– Eine Einführung

Bielefeld, 15. Januar 2004

Jörn Stuphorn

Themenübersicht

- Was ist Bluetooth?
- Spezifikation / Organisation
  - Die Bluetooth Special Interest Group
  - Der Bluetooth Protocol Stack
- Anwendungen / Einsatz
  - Die Bluetooth Profile
  - Bluetooth und Sicherheit
  - Bluetooth Anwendungen

Was ist Bluetooth?

Historisches

Was ist Bluetooth?

- drahtlosen Verbindung von Geräten
- gesicherte Verbindung zwischen den Geräten
- kein proprietäres Protokoll
  Verbindung von Geräten unterschiedlicher Hersteller
- „Kabelersatz“
- Funkgestützte Kommunikation
  auch ohne Sichtkontakt ist Verbindung möglich
- Verbindung von Endgeräten
  Drucker, PC, PDA, Maus, Handy, ...
- Vernetzung von Geräte
  spontaner Aufbau von Netzwerk unterschiedlicher Geräte möglich
- preisgünstige Lösung („Ein-Chip Lösung“)

Was ist Bluetooth?

„ … eine offene Spezifikation für drahtlose Übertragung von Daten und Sprache“

Fujitsu Siemens Computers

- offene Spezifikation
- drahtlose Übertragung
- digitale Übertragung von Daten und Sprache

Namensgeber: **Harald Blåtand** (dänisch für Blauzahn)
geboren um 910, gestorben am 1.11.986

Blåtand vereinigte 983 Dänemark und Norwegen

Was ist Bluetooth?

Geschichte der Bluetooth-Entwicklung

1994	Ericsson Mobile Communications untersucht Alternativen zur kabelgebundenen Verbindung von Geräten
Feb. 1998	Bluetooth SIG (Special Interest Group) gegründet
20.5.1998	Bluetooth offiziell angekündigt
26.6.1999	Bluetooth 1.0a Spezifikation
1.12.1999	Bluetooth 1.0b Spezifikation
1.12.2000	Bluetooth 1.1 Spezifikation
5.11.2003	Bluetooth 1.2 Spezifikation

Die Bluetooth Special Interest Group

Spezifikation & Organisation

Bluetooth Special Interest Group

Aufgaben der SIG

- Entwicklung eines einheitlichen Systems zur Funkverbindung
- Bildung eines breiten Produktspektrums
- Spezifizierung des Protocol Stacks
- Spezifizierung der Anwendungsprofile
- Zertifizierung von Geräten Vergabe des Bluetooth Logos
- Entwicklung von Prüfverfahren
- Veranstaltung von Entwicklertreffen (UnPlugFests)
- Marketing
- Rechtliche Fragen
- Berücksichtigung nationaler und systemspezifischer Verordnungen

Bluetooth Special Interest Group

Mitglieder der SIG

Februar 1998:	5 Gründungsmitglieder *(Ericsson, Intel, IBM, Toshiba, Nokia)*
Dezember 1999:	4 weitere Mitglieder im SIG-Kern *(Microsoft, Lucent, 3com, Motorola)*
2000:	1790 Mitglieder
2002:	über 2000 Mitglieder
2004:	ca. 3750 Mitglieder

3 Mitgliedschaftsklassen:

1. *Promoter Members* (8 Kernmitglieder)
2. *Associate Members*
   (Möglichkeit Entwicklung zu beeinflussen)
3. *Adopter Members* (kostenlos, Entwicklung von Produkten)

Bluetooth Special Interest Group

Struktur der SIG

Der Bluetooth Stack

Spezifikation & Organisation

Der Bluetooth Stack

Versuch BT-Protokollstack in OSI Modell zu ordnen

7 Application	Anwendungen			
6 Presentation				
5 Session Layer				
4 Transport Layer	SDP	BNEP	RFCOMM	CMTP
3 Network Layer	L2CAP			
	HCI			
2 Data Link Layer	Link Manager Protocol			
	Baseband / Link Controller			
1 Physical Layer	RF / Funk			

Problem beim Vergleich OSI-Stack / Bluetooth-Stack:

OSI entwickelt als streng geordneter Stack
Bluetooth entwickelt um Anwendungsbereich zu erfüllen

Der Bluetooth Stack

Die Core System Architektur

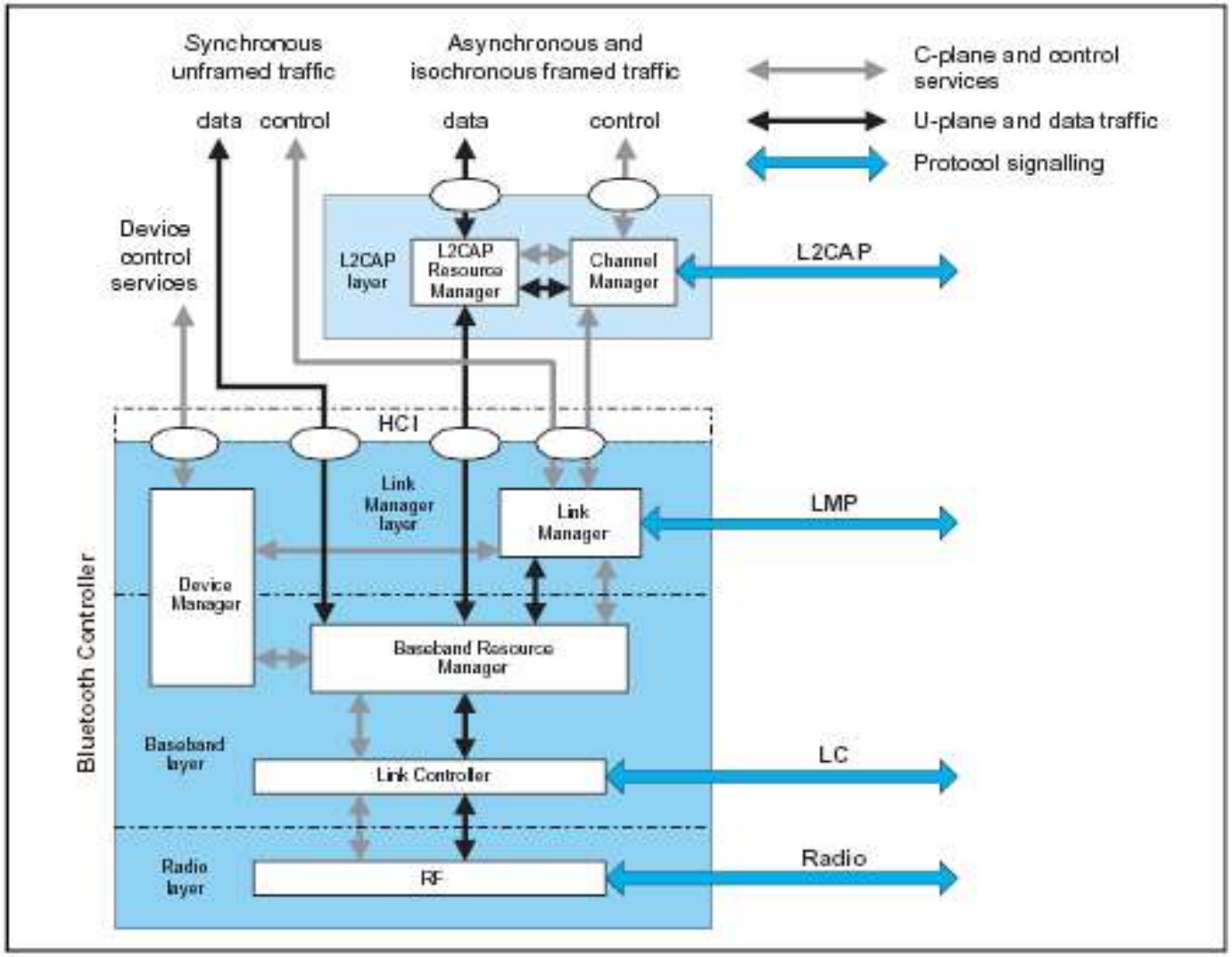
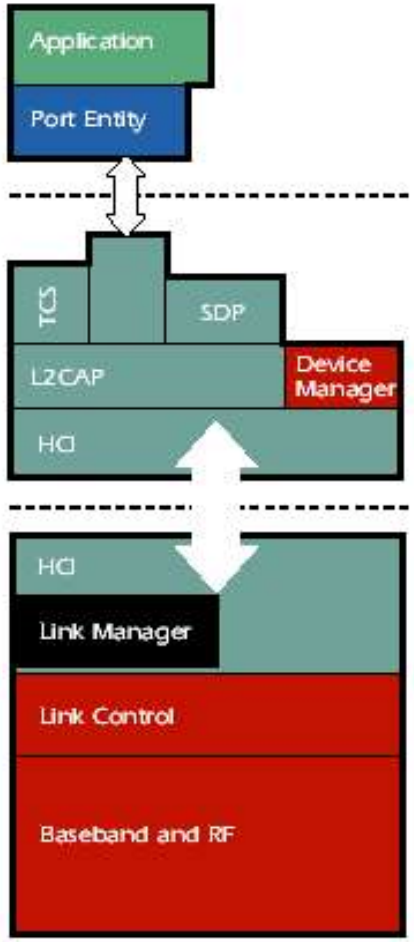


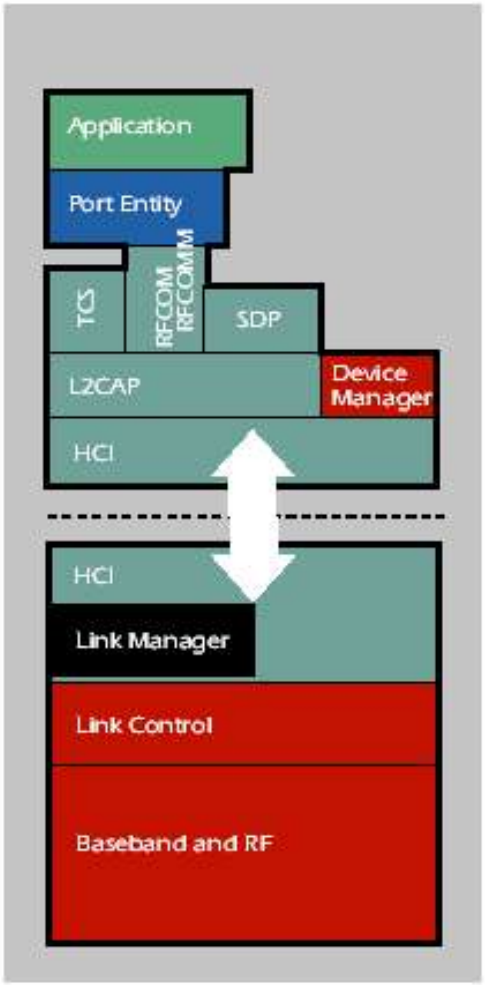
Figure 2.1: Bluetooth core system architecture

Der Bluetooth Stack

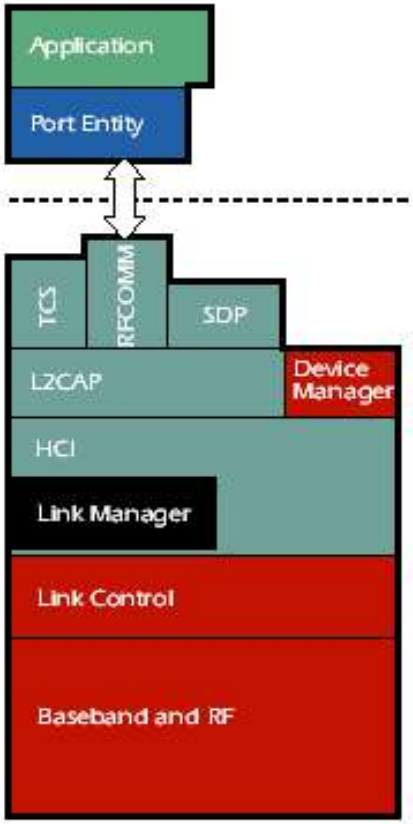
Unterschiedliche Aufteilungsmöglichkeiten



3 Processor Configuration



Standard 2 Processor



Embedded 2 Processor

RF / Funk

Bluetooth funkt im 2.4 GHz Band (ISM-Band)

ISM: **I**ndustrial **S**cientific **M**edical

Bandbreite von 83.5MHz

aufgeteilt in 79 RF Kanäle (à 1MHz Bandbreite)

Übertragungsrate: ca. 1Mbit/s (Bluetooth 1.1)

Reichweiten: 10cm (Class III, 1mW Sendeleistung)
10m (Class II, 2.5mW Sendeleistung)
100m (Class I, 100mW Sendeleistung)

für Duplex Kommunikation wird
Time Division Duplex (TDD) benutzt

RF / Funk

ISM: Industrial Scientific Medical

+ global verfügbar
+ lizensfrei

- oft verwendet
  z.B. in Mikrowellengeräten, DECT/2.4GHz,
  HomeRF, IEEE802.11b/g, ...
- Bandbreite in Japan, Spanien und Frankreich eingeschränkt

Time Division Duplex

- Kommunikation über Funk
- jedes Gerät kann
  entweder senden oder empfangen
- Aufteilung des Sendekanals nach der Zeit
- jedes Gerät darf in einem Zeitfenster senden

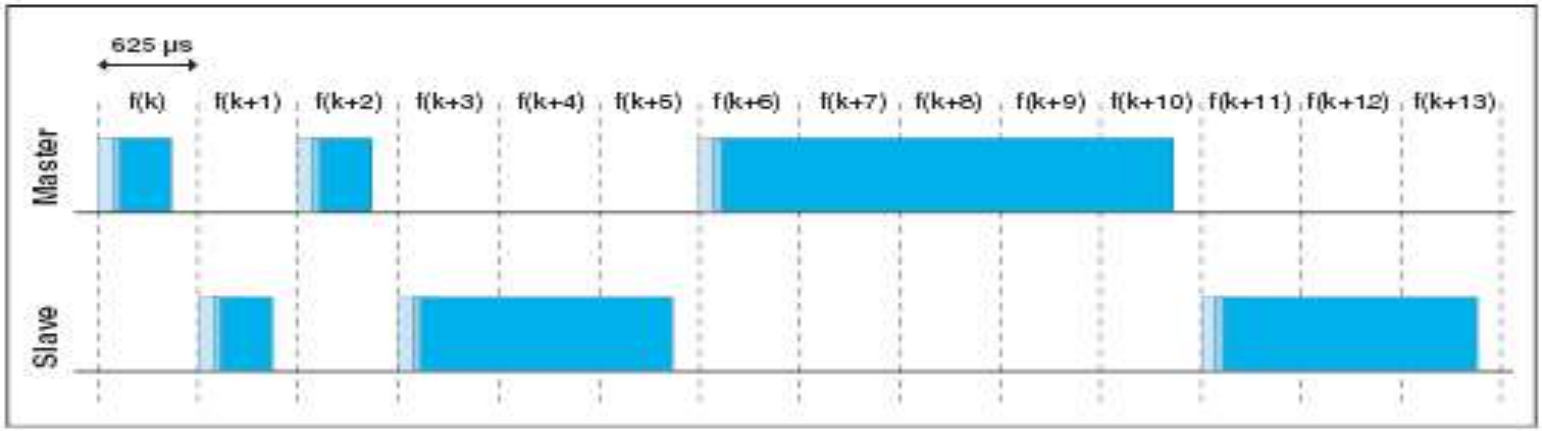


Figure 2.1: Multi-slot packets

wegen hoher Übertragungsrate:

Full-Duplex für Sprache

Baseband / Link Controller

Wichtige Punkte um Bluetooth Ziele zu erreichen:

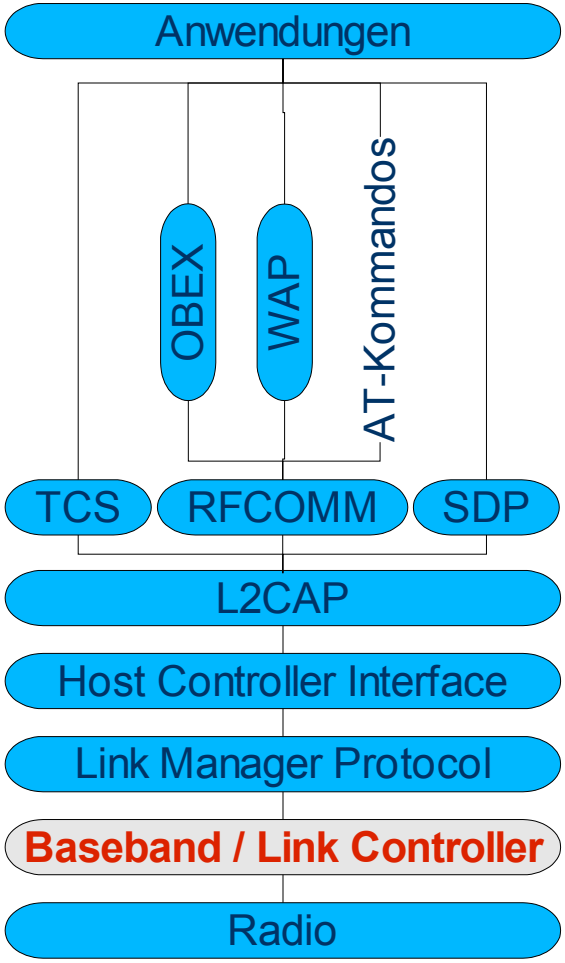
- Robuste Übertragung (*Baseband*)
  Frequency Hopping Spread Spectrum
- geringer Stromverbrauch (*Link Manager*)
  verschiedene Betriebsmodi
- Niedrige Komplexität (*SIG*)
  Stack-Struktur
- geringe Kosten (*Hersteller*)

Baseband / Link Controller

Baseband

steuert:

- Funkkanäle
- Frequenzwechsel
- Funkverbindungen
- Data whitening
- Fehlerkorrektur
- Multiplexing



Baseband / Link Controller

Verbindungsarten

Bluetooth unterstützt

- verbindungsorientierte Dienste und
- verbindungslose Datendienste

Zwei Verbindungsarten im Baseband:

- SCO *(Synchronous Connection Oriented)*
- ACL *(Asynchronous Connection Less)*

SCO Verbindung unterstützt Echtzeit Sprachübertragung

Bandbreite kann über Timeslots reserviert werden

ACL unterstützt „best-effort“ Verbindungen

Baseband / Link Controller

Verbindungsarten

Bluetooth erlaubt

- gleichzeitige Existenz von SCO und ACL Verbindungen
- maximal 3 SCO Sprachkanäle
- einen ACL Datenkanal

SCO *(Synchronous Connection Oriented)*

- jeder Sprachkanal fasst 64kBit/s

ACL *(Asynchronous Connection Less)*

- *asymmetrisch: 723.2kBit/s in Richtung 1 und 57.6kBit/s in Richtung 2*
- *symmetrisch: 433.9kBit/s in beiden Richtungen*

Baseband / Link Controller

Frequency Hopping Spread Spectrum (FHSS)

- Gerechte Methode Frequenzen in einem nicht regulierten Band zu verteilen
- Nachteil: Bandbreite auf Teil des Gesamtbandes (1MHz) beschränkt
- FHSS ist sehr robust gegen Störungen
- Pseudozufallszahlensequenz
  über Startparameter initialisiert
- alle Stationen, die Startparameter kennen, können Wechselsequenz nachvollziehen
- Jede Frequenz wird mindestens für 625µs gehalten
- Tritt Kollision auf (ist Frequenz bereits belegt)
  verfällt Block und es wird im nächsten Block mit der nächsten Frequenz erneut versucht

Baseband / Link Controller

Data Whitening

Methode zur Unterscheidung von 0/1 bei Übertragung erforderlich.

Bsp.: 0 kein Signal
1 Signal

Ist Funkstille Sequenz von 0?

Aufgaben des Data Whitening:

- Verringerung von redundante Informationen in Paket
- Minimierung des Stromflusses
  bei Wechselstrom fließt nur wenig Strom

Methode des Data Whitening: Mischen der Bits eines Pakets um kurze Sequenzen von 0 und 1 zu erhalten

Baseband / Link Controller

Fehlerkorrektur

Bei Funkübertragungen muss mit Störungen gerechnet werden

2 Arten:

- Einzelne Bits fehlerhaft übertragen
- Übertragung durch Burst gestört

Lösung für kabelgebundene Netze: Erneutes Senden

Bei kabellosen Netzen gewünscht: Fehlerkorrektur

Forward Error Correction (FEC)

- 1/3 FEC Jedes Bit wird 3mal übertragen, Mehrheit hat Recht
- 2/3 FEC 10bit Information, 5bit Fehlerkorrekturcode
- *ARQ* *fehlerhafte Pakete werden neu übertragen*

Baseband / Link Controller

Piconet / Scatternet

- mehrere Geräte teilen sich eine Frequenz
- 1 *Master*-Device
- mehrere *Slave*-Devices
- Frequenzwechsel vom *Master* gesteuert

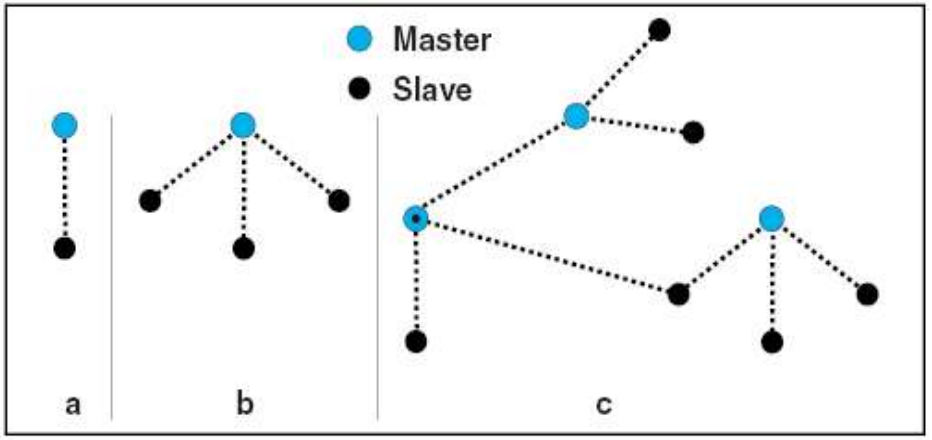
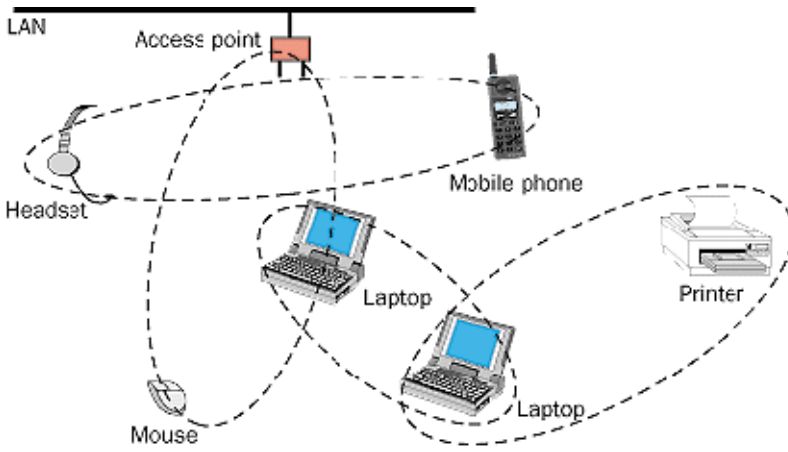


Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

- Piconet bricht zusammen, wenn Master weg fällt
- Scatternet: Gruppe von Piconets
- Ein Gerät kann *Mitglied* von mehreren Piconetzen sein
- aber nur in einem *Master*



Baseband / Link Controller

Scatternet Routing?

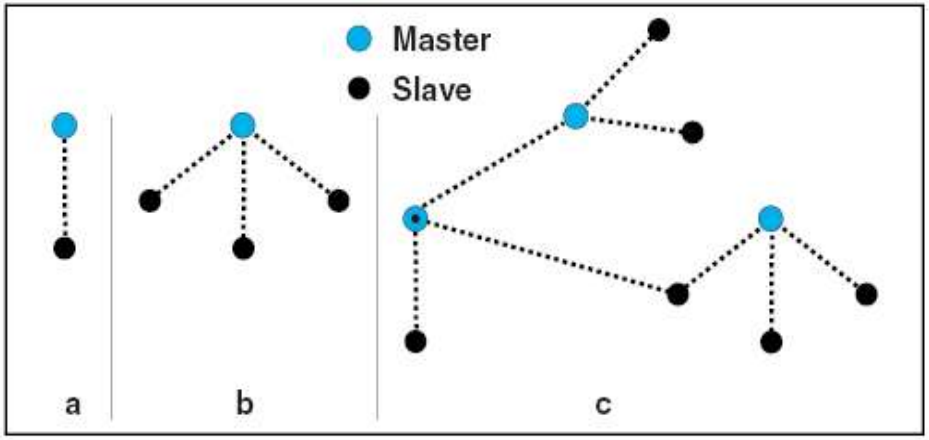


Figure 1.1: Piconets with a single slave operation (a), a multi-slave operation (b) and a scatternet operation (c).

Datenübertragung in einem Netzwerk:

- Routing zwischen den Knoten
- Routingalgorithmus

Bluetooth SIG:

- Routing ist Aufgabe der höheren Protokollschichten
- Bluetooth Spezifikation wird kein Routing enthalten

LMP

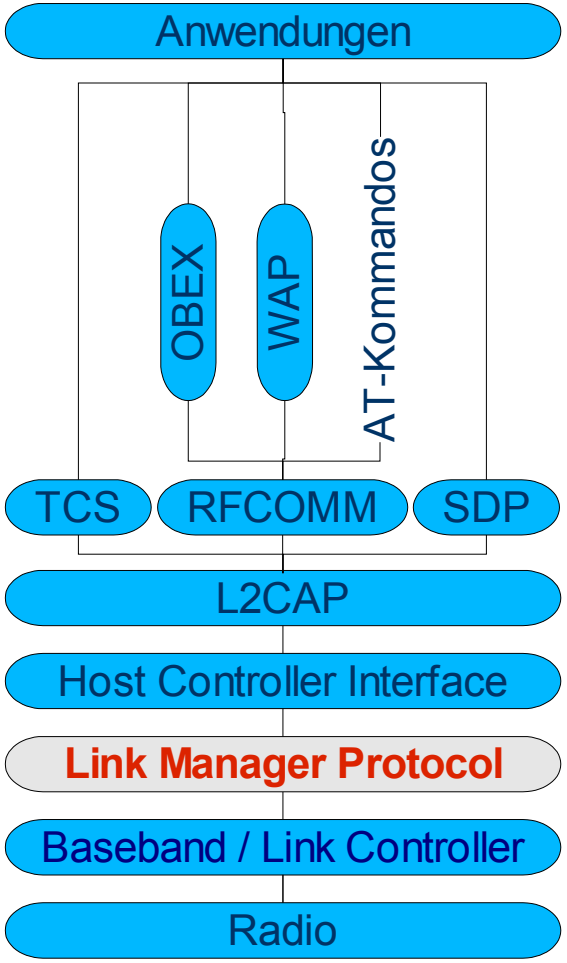
Link Manager Protocol

Aufgaben:

- Verbindungssetup
- Sicherheit
- Verbindungskontrolle

Verbindungssetup:

- Verbindungsaufbau
- Name-Request
  (lesbare Bezeichnung)
- HOLD-Mode
- PARK-Mode
- SNIFF-Mode
- Verbindungsabbau



LMP

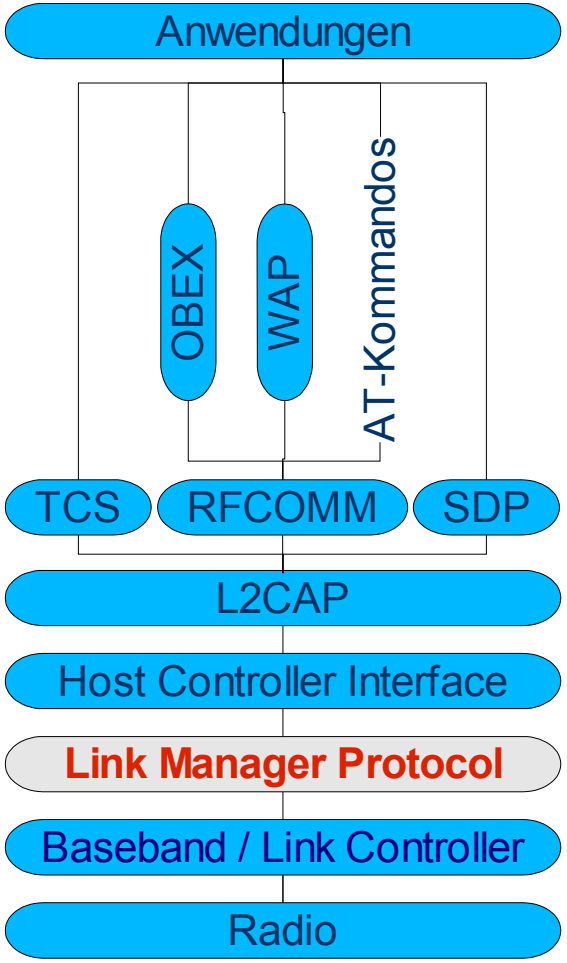
Link Manager Protocol

Sicherheit

- Authentifizierung
- Verschlüsselung

Verbindungskontrolle

- Clock Offset
  für FHSS Wechselsequenz
- Wechsel der Master/Slave Rollen
- Kontrolle der Sendeleistung
- Quality of Service Kontrolle



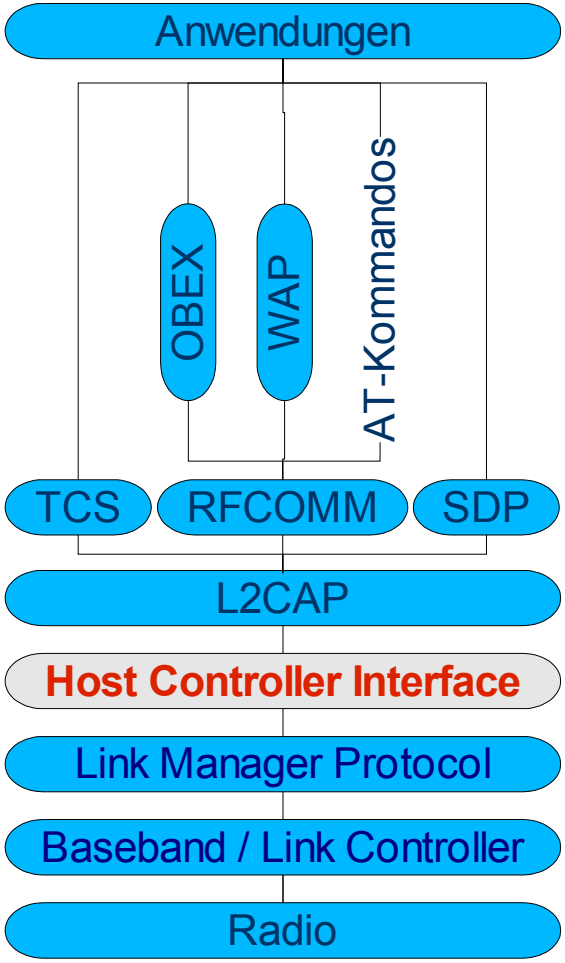
HCI

Host Controller Interface

Command Interface für
- Link Manager und
- Baseband Controller

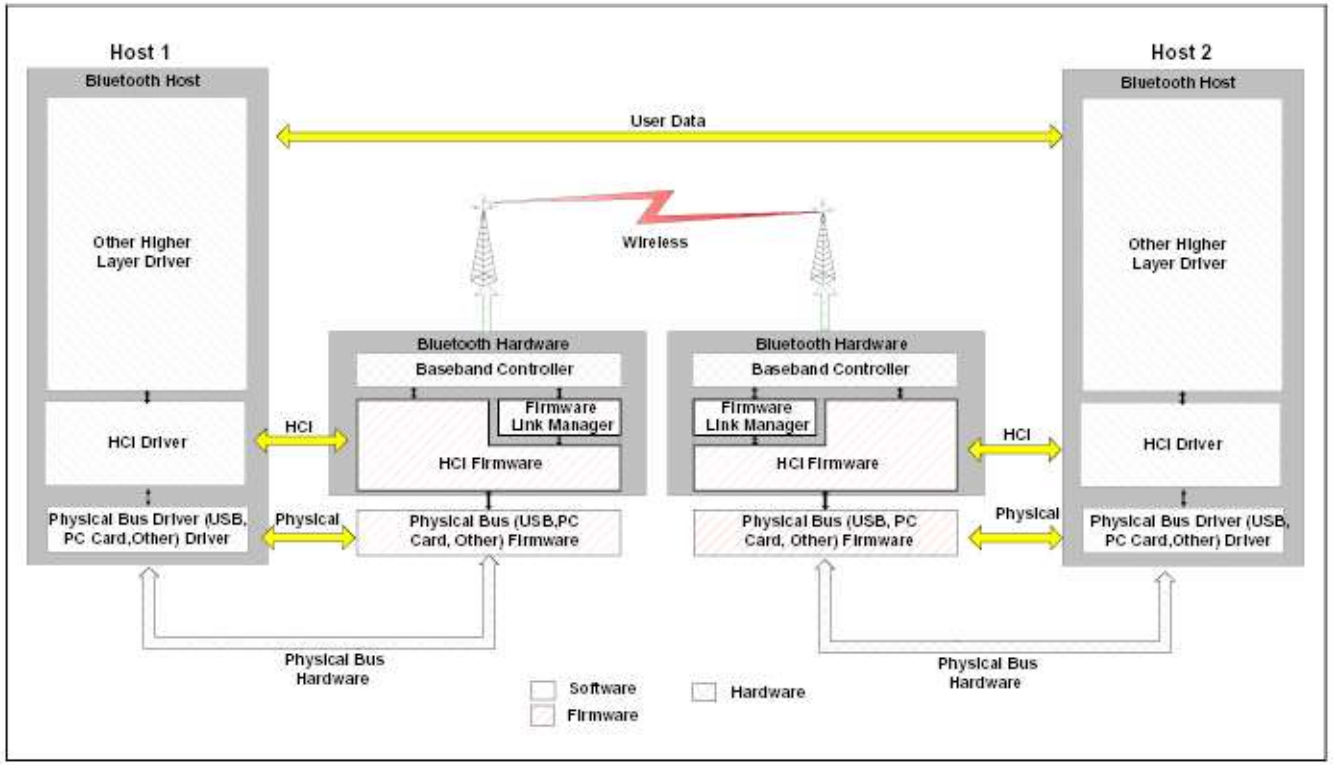
liefert
- einheitliche Zugriffsmethode
- auf Basebandfunktionen

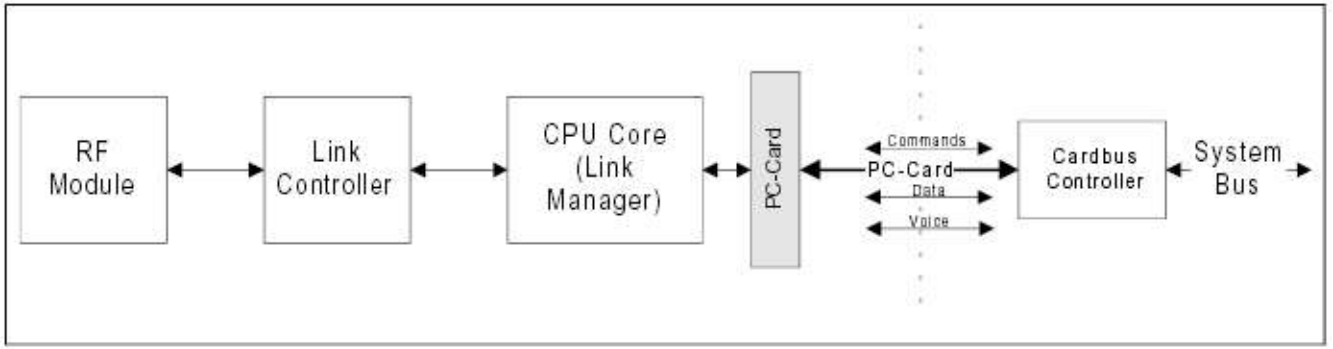
implementiert durch
- PC-Card, CF-Card,
- USB-Dongle, Chip, ...



HCI

Host Controller Interface





L2CAP

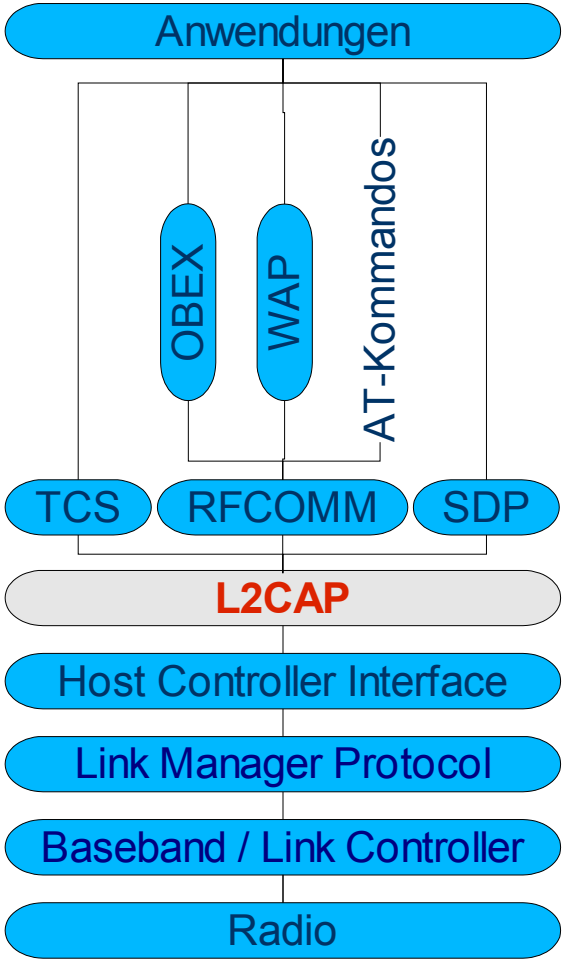
Logical Link Control and Adaptation Protocol

Aufgaben:

- Multiplexing der höheren Protokolle
  Unterscheidung z.B. von
  RFCOMM, SDP, BNEP ...

- Segmentierung und Zusammenfügen
  (segmentation and reassembly SAR)
  Baseband Paket fasst 341 Byte
  IPv4 Paket enthält maximal 64 KByte

- Group Management
  Unicast (ein Sender / ein Empf.)
  Multicast (ein Sender / viele Empf.)
  ACL Kanal erlaubt Multicast
  SCO Kanal muss Unicast sein



RFCOMM

Der serielle Anschluss von Bluetooth

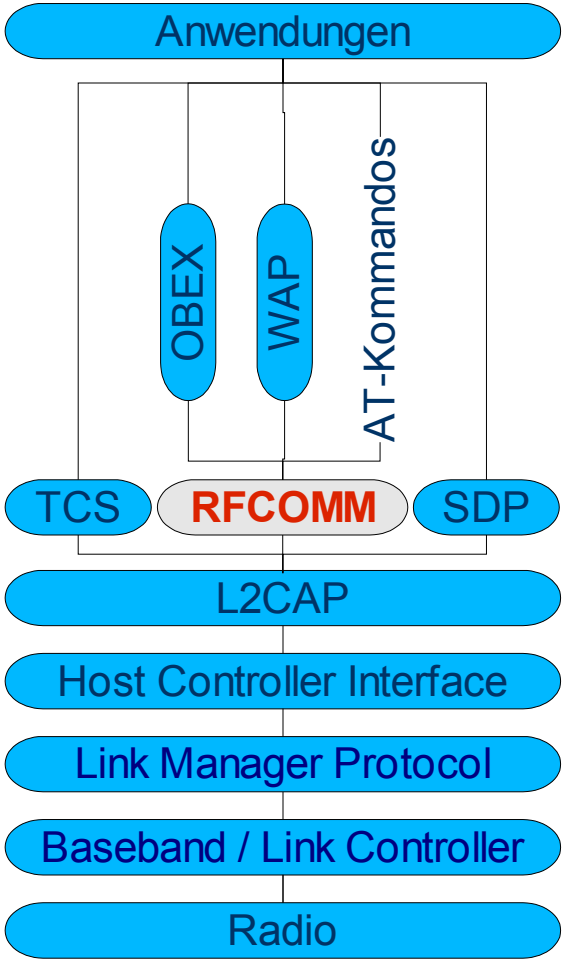
RFCOMM emuliert
serielle Schnittstellen
(RS232 Schnittstellen) über L2CAP

einfaches Transportprotokoll

unterstützt bis zu 60 simultanen
Verbindungen zwischen 2 Bluetooth
-Geräten

unterstützt 2 Gerätearten:

- Typ 1: Endpunkte
  (Drucker, Computer)
- Typ 2: Teile der Verbindung
  (z.B. Modems)



allerdings keine direkte Unterscheidung der Typen

SDP

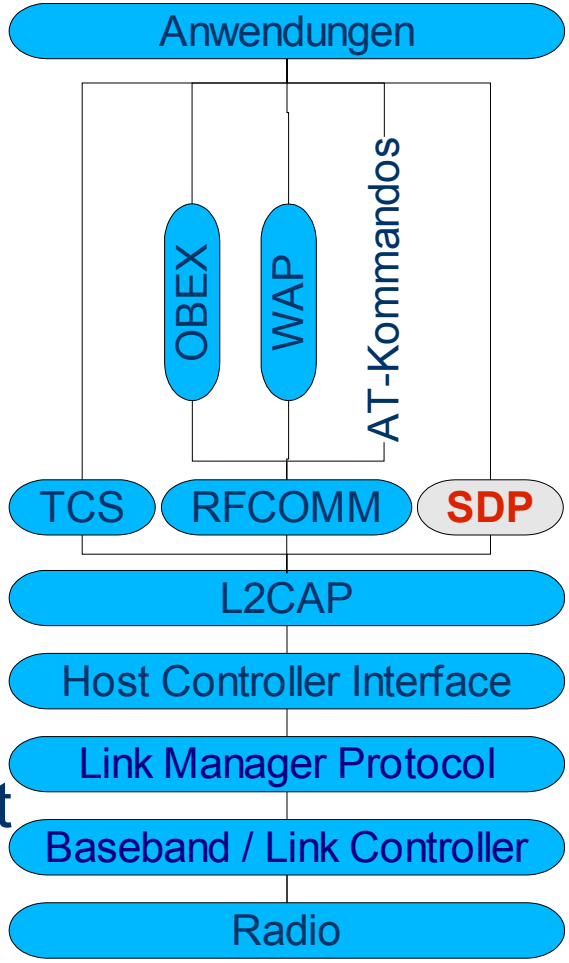
Service Discovery Protocol

Anfragen:

- Welche Dienste stehen zur Verfügung?
- Welche Charakteristiken haben die gefundenen Dienste?

Anfragen nötig, weil:

- Bluetooth arbeitet in dynamischer Umgebung
- angebotene Dienste können geändert werden
- Dienstanbieter kann außer Reich-weite geraten



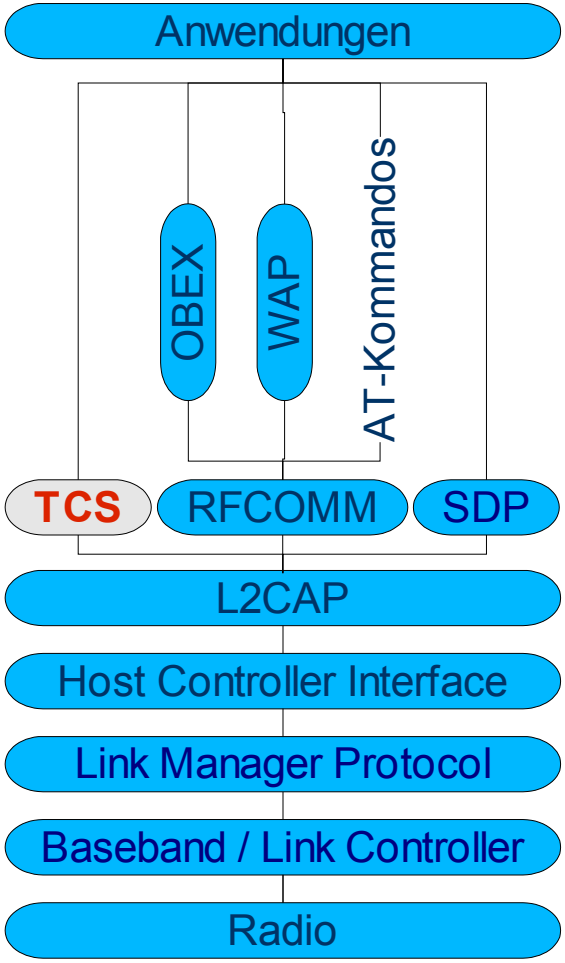
TCS

Telephony Control Protocol Spezification

Signalisierung zwischen mehreren Bluetooth Telefonen

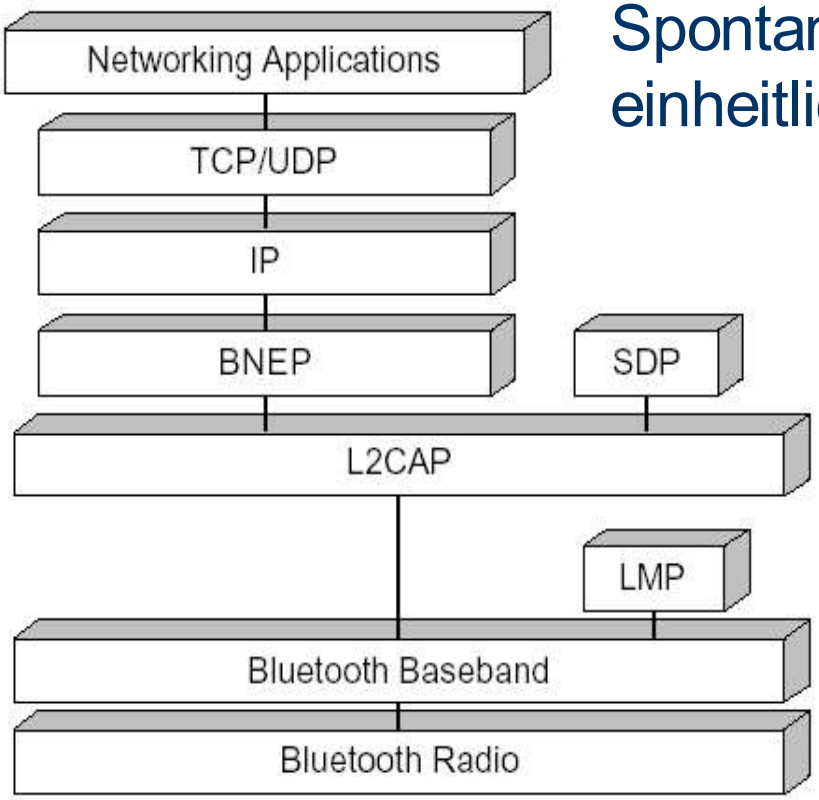
Funktionen:

- Call Control (CC)
  Signalisierung zur Einrichtung und Trennung von Sprach- und Daten-verbindungen
- Group Management
  Signalisierung um Gruppenverwaltung zu vereinfachen
- ConnectionLess TCS (CL)
  Übertragung von Signalisierungs-informationen unabhängig von Verbindung



BNEP

Bluetooth Network Encapsulation Protocol



Spontan gebildete Netze benötigen einheitliches Übertragungsprotokoll

Lösung: Kapselung

2 wichtige Eigenschaften für Kapselung:

- Unterstützung verbreiteter Protokolle
- Geringer Overhead

BNEP kapselt Pakete diverser Netzprotokolle (IPv4, IPv6, IPX)
BNEP leitet die Pakete direkt an L2CAP

Bluetooth mit BNEP ist daher mit Ethernet vergleichbar

Die Bluetooth Profile

Anwendungen & Einsatz

Was sind Bluetooth Profile?

In Profilen sind Anwendungsfälle für Bluetooth gesammelt.

Bsp.: SIM Access Profile, Human Interface Device Profile
Fax Profile, Common ISDN Access Profile

- Vorschläge, zur Implementation von Anwendungsfällen
- standardisierte Anwendungssysteme

Wofür Profile?

- systematischer Aufbau von Abhängigkeiten und Anforderungen
- Kombination unterschiedlicher Geräte problemloser
- nicht für jeden Anwendungsbereich werden alle Bluetooth-Protokolle benötigt

Welche Profile gibt es?

A2DP	Advanced Audio Distribution Profile
AVRCP	A / V Remote Control Profile
GAVDP	Generic A / V Distribution Profile
VCP	Video Conferencing Profile
VDP	Video Distribution Profile
HFP	Hands Free Profile
HP	Headset Profile
SIM	SIM Access Profile
HID	Human Interface Device Profile
CIP	Common ISDN Access Profile
CTP	Cordless Telephony Profile
ICP	Intercom Telephony Profile
LPP	Local Positioning Profile
ESDP	Extended Service Discovery Profile
FTP	File Transfer Profile Specification
PAN	Personal Area Network Profile
WAP	WAP Over Bluetooth
BPP	Basic Printing Profile
HCRP	Hard Copy Replacement Profile
BIP	Basic Imaging Profile
UDI	UDI Profile
SYNCH	Synchronization Profile
GOEP	Generic Object Exchange Profile
SDAP	Service Discovery Application Profile
DUN	Dial Up Networking Profile
OPP	Object Push Profile
FAX	Fax Profile
SPP	Serial Port Profile

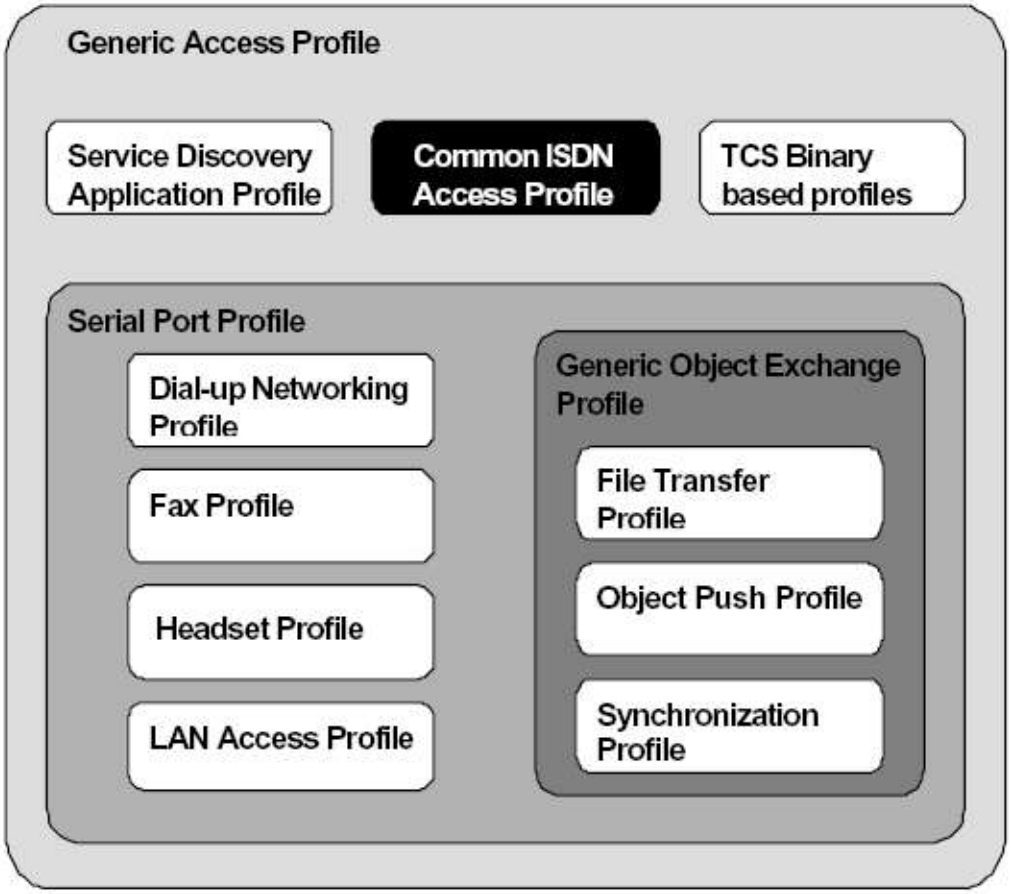
Grundstruktur der Bluetooth Profile

CIP muss folgende Anforderungen erfüllen:

- Generic Access Profile

FTP muss folgende Anforderungen erfüllen:

- Generic Access Profile
- Serial Port Profile
- Generic Object Exchange Profile

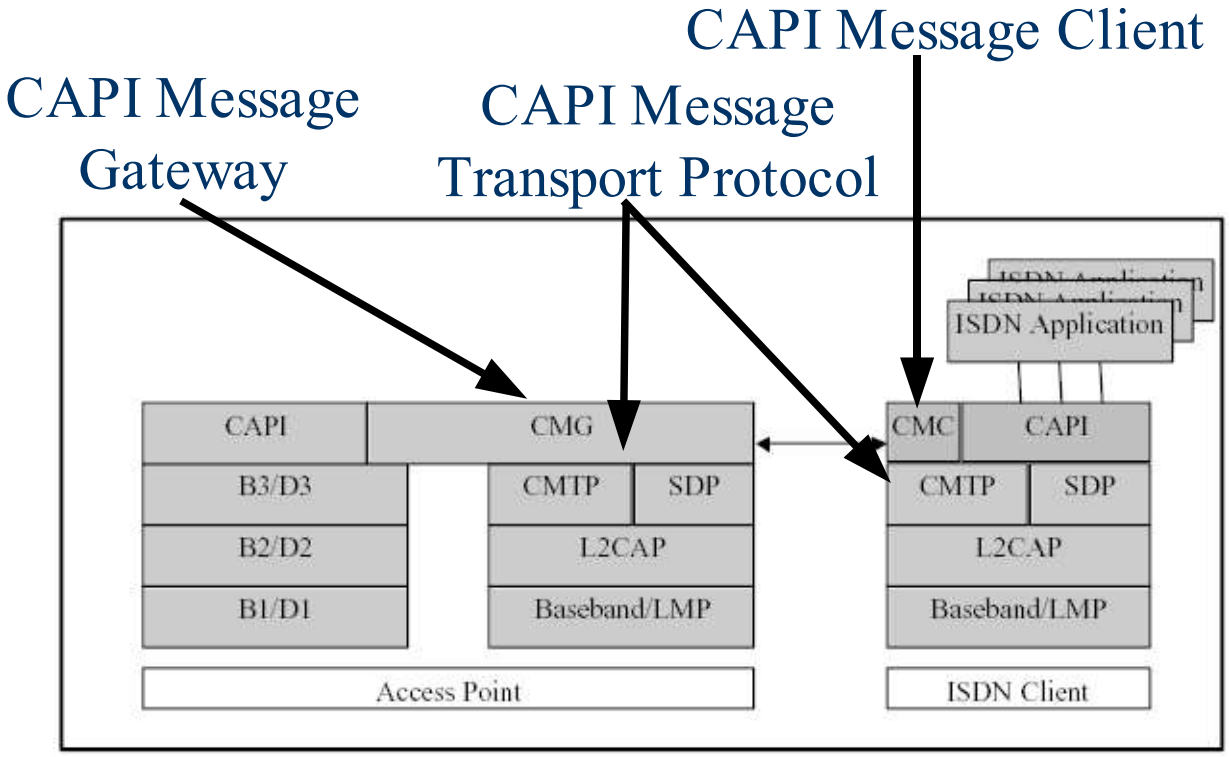


Beispiel: ISDN über Bluetooth

Ziele dieses Profils:

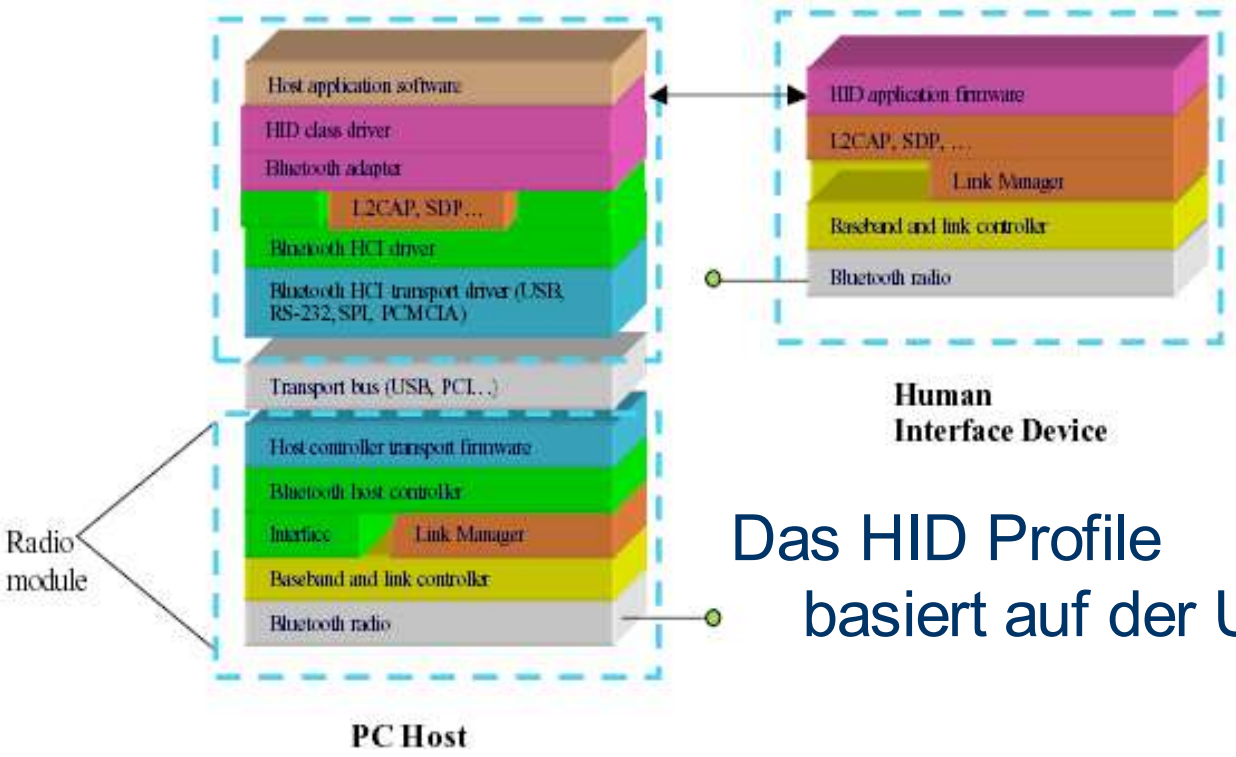
- Bereitstellung einer CAPI Schnittstelle über Bluetooth
- Unterstützung von ISDN Leistungsmerkmalen
- Unterstützung bestehender ISDN Anwendungen

CAPI:
Common
Application
Protocol
Interface



Beispiel: Human Interface Device Profile

Eingabe / Steuerung über Bluetooth



Das HID Profile
basiert auf der USB HID Klasse

Ziel: Verwendung existierender USB Treiber
Implementation des USB-HID Protokolls über Bluetooth

HID muss nicht mit Menschen interagieren!

Das HID muss die Anforderungen des GAP erfüllen

Bluetooth und Sicherheit

Anwendungen & Einsatz

Bluetooth Sicherheit

Einschätzung der Gefährdung:

+ Geringe Reichweite
  durch „Output-Power-Selection“ zusätzlich minimiert
+ Schneller Frequenzwechsel
  nur erschwerend, da jedem Gerät in einem Piconet die Sprungfolge mitgeteilt wird.
+ Authentifizierung
+ Verschlüsselung der übertragenen Daten (Payload)

- Sensible Daten
  - Passwörter
  - Kontakte
  - Zugriff auf SIM Karte des Handies

Bluetooth Sicherheit

Authentifizierung:

- Grundlage für Verschlüsselung
- Sender schickt 128bit Challenge,
- die Empfänger mit 48bit Adresse und Link-Key bearbeitet.
- Die 32 wichtigsten Bit werden zurückgesendet.
- Der Sender kontrolliert Ergebnis.

Verschlüsselung:

- Schlüsselerzeugung mit 128bit SAFER+ Verfahren
- Verschlüsselung mit 8-128bit symmetrischen Schlüssel
- einige Bits des Schlüssels können öffentlich sein
  (zur Erfüllung staatlicher Beschränkungen)

Bluetooth Sicherheit

Kommentare:

- Die Verschlüsselung wurde (noch?) nicht gebrochen
- Die Verschlüsselungsimplementation auf einigen Mobiltelefonen ist aber fehlerhaft
- wegen geringer Reichweite gute Vertraulichkeit
- FHSS erschwert das Abhören der Kommunikation (wenn Angreifer unbemerkt bleiben will)
- Bluetooth authentifiziert nur Geräte, nicht Benutzer
- zusätzliche Sicherheit für sensible Programme wünschenswert
- Sicherheit ist standardmäßig deaktiviert.

Bluetooth Anwendungen

Anwendungen & Einsatz

Bluetooth Produkte

- Mobiltelefone
- PDAs
- Drucker
- Digitalkameras
- Headsets / Freisprecheinrichtungen
- Modems / ISDN-Anlagen
- Notebooks / Computer
- Festplatten (externer Speicher)
- Router / Accesspoints
- Autoradios
- GPS Antennen
- Video- / Fotokameras

Bluetooth Anwendungsbereiche

Telekomunikation

- Wireless Headsets, Freisprecheinrichtungen
- Netzverbindungen

Peripherie Verbindungen

- Drucker
- Maus
- Tastatur

Verbindungen zwischen Computern

- Filesharing
- Dateitransfer
- Datenabgleich (PDAs, vCards)

Anwendungsbeispiele

- Spiele Head-to-Head über Bluetooth (Nokia N-Gage)
- Informationsabgleich
  - Daten
  - Adressen
  - Termine
- Sprachübertragung (Head Set)
- Einbindung des Mobiltelefons in Auto-HiFi
- Einbindung des PDAs in Navigations-System über Adresseintrag wird Route berechnet
- Location Based Services
  - Örtliches Parkleitsystem
  - Werbung

Zukunftsaussichten

- schnellere Übertragung
- größere Verbreitung von Geräten auf dem Markt
- weitere Profile & Anwendungsbereiche
- Als Ergänzung zu Master/Slave im Piconet: Supervisor, der Zustand des Piconets überwacht
- billigere Chips und Geräte

- IEEE entwickelt Wireless PAN (IEEE 802.15)
  kabellose Verbindung von Geräten im Haushalt
  z.B. für interaktive Spiel- und Multimedia-Anwendungen