IEEE 802.15 (WPAN)
(Bluetooth)

Luciano Bononi (bononi@cs.unibo.it)

Figure Credits: some figures have been taken form slides found on the web by the following authors (in alphabetical order):
Pravin Bhagwat (acm.org), Chatschik Bisdikian (ibm.com), Tom Siep (ti)

IEEE 802.xy Wireless Standards

- WWAN
- WMAN
- WLAN
- WPAN

Data Rate (Mbps)

IEEE 802.22
IEEE 802.20
WiMax
IEEE 802.16
WiFi
802.11
802.15.3
802.15.3a
802.15.3c

ZigBee
802.15.4
Bluetooth
802.15.1

W-USB (UWB) = 480 Mbps
Bluetooth 3.0 = 24 Mbps (wi-fi)
Working Group 802.15 and the Other IEEE Wireless Standards Areas

IEEE 802.15 Wireless Personal Area Network (WPAN) Working Group

Task Group 1 WPAN/Bluetooth™
Task Group 2 Coexistence
Task Group 3 WPAN High Rate
Task Group 3a WPAN Alt. Higher Rate
Task Group 4 WPAN Low Rate

IEEE 802.11 WLAN Working Group
IEEE 802.16 WMAN Working Group
IEEE 802.18 Radio Regulatory TAG
IEEE 802.19 Coexistence TAG
IEEE 802.20 Mobile BWA Working Group
IEEE 1451.5 Working Group for Wireless Sensors

Working Group 15: Wireless Personal Area Networks

Synopsis:

802.15 focuses on the development of consensus standards for Personal Area Networks or short distance wireless networks. These WPANs address wireless networking of portable and mobile computing devices such as PCs, PDAs, peripherals, cell phones and consumer electronics. The goal is to publish standards, recommended practices, or guides that have broad market applicability and deal effectively with the issues of coexistence and interoperability with other wired and wireless networking solutions.

802.15 is part of the 802 Local and Metropolitan Area Network Standards Committee of the IEEE Computer Society. The IEEE-SA is an international membership organization serving today’s industries with a complete portfolio of standards programs.

The latest status of 802.15 and other IEEE802 activities is available at http://standards.ieee.org/802news/.
802.15 WG is developing 3 MACs and 5 PHYs, TG3a is the 6th PHY

Task Group 1: WPAN/Bluetooth™

Synopsis:

Bluetooth is an industry specification for short-range RF-based connectivity for portable personal devices. The WPAN/Bluetooth™ Task Group (TG1) has reviewed and provided a standard adaptation of the Bluetooth Specification v1.1 Foundation MAC and PHY (L2CAP, LMP, Baseband, and radio). Also specified are: a clause on SAPs which includes a LLC/MAC interface for the ISO/IEC 8802-2 LLC; a normative annex which provides a Protocol Implementation Conformance Statement (PICS) proforma; and a informative annex high level behavioral ITU-T Z.100 Specification and Description Language (SDL) model for an integrated Bluetooth MAC Sublayer.

More info is available at http://ieee802.org/15/pub/TG1.html
Task Group 2: Coexistence

Synopsis:
The Coexistence Task Group (TG2) is developing Recommended Practices to facilitate coexistence of Wireless Personal Area Networks (802.15) and Wireless Local Area Networks (802.11). The group is developing a Coexistence Model to quantify the mutual interference of a WLAN and a WPAN. They are also developing a set of Coexistence Mechanisms to facilitate coexistence of WLAN and WPAN devices.

More info is available at [http://ieee802.org/15/pub/TG2.html](http://ieee802.org/15/pub/TG2.html).

---

Task Group 3: WPAN High Rate

Synopsis:
The WPAN High Rate Task Group (TG3) for Wireless Personal Area Networks (WPANs™) is chartered to draft and publish a new standard for high-rate (20Mbps or greater) WPANs. Besides a high data rate, the new standard will provide for low power, low cost solutions addressing the needs of portable consumer digital imaging and multimedia applications.

Task Group 3a: WPAN Alternate Higher Rate

Synopsis:
The WPAN Higher Rate Alternate PHY Task Group (TG3a) is chartered to draft and publish a new standard which will provide a higher speed (110 Mbps or greater) PHY amendment to the draft P802.15.3 standard. This will address streaming video and other multimedia applications. The new PHY will use the P802.15.3 MAC with limited modification.

More info is available at [http://ieee802.org/15/pub/SG3a.html](http://ieee802.org/15/pub/SG3a.html).
And [http://grouper.ieee.org/groups/802/15/arc/802-wpanlist/msg00735.html](http://grouper.ieee.org/groups/802/15/arc/802-wpanlist/msg00735.html).

Task Group 4: WPAN Low Rate

Synopsis:
The WPAN Low Rate Task Group (TG4) is chartered to investigate a low data rate solution with multi-month to multi-year battery life and very low complexity. This standard specifies two physical layers: an 868 MHz/915 MHz direct sequence spread spectrum PHY and a 2.4 GHz direct sequence spread spectrum PHY. The 2.4 GHz PHY supports an over air data rate of 250 kb/s and the 868 MHz/915 MHz PHY supports over the air data rates of 20 kb/s and 40 kb/s. The physical layer chosen depends on local regulations and user preference. Potential applications are sensors, interactive toys, smart badges, remote controls, and home automation.

More info is available at [http://ieee802.org/15/pub/TG4.html](http://ieee802.org/15/pub/TG4.html).
### WPAN Application Feature List

<table>
<thead>
<tr>
<th>Consensus</th>
<th>Priority</th>
<th>Low</th>
</tr>
</thead>
<tbody>
<tr>
<td>Strong</td>
<td>low cost</td>
<td>packet + isochronous</td>
</tr>
<tr>
<td></td>
<td>low power</td>
<td>encryption</td>
</tr>
<tr>
<td></td>
<td>small size</td>
<td>mobility ≤ 10 mph</td>
</tr>
<tr>
<td></td>
<td>packet data ≤ 1 Mbps</td>
<td>gateway</td>
</tr>
<tr>
<td></td>
<td>range ≤ 10m</td>
<td>native IP</td>
</tr>
<tr>
<td></td>
<td>active devices ≤ 10</td>
<td></td>
</tr>
<tr>
<td></td>
<td>manual auth/auto attach</td>
<td></td>
</tr>
<tr>
<td></td>
<td>coexistence with 802.11</td>
<td></td>
</tr>
<tr>
<td>Weak</td>
<td>topology</td>
<td>inter-pan connectivity</td>
</tr>
<tr>
<td></td>
<td>active devices 10 - 128</td>
<td></td>
</tr>
<tr>
<td></td>
<td>coexisting PANs 4-30</td>
<td></td>
</tr>
</tbody>
</table>

Source: doc.: IEEE 802.11-98/353 (Bruce Kraemer, Harris)

### Possible Coalescence of Standards

- Bluetooth
- IEEE 802.11x
- HomeRF (firefly)
- others

IEEE 802.15 Standards

© 2005 Luciano Bononi  Sistemi e Reti Wireless
WPAN usage model in existing Solutions

Bluetooth
- Three-In-One Phone
- Interactive Conference
- Briefcase Trick
- Forbidden Message
- Automatic Synchronizer
- Instant Postcard
- Portable PC Speaker Phone
- Cordless Desktop
- Videos
- Ultimate Headset
- Internet Bridge

HomeRF
- wireless home network to share voice and data between PC’s, peripherals, PC-enhanced cordless phones, and new portable display pads
- Access the Internet and share ISP connection
- Share files/modems/printers in multi-PC homes
- Intelligently forward and review incoming telephone call, FAX, e-mail messages to multiple cordless handsets, FAX machines and voice mailboxes
- Activate other home electronic systems by simply speaking a command into a PC-enhanced cordless handset
- Multi-player games

WPAN standard: Levels of Compatibility

- Limited Transmit and Receive
- Detect Energy and Defer
- Communication Prevention
- Full MAC and PHY Compliance
- Receive Only
- Throughput Degradation
- Interoperate
- IEEE 802.15 WPAN Goal
- Interfer
- Coexist
HomeRF®: Bringing Wireless Connectivity Home

HomeRF Origins

802.11
Uses CSMA/CA
Good for Data

DECT
Uses TDMA
Good for Voice

SWAP
TDMA + CSMA/CA
Good for Voice & Data
Optimized for small networks (in home)
Simplified radio & protocol to reduce cost

Both voice and data are important for home RF
Harald Blaatand “Bluetooth” II
King of Denmark 940-981

- Harald christianized the Danes
- Harald controlled Denmark and Norway

Bluetooth™

- Cable Replacement, low cost, low power, low range

<table>
<thead>
<tr>
<th>Feature</th>
<th>Details</th>
</tr>
</thead>
<tbody>
<tr>
<td>Topology</td>
<td>Supports up to 7 simultaneous links</td>
</tr>
<tr>
<td>Flexibility</td>
<td>Goes through walls, bodies, cloths...</td>
</tr>
<tr>
<td>Data rate</td>
<td>1 MSPS, 720 Kbps</td>
</tr>
<tr>
<td>Power</td>
<td>0.1 watts active power 0.05 watts active power or higher</td>
</tr>
<tr>
<td>Size/Weight</td>
<td>25 mm x 13 mm x 2 mm, several grams</td>
</tr>
<tr>
<td>Cost</td>
<td>Long-term $5 per endpoint $3-$100/meter (end user cost)</td>
</tr>
<tr>
<td>Range</td>
<td>10 meters or less  Up to 100 meters with PA</td>
</tr>
<tr>
<td>Universal</td>
<td>Intended to work anywhere in the world</td>
</tr>
<tr>
<td>Security</td>
<td>Very, link layer security, SS radio Secure (its a cable)</td>
</tr>
</tbody>
</table>
**Wireless Positioning**

- **Wireless LANs**
  - IEEE802.11
  - Wireless Ethernet
  - On-campus: Office, School, Airport, Hotel, Home

- **Cellular**
  - Convergence Phone-Internet
  - Off-Campus Global Coverage

- **Bluetooth**
  - Cable Replacement
  - Person Space: Office, Room, Briefcase, Pocket, Car
  - Short Range/Low Power
  - Voice AND Data
  - Low-cost
  - Small form factor
  - Many Co-located Nets
  - Universal Bridge

---

**Bluetooth: new applications**

- **Data/Voice Access Points**
- **Cable Replacement**
- **Personal Ad-hoc Connectivity**

---

© 2005 Luciano Bononi

Sistemi e Reti Wireless
Characteristics

- Operates in the **2.4 GHz** band at a data rate of **720Kb/s** (1 Mbps v1.2, 3 Mbps v2.0, 24 Mbps v3.0, 54-480 Mbps UWB)

- Uses **Frequency Hopping (FH) spread spectrum**, which divides the frequency band into a number of channels (2.402 - 2.480 GHz yielding 79 channels).

- Radio transceivers **hop** from one channel to another in a **pseudo-random fashion, determined by the master**.

- Supports up to **8 devices in a piconet** (1 master and 7 slaves).

- Piconets can combine to form **scatternets**.

---

Characteristics

**Bluetooth 1.0 and 1.0B**
- many interoperability problems, and anonymity impossible at the protocol level

**Bluetooth 1.1**
- 1.0B errors fixed.
- Added support for non-encrypted channels.
- Received Signal Strength Indicator

**Bluetooth 1.2**
- backward compatible with 1.1
- Faster Connection and Discovery
- **Adaptive frequency-hopping spread spectrum (AFH)**
- Higher transmission speeds up to 720 kbit/s
- Extended Synchronous Connections (eSCO), improve voice quality via retransmissions of corrupted packets
Characteristics

Bluetooth 2.0
- Introduction of an Enhanced Data Rate (EDR) 3 megabits per second (2.1)
- Gaussian Frequency Shift Keying (GFSK) + EDR = a combination of GFSK and Phase Shift Keying modulation (PSK) with two variants, π/4-DQPSK and 8DPSK.
- Lower power consumption through a reduced duty cycle.

Bluetooth 2.1
backward compatible with 1.2, July 26, 2007.
- **Extended inquiry response**: better filtering of devices before connection.
- **Sniff subrating**: reduces the power consumption when devices are in the sniff low-power mode.
- **Encryption Pause Resume**: refresh of encryption key enabled
- **Secure Simple Pairing**: radically improves the pairing experience

Bluetooth 3.0
The 3.0 specification was adopted April 21st, 2009. Its main new feature is AMP (Alternate MAC/PHY), the addition of Wi-Fi as a high speed transport. Two technologies had been anticipated for AMP: Wi-Fi and UWB, but UWB is missing from the specification.
- **Alternate MAC PHY**: enables the use of alternative MAC and PHY’s for transporting Bluetooth profile data. The Bluetooth Radio is still used for device discovery, initial connection and profile configuration. The high speed alternate MAC PHY (802.11, Wi-Fi) will be used to transport the data.
- **Unicast Connectionless Data**: permits service data to be sent without establishing an explicit L2CAP channel. It is intended for use by applications that require low latency between user action and reconnection/transmission of data. This is only appropriate for small amounts of data.
### Characteristics

#### Power classes

<table>
<thead>
<tr>
<th>Class</th>
<th>Max power (mW, dBm)</th>
<th>Approx. Range (m)</th>
</tr>
</thead>
<tbody>
<tr>
<td>Class 1</td>
<td>100 mW (20 dBm)</td>
<td>100 m</td>
</tr>
<tr>
<td>Class 2</td>
<td>2.5 mW (4 dBm)</td>
<td>10 m</td>
</tr>
<tr>
<td>Class 3</td>
<td>1 mW (0 dBm)</td>
<td>1 m</td>
</tr>
</tbody>
</table>

---

### What is a Piconet?

- A collection of devices connected in an ad hoc fashion.
- One unit will act as a master and the others as slaves for the duration of the piconet connection.
- Master sets the clock and hopping pattern.
- Each piconet has a unique hopping pattern/ID.
- Each master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet.

![Diagram of piconet connections]

- M=Master
- P=Parked
- S=Slave
- SB=Standby
What is a Scatternet?

• A **Scatternet** is the **linking** of multiple co-located piconets through the sharing of common master or slave devices.

• A device can be both a **master** and a **slave**.

• Radios are **symmetric** (same radio can be master or slave)

• **High capacity system**, each piconet has maximum capacity (720 Kbps)

---

The Bluetooth protocols: specifications

- A hardware/software protocol description
- An application framework
Interoperability & Profiles

- Represents default solution for a usage model
- Vertical slice through the protocol stack
- Basis for interoperability and logo requirements
- Each Bluetooth device supports one or more profiles

Profiles (spec v.1)

- **Generic Access Profile (GAP)**
  - Service Discovery Application Profile (SDAP)
  - Serial Port Profile (SPP)
  - Dial-up Networking Profile (DUNP)
  - Fax Profile
  - Headset Profile (HSP)
  - LAN Access Profile (using PPP) (LAP)
  - Generic Object Exchange Profile (GOEP)
    - File Transfer Profile (FTP)
    - Object Push Profile (OPP)
    - Synchronization Profile (SP)
  - **TCS_BIN-based profiles**
    - Cordless Telephony Profile (CTP)
    - Intercom Profile (IP)
The Radio Frequency (PHY RF) layer

- **Radio (RF)**
  - The Bluetooth radio front-end: ISM band; 1Mbps
    - Frequency hopping spread spectrum
    - \( CH = 2.402 \text{ GHz} + k \text{ MHz} \), \( k=0..78 \)
    - 1,600 hops/sec
    - GFSK modulation: 1Mb/s symbol rate
      - \( CH-115\text{khz} \) (binary 0), \( CH+115\text{khz} \) (binary 1)
    - PTx: \( 0\text{dBm} \) (1mW) radio (up to \( 20\text{dBm} \))

The Baseband layer

- **Baseband (BB)**
  - TDD, frequency hopping physical layer
  - Device Inquiry and Paging
  - Two type of links: SCO and ACL
  - multiple packet types
    - multiple data rates, with/without FEC
The Baseband layer

- **Baseband (BB)**
  - point to point channel
  - Piconet
    - 1 master
    - max 7 active slaves
    - 1Mb/s per piconet
    - hopping sequence given by master Id
  - “Low-level” packet definition
  - channel sharing

The Bluetooth network topology

- **Radio designation**
  - Connected radios can be master or slave
  - Radios are symmetric (same radio can be master or slave)

- **Piconet**
  - Master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet
  - Each piconet has maximum capacity
  - Unique hopping pattern/ID

- **Scatternet**
  - Piconets can coexist in time and space
The piconet

- All devices in a piconet hop together
  - To form a piconet: master gives slaves its clock and device ID
  - Hopping pattern determined by device ID (48-bit)
  - Phase in hopping pattern determined by clock

Piconet Addressing
- Bluetooth device address (BD_ADDR): 48 bit IEEE MAC Address
- Active Member Address (AM_ADDR): 32-bit active slave, all-zero broadcast
- Parked Member Address (PM_Addr): 8-bit parked slave

The baseband states: piconet formation

- **Standby**
  - Waiting to join a piconet

- **Inquire**
  - looking about radios to connect to

- **Page**
  - Connect to a specific inquired radio

- **Connected**
  - Actively on a piconet (master or slave)

- **Park/Hold**
  - Low Power connected states
Paging sequence

A: slave acquires half-slot synchronization
B: slave acquires full-slot synchronization
C: slave capable to join master’s piconet
D: piconet communications start with master Tx slot

Page and Inquire Scans

• A radio must be enabled to accept pages or inquires
• Consumes 18 slots (18*0.625=11ms) every 1.25 sec. (or so) for each scan
• Inquiry has unique device address (all BT radio use)
  • Unique set of “Inquiry” hop frequencies (32 predefined channels)
  • Any device can inquire by paging the Inquiry address
  • Correlator hit causes slave to respond with FHS packet (Device ID and Clock)
Inquire Summary

- Paging radio Issues page packet with Inquire ID

- Any radio doing an Inquire scan will respond with an FHS packet
  - FHS packet gives Inquiring radio information to page
    - Device ID
    - Clock
  - If there is a collision then radios wait a random number of slots before responding to the page inquire

- After process is done, Inquiring radio has Device IDs and Clocks of all radios in range

Inquiring for Radios

- Radio Wants to find other radios in the area
Radio Wants to find other radios in the area
- Radio A issues an Inquire (pages with the Inquire ID)
- Radios B, C and D are doing an Inquire Scan

Radio B recognizes Inquire and responds with an FHS packet
- Has slave’s Device ID and Clock
Inquiring for Radios

Radio A Wants to find other radios in the area
  • Radio A Issues an Inquire (again)

Radios C and D respond with FHS packets
  • As radios C & D respond simultaneously packets are corrupted and Radio A won’t respond
  • Each radio waits a random number of slots and listens
Inquiring for Radios

- Radio A Wants to find other radios in the area
  - Radio A Issues an Inquire (again)

Radios C respond with FHS packets
Inquiring for Radios

- Radio A Wants to find other radios in the area
  - Radio A Issues an Inquire (again)

Radios D respond with FHS packets
**Inquiring for Radios**

- Radio A now has information of all radios within range.

**Master Paging a Slave**

- **Master pages slave (packet has slave ID) at slave page frequency (1 of 32)**
  - Master sends page train of 16 most likely frequencies in slave hop set
    - Slave ID sent twice a transmit slot on slave page frequency
    - Master listens twice at receive slot for a response
  - If misses, master sends second train on remaining 16 frequencies

- **Slave listens for 11 ms (page scan)**
  - If correlater triggers, slave wakes-up and relays packet at response frequency
  - Master responds with FHS packet (provides master's Device ID and Clock)
  - Slave joins piconet
Master Paging a Slave

- Paging assumes master has slaves *Device ID* and an idea of its *Clock*

---

Master Paging a Slave

- A pages C with C’s *Device ID*
Master Paging a Slave

- C Replies to A with C’s Device ID

- A sends C its Device ID and Clock (FHS packet)
Master Paging a Slave

- A connects as a master to C

Paging Procedure

- Each slave page scans on unique sequence of 32 channels $f_k$
  - Master pages 16 most likely channels for entire sleep period (nominally 1.25 seconds)
- If clocks are off, then second train sent on last 16 frequencies for entire sleep period
Scatternet Formation

- Scatternet Formation
  - Gateway node management and synchronization?

Baseband packet

- (68|72) bits
- 54 bits
- 0-2744 bits

- access code
- header
- payload

Synchronization, Identification, Signalling

- addressing (3 bit)
- packet type (4 bit)
- flow control (1 bit)
- ARQ (1 bit)
- sequencing (1 bit)
- Header integrity (8 bit)
- Total: 18 bit + 1/3 FEC = 54 bit

Voice: No retry, FEC optional

Data: CRC, ARQ, FEC optional
Baseband packet transmission

- **Polling-based (TDD) packet transmissions**
  - 1 slot: 0.625msec (max 1600 slots/sec)
  - master/slave slots (even-/odd-numbered slots)
  - polling: master always "polls" slaves

Baseband packet links

- **Synchronous connection-oriented (SCO) link**
  - "circuit-switched": periodic single-slot packet assignment
  - symmetric 64Kbps full-duplex
  - Up to 3 for one master and 2-3 for one slave

- **Asynchronous connection-less (ACL) link**
  - packet switching, asymmetric bandwidth
    - variable packet size (1-5 slots)
    - max. 721 kbps (57.6 kbps return channel), 108.8 - 432.6 kbps (symmetric)
### Baseband packet types

<table>
<thead>
<tr>
<th>ID*</th>
<th>Voice (SIG)</th>
<th>Data/voice packets</th>
</tr>
</thead>
<tbody>
<tr>
<td>Null</td>
<td>10 info B</td>
<td>2/3 FEC no FEC</td>
</tr>
<tr>
<td>Poll</td>
<td>20 info B</td>
<td>2/3 FEC no FEC</td>
</tr>
<tr>
<td>FHS</td>
<td>30 info B</td>
<td>2/3 FEC no FEC</td>
</tr>
<tr>
<td>DM1</td>
<td>2/3 FEC</td>
<td>2/3 FEC no FEC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>1/3 FEC no FEC</td>
</tr>
<tr>
<td></td>
<td></td>
<td>no FEC</td>
</tr>
</tbody>
</table>

### The Link Management layer

- **Link Management (LM)**
  - piconet management
  - link configuration: link properties
    - polling intervals set-up
    - SCO link set-up
    - low power mode set-up (parked slaves)
  - QoS
  - Packet type
  - security
    - encryption/authentication
Bluetooth security features

- **Initialization**
  - shared key(s): authentication and cyphering
  - PIN entry by user

- **Authentication of remote device**
  - based on link key (128 bit)
  - challenge/response (shared secret)
  - may be performed in both directions

- **Encryption of payload data**
  - stream cipher algorithm ($\leq$ 128 Bit)
    - Safer+ (Massey and Rueppel)
  - affects all traffic on a link

---

Key generation and usage

- PIN
  - $E_2$
  - Link Key
    - $E_3$
    - Encryption Key

- User Input (Initialization)
  - Link Key
    - Permanent Storage
      - $E_2$
  - (possibly)
    - Temporary Storage
      - $E_3$
      - Encryption Key

© 2005 Luciano Bononi Sistemi e Reti Wireless
Bluetooth authentication and encryption

user enters common PIN (initialization)

Dev_A

Dev_B

temporary link key
generation algorithm

temporary link key

initial authentication

temporary link key

trust device?

no

yes

trust is a mutual relation

in future authentications

use permanent link key

generate and store permanent link key

encrypt link?

no

yes

encryption is a mutual operation

encrypt link?

no

yes

generate temporary encryption link

The LLC and Adaptation layer

- Link Layer Control & Adaptation (L2CAP)
  - A simple data link protocol on top of the baseband
    - connection-oriented & connectionless
    - protocol multiplexing
    - segmentation & reassembly
    - QoS flow specification per connection (channel)
    - group abstraction
The middleware protocols

- Host Controller Interface (HCI)
  - provides a common interface between the Bluetooth host and a Bluetooth module
    - Interfaces in spec 1.0: USB; UART; RS-232
Middleware protocols

- **Service Discovery Protocol (SDP)**
  - Defines an inquiry/response protocol for discovering services
    - Searching for and browsing services
  - Defines a service record format
    - Information about services provided by attributes
    - Attributes composed of an ID (name) and a value
    - IDs may be universally unique identifiers (UUIDs)

- **RFCOMM (based on GSM TS07.10)**
  - emulates a serial-port to support a large base of legacy (serial-port-based) applications
  - allows multiple “ports” over a single physical channel between two devices
  - similar to HDLC
Middleware protocols

- **Telephony Control Protocol Spec (TCS)**
  - call control (setup & release)
  - group management for gateway serving multiple devices

- **Legacy protocol reuse**
  - reuse existing protocols, e.g., IrDA’s OBEX, or WAP for interacting with applications on phones

LAN access point profile

- PPP: security, authentication, access control
- Efficiency
- Auto-configuration
IP over Bluetooth

BNEP: Bluetooth Network Encapsulation Protocol: Ethernet emulation over L2CAP

48 bit MAC address
BNEP frame encapsulation in L2CAP

e.g. other profiles

Synchronization

Headset

LAN access point

© 2005 Luciano Bononi Sistemi e Reti Wireless
The protocol scheme

The 802.15.1 standard
Summary

- Bluetooth is a global, RF-based (ISM band: 2.4 GHz), short-range, connectivity solution for portable, personal devices
  - it is not just a radio, it is an end-to-end solution

- The Bluetooth spec comprises
  - a HW & SW protocol specification
  - usage case scenario profiles and interoperability requirements

- IEEE 802.15.1 is working on standardizing the PHY and MAC layers in Bluetooth

- http://www.bluetooth.org