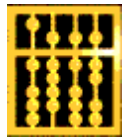
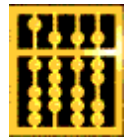


Protokolle ...

... und Kommunikationsstandards

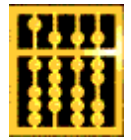
Referenten: Matthias Bechtold & Winfried Thalmeier

Gliederung



1. Internet: Standards und Protokolle
2. Wireless Wide Area Networks (WWAN)
3. Nahbereichsdatenübertragung
4. Service Discovery
5. Zusammenfassung und Quellen

Internet: Standards und Formate
Übersicht



Drahtgebundenes Internet:

- Hypertext Transfer Protocol (HTTP)
- Hypertext Markup Language (HTML), Extensible HTML (XHTML) und Extensible Markup Language (XML)

Drahtloses Internet:

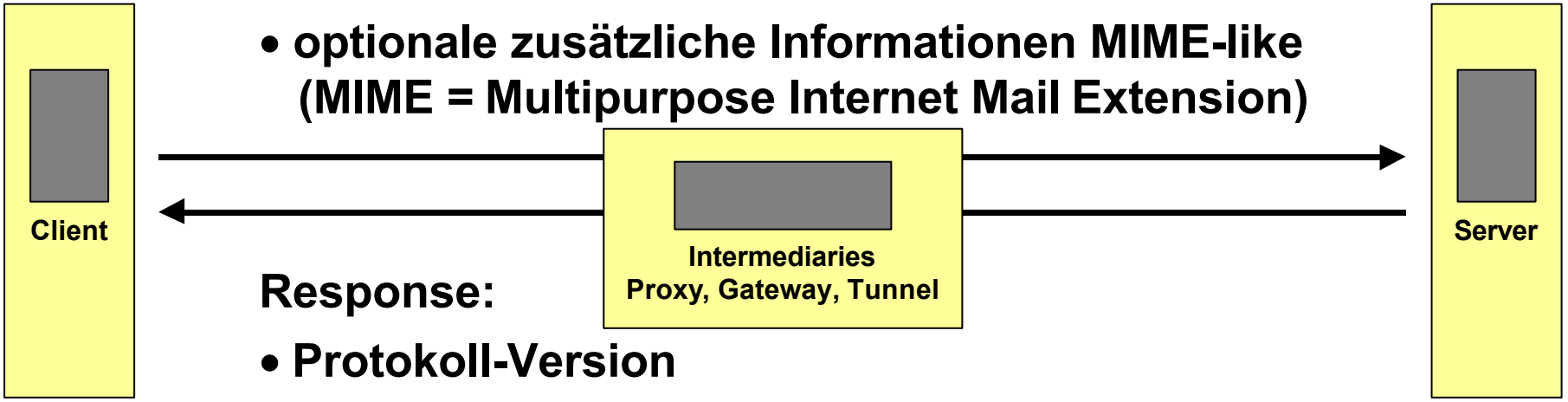
- WAP-Architektur (WAP = Wireless Application Protocol)
- Wireless Application Environment (WAE)
- Wireless Markup Language (WML) und WML-Script

Hypertext Transfer Protokoll (HTTP)

Application Level Protocol nach dem Request-Response Paradigma:

Request:

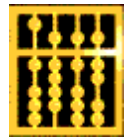
- **HTTP-Methode: z.B. GET oder POST**
- **URI (Universal Resource Identifier)**
- **Protokoll-Version**
- **optionale zusätzliche Informationen MIME-like (MIME = Multipurpose Internet Mail Extension)**



Response:

- **Protokoll-Version**
- **Status-Code: Zahlen-Code und Text**
- **Metadaten z.B. MIME-Type**
- **zu übermittelnde Daten (Nachrichten-Body)**

HTML, XHTML und XML



Hypertext Markup Language (HTML):

Die bekannte Internet Publikationssprache

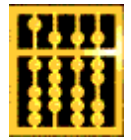
Extensible Hypertext Markup Language (XHTML):

Reformulierung von HTML in XML

Extensible Markup Language (XML):

- **Standardisierte Metasprache für Markup-Sprachen**
- **logische Beschreibung eines strukturierten Dokuments in Plain-Text**
- **XML-Dokument kann mit einer DTD (Document Type Definition) oder mit XSchema (XML Schema) detailliert beschrieben werden**
- **XSL und XSLT (Extensible Stylesheet Language und XSL Transformations) erlauben die Formatierung und die Umwandlung von XML-Dokumenten**
- **Protokolle in XML: z.B. XML-RPC**

Wireless Application Protocol (WAP)



Drahtgebundenes Internet: HTTP + (X) HTML

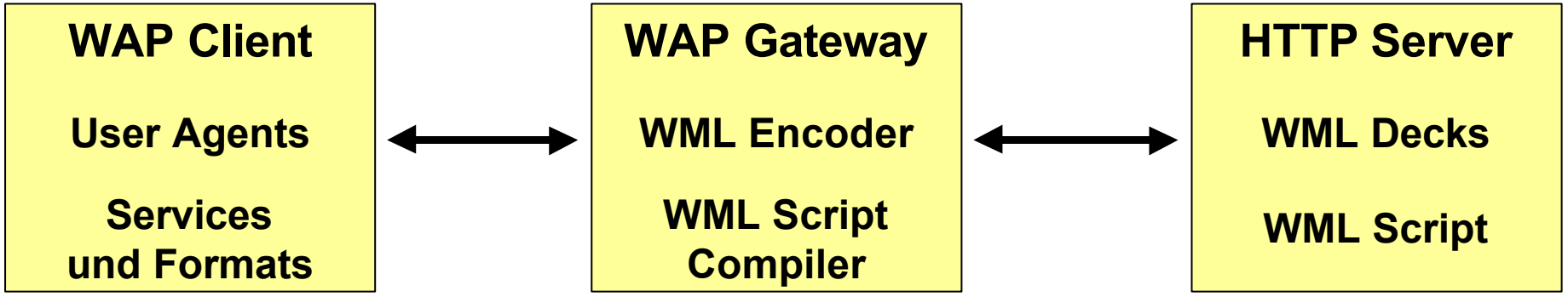
Drahtloses Internet: WAP und WML (Wireless Markup Language)

Verbindendes Element: WAP-Gateway

WAP Layer Modell:

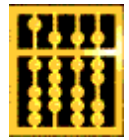
Application Layer:	**Wireless Application Environment**	**(WAE)**
Session Layer:	**Wireless Session Protocol**	**(WSP)**
Transaction Layer:	**Wireless Transaction Protocol**	**(WTP)**
Security Layer:	**Wireless Transport Layer Security**	**(WTLS)**
Transport Layer:	**Wireless Datagramm Protocol**	**(WDP)**
Network / Physical Layer:	**WAP unabhängig**	

WAE-Architektur



- **User Agents: z.B. WAE und WTA**
  Darstellung von WML-Dokumenten, Ausführung von WML-Script und Wireless Telephone Applications (WTA)
- **Services und Formats:**
  Einzelne Services & standard. Schnittstellen für versch. Bereiche
- **WML Encoder:**
  WML → WBXML (WAP Binary XML Format)
- **WML Script Compiler:**
  WML-Script → Byte-Code
- WAP unterstützt **Push- und Pull Mode** (WAP 1.2)

WML und WMLScript



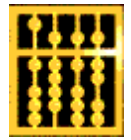
WML:

- WML ist eine XML-Applikation
- WML Deck (WML Seite) = 1 oder mehrere WML Cards
- Capability Data in WSP: WAE Client beschreibt seine Fähigkeiten, z.B. Sprache, Character Set, WML Version, ...
- Navigations- und Aktions-Tags inkl. Variablen
- Analoge Elemente zu HTML-Forms
- Tags für Links und Bilder (z.B. WBMP: Wireless Bitmaps)

WML Script:

- Von Java Skript abgeleitet
- Reduzierung von sog. Turn-Arounds
- WML-Script Standard Libraries (z.B. Dialoge, Strings, URL, ...)

Wireless Wide Area Networks
Übersicht



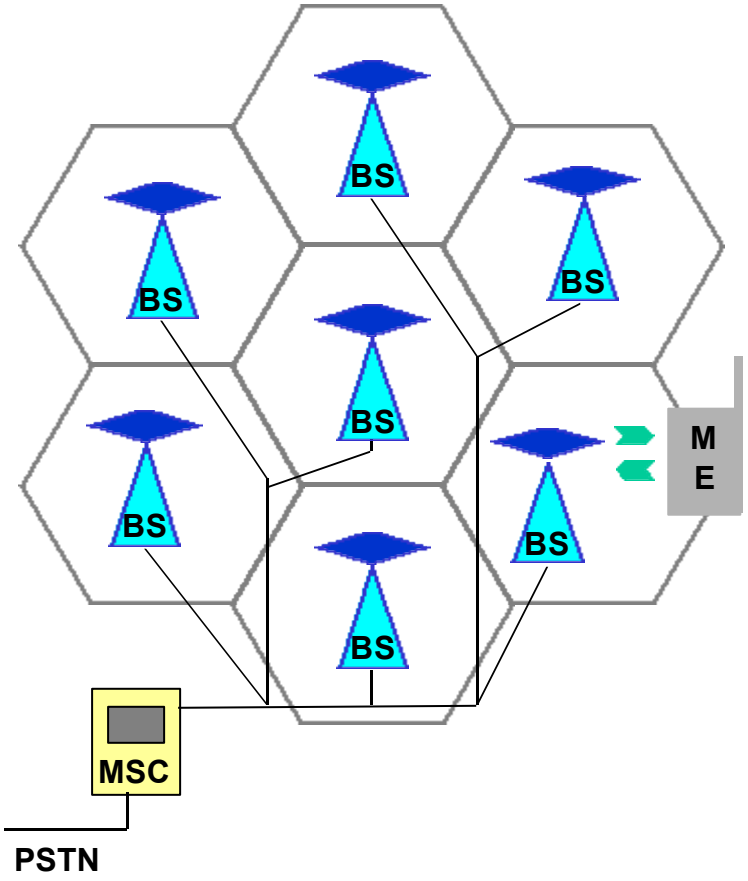
Grundlagen:

- Zellen, Kommunikation und Handover
- Multiple Access Methods:
  FDMA, TDMA, CDMA und Full-Duplex
- Sicherheit:
  Authentifizierung und Datenverschlüsselung
- Short Messages Service (SMS)

Wichtige digitale Zellsysteme:

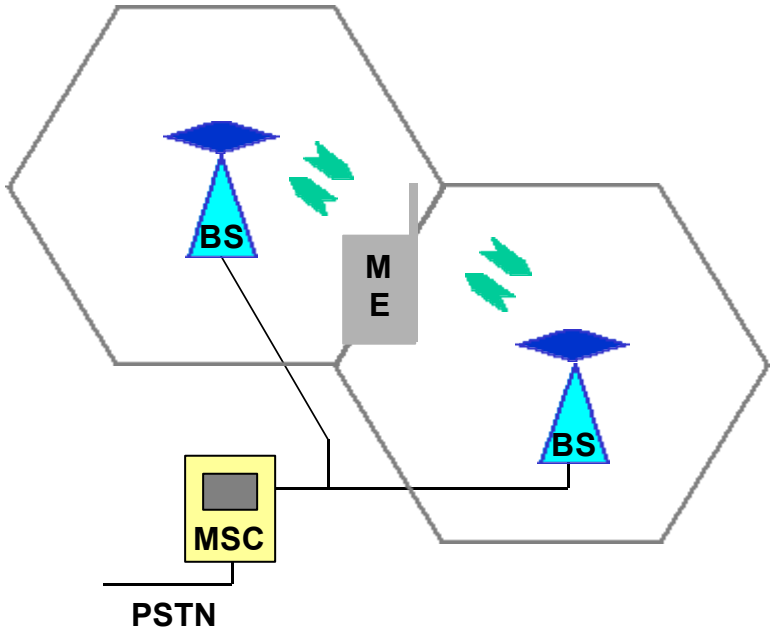
- GSM:
  Infrastruktur, phys. Kommunikation und Sicherheit
- IS-95 CDMA
- IS-136 TDMA
- Japanese PDC

Zellen und Kommunikation



- Zu überdeckende Fläche ist in Zellen mit je einer Basisstation (BS) aufgeteilt
- Mobiles Endgerät (ME) befindet sich in ständigem Kontakt mit der BS
- Kommunikation zwischen ME und BS ist rein digital
- Mehrere BS sind einem Mobile Switching Center (MSC) verbunden
- MSC ist mit dem Telephonnetz (Public Switched Telephone Network, PSTN) verbunden

Handover / Handoff

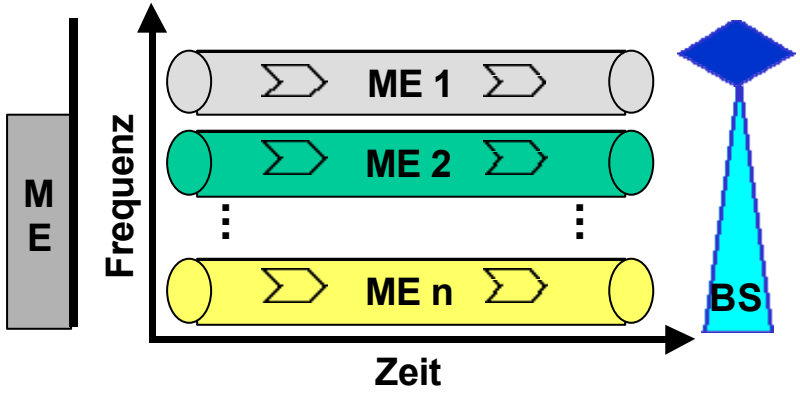


- ME ist in ständiger Bereitschaft für ein Handover
- ME führt nach Empfangsstärke geordnete Liste von erreich-baren BSen
- ME sendet diese Liste an BS (periodisch nach Zeitintervall)
- BS überwacht Signalstärke des MEs
- Fällt ME-Signal unter festgelegte Grenze: BS informiert MSC
- MSC führt Handover durch: BSen und ME werden informiert

Multiple Access Methods I

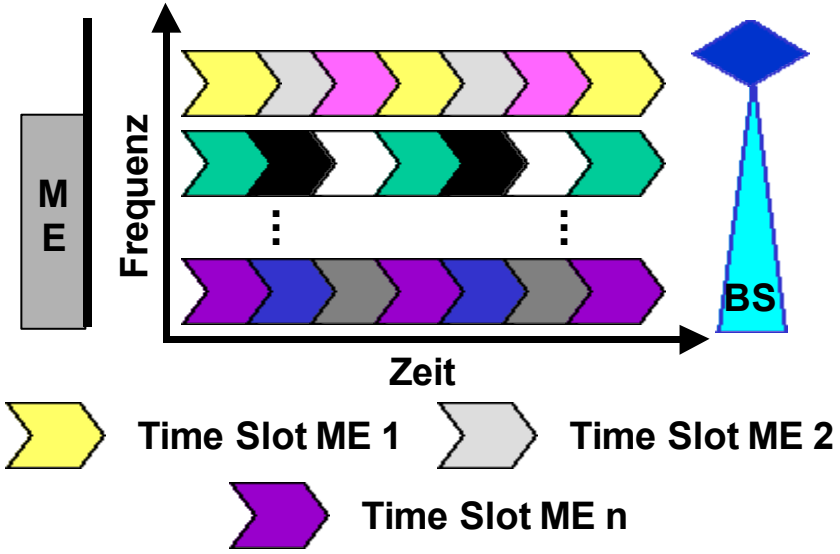
FDMA: Frequency Division Multiple Access

Jede ME belegt exklusiv einen Kanal



TDMA: Time Division Multiple Access

Jede ME belegt einen periodischen Zeitschlitz (Time Slot) in einem Kanal

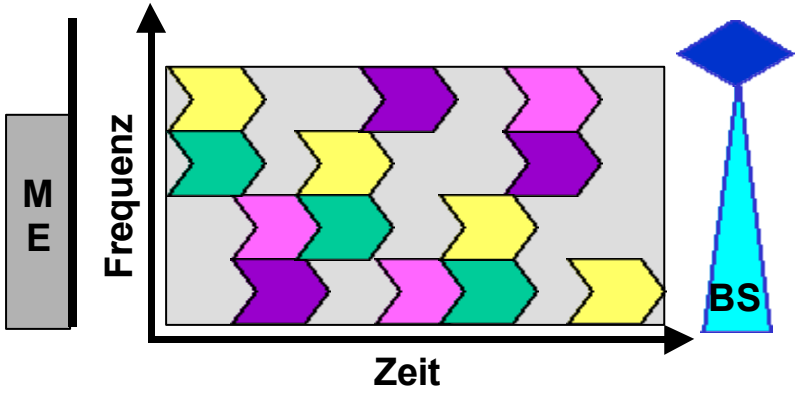


In der Praxis werden oft beide Verfahren kombiniert.

Multiple Access Methods II

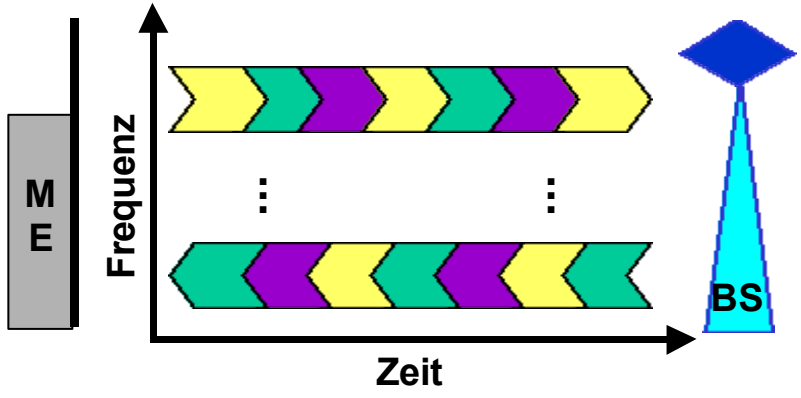
CDMA: Code Division Multiple Access

- Spread Spectrum Technology
- Verteilung d. Datenpakte nach einem Pseudo-Random Noise Code (PN-Code) über einen festgelegten Frequenzbereich
- ME kann mit mehreren BSen gleichzeitig kommunizieren

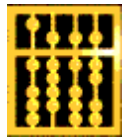


Full-Duplex Communication

- FDD: Frequency Domain Duplex (je ein Hin- und Rückkanal)
- TDD: Time Domain Duplex (unterschiedliche Time Slots auf gleichem Kanal)
- In der Praxis: FDD und TDD (separate Kanäle mit time slots)



Sicherheit I:
HW- und Netzbetreiber Ebene



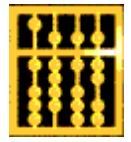
Hardware Ebene:

- Jede ME bekommt bei der Herstellung eine eindeutige Identifizierungsnummer (HID)
- ME identifiziert sich gegenüber MSC mit HID
- MSC führt drei Listen für HIDs:
  - White:
    Zugang wird gewährt
  - Black:
    Zugang wird verweigert
  - Grey:
    ME steht unter Beobachtung aufgrund von Problemen

Netzbetreiber Ebene:

- Vom Netzbetreiber vergebene Identifikationsnummer für den Kunden (CID)
- CID kann unterschiedlich gespeichert werden, z.B.:
  - In ME einprogrammiert
  - Auf Karte gespeichert: Subscriber Identity Module (SIM)
- CID wird in ME und in einem Authentification Center (AuC) des Netzbetreibers in einer Datenbank gespeichert

SMS und Sicherheit II: Authentifizierung und Verschlüsselung



Authentifizierung: Challenge-Response Verfahren

- Challenge = generierte Zufallszahl (AuC)
- von beiden Seiten verwendeter geheimer Schlüssel wird nicht übertragen

Datenverschlüsselung bei der Übertragung:

- ME generiert Session Key (aus Challenge und geheimem Schlüssel)
- Session Key dient genau eine Verbindung lang zur Verschlüsselung

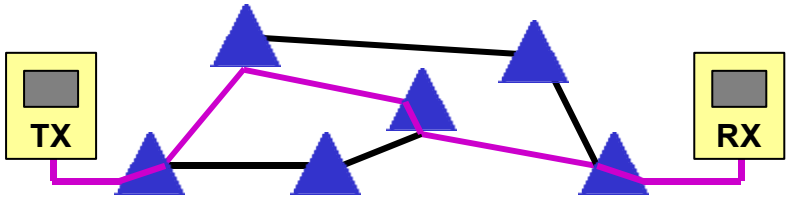
SMS (Short Message Service):

- Text-Mitteilungen mit max. 160 Single- oder 70 Double-Byte Zeichen
- Store-and-Forward Prinzip über Short Message Service Center
- Drei Arten von Mitteilungen:
  Point-to-Point, Multipoint und Broadcast

Grundlegende Switching Verfahren

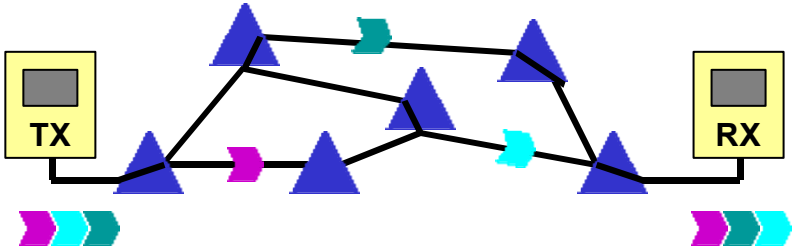
Circuit Switched Data:

- kontinuierlicher Datenstrom
  → Kapazitätsauslastung?
- Kanal für Punkt-zu-Punkt Verbindung wird bei Aufbau reserviert
  → einmaliger Overhead
- Routing wird bei Verbindungs-aufbau starr festgelegt

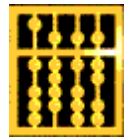


Paket Switched Data:

- Verbindungsstrom wird in Pakete unterteilt
  → Paket-Overhead
- Einzelne Pakete werden unab-hängig voneinander flexibel geroutet
- Out-of-Order- und Paket-Loss-Problem



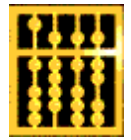
GSM-Elemente I:
SIM, BTS und BSC



GSM: Global System for Mobile Communications:

- Weltweit mehr als 250 Mio. Kunden hauptsächlich in Europa
- ME mit SIM:
  - International Mobile Equipment Identity (IMEI)
  - International Subscriber Mobile Identity (ISMI)
  - geheimer Schlüssel zur Authentifizierung
  - Telephonbuch
- Base Transceiver Station (BTS):
  Physical Radio Link Layer zum ME
- Base Station Controller (BSC):
  - Verwaltung mehrerer BTS
  - Verwaltung der Kanäle
  - Regelt Handover zwischen an es angeschlossenen BTSs

GSM-Elemente II:
MSC, HLR und VLR



- Mobile Services Switching Center (MSC):
  - Zugangskontrolle über AuC und Equipment Identity Register (EIR)
  - Gateway zum PSTN
  - Regelt Verbindungen zwischen unter ihm angeschlossenen MEs
  - Regelt Handover zwischen unter ihm angeschlossenen BSCs

- Home Location Register (HLR):
  - Kundendatenbank
  - Jeder GSM-Netzbetreiber besitzt genau ein HLR
  - Kundenprofil inkl. Identifizierungs-Information
  - Generiert Referenz VLR-Eintrag bei aktivem ME („Aufenthaltsort“)

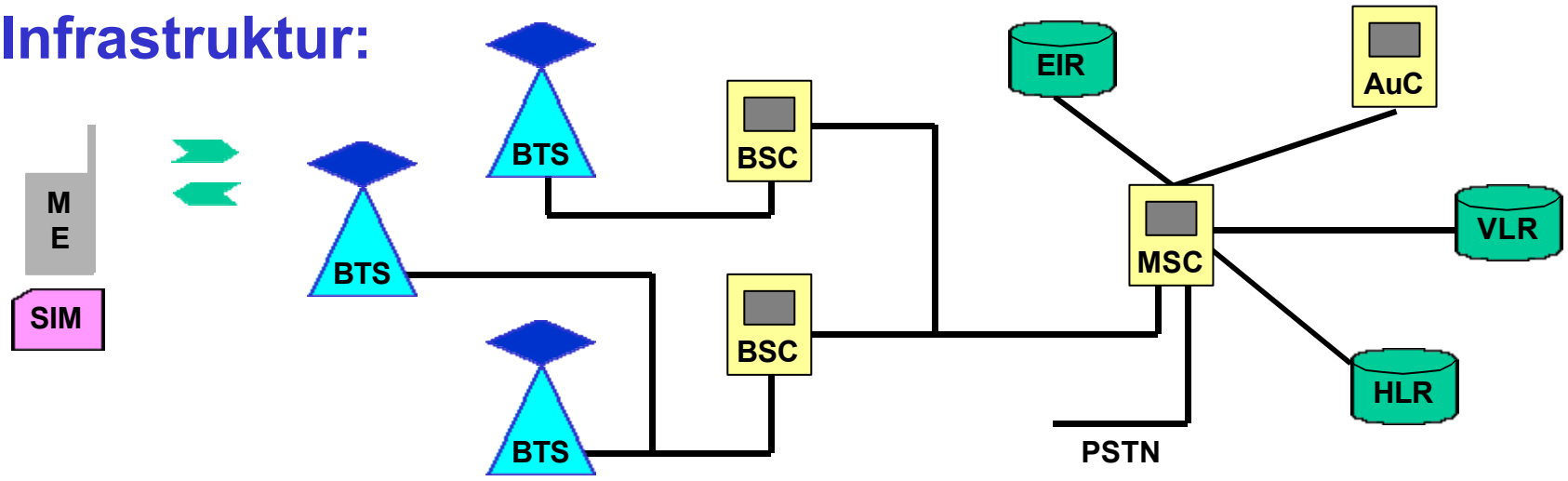
- Visitor Location Register (VLR):
  - Jedes aktive ME hat einen Eintrag
  - Jedes MSC verfügt über ein eigenes VLR
  - Administration-Verzeichnis für MSC

Roaming und Infrastruktur

Roaming:

- Unterscheidung von:
  - Roaming zwischen MSCs des gleichen Netzbetreibers
  - Roaming zwischen MSCs verschiedener Netzbetreiber über sog. Gateway MSC
- Vorgehen:
  - VLR des neuen MSCs übernimmt die Daten des VLRs des alten MSCs
  - Referenz auf VLR des HLRs wird auf aktuelles VLR gesetzt

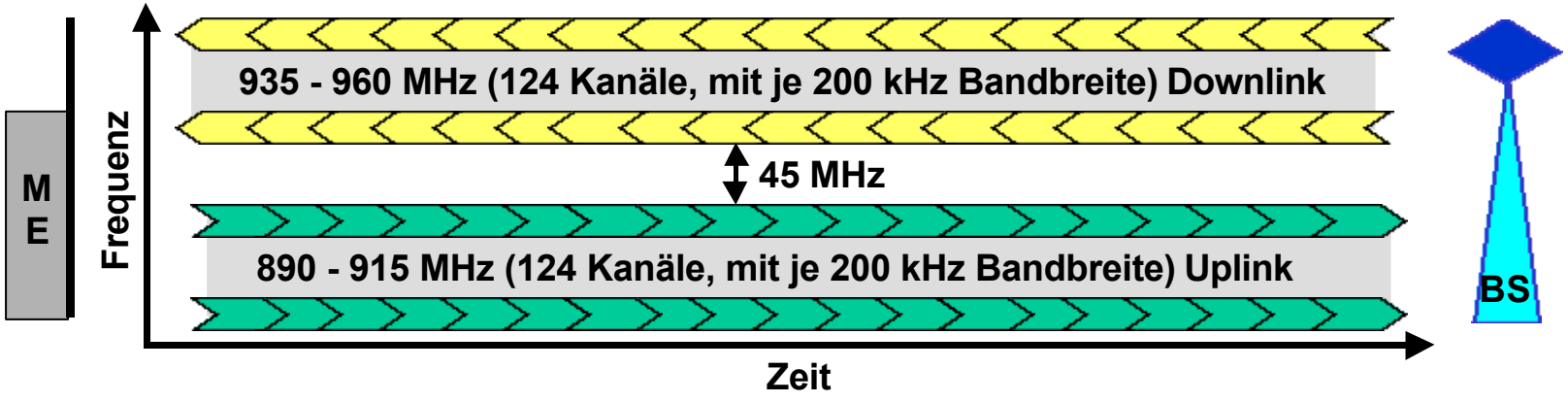
Infrastruktur:



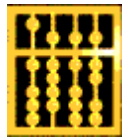
Physikalische Kommunikation und Signalling Protokoll

GSM:

- Verwendet Kombination aus FDMA und TDMA (s.u.)
- Signalling Sytem Number 7 (SS7) -Protokoll (vgl. ISDN)
  - zwischen MSCs, MSC und BSC sowie MSC und PSTN
  - Features: Fax, Rufumleitung, Anruferidentifikation, ...
- Bandbereiche:
  - GSM 900: Europa / Asien
  - GSM 1800: Europa / Asien
  - GSM 1900: Amerika
- Raw-Datenrate einer Träger-frequenz beträgt 270 kbit/s



Sprachkodierung und Kontrollkanäle



Sprachkodierung:

- Full-Rate Voice Encoding:
  - 20ms Sprach-Sample wird zu 260 bit-Sample
  - 13 kbit/s Datenrate
- Half-Rate Voice Encoding:
  - 7 kbit/s Datenrate
- Convolutional Encoding: addiert 196 bits zum 260 bit-Sample hinzu
- Gesamte Datenrate: 22,8 kbit/s (Full-Rate Voice Encoding)

Kontrollkanäle:

- Benutzung:
  - Synchronisation
  - Statusinformationen
  - Identifizierung
  - ...
- Sind in Datenkanälen integriert oder belegen dedizierte Frequenzen
- Beispiel:
  Slow Associated Control Channel (SACCH):
  periodische Übermittlung allgemeiner Kontrollinformationen, wie z. B. Signalstärke

GSM-Datenübertragung: Frames

Hyperframe	**2048 Superframes**	**2,27 Gbit, 3,5 h**

Jeder Burst in einem Hyperframe ist eindeutig gekennzeichnet

Superframe	**51 Multiframes**	**1,14 Mbit, 6,12 s**
Multiframe	**26 TDMA Frames**	**22,8 kbit, 120 ms**

Multiframe-Struktur:

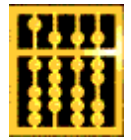
24 Data Frames, Frame 12 = SACCH, Frame 25 = unbenützt

TDMA Frame	**8 Bursts**	**1,22 kbit, 4,62 ms**

Jeder Burst eines Frames ist einem anderem Kanal zugewiesen

(Normal) Burst	**2 Datenblöcke zu je 75 Bits + Synchronisationsdaten**	**156 bit, 0,577 ms**

IS-95 CDMA, IS-136 TDMA und Japanese PDC



IS-95 CDMA:

- Ungefähr 45 Mio. Kunden weltweit, hauptsächlich in den USA
- Kompatibel zum analogen Advanced Mobile Phone Service (AMPS)
  → Dual-Mode Phones
- Sprache wird mit variabler Datenrate von 1200 bis 9600 bps kodiert

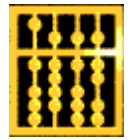
IS-136 TDMA:

- Ungefähr 40 Mio. Kunden weltweit, hauptsächlich in Amerika
- Kompatibel zum AMPS und starker Einfluß von GSM
- Verwendet Kombination aus FDMA und TDMA, genau wie GSM

Japanese PDC (Personal Digital Cellular):

- Ungefähr 50 Mio. Kunden weltweit, hauptsächlich in Japan
- Kombination von FDMA und TDMA

2,5te Generation des Mobilfunks



Was?

- Zwischenlösung

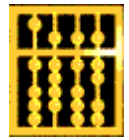
Warum?

- 3G Mobilfunk teurer
- 3G Netz noch nicht verfügbar
- Weiternutzung der GSM-Infrastruktur

Wie?

- HSCSD
- GPRS
- EDGE

HSCSD



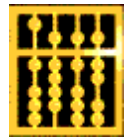
High-Speed Circuit Switched Data (HSCSD):

- Circuit-Switching
- erhöhte Datenrate: 14,4 kbps/channel
- Leitungsbündelung (x4) bis 57.6 kbps

Vorteil bei:

- audio/video streaming
- Bandbreite bleibt über gesamte Verbindung erhalten

GPRS



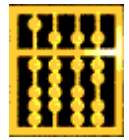
General Packet Radio Service (GPRS):

- packet switched
- always on
- erhöhte Datenrate: 14,4 kbps / channel
- Leitungsbündelung bis 115 kbps
- voice data läuft priorisiert
- Volumenabhängige Abrechnung

Vorteil:

- Schnelle Antwortzeit bei WAP
- Bessere Auslastung der Gesamtkapazität

EDGE



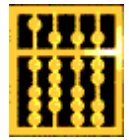
Enhanced Data Rates for GSM Evolution (EDGE):

- Anderes Modulationsverfahren
- 48 kbps / channel
- Beibehaltung von frame- und channel-Struktur
- nur kleine Änderungen der Infrastruktur

Dadurch profitieren:

- HSCSD bis 192 kbps
- GPRS bis 384 kbps

Highlights der 3. Generation



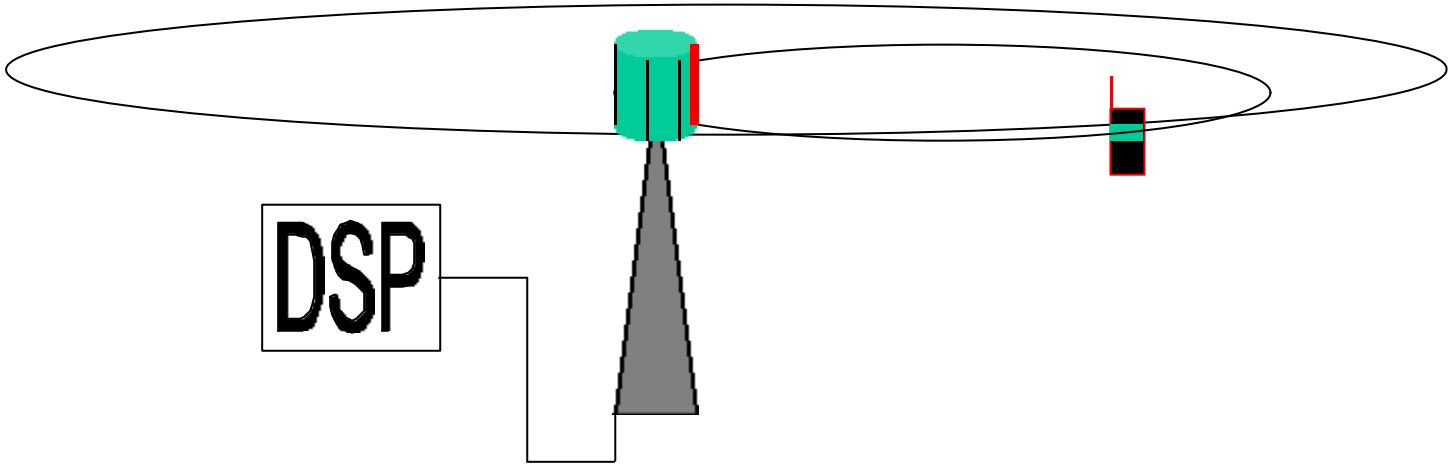
Software radio technology:

- Software regelt Sendevorgang
- Teile der Hardware (Modulation, Codierung) in Software

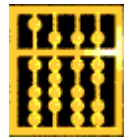
Smart Antennas

Smart Antenna

- **Multi-Element-Antennen**
- **gekoppelt mit DSP**

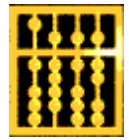


Kurzstrecken Verbindung



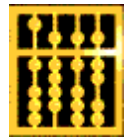
- DECT (hauptsächlich Telefon)
- IrDA
- **Bluetooth**

Bluetooth



- Seit 1994 (Ericcson)
- Telephon-Peripherie
- 1 Mbps basic data rate
- low-power
- low-cost
- real-time fähig
- single-chip Lösungen
- blå tan

Bluetooth Funktechnik

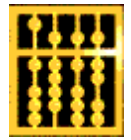


- 2.4 GHz Frequenzband
- 78 Carrier-Frequenzen
- 625 µs Slotlänge mit 625 bit
- frequency hopping (1600 hops/s)
- time domain duplex (TDD)

Finden anderer Geräte:

- general inquire access code (GIAC)
  alle Geräte antworten
- dedicated inquire access code (DIAC)
  nur bestimmte Geräte-Klassen antworten

Bluetooth

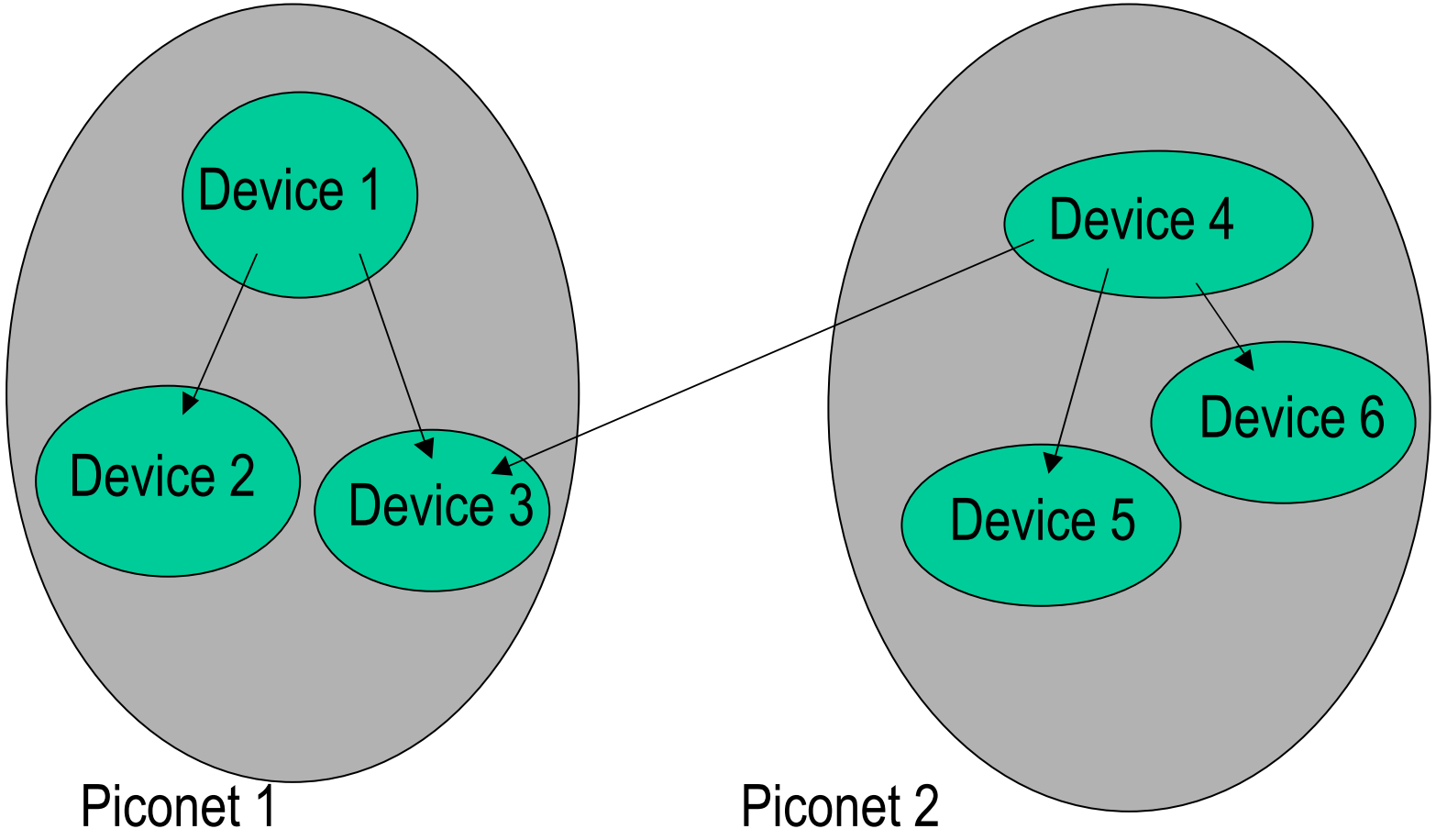


- **Synchronous Connection-Orientated (SCO)**
  real-time, voice 64 kbps - 433.9 kbps

- **Asynchromous Connection-Less (ACL)**
  723.2 kbps / 57.6 kbps

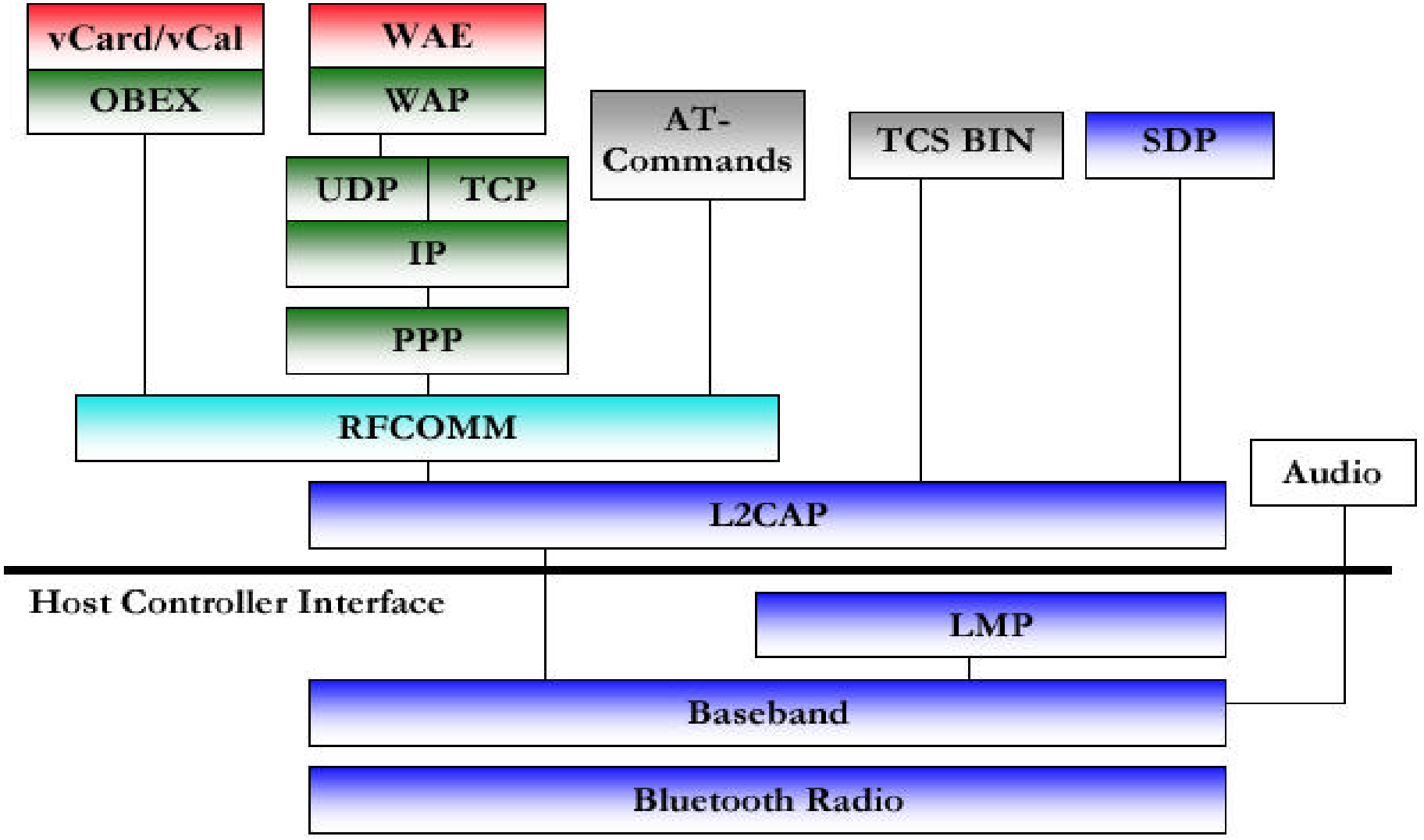
Piconet Konzept

- Scatternet

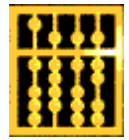


3 bit adressen => 8 Geräte

Bluetooth



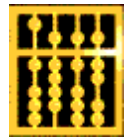
Bluetooth SDP



Service Discovery Protocol

- SDP-Server in jedem device
- Service record (service class ID, provider name, service name, icon URL, service ID)

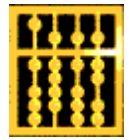
Service Discovery



Systeme

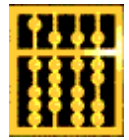
- Universal Plug and Play
- Jini
- Salutation

Universal Plug and Play



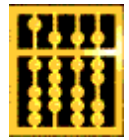
- TCP/IP
- DHCP
- XML
- HTTP
- Simple Service Discovery Protocol
  - Jedes Gerät sucht nach ansprechbaren Diensten anderer Geräte
- Kein Service-Aufruf

Jini



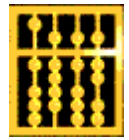
- Java RMI/Java Beans
- Proxies möglich
- Informationen als Java-Objekte
- Aufruf-Klasse wird bereitgestellt
- Zugriff über Java-Interfaces
- Transaktionen

Salutation



- Salutation Transport Manager (local oder remote)
- Transportprotokollunabhängig
- Flexibler

Quellen



[1] ftp://ftp.isis.edu/in-notes/rfc2068.txt (HTTP 1.1)

[2] http://www.wapforum.org

[3] http://www.w3c.org

[4] http://www.protocols.com

[5] http://www.comms.eee.strath.ac.uk/~gozalvez/gsm/gsm.html

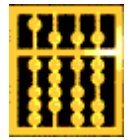
[6] http://www.gsmworld.com

[7] http://umi.eee.rgu.ac.uk/modules/eee/mobile/procent/20comms/menu.html

[8] White Paper: Bluetooth Protokoll Architectur 1.0

[9] http://www.bluetooth.com

Ende



Danke !