs-Gateways, erweiterte Server: Kompression, Filterung, Inhaltsextraktion, automatische Anpassung an Netzwerkgegebenheiten. (Beispiel: HGML (handheld Device Markup Language), Extraktion von Überschriften, Zusammenfassen der Texte)
- Probleme: proprietäre Ansätze → eine Menge spezieller Zusätze für Browser, große Geräteheterogenität erschwert Ansätze.

Neue Techniken, die der Mobilität helfen:

- Push-Technik (echtes Push, kein Client-Pull, channels etc.)
- HTTP/1.1: client/server nutzen dieselbe Verbindung, erweiterte Zwischenspeicherung möglich, neue Tags und Optionen um Cache besser zu steuern, Kodierung/Kompression, Authentisierung, Sicherheit von Proxies
- Cookies: ...

Systemunterstützung für WWW im Mobilnetz

- Erweiterte Browser: pre-fetching, caching, abgekoppelte Nutzung (z.B. IE)
- Zusätzliche, begleitende Anwendung (s.o.)
- Client Proxy (s.o.)
- Netzwerk Proxy: Adaptive Inhaltsinformation bei schlechter Verbindung, pre-fetching, caching
- Client und Netzwerk Proxy: s.o. + Protokollvereinfachungen

- Spezielles Netzwerk Subsystem: siehe Netzwerkproxy
- Zusätzlich viele Server-Erweiterungen machbar: “Channels”, Inhaltsaushandlung, ...

WAP Wireless Application Protocol:

- Ziele: Internet-Inhalte auf mobiles Endgerät, Unabhängigkeit von Standards, offen für alle, Skalierbarkeit
- Plattformen: z.B. GSM, CDMA, UMTS
- Browser: Micro-Browser
- Script-Sprache: ähnlich Java-Script
- WTA/WTAI
- Inhaltsformate: z.B. Visitenkarten (vCard)
- Protokollstapel: Transport-, Sicherheits-, Sitzungsschicht

WTA Wireless Telephony Application
 WTAI WTA Interface
 CDPD Cellular Digital Packet Data
 WCMP Wireless Control Message Protocol
 WDP Wireless Datagramm Protocol
 WTLS Wireless Transport Layer Security
 WTP Wireless Transaction Protocol
 WSP Wireless Session Protocol
 WAE Wireless Application Environment

WAP - Schichtenarchitektur und Protokolle: (bottom → top)

- Übertragungstechniken (GSM, CDPD) ((Internet: TCP/IP, UDP/IP, Medien))
- Transport Layer (WDP), WCMP, ((s.o.))
- Security Layer (WTLS), ((SSL/TLS))
- Transaction Layer (WTP), ((HTTP))
- Session Layer (WSP), ((s.o.))
- Application Layer (WAE), ((HTML, Java))

Filter → WAP-Proxy, Filter/WAP-Proxy oder WTA-Server (Netzwerkelemente WAP).

- WDP: liegt direkt auf Übertragungsdiensten, bietet einheitliche Schnittstelle für Protokolle höherer Schichten, erlaubt transparente Kommunikation; Ziel: Mit Hilfe von WDP global interoperables Transportsystem schaffen.
- WTLS: Ziele: Datenintegrität (Verhindern von Ändern), Privatheit (Verhindern von Mithören), Authentifikation (Aufbau entsprechender Beziehung MN und Server), Schutz vor DoS-Attacken (Wiederholung von Daten, nicht verifizierbare Daten ablehnen). Basiert auf TLS (Transport Layer Security (ehemals SSL)), hier optimiert für schmalbandige Kommunikationskanäle

- WTP: Ziele: einheitliche Schnittstelle zu physikalischen Transportmechanismen, port-basiertes Interface zu Anwendungen (Anwendung unabhängig von Transporttechnik); Unter-stützung verschiedener Kommunikationsformen (verbindungorientiert (nachrichtenorien-tiert, QoS-Aushandlung, duplex, zuverlässig, Flusskontrolle), transaktionsorientiert (zu-verlässig, Daten im ersten Paket, Flusskontrolle), verbindungslos (unzuverlässig, UDP falls Schicht 3)), unterstützt C/S, peer/peer, Multicast-Anwendungen; speicherplatzschonend; Ef-fizient bzgl. Luftschnittstelle (SAR, selektive Ü-wdh, Kompression der Protokollköpfe, opti-mierte Verbindungsaufbauten (Aufbau mit Datenübertragung))
- WSP: Ziele: HTTP/1.1 Funktionalität, support von Transaktionen, Push-Technik; Schlüssel-verwaltung, Authentifikation; Verwaltung von Sitzungen(Unterbrechung, Wiederaufnah-me...); Offene Punkte: QoS, Gruppenkommunikation, Isochrone Multimedia-Objekte, Ver-waltung
- WAE: Ziele: netzwerkunabh. Anw.umgeb. für schmalbandige drahtlose Geräte; Anforderun-gen: internationale Unterstützung, Mensch-Maschine-Schnittstelle (herstellerbestimmbar), Beachtung langsame Verbindungen, geringer Speicher, begrenzte Rechenleistung, kleiner Bildschirm, einfache Eingabe; Komponenten: Architektur: Anwendungsmodell, Browser, Gateway, Server; WML, WMLScript, WTA, Inhaltsformate
- WAE logisches Modell: (Kodierer & Decodierer im Gateway (zwischen Ursprungs-Server und Client))
- WML: Stapel/Blatt (deck) und Karten (card) Metapher (HTML ähnlich), beschreibt nur die ABSICHT einer Interaktion (Umsetzung hängt von Gerätefähigkeiten ab). Eigenschaften: Texte, Bilder, Benutzereinteraktion, Navigation, Inhaltsverwaltung
- WMLScript: Ergänzung zu WML, Eigenschaften: Gültigkeitsprüfung von Benutzereingaben, Zugriff auf Gerätefunktionen, lokale Benutzerinteraktion (RTT (Real Time Transaction)), Erweiterung der Geräte-Software.
- WTA: Sammlung telephonspezifischer Erweiterungen (content push (server kann Inhalte di-rekt auf Client schreiben), Behandlung von Netzereignissen, Zugang zu Telefonfunktionen)
- WAP-Protokollstapel: ((((((IP (GPRS, General Packet Radio Service), non IP (SMS)), (UDP, WDP)), (WTLS) bisher: datagrammbasierte Anwendungen), (WTP) bisher: transaktionsba-sierte Anwendungen), (WSP)), (WAE) WAE user agent)