

# IEEE 802.15 (WPAN)

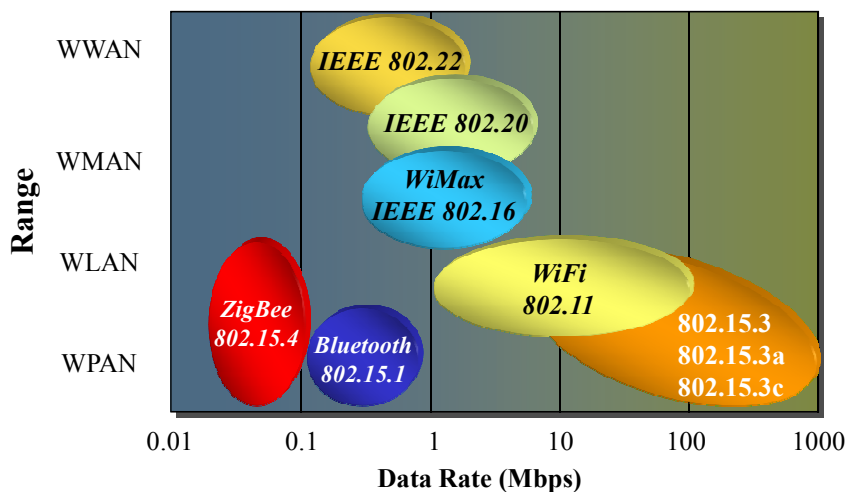
## (Bluetooth)

Luciano Bononi (bononi@cs.unibo.it)

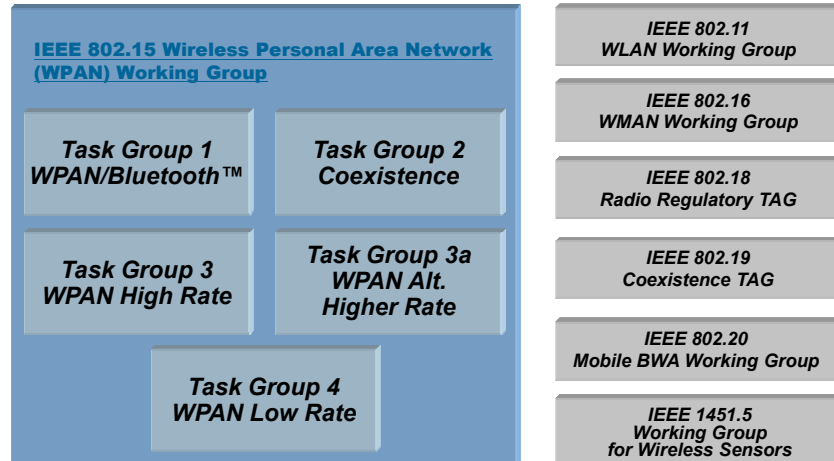
Figure Credits: some figures have been taken from slides found on the web by the following authors (in alphabetical order):

Pravin Bhagwat (acm.org), Chatschik Bisdikian (ibm.com), Tom Slep (ti)

### IEEE 802.xy Wireless Standards



## Working Group 802.15 and the Other IEEE Wireless Standards Areas



© 2005 Luciano Bononi

Sistemi e Reti Wireless

3

## 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.*

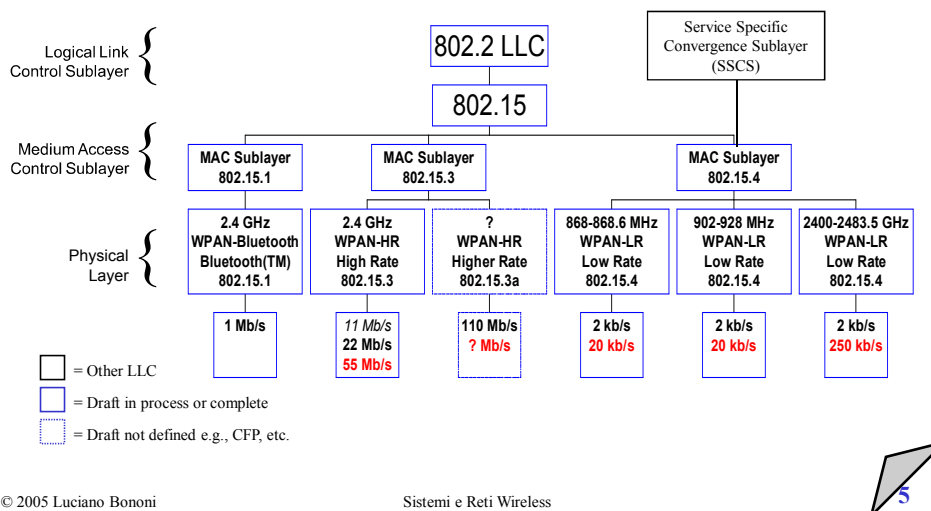
*The latest status of 802.15 and other IEEE802 activities is available at <http://standards.ieee.org/802news/>.*

© 2005 Luciano Bononi

Sistemi e Reti Wireless

4

## 802.15 WG is developing 3 MACs and 5 PHYs, TG3a is the 6<sup>th</sup> 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 an informative annex high level behavioral ITU-T Z.100 Specification and Description Language (SDL) model for an integrated Bluetooth MAC Sublayer.

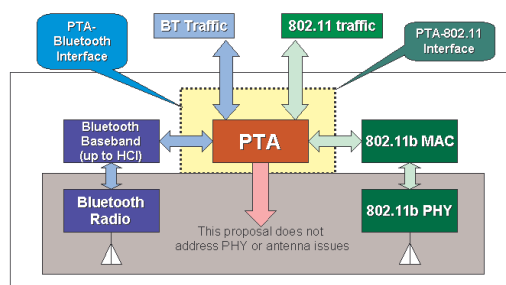
More info is available at <http://ieee802.org/15/pub/TG1.html>.

## 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>.



## 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.

More info is available at <http://ieee802.org/15/pub/TG3.html>.

## **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>.  
And <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>.

## WPAN Application Feature List

Consensus	Priority	
	High	Low
Strong	low cost low power small size packet data $\leq 1$ Mbps range $\leq 10$ m active devices $\leq 10$ manual auth/auto attach coexistence with 802.11	packet + isochronous encryption mobility $\leq 10$ mph gateway native IP
Weak	topology active devices 10 - 128 coexisting PANs 4-30	inter-pan connectivity

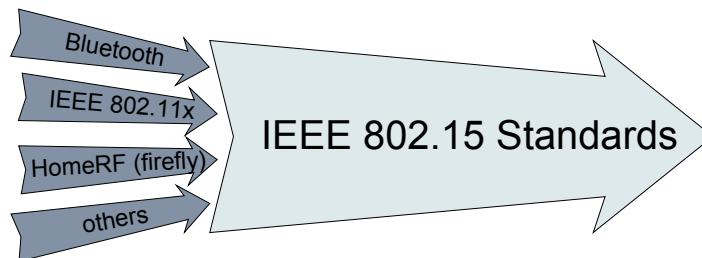
Source: doc.: IEEE 802.11-98/353 (Bruce Kraemer, Harris)

© 2005 Luciano Bononi

Sistemi e Reti Wireless

11

## Possible Coalescence of Standards



© 2005 Luciano Bononi

Sistemi e Reti Wireless

12

## WPAN usage model in existing Solutions

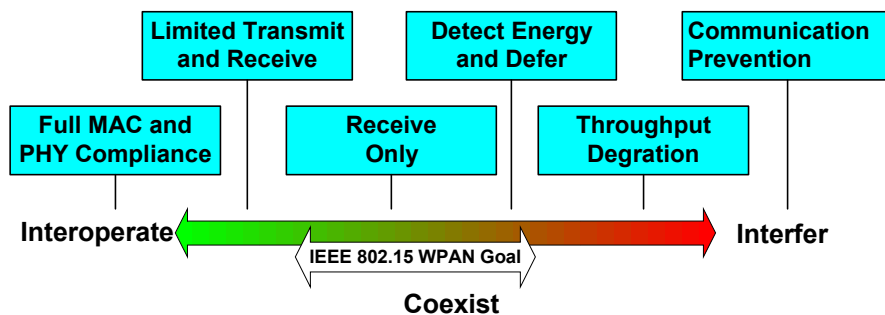
### Bluetooth

- 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



## 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**



## Bluetooth™

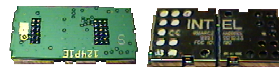


**Harald Blaataand “Bluetooth” II  
King of Denmark 940-981**

- Harald christianized the Danes
- Harald controlled Denmark and Norway

## Bluetooth

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



<b>Topology</b>	Supports up to 7 simultaneous links	Each link requires another cable
<b>Flexibility</b>	Goes through walls, bodies, cloths...	Line of sight or modified environment
<b>Data rate</b>	1 MSPS, 720 Kbps	Varies with use and cost
<b>Power</b>	0.1 watts active power	0.05 watts active power or higher
<b>Size/Weight</b>	25 mm x 13 mm x 2 mm, several grams	Size is equal to range. Typically 1-2 meters. Weight varies with length (ounces to pounds)
<b>Cost</b>	Long-term \$5 per endpoint	~ \$3-\$100/meter (end user cost)
<b>Range</b>	10 meters or less Up to 100 meters with PA	Range equal to size. Typically 1-2 meters
<b>Universal</b>	Intended to work anywhere in the world	Cables vary with local customs
<b>Security</b>	Very, link layer security, SS radio	Secure (its a cable)

## Wireless Positioning

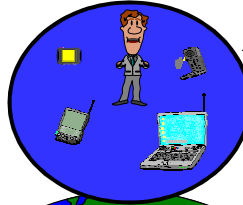
### Wireless LANs

#### 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

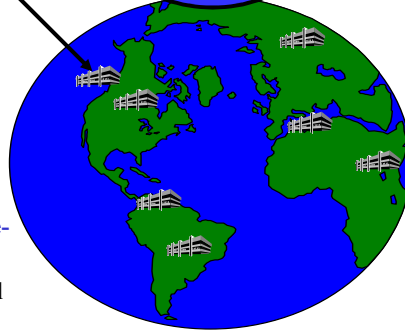
Voice AND Data

Low-cost

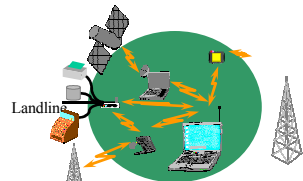
Small form factor

Many Co-located Nets

Universal Bridge



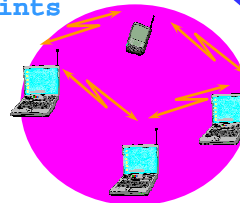
## Bluetooth: new applications



Data/Voice Access Points



Cable  
Replacement



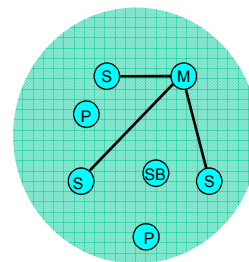
Personal Ad-  
hoc  
Connectivity

## Characteristics

- Operates in the **2.4 GHz** band at a data rate of **720Kb/s**.
- 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**.

## 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



M=Master P=Parked  
S=Slave SB=Standby

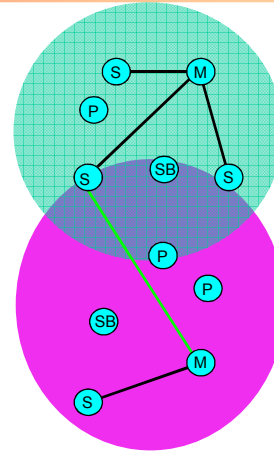
## What is a Scatternet?

•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**.

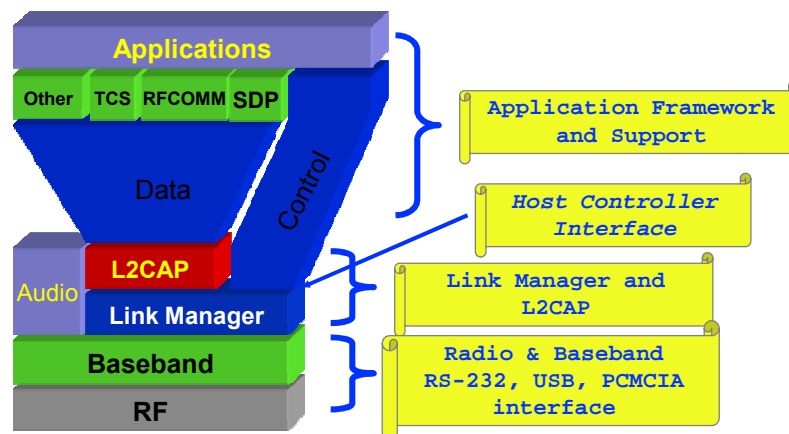
•Radios are **symmetric** (same radio can be master or slave)

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



M=Master  
S=Slave  
P=Parked  
SB=Standby

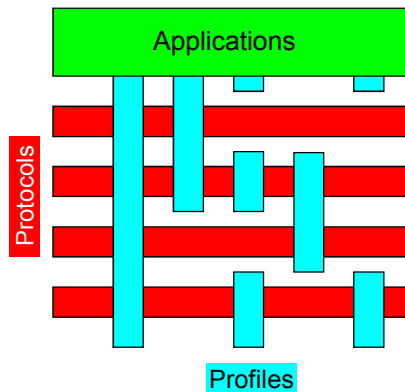
## The Bluetooth protocols: specifications



- 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



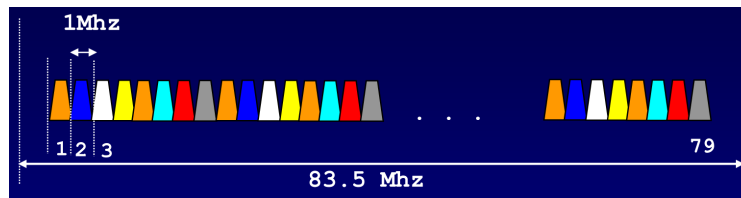
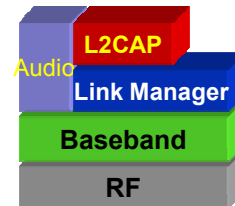
## Profiles (spec v.1)

- **Generic Access Profile**
  - Service Discovery Application Profile
  - Serial Port Profile
    - Dial-up Networking Profile
    - Fax Profile
    - Headset Profile
    - LAN Access Profile (using PPP)
    - Generic Object Exchange Profile
      - File Transfer Profile
      - Object Push Profile
      - Synchronization Profile
  - *TCS\_BIN-based profiles*
    - Cordless Telephony Profile
    - Intercom Profile

## The Radio Frequency (PHY RF) layer

### Radio (RF)

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



© 2005 Luciano Bononi

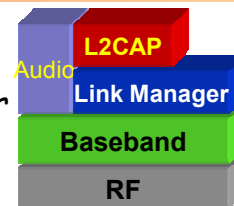
Sistemi e Reti Wireless

27

## 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



© 2005 Luciano Bononi

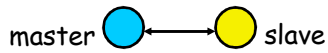
Sistemi e Reti Wireless

28

## The Baseband layer

### Baseband (BB)

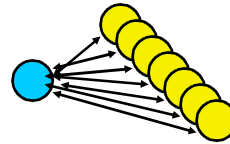
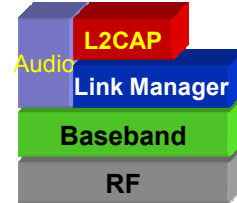
- point to point channel



- 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

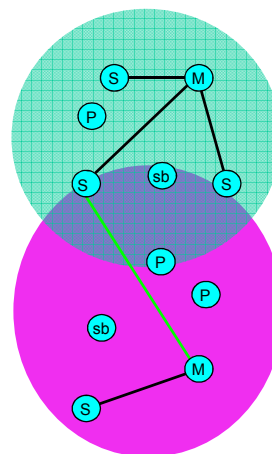
- Connected radios can be master or slave
- Radios are symmetric (same radio can be master or slave)

### Piconet

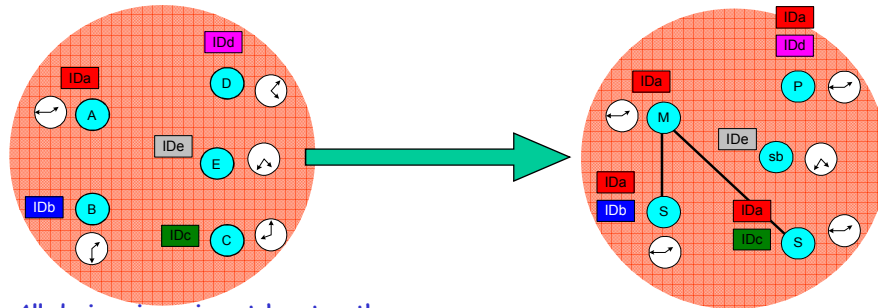
- Master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet
- Each piconet has maximum capacity
- Unique hopping pattern/ID

### 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): 3-bits active slave, all-zero broadcast
  - Parked Member Address (PM\_Addr): 8-bits parked slave

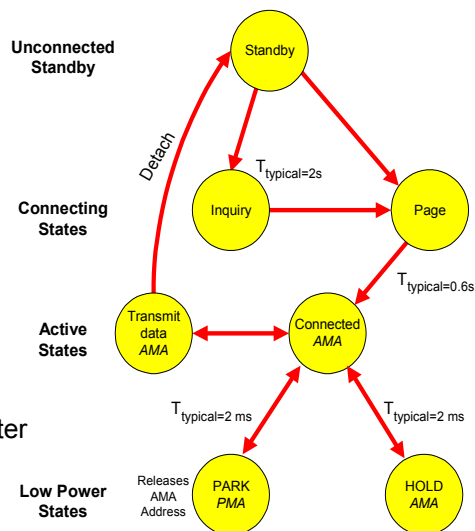
© 2005 Luciano Bononi

Sistemi e Reti Wireless

31

## 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



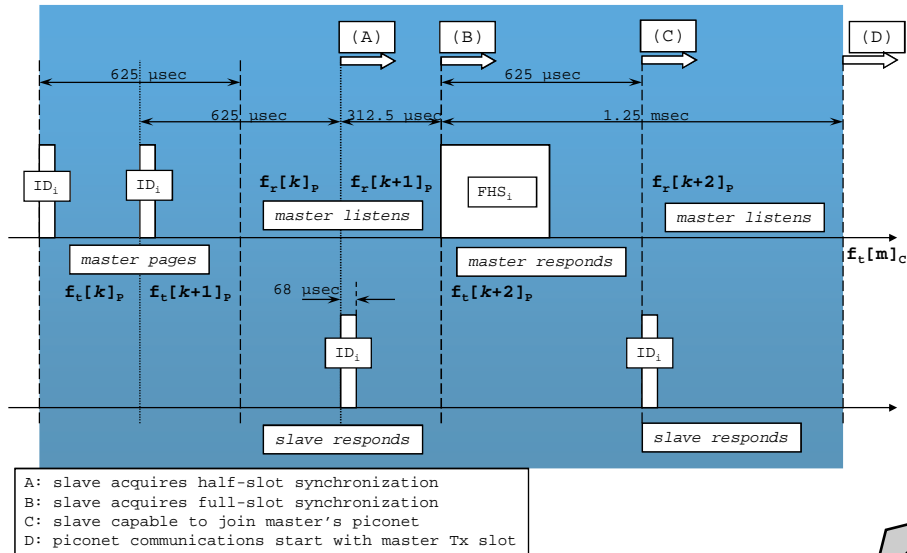
© 2005 Luciano Bononi

Sistemi e Reti Wireless

32



## Paging sequence

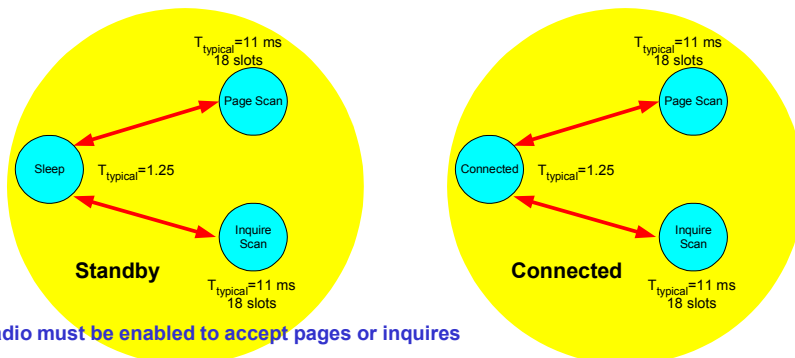


© 2005 Luciano Bononi

Sistemi e Reti Wireless

33

## Page and Inquire Scans



- A radio must be enabled to accept pages or inquires

- Consumes 18 slots ( $18 \cdot 0.625 = 11 \text{ ms}$ ) 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)


© 2005 Luciano Bononi

Sistemi e Reti Wireless

34

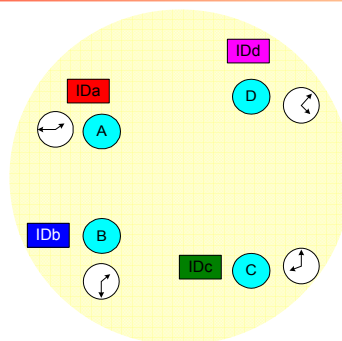
## Inquire Summary

---

- **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** IDa
    - **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**

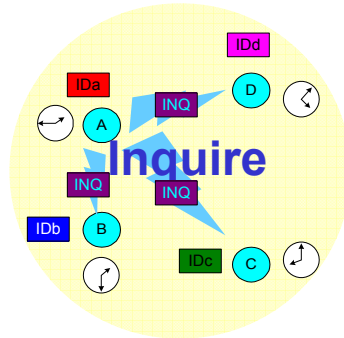
## Inquiring for Radios

---



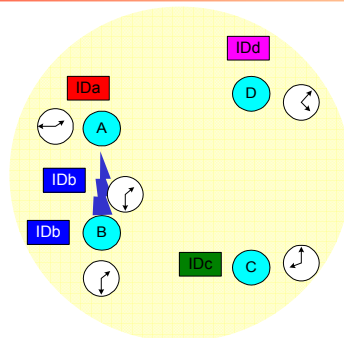
- **Radio Wants to find other radios in the area**

## Inquiring for Radios



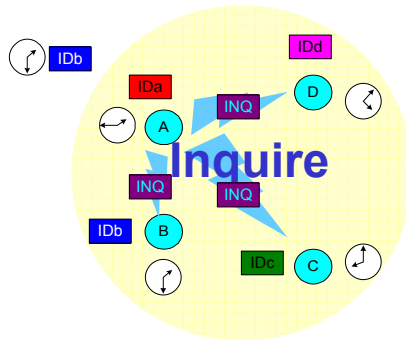
- **Radio Wants to find other radios in the area**
  - Radio A issues an Inquire (pages with the Inquire ID)
  - Radios B, C and D are doing an Inquire Scan

## Inquiring for Radios



- **Radio B recognizes Inquire and responds with an FHS packet**
  - Has slave's *Device ID* and *Clock*

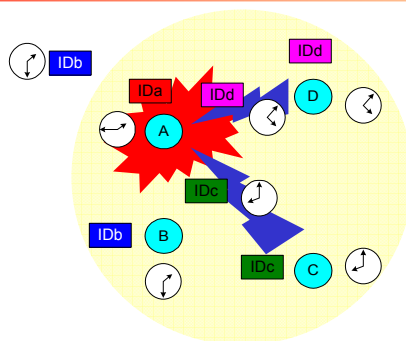
## Inquiring for Radios



Radio A Wants to find other radios in the area

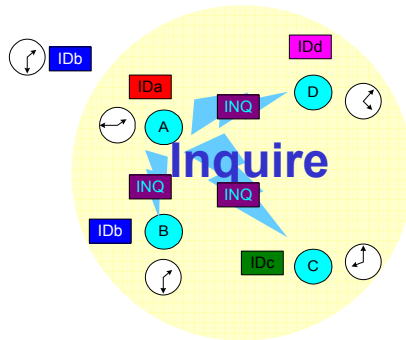
- Radio A Issues an Inquire (again)

## Inquiring for Radios



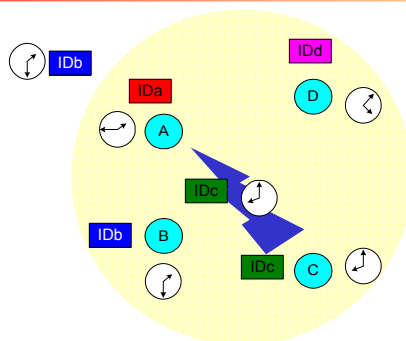
- **Radios C and D respond with FHS packets**
  - As radios C & D respond simultaneously packets are corrupted and Radio A won't respond
  - Each radio waits a random number of slots and listens

## Inquiring for Radios



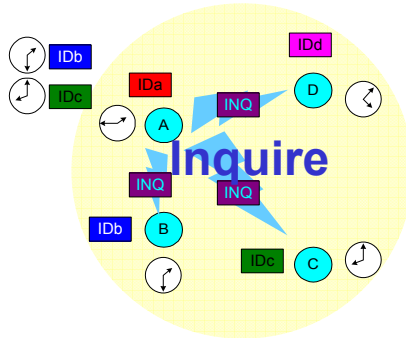
- **Radio A Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)

## Inquiring for Radios



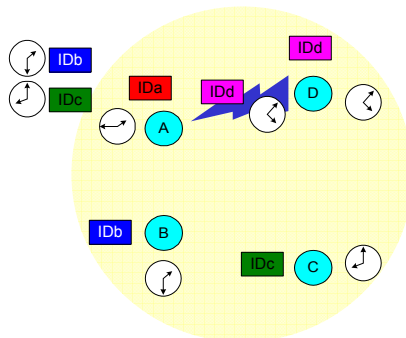
- **Radios C respond with FHS packets**

## Inquiring for Radios



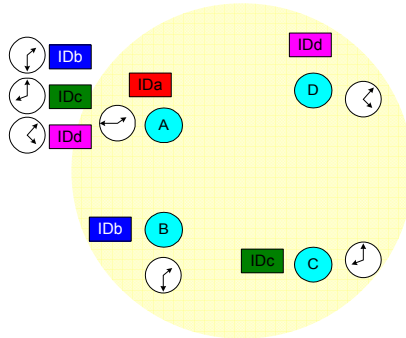
- Radio A Wants to find other radios in the area
  - Radio A Issues an Inquire (again)

## Inquiring for Radios



- Radios D respond with FHS packets

## Inquiring for Radios

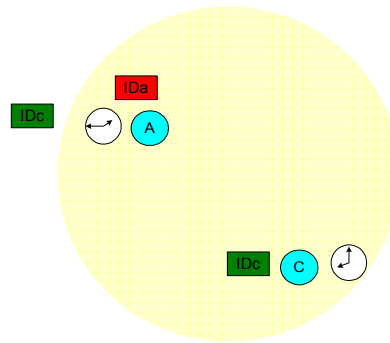


- Radio A now has information of all radios within range

## Master Paging a Slave

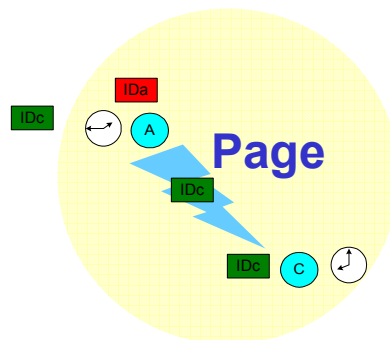
- Master pages slave (packet has slave ID) at slave page frequency (1 of 32)
  - Master sends page train of 16 most likely frequencies in slave hop set
    - Slave ID sent twice a transmit slot on slave page frequency
    - Master listens twice at receive slot for a response
  - If misses, master sends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

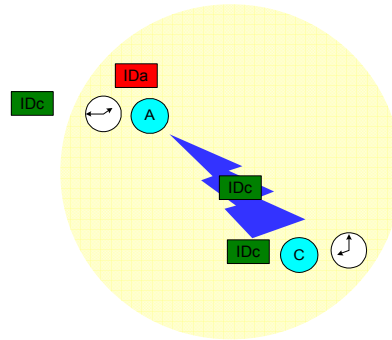
## Master Paging a Slave



- A pages C with C's *Device ID*

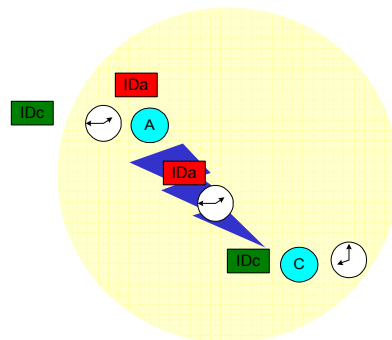


## Master Paging a Slave



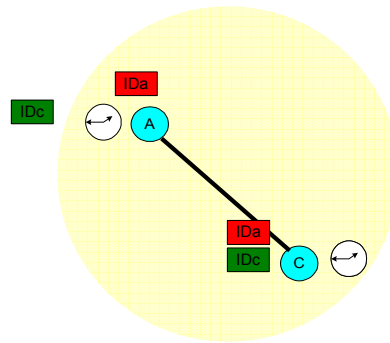
- C Replies to A with C's Device ID

## Master Paging a Slave



- A sends C its Device ID and Clock (FHS packet)

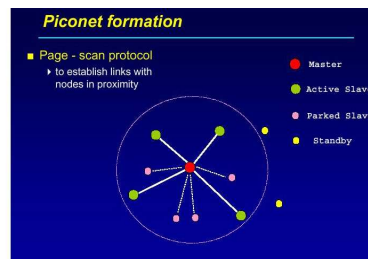
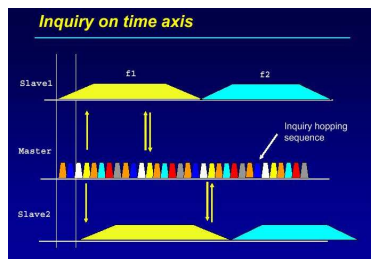
## Master Paging a Slave



- A connects as a master to C

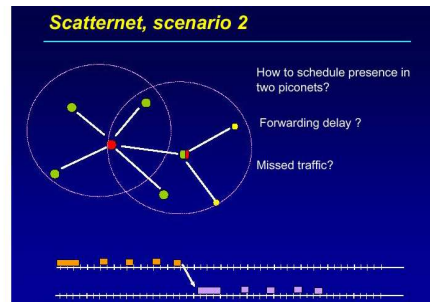
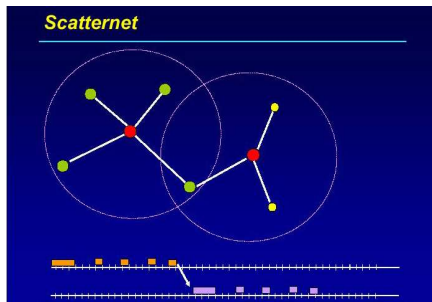
## Paging Procedure

- 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?

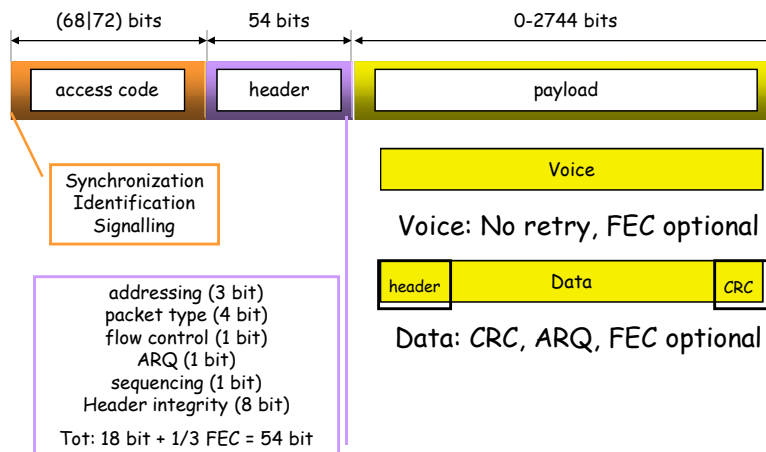


© 2005 Luciano Bononi

Sistemi e Reti Wireless

53

## Baseband packet



© 2005 Luciano Bononi

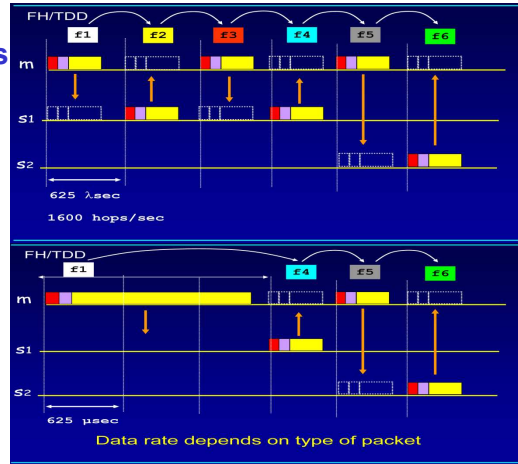
Sistemi e Reti Wireless

54

## 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



© 2005 Luciano Bononi

Sistemi e Reti Wireless

55

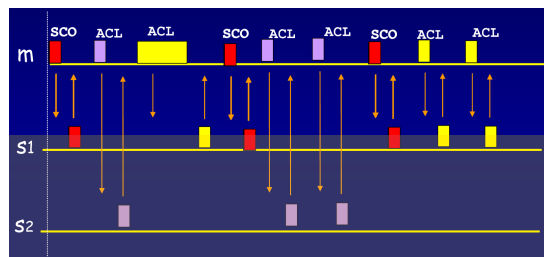
## Baseband packet links

### ▪ 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)

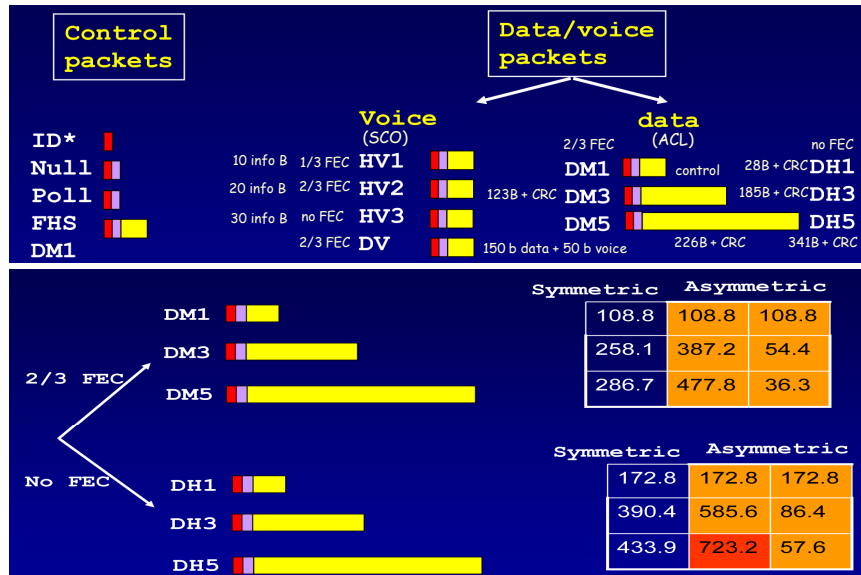


© 2005 Luciano Bononi

Sistemi e Reti Wireless

56

## Baseband packet types



© 2005 Luciano Bononi

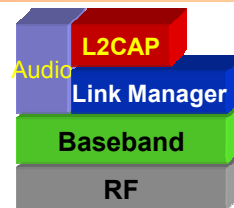
Sistemi e Reti Wireless

57

## 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



© 2005 Luciano Bononi

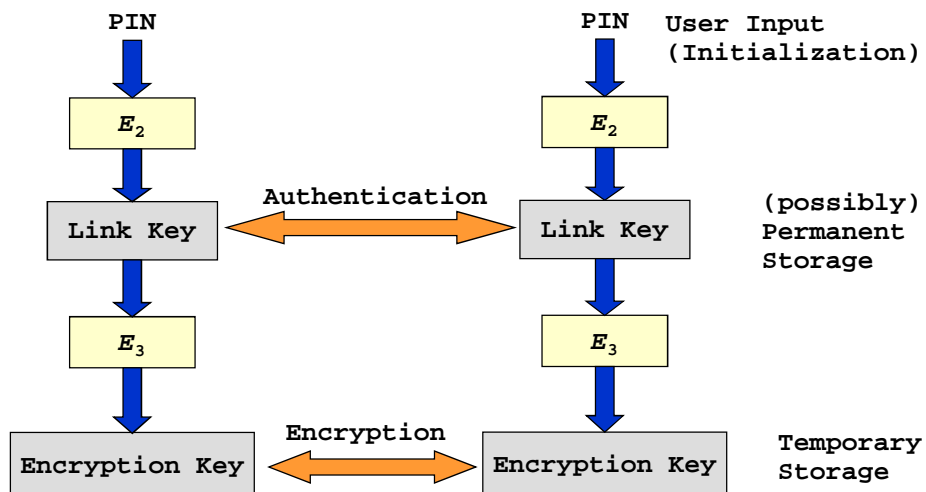
Sistemi e Reti Wireless

58

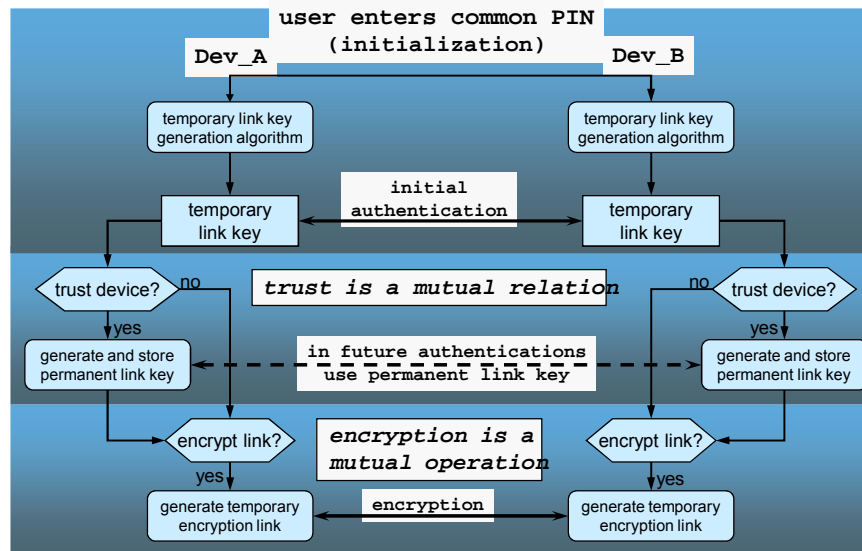
## Bluetooth security features

- **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



## Bluetooth authentication and encryption



© 2005 Luciano Bononi

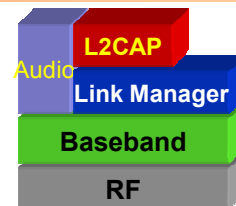
Sistemi e Reti Wireless

61

## 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

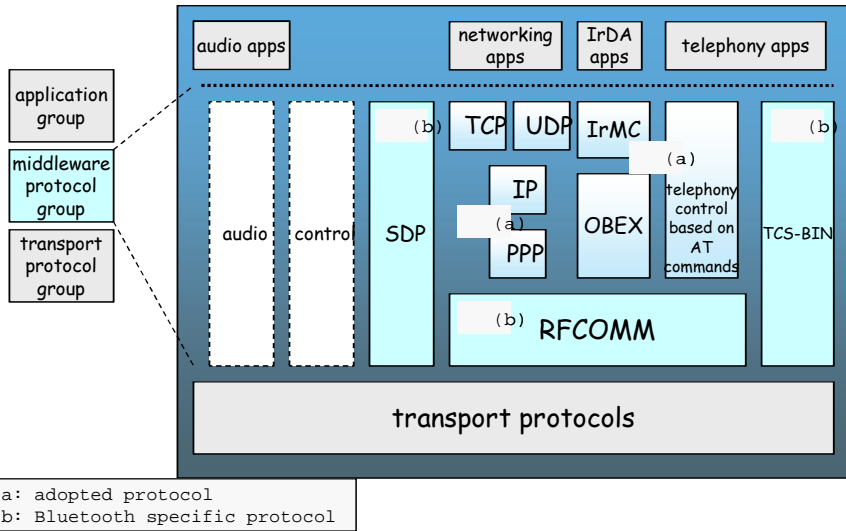


© 2005 Luciano Bononi

Sistemi e Reti Wireless

62

## The middleware protocols



© 2005 Luciano Bononi

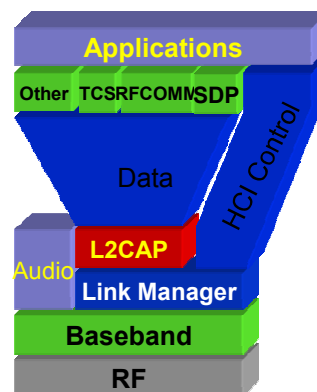
Sistemi e Reti Wireless

63

## 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



© 2005 Luciano Bononi

Sistemi e Reti Wireless

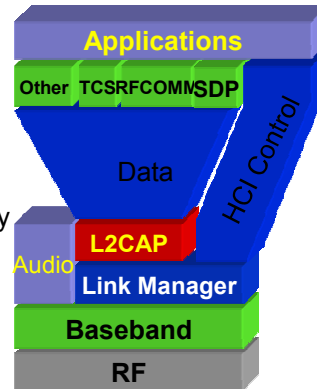
64



## Middleware protocols

### ▪ Service Discovery Protocol (SDP)

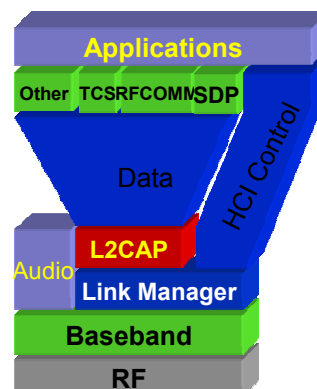
- Defines an inquiry/response protocol for discovering services
  - Searching for and browsing services
- Defines a service record format
  - Information about services provided by *attributes*
  - Attributes composed of an ID (name) and a value
  - IDs may be universally unique identifiers (UUIDs)



## Middleware protocols

### ▪ 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



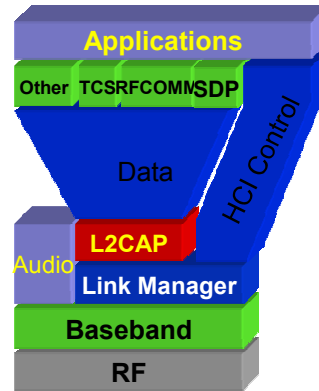
## Middleware protocols

### 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

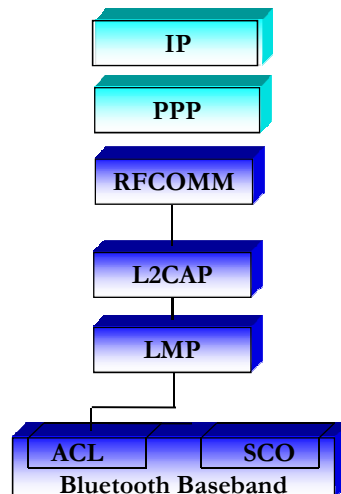


LAN  
Access  
Point

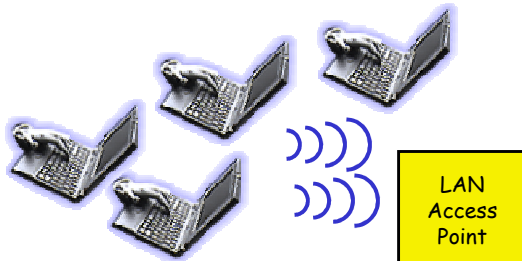
PPP: security, authentication,  
access control

Efficiency

Auto-configuration



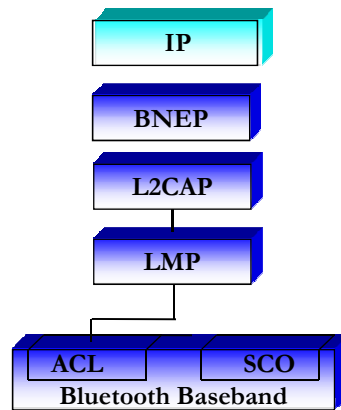
## IP over Bluetooth



BNEP: Bluetooth Network Encapsulation Protocol: Ethernet emulation over L2CAP

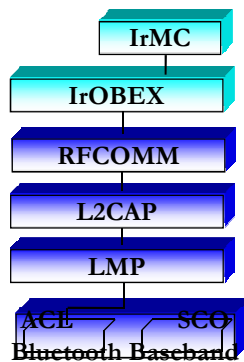
48 bit MAC address

BNEP frame encapsulation in L2CAP

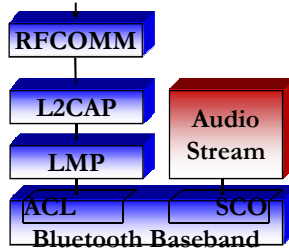


## e.g. other profiles

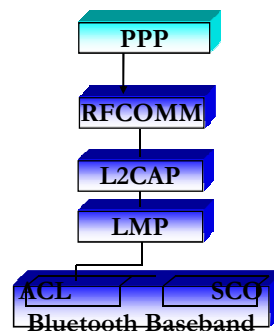
### Synchronization



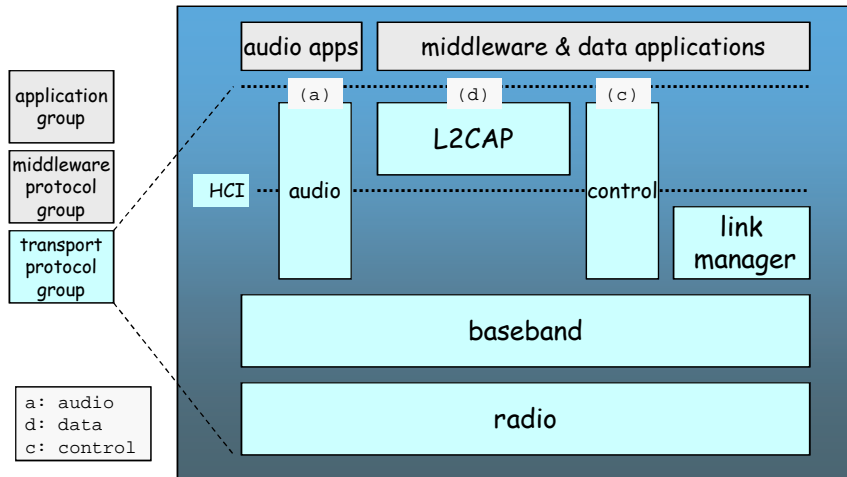
### Headset



### LAN access point



## The protocol scheme

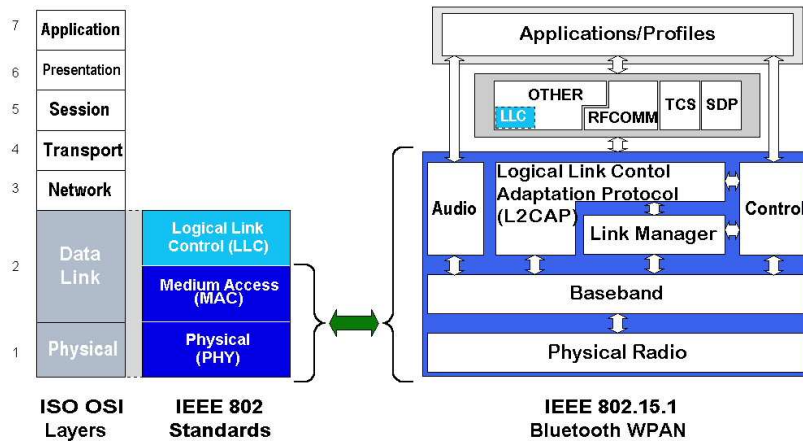


© 2005 Luciano Bononi

Sistemi e Reti Wireless

71

## The 802.15.1 standard



© 2005 Luciano Bononi

Sistemi e Reti Wireless

72

## 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>***