Bluetooth

- Basic idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, very cheap
  - Short range (10 m), low power consumption, license-free 2.45 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s data rate

One of the first modules (Ericsson).

Bluetooth

- History
  - 1994: Ericsson (Mattisson/Haartsen), “MC-link” project
  - Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1999: erection of a rune stone at Ericsson/Lund
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week

- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 10000 members
  - Common specification and certification of products
History and hi-tech…

…and the real rune stone

Located in Jelling, Denmark, erected by King Harald "Blåtand" in memory of his parents. The stone has three sides – one side showing a picture of Christ.

Inscription:
"Harald king executes these sepulchral monuments after Gorm, his father and Thyra, his mother. The Harald who won the whole of Denmark and Norway and turned the Danes to Christianity."

Btw: Blåtand means "of dark complexion" (not having a blue tooth…)

This could be the "original" colors of the stone.

Characteristics

- 2.4 GHz ISM band, 79 RF channels, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - G-PSK modulation, 1-100 mW transmit power
- FHSS and TDD
  - Frequency hopping with 1600 hops/s
  - Hopping sequence in a pseudo random fashion, determined by a master
  - Time division duplex for send/receive separation
- Voice link – SCO (Synchronous Connection Oriented)
  - FEC (forward error correction), no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- Data link – ACL (Asynchronous ConnectionLess)
  - Asynchronous, acknowledgments, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology
  - Overlapping piconets (stars) forming a scatternet
### Piconet

- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)

### Forming a piconet

- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
  - Hopping pattern determined by device ID (48 bit, unique worldwide)
  - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)

### Scatternet

- Linking of multiple co-located piconets through the sharing of common master or slave devices
- Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets
### SCO payload types

- **payload (30)**
- **Hv1**
  - audio (10)  
  - FEC (20)  
- **Hv2**
  - audio (20)  
  - FEC (10)  
- **Hv3**
  - audio (30)

- **DV**
  - audio (10)  
  - Header (1)  
  - Payload (0-9)  
  - 2/3 FEC  
  - CRC (2)

### ACL Payload types

- **payload (0-343)**
- **Header (1/2)**
  - payload (0-339)  
  - CRC (2)  

- **DM1**
  - header (1)  
  - payload (0-17)  
  - 2/3 FEC  
  - CRC (2)

- **DH1**
  - header (1)  
  - payload (0-27)  
  - CRC (2)

- **DM3**
  - header (2)  
  - payload (0-121)  
  - 2/3 FEC  
  - CRC (2)

- **DH3**
  - header (2)  
  - payload (0-183)  
  - CRC (2)

- **DM5**
  - header (2)  
  - payload (0-224)  
  - 2/3 FEC  
  - CRC (2)

- **DH5**
  - header (2)  
  - payload (0-339)  
  - CRC (2)

- **AUX1**
  - header (1)  
  - payload (0-29)

### Baseband data rates

<table>
<thead>
<tr>
<th>ACL</th>
<th>Payload Header</th>
<th>User Payload</th>
<th>Symmetric max. Rate</th>
<th>Asymmetric max. Rate</th>
</tr>
</thead>
<tbody>
<tr>
<td></td>
<td>[kbit/s] [byte]</td>
<td>[byte]</td>
<td>FEC</td>
<td>CRC</td>
</tr>
<tr>
<td>1 slot</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM1</td>
<td>1</td>
<td>0-17</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0-27</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0-121</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0-183</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0-224</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0-339</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>3 slot</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM3</td>
<td>1</td>
<td>0-17</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0-27</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0-121</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0-183</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0-224</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0-339</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>5 slot</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>DM5</td>
<td>1</td>
<td>0-17</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>0-27</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>0-121</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>4</td>
<td>0-183</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>5</td>
<td>0-224</td>
<td>2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>6</td>
<td>0-339</td>
<td>no</td>
<td>yes</td>
</tr>
<tr>
<td>AUX1</td>
<td>1</td>
<td>0-29</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>10</td>
<td>1/3</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>20</td>
<td>2/3</td>
<td>no</td>
</tr>
<tr>
<td>DM/2</td>
<td>1</td>
<td>0-29</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>10</td>
<td>1/3</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>20</td>
<td>2/3</td>
<td>no</td>
</tr>
<tr>
<td>HV/3</td>
<td>1</td>
<td>0-29</td>
<td>no</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>2</td>
<td>10</td>
<td>1/3</td>
<td>no</td>
</tr>
<tr>
<td></td>
<td>3</td>
<td>20</td>
<td>2/3</td>
<td>no</td>
</tr>
<tr>
<td>DV</td>
<td>1 D</td>
<td>10+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>2 D</td>
<td>20+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>3 D</td>
<td>30+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>4 D</td>
<td>40+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>5 D</td>
<td>50+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>6 D</td>
<td>60+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>7 D</td>
<td>70+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>8 D</td>
<td>80+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
<tr>
<td></td>
<td>9 D</td>
<td>90+(0-9)</td>
<td>D 2/3</td>
<td>yes</td>
</tr>
</tbody>
</table>

**Data Medium/High rate, High-quality Voice, Data and Voice**
Baseband link types

- Polling-based TDD packet transmission
  - 625µs slots, master polls slaves
- SCO (Synchronous Connection Oriented) – Voice
  - Periodic single slot packet assignment, 64 kbit/s full-duplex, point-to-point
- ACL (Asynchronous ConnectionLess) – Data
  - Variable packet size (1, 3, 5 slots), asymmetric bandwidth, point-to-multipoint

Robustness

- Slow frequency hopping with hopping patterns determined by a master
  - Protection from interference on certain frequencies
  - Separation from other piconets (FH-CDMA)
- Retransmission
  - ACL only, very fast
  - Forward Error Correction
    - SCO and ACL

Baseband states of a Bluetooth device

- Standby: do nothing
- Inquire: search for other devices
- Page: connect to a specific device
- Connect: participate in a piconet
- Unconnected
- Connecting
- Active
- Low power

- Park: release AMA, get PMA
- Sniff: listen periodically, not each slot
- Hold: stop ACL, SCO still possible, possibly participate in another piconet
**Example: Power consumption/CSR BlueCore2**

**Typical Average Current Consumption**

- **VDD=1.8V  Temperature = 20°C**
- **Mode**
  - SCO connection HV3 (1s interval Sniff Mode) (Slave) 26.0 mA
  - SCO connection HV3 (1s interval Sniff Mode) (Master) 26.0 mA
  - SCO connection HV1 (Slave) 53.0 mA
  - SCO connection HV1 (Master) 53.0 mA
  - ACL data transfer 115.2kbps UART (Master) 15.5 mA
  - ACL data transfer 115.2kbps USB (Slave) 53.0 mA
  - ACL data transfer 115.2kbps UART (Master) 53.0 mA
  - ACL connection, Sniff Mode 40ms interval, 38.4kbps UART 4.0 mA
  - ACL connection, Sniff Mode 1.28s interval, 38.4kbps UART 0.5 mA
  - Parked Slave, 1.28s beacon interval, 38.4kbps UART 0.6 mA
  - Standby Mode (Connected to host, no RF activity) 47.0 µA
  - Deep Sleep Mode 20.0 µA

**Notes:**

1. Current consumption is the sum of both BC212015A and the flash.
2. Current consumption is for the BC2120/15A device only.

---

**L2CAP - Logical Link Control and Adaptation Protocol**

- Simple data link protocol on top of baseband
- Connection oriented, connectionless, and signaling channels
- Protocol multiplexing
  - RFCOMM, SDP, telephony control
- Segmentation & reassembly
  - Up to 64kbyte user data, 16 bit CRC used from baseband
- QoS flow specification per channel
  - Follows RFC 1363, specifies delay, jitter, bursts, bandwidth
- Group abstraction
  - Create/destroy group, add/remove member

---

**L2CAP logical channels**

[Diagram of L2CAP logical channels with labels]
L2CAP packet formats

Connectionless PDU

- Length: 2 bytes
- PSM: 0-65533

Connection-oriented PDU

- Length: 2 bytes
- PSM: 0-65536

Signalling command PDU

- Length: 2 bytes
- PSM: 0-65536

Profiles

- Represent default solutions for a certain usage model
  - Vertical slice through the protocol stack
  - Basis for interoperability
- Generic Access Profile
- Service Discovery Application Profile
- Cordless Telephony Profile
- Intercom Profile
- Serial Port Profile
- Headset Profile
- Dial-up Networking Profile
- Fax Profile
- LAN Access Profile
- Generic Object Exchange Profile
- Object Push Profile
- File Transfer Profile
- Synchronization Profile

Security

- PIN (1-16 bytes)
- Encryption key generation (possibly permanent storage)
- Authentication
- Encryption key generation (temporary storage)
- Keystream generator
- Payload key
- Cipher data

Profiles

- Additional Profiles
  - Advanced Audio Distribution
  - PAN
  - Audio Video Remote Control
  - Basic Printing
  - Basic Imaging
  - Extended Service Discovery
  - Generic Audio Video Distribution
  - Hands Free
  - Hardcopy Cable Replacement
Bluetooth versions

- **Bluetooth 1.1**
  - also IEEE Standard 802.15.1-2002
  - initial stable commercial standard

- **Bluetooth 1.2**
  - also IEEE Standard 802.15.1-2005
  - eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
  - AFH (adaptive frequency hopping) to avoid interference

- **Bluetooth 2.0 + EDR (2004, no more IEEE)**
  - EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
  - lower power consumption due to shorter duty cycle

- **Bluetooth 2.1 + EDR (2007)**
  - better pairing support, e.g., using NFC
  - improved security

WPAN: IEEE 802.15.1 – Bluetooth

- **Data rate**
  - Synchronous, connection-oriented: 64 kbit/s
  - Asynchronous, connectionless
    - 433.9 kbit/s symmetric
    - 723.2 / 57.6 kbit/s asymmetric

- **Transmission range**
  - POS (Personal Operating Space) up to 10 m
  - with special transceivers up to 100 m

- **Frequency**
  - Free 2.4 GHz ISM-band

- **Security**
  - Challenge/response, hopping sequence

- **Availability**
  - Integrated into many products, several vendors

- **Connection set-up time**
  - Depends on power-mode
    - Max. 2.95s, avg. 0.64s

WPAN: IEEE 802.15 – future developments 1

- **802.15.2: Coexistence**
  - Coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11), quantify the mutual interference

- **802.15.3: High-Rate**
  - Standard for high-rate (20Mbit/s or greater) WPANs, while still low-power/low-cost
  - Data Rates: 11, 22, 33, 44, 55 Mbit/s
  - Quality of Service
  - Ad hoc peer-to-peer networking
  - Security
  - Low power and low cost
  - Designed to meet the demanding requirements of portable consumer imaging and multimedia applications
WPAN: IEEE 802.15 – future developments 2

- Several working groups extend the 802.15.3 standard
  - 802.15.3a: withdrawn
    - Alternative PHY with higher data rate as extension to 802.15.3
    - Applications: multimedia, picture transmission
  - 802.15.3b:
    - Enhanced interoperability of MAC
    - Correction of errors and ambiguities in the standard
  - 802.15.3c:
    - Alternative PHY at 57-64 GHz
    - Goal: data rates above 2 Gbit/s
- Not all these working groups really create a standard, not all standards will be found in products later...

WPAN: IEEE 802.15 – future developments 3

- 802.15.4: Low-Rate, Very Low-Power
  - Low data rate solution with multi-month to multi-year battery life and very low complexity
  - Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation
  - Data rates of 20-250 kbit/s, latency down to 15 ms
  - Master-Slave or Peer-to-Peer operation
  - Up to 254 devices or 64516 simpler nodes
  - Support for critical latency devices, such as joysticks
  - CSMA/CA channel access (data-centric), slotted (beacon), unslotted
  - Automatic network establishment by the PAN coordinator
  - Dynamic device addressing, flexible addressing format
  - Fully handshake protocol for transfer reliability
  - Power management to ensure low power consumption
  - 16 channels in the 2.4 GHz ISM band, 10 channels in the 915 MHz US ISM band and one channel in the European 868 MHz band
  - Basis of the ZigBee technology – www.zigbee.org

ZigBee

- Relation to 802.15.4 similar to Bluetooth / 802.15.1
- Pushed by Chipcon (now TI), Ember, Freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung...
- More than 260 members
  - about 15 promoters, 133 participants, 111 adopters
  - must be member to commercially use ZigBee spec
- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications
WPAN: IEEE 802.15 – future developments

- **802.15.4a:**
  - Alternative PHY with lower data rate as extension to 802.15.4
  - Properties: precise localization (< 1m precision), extremely low power consumption, longer range

- **802.15.4b, c, d:**
  - Extensions, corrections, and clarifications regarding 802.15.4
  - Usage of new bands, more flexible security mechanisms

- **802.15.5: Mesh Networking**
  - Partial meshes, full meshes
  - Range extension, more robustness, longer battery live

- **802.15.6: Body Area Networks**
  - Low power networks e.g. for medical or entertainment use

- Not all these working groups really create a standard, not all standards will be found in products later...

### Some more IEEE standards for mobile communications

- **IEEE 802.16: Broadband Wireless Access / WirelessMAN / WiMax**
  - Wireless distribution system, e.g., for the last mile, alternative to DSL
  - 75 Mbit/s up to 50 km LOS, up to 10 km NLOS; 2.46 GHz band
  - Initial standards without roaming or mobility support
  - 802.16e adds mobility support, allows for roaming at 150 km/h

- **IEEE 802.20: Mobile Broadband Wireless Access (MBWA)**
  - Licensed bands < 3.5 GHz, optimized for IP traffic
  - Peak rate > 1 Mbit/s per user
  - Different mobility classes up to 250 km/h and ranges up to 15 km
  - Relation to 802.16e unclear

- **IEEE 802.21: Media Independent Handover Interoperability**
  - Standardize handover between different 802.x and/or non 802 networks

- **IEEE 802.22: Wireless Regional Area Networks (WRAN)**
  - Radio-based PHY/MAC for use by license-exempt devices on a non-interfering basis in spectrum that is allocated to the TV Broadcast Service

### ISM band interference

- **Many sources of interference**
  - Microwave ovens, microwave lighting
  - 802.11, 802.11b, 802.11g, 802.15, ...
  - Even analog TV transmission, surveillance
  - Unlicensed metropolitan area networks
  - ...

- **Levels of interference**
  - Physical layer: interference acts like noise
    - Spread spectrum tries to minimize this
    - FEC/interleaving tries to correct
  - MAC layer: algorithms not harmonized
    - E.g., Bluetooth might confuse 802.11
802.11 vs. 802.15/Bluetooth

- Bluetooth may act like a rogue member of the 802.11 network
  - Does not know anything about gaps, inter frame spacing etc.

- IEEE 802.15-2 discusses these problems
  - Proposal: Adaptive Frequency Hopping
  - A non-collaborative Coexistence Mechanism

- Real effects? Many different opinions, publications, tests, formulae, ...
  - Results from complete breakdown to almost no effect
  - Bluetooth (FHSS) seems more robust than 802.11b (DSSS)