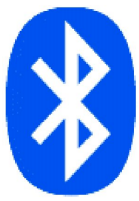
Episode 4: Bluetooth

Hannes Frey and Peter Sturm
University of Trier

Outline

- Introduction
- Bluetooth Fundamentals
- Bluetooth Protocol Stack
- Selected Protocol Components
- Bluetooth Profiles
- Summary



References

- [1] Brent A. Miller, and Chatschik Bisdikian, „Bluetooth Revealed“, Prentice Hall PTR, 2001
- [2] Bluetooth Special Interest Group, „Specification of the Bluetooth System, Volume1 and 2“, http://www.bluetooth.com, 2001

UBICOMP

4.1 Introduction

What is Bluetooth?

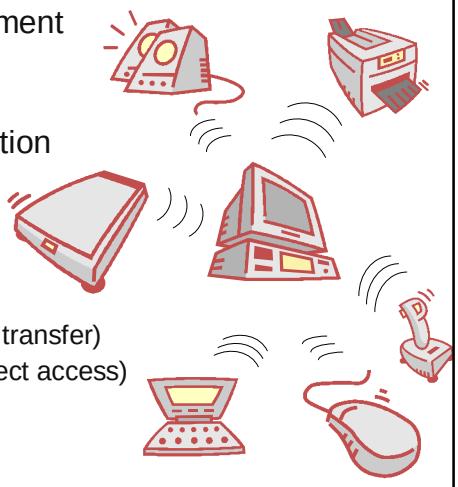
The term Bluetooth refers to an open specification for a technology to enable short-range wireless voice and data communications anywhere in the world [1].

© XILINX

Bluetooth History

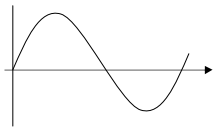
- Early 1998 - Special Interest Group formed
  - Code name “Bluetooth”
  - Promoter Companies: Ericsson, IBM, Intel, Nokia, and Toshiba
- May 20, 1998 - Bluetooth publicly announced
- July 26, 1999 - Bluetooth 1.0 Specification Release
- Today - Bluetooth 2.0 work is ongoing
  - Promoter Companies: 3Com, Ericsson, IBM, Intel, Lucent Technologies, Microsoft, Motorola, Nokia and Toshiba
  - Currently 1883 SIG Members
- Harald Blåtand – 10th Century King of Denmark
  - Literal translated to “Bluetooth”
  - United Denmark and Norway and brought Christianity to Scandinavia
- What means Bluetooth today?
- Bluetooth tomorrow?

Bluetooth Usage Models



- Bluetooth as a cable replacement
  - The cordless computer
  - The instant postcard
- Supporting voice communication
  - The ultimate headset
  - Three-in-one-Phone
  - The speaking Laptop
- Networking
  - The interactive conference (file transfer)
  - The internet bridge (dial up, direct access)
  - The automatic synchronizer
  - Ad-hoc Networking
- Hidden Computing

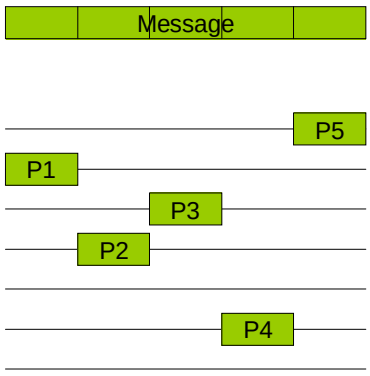
Radio Frequency Wireless Communication



- RF Communication range
  - transmitter‘s power and receiver's sensitivity
  - Long range communication requires high transmission power
  - Battery power achieves communication within a few meters
- Radio waves can penetrate many obstacles
- Usable radio frequency space is finite -> Licensed frequencies and power levels
- 2.4 GHz spectrum is globally unlicensed, however …
  - Spectrum divided into 79 channels
  - 1 MHz per channel (2.402, 2.403, …, 2.480; LGB=2.0, UGB=3.5)
  - Frequency hopping spread spectrum must be employed
  - Interference must be anticipated and appropriate handled

Spread Spectrum RF Communications

- Dividing available spectrum
  - Frequency, time, coding, …
- Dividing message in packets
- Frequency hopping spread spectrum (FHSS)
  - Spectrum divided into channels
  - Each packet on one channel
  - Sender and Receiver agree on the same hopping pattern
- Benefits of FHSS
  - Reduced RF interference
  - Retransmission of single packets
  - Provides a low degree of security

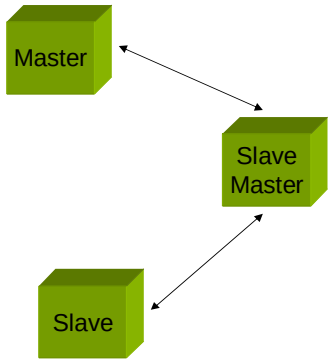


UBICOMP

4.2 Bluetooth Fundamentals

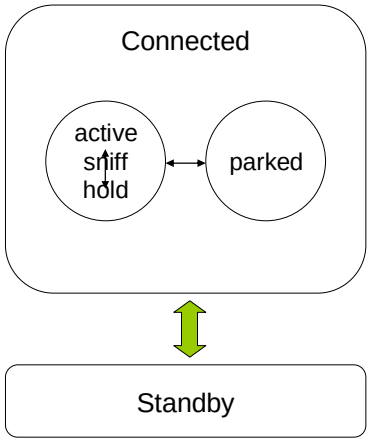
Master and Slave Role

- For each link one master and one slave
- Role of the master
  - Determines frequency hopping pattern (based on its address)
  - Determines phase of hopping sequence (based on its clock)
  - Current frequency
  - Polling slaves to transmit/receive
  - No special privileges
- Role of the slave
  - Follow the hop sequence
- Devices may act as master and slave for different links



Energy Conserving Baseband Modes

- When not connected the baseband in standby mode
- Connected slaves maintain synchronization with master
  - Active: slave always listens
  - Sniff, Hold: master and slave agree on certain time interval
  - Parked: slave must do the transition to an active mode
- Responsiveness vs. Power Consumption
- In all modes adaptive transmission power using RSSI



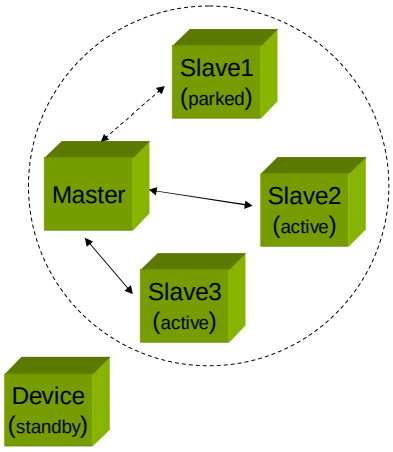
Question from the last lecture?

Bluetooth Energy-Conserving Facts

- Joule, Caliorie and Watts
  - 1 Joule = 1 kg m^2/sec^2
  - 1 Watt = 1J/sec = 1 kg m^2/sec^3
  - 1 calorie = 4.19J
  - 1 g fat = 9 kcal = 38 kJ
  - 1 Mars = 300 kcal = 1257 kJ (approx. 3h bycicle ride)
- Bluetooth supports two communication ranges
  - 10m: 1mW (pure transmission power)
  - 100m: 100mW (pure transmission power) (= 360 J/h = ? Mars/h)
- Computation is cheaper than wireless communication
  - Pentium4: 26,4 nJ/Operation (2.8GHz@74,9W)
  - ARM7TDMI: 0,06 nJ/Operation (133MHz@8mW)
  - Bluetooth(10m): 90nJ/Bit (brutto 1MBit/s@90mW)
  - Bluetooth(100m): 500nJ/Bit (brutto 1MBit/s@500mW)
  - WLAN: 358nJ/Bit ??? (see episode 3)
- Short range Communication is cheaper
  - 100m in one hop: 100 nJ/Bit
  - 100m in ten hops: 10nJ/Bit

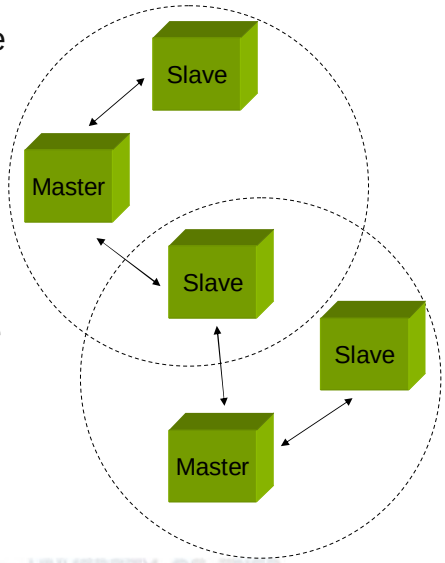
Piconet

- Master may communicate with multiple slaves
  - 7 active, 255 parked
- Piconet is defined by one master and its slaves
  - All slaves follow the same hopping sequence
  - Not all devices in proximity of the master are in the Piconet
- Typical piconets are expected to have a few devices



Scatternet

- Device may take part in more than one piconet
- Scatternets are defined by such overlapping piconets
  - Piconets remain as described
  - Each piconet has its own hopping sequence
- Different roles and states are possible (master, slave; active, parked)

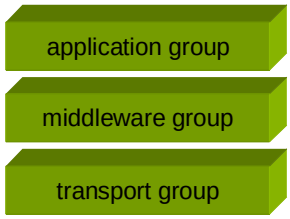


UBICOMP

4.3 Bluetooth Protocol Stack

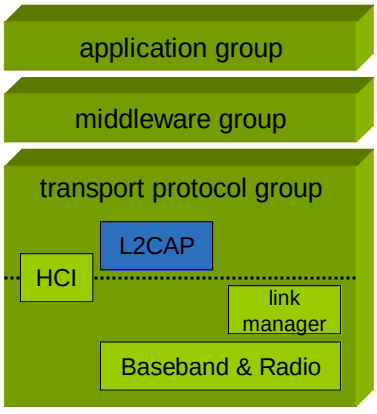
Protocol Stack Components

- Transport protocol group
  - Locate other devices
  - Create, configure and manage both physical and logical links
  - Transport of data from higher-layer protocols and applications (asynchronous/synchronous)
- Middleware protocol group
  - Provide existing and new applications
  - Existing protocols like PPP, IP, TCP, OBEX, …
  - New Bluetooth aware protocols like RFCOMM, TCS, SDP
- Application group
  - Legacy applications unaware of Bluetooth (e.g. modem dialer, web browser)
  - Bluetooth aware applications (e.g. telephony control via TCS)



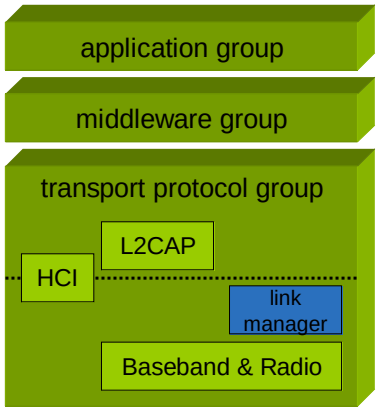
Logical Link Control and Adaption Protocol

- Shields higher-layer protocols and applications from BT details
  - Frequency hopping
  - Packet formats used for transmission
- Enables protocol multiplexing
- Segmentation/reassembly of large packets
- Negotiate/control the level of service



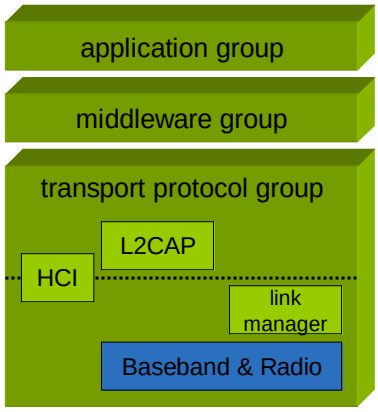
Link Manager

- Bandwidth allocation for data traffic
- Periodic bandwidth for audio traffic
- Device authentication (device pairing)
- Encryption if needed
- Power Control
  - Active modes, hold mode
  - Adaptive transmission power (RSSI)



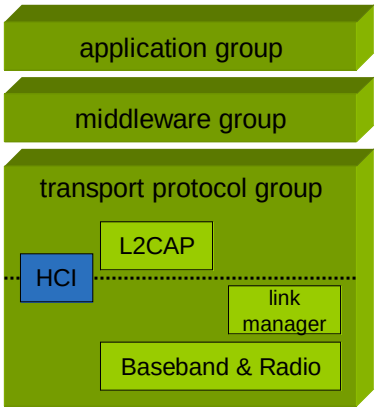
Baseband & Radio

- Device discovery and Link establishing
- Definition of Master/Slave role
- Forming of the frequency hopping sequences
- Rules for sharing the air-interface
- Defines the packet types for asynchronous/synchronous traffic
- Packet error detection/correction, encryption, transmission/retransmission
- (Audio has direct access)



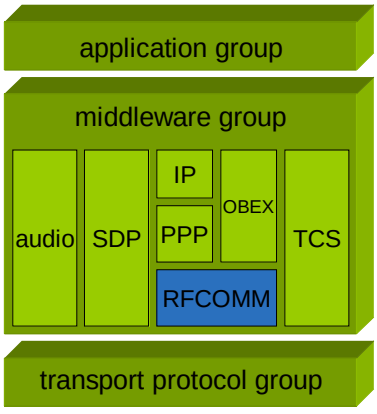
Host Controller Interface

- standard interface to access lower layers in a BT module
- Interoperability of modules from different vendors
- HCI Command: set a BT module in certain mode of operation
  - device discovery, request settings, …
- HCI Event: inform upper layers about a BT event
  - Result of device discovery, requested module settings, …
  - Traffic passes through the HCI as well



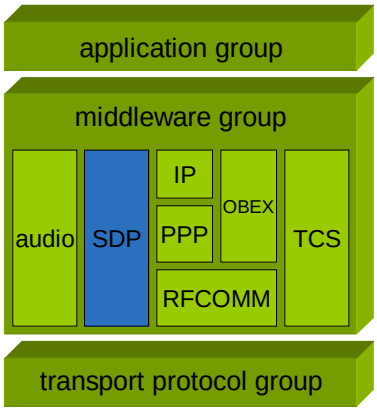
RFCOMM

- Serial port abstraction
- Facilitate easy migration of serial port-based applications (e.g. dial-up networking, synchronization)
- Modeled on ETSI TS 07.10 standard
  - Multiplexed serial communications over a single link
- Termed as one important part of the protocol stack



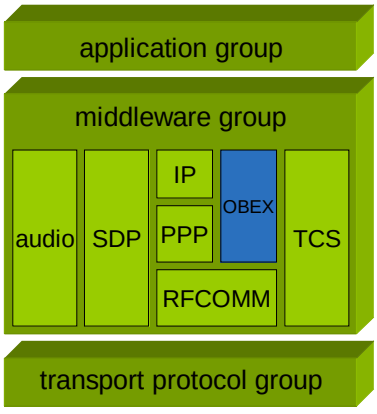
Service Discovery Protocol

- Services in traditional networks: File serving, print serving, name serving, bridges, gateways
- Static configuration of services insufficient for dynamic ad-hoc networks
- SDP provides standard methods to discover services at connected devices
- Symmetrically, SDP enables description of own services



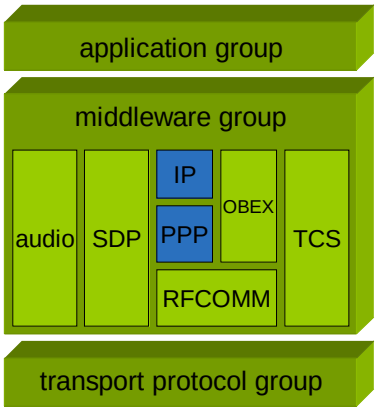
IrDA Interoperability

- IrDA defined protocols for infrared Data exchange and synchronization
- Fundamental: data format (syntax, semantics)
- IrOBEX: exchange of well defined objects
  - Electronic business cards, e-mail, messages, calendar entries
- IrMC: Synchronization of those objects
- Bluetooth adopts IrDA protocols
  - share some important attributes
  - Provide interoperability at the application layer



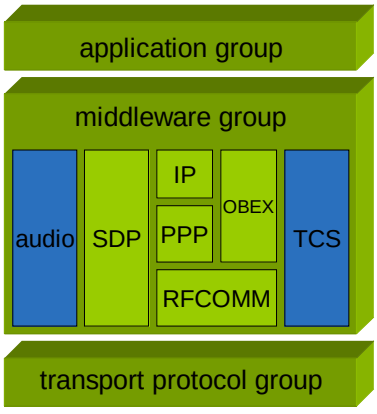
Networking

- Enables connecting to larger Networks
- dial-up networking
  - Via AT command layer and RFCOMM
- Networks access point and PPP
- IP over PPP
  - TCP, UDP, HTTP
  - Interoperability with WAP
- Future: Direct use of Internet protocols with Bluetooth



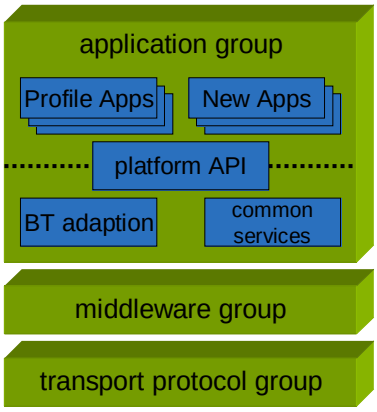
Telephony control specification and Audio

- Bluetooth carries voice traffic as well as data
- TCS layer supports telephony control
  - Voice calls are carried over audio channel
  - Data calls carried over L2CAP
- Audio is routed directly to the Baseband (isochronous traffic)
- Up to three audio channels at a time
- 64 Kbps (PCM, CVSD)



Application Group

- Software that resides above the stack
- BT expected to be supported by many device types
- Specification defines no single API
- BT defines profiles to provide interoperability
- Profiles give direction to developers of APIs, common services, and applications

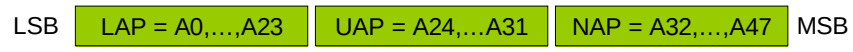


UBICOMP

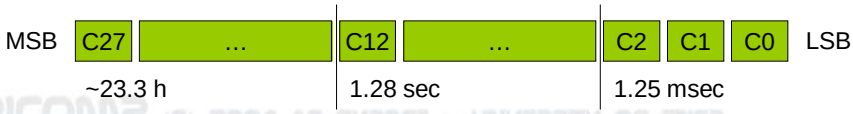
4.4 Selected Protocol Components

Fundamental Elements

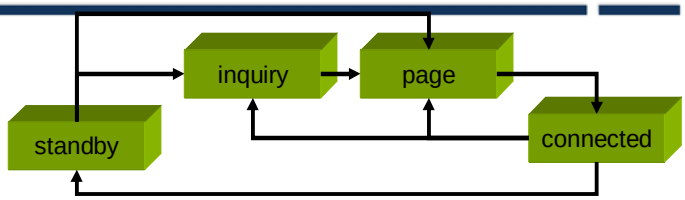
- The Bluetooth Device Address (BD_ADDR)
  - Globally unique 48-bit address
  - Partitioned into different parts (LAP, UAP, NAP) involved in nearly all baseband operations



- The Bluetooth Clock
  - Free running 28-bit native clock (never adjusted and turned off)
  - Clock rate 3.2 KHz (approx. wraps around in a day)
  - Accuracy 20ppm (250 ppm in low power modes)
  - Clock value of master fundamental for piconet communication



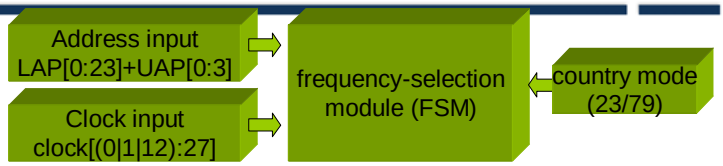
Operational device states



- standby: native clock, low power mode
- connected: member of a piconet
- inquiry, page: Transition to connected state
- Scatternet formation also possible
- Inquiry + paging may take several seconds

- Inquiry state
  - Learn about other devices in vicinity
  - devices in inquiry scan state reply
- Page mode
  - Used by master to invite in piconet
  - Slave device must be in page scan mode and has to reply

Frequency-Selection Module



- FSM Comprised of ADD, XOR, and MULTIPLEXER units
- Some countries allow only 23 channels used in 2.4GHz band
- Address and country mode determine channel-hopping sequence
- Slave uses address and clock value of master device
- Clock determines the current phase

- Normal piconet operation
  - Channel-hopping sequence
  - Bit C0 not used (0.625 msec, 1600/sec)
  - Long period (pseudo randomly)
- Page operation
  - Page-hopping sequence
  - Paging device uses C0…C27 (0.3125 msec, 3200/sec)
  - Paged device uses C12…C27 (1.28 sec)
  - Period 32 hops
- Inquiry operation similar to page

Baseband Packet Communication

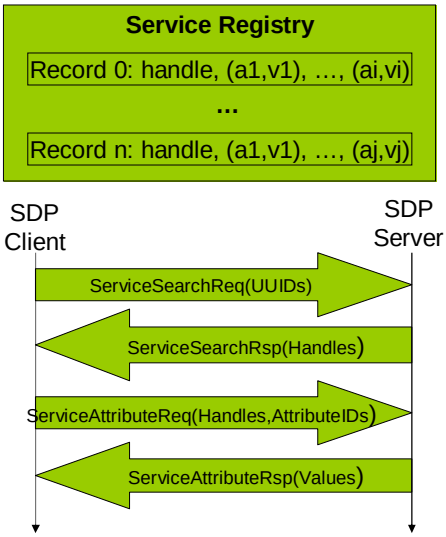
- Modulation: GFSK (application of FFT), 1 Mbps raw link speed
- Signaling Packets for inquiry, paging, polling, …
- Data communication via ACL packets
  - Master sends to slave or polls a slave to send
  - Multislot packets possible (1, 3, and 5 slots)
  - Frequency remains the same for multislot packets
  - Sending 5 slot packets in one and 1 slot packets in the opposite direction is possible
  - Maximum achievable rate 723.2 Kbps in one direction and 57.6 Kbps possible
- Voice Communication via SCO packets
  - Periodically reserved transmission intervals
  - One slot packets only
  - Communication in both directions support 64Kbps
  - SCO channels limited to 3

Communication over L2CAP

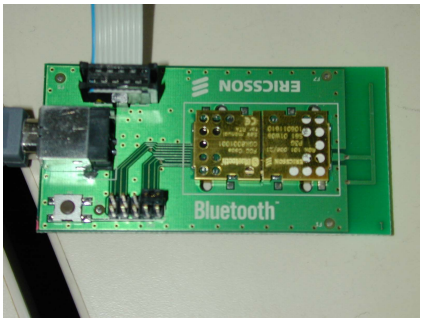
- L2CAP based on ACL packet
- L2CAP exports a maximum packet size information (max. 65k)
- Fragmentation of larger messages is up to higher layer protocols
- Communication between L2CAP layers based on logical links (channels)
- Each channel endpoint is assigned a unique channel identifier CID (16 Bit)
- Time for Link establishment in the magnitude of seconds

SDP Examined

- Locate available services
- Service registry contains list of service records
- Service record comprised of handle and (id,value) list
- Universal attributes apply to all services (e.g. service class, protocol stack info)
- Specific attributes defined by profiles (e.g. color, duplex)
- Services are identified by UUIDs (created algorithmically)
- Client requests services by using its UUID
- Each published profile (see next) has a well known UUID



Low-level Programming





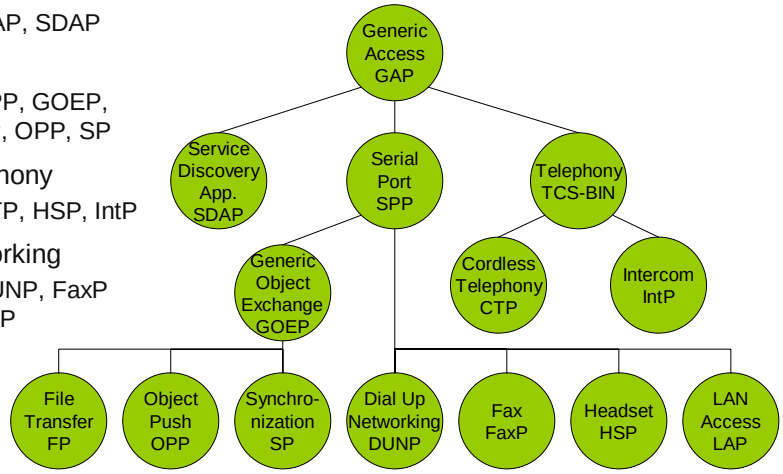
Sample Code

UBICOMP

4.5 Bluetooth Profiles

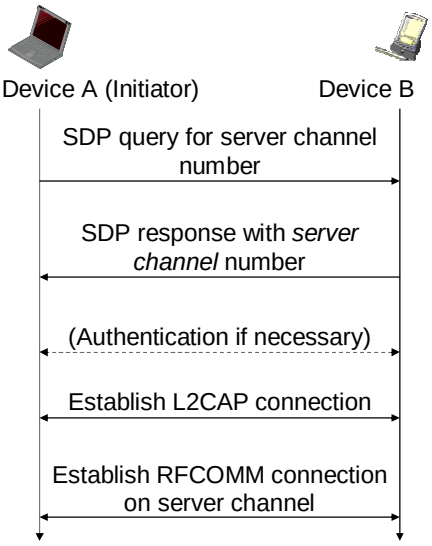
Profile Class Hierarchy

- Generic
  - GAP, SDAP
- Serial
  - SPP, GOEP, FP, OPP, SP
- Telephony
  - CTP, HSP, IntP
- Networking
  - DUNP, FaxP LAP



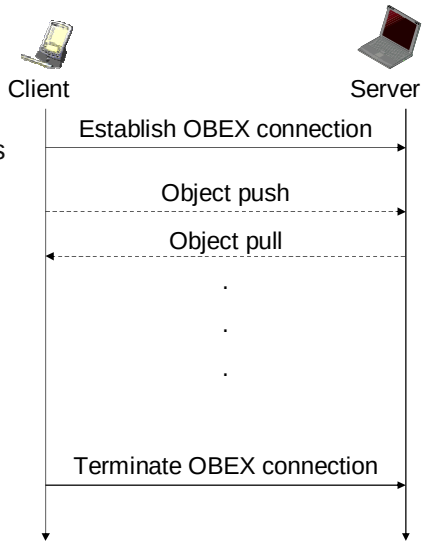
Serial Port Profile (SPP)

- Serial communication essential for many BT applications
- SPP used to establish RFCOMM communication
- Devices are peers (master/slave role does not matter)
- Server channel used to multiplex RFCOMM connections
- Service mapped on server channel
- Optional authentication and encryption
- Applications are not aware of Bluetooth once SPP completed



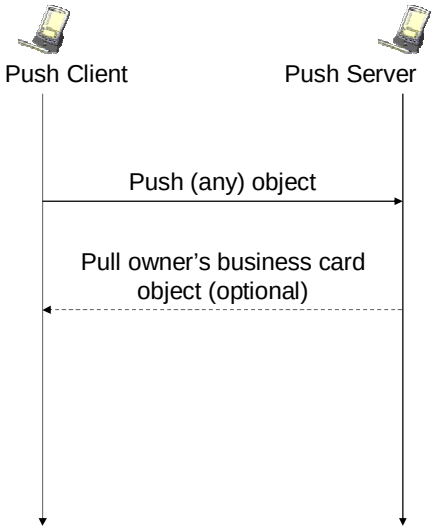
Generic Object Exchange Profile (GOEP)

- Foundation for other object exchange profiles
- Definition of client/server role (independent of master/slave role)
- Initiator acts as client, responder as server
- GOEP defines fundamental operations
  - Establish/terminate OBEX connection
  - Object push
  - Object pull
- OBEX Object exchange protocol from IrDA
  - Object formats: vCard, vCalendar, vMessage, vNote



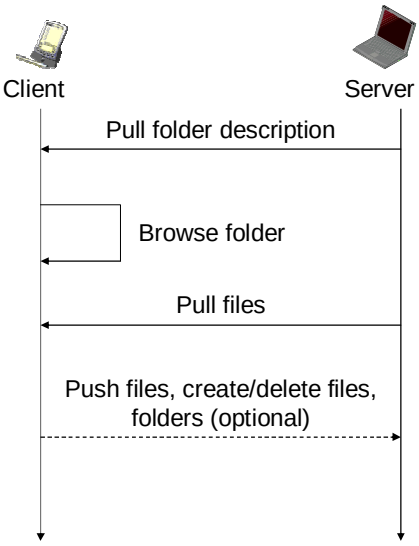
Object Push Profile (OPP)

- Used primary for business card exchange: vCard
- OOP Functions
  - object push
  - business card pull
  - business card exchange
- Server not required to support Pull operation
- Pull operation restricted on business vCard (V2.1)
- Push might be any object
- Required but optional: authentication, encryption, and user interaction



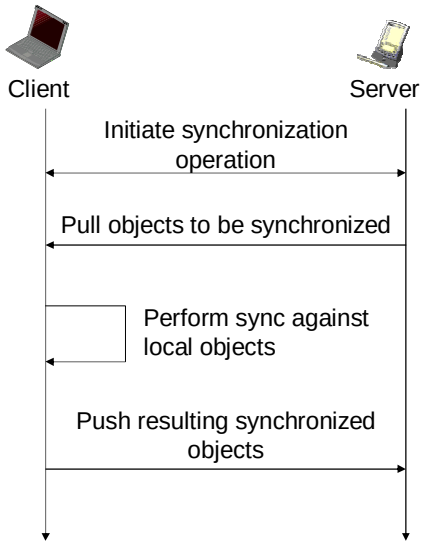
File Transfer Profile (FP)

- Supports bidirectional pushing pulling of objects distinguished as file and folder (no other OBEX Objects)
- Device may support both client and server role
- FP defines typical file manipulation operations:
  - Pulling/Pushing files and folders
  - Browsing and navigating folders
  - Deleting/creating files and folders
- Mandatory: Pulling folder description, selecting and pulling files
- Mandatory but optional: Authentication and encryption
- Future BT Version will additionally support IP over Bluetooth links + FTP



Synchronization Profile (SP)

- Based on IrMC synchronization protocol
- Client contains synchronization logic
  - Server usually a Phone/PDA
  - Client usually a PC (has more storage/processing power to operate sync)
- Rules for synchronization engine adopted from IrMC
- Process may be invoked by both client or server
- Automated synchronization for bonded devices
- SDP used to discover supported object types
- Disconnection during sync?



UBICOMP

4.6 Summary

Bluetooth vs. IrDA and WLAN

Feature	Bluetooth	IrDA	WLAN
Connection Establishment	Penetrates obstacles	Line of sight	Penetrates obstacles
Transmission pattern	Relatively spherical	Relatively narrow conical	Relatively spherical
Data rate	1Mbps	4Mbps	11Mbps and more
Range	10-100 meters	1 meter	300 meters
Power consumption	100mW	10mW	About 7W
Transceiver module	Expected $5.00	<$1.00	Similar to WLAN

Conclusion

- Bluetooth design goals: cheap and power efficient wireless communication
  - Short range communication
  - FHSS communication in 2.4GHz band
- Open Protocol stack specification (about 1000 pages) -> many product vendors
- Definition of Profiles (about 400 pages) -> many different device types
- Today's main Bluetooth application: Mobile Phones, Cable replacement
- Some of the usage models really addressed by Bluetooth today? (e.g. mobile ad-hoc networks)
- Discussion: Bluetooth opposed to WLAN