

Bluetooth

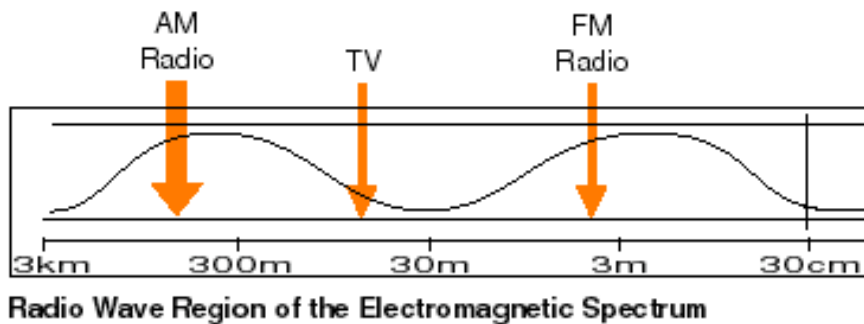
Larry Rudolph
Feb 16, 2006



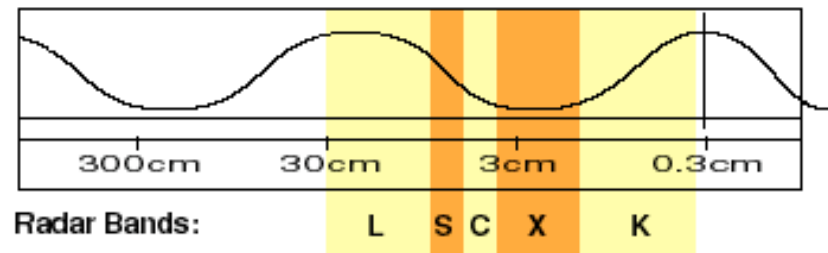
Albert Einstein, when asked to describe radio, replied:

"You see, wire telegraph is a kind of a very, very long cat. You pull his tail in New York and his head is meowing in Los Angeles. Do you understand this? And radio operates exactly the same way: you send signals here, they receive them there. The only difference is that there is no cat."

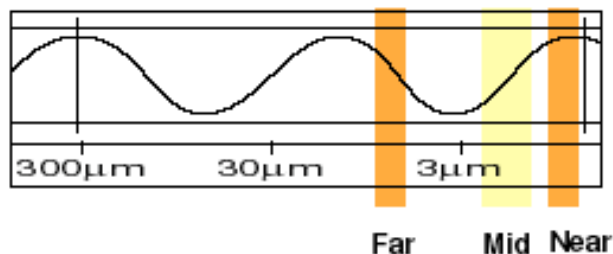
Wireless Digital Communication



Microwave region of the Electromagnetic Spectrum



Infrared Region of the Electromagnetic Spectrum



- IR (infrared)
 - low cost, low power, directional
 - OK for Remote control -- few bits
 - Failed for communication
 - laptop:printer, laptop:phone

Some Standards

- IR (infrared)
 - low cost, low power, directional
 - Short distances (about 1 meter)
 - OK for Remote control -- few bits
 - Failed for communication
 - laptop:printer, laptop:phone
- 802.11 and HomeRF
 - Higher bandwidth
 - more expensive, more power
 - voice not directly supported



History of Bluetooth



- King Harold Blatand, known as Bluetooth, was a Viking and King of Denmark 940-981, who united Denmark and Norway
- 1994 -- Technology was born in an Ericsson study on a wireless technology to link mobile phones and accessories

In the middle is Bluetooth



- “Bluetooth wireless technology is an **open specification** for a **low-cost, low-power, short-range** radio technology for **ad-hoc** wireless communication of **voice and data** anywhere in the world”



Bluetooth Vision

- Cable replacement, especially USB
- Local area network
- Automatic connecting of local devices
- Ability to blast advertisements at people who are physically near by.
- may kill success of bluetooth



Some details

- Unlicensed ISM band centered at 2.45 GHz
 - 79 channels; every 1 MHz (2.420 to 2.498)
- Mostly for devices within 10 meters
- Expect chips to cost \$5
- 2001: first retail products (10 million devices)
- 2003 specification 1.2 (70 million devices)
- Today, mostly in phones & headsets



Some more details

- Interference comes from
 - Wifi (802.11)
 - Microwave ovens
 - other bluetooth devices
- To minimize packet loss
 - Frequency hopping
 - Adaptive power control
 - Short data packets



A blonde went to the appliance store sale and found a bargain. "I want to buy this TV," she told the salesman.

"Sorry, we don't sell to blondes," he replied.

She hurried home and dyed her hair, then came back and again told the salesman, "I would like to buy this TV."

"Sorry, we don't sell to blondes," he replied.

"Damn, he recognized me," she thought. She went for a complete disguise this time, haircut and perm, new outfit, big sunglasses, then waited a few days before she again approached the salesman.

"I'd like to buy this TV."

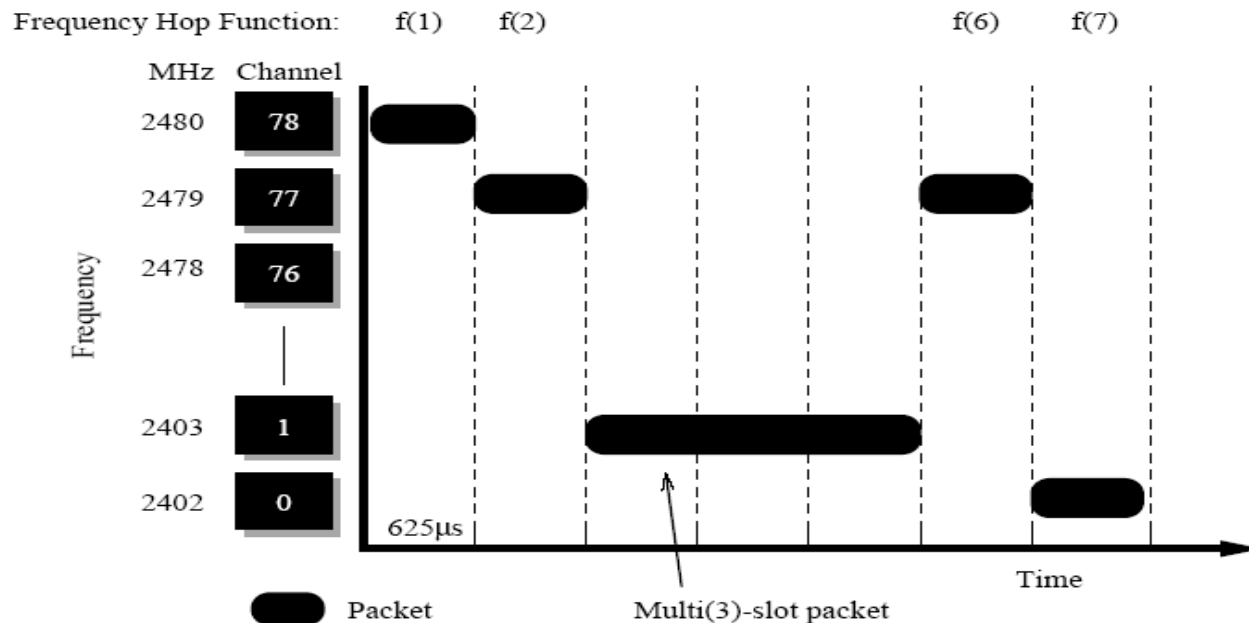
"Sorry, we don't sell to blondes," he replied.

Frustrated, she exclaimed "How do you know I'm a blonde?"

"Because that's a microwave," he replied.

Frequency Hopping

- Big thing about bluetooth is its hopping
 - 1600 hops per second, 625 microseconds / hop
- If there is interference, then just wait
- Makes it hard to eavesdrop (snoop)



Power & Packet Size

- Three power classes (defined as max power)
 - Classes (1,2,3): 1, 10, 100 mW
- Small packets (compared to ethernet)



BLUETOOTH SIG PROFILES

Profile = Interoperability Spec

GENERIC ACCESS PROFILE (GAP)

Service Discovery App Profile

Personal Area Networking Profile

Hard Copy Cable Replacement Profile

Human Interface Device Profile

Telephony Control Protocol Spec (TCS)

Cordless Telephony Profile

Intercom Profile

Serial Port Profile

Dial-Up Networking Profile

FAX Profile

Headset Profile

LAN Access Profile

Hands Free Profile

Generic Object Exchange Profile (GOEP)

File Transfer Profile

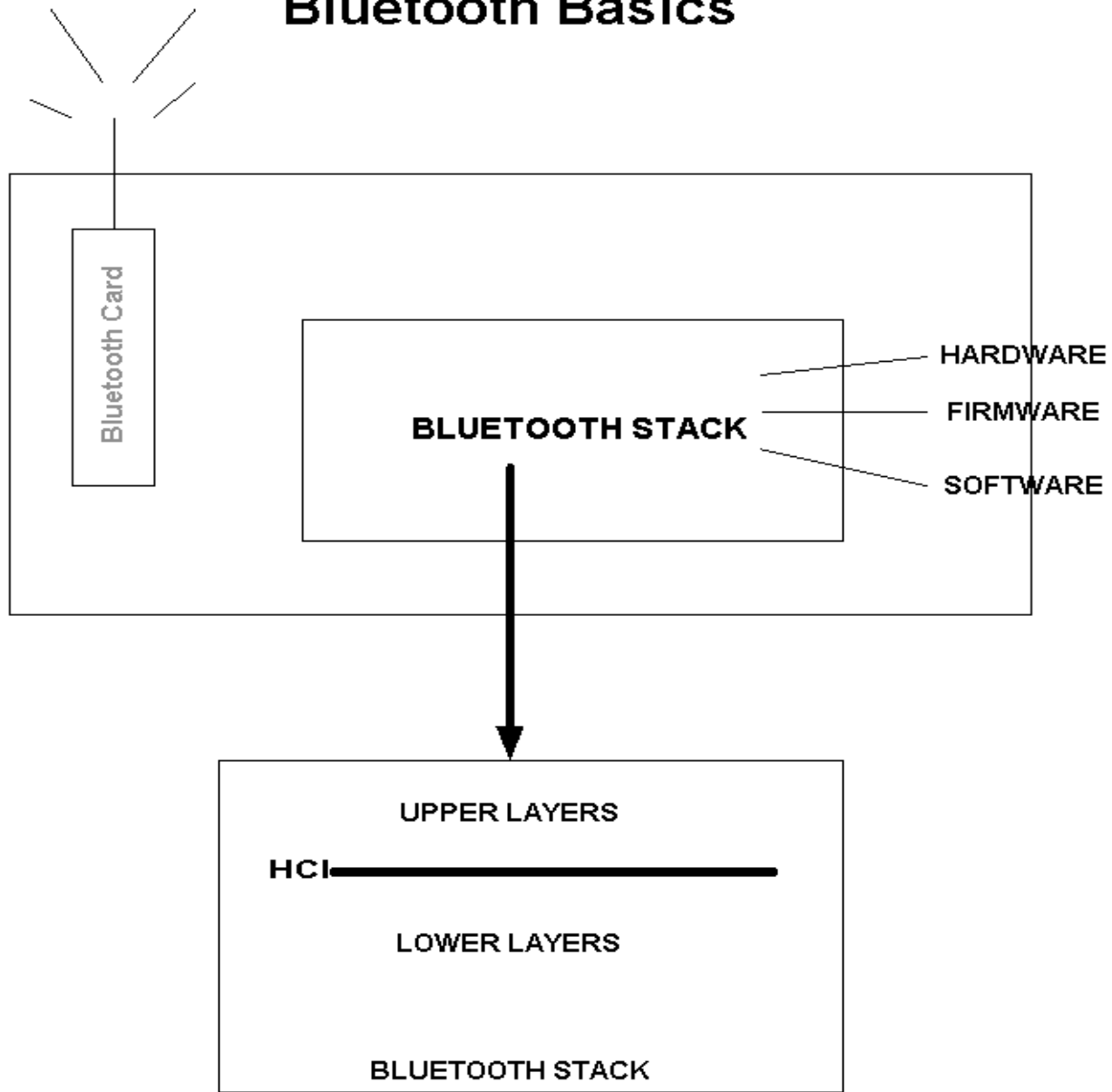
Object Push Profile

Synchronization Profile

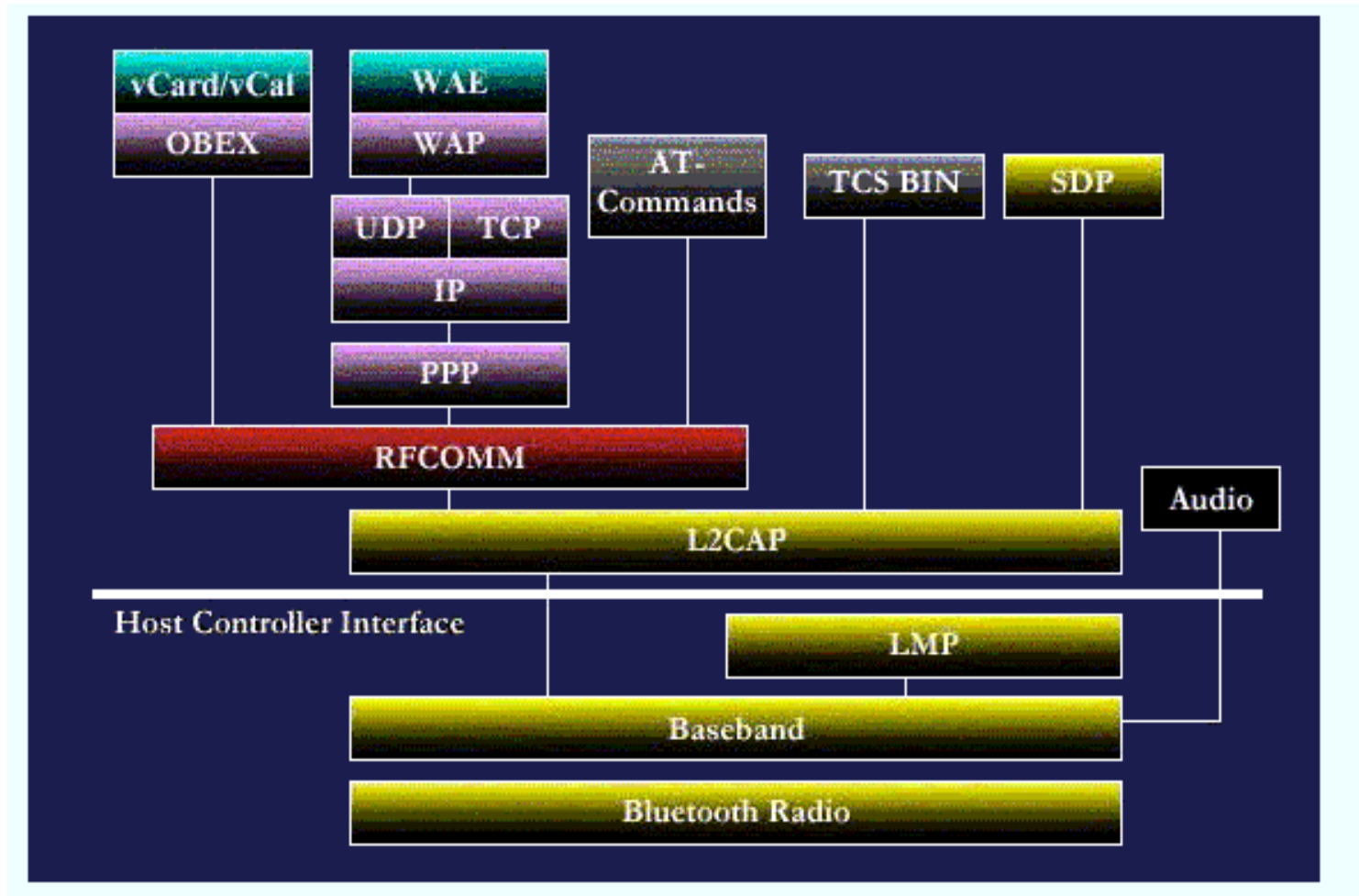
Basic Printing Profile







Bluetooth Basics



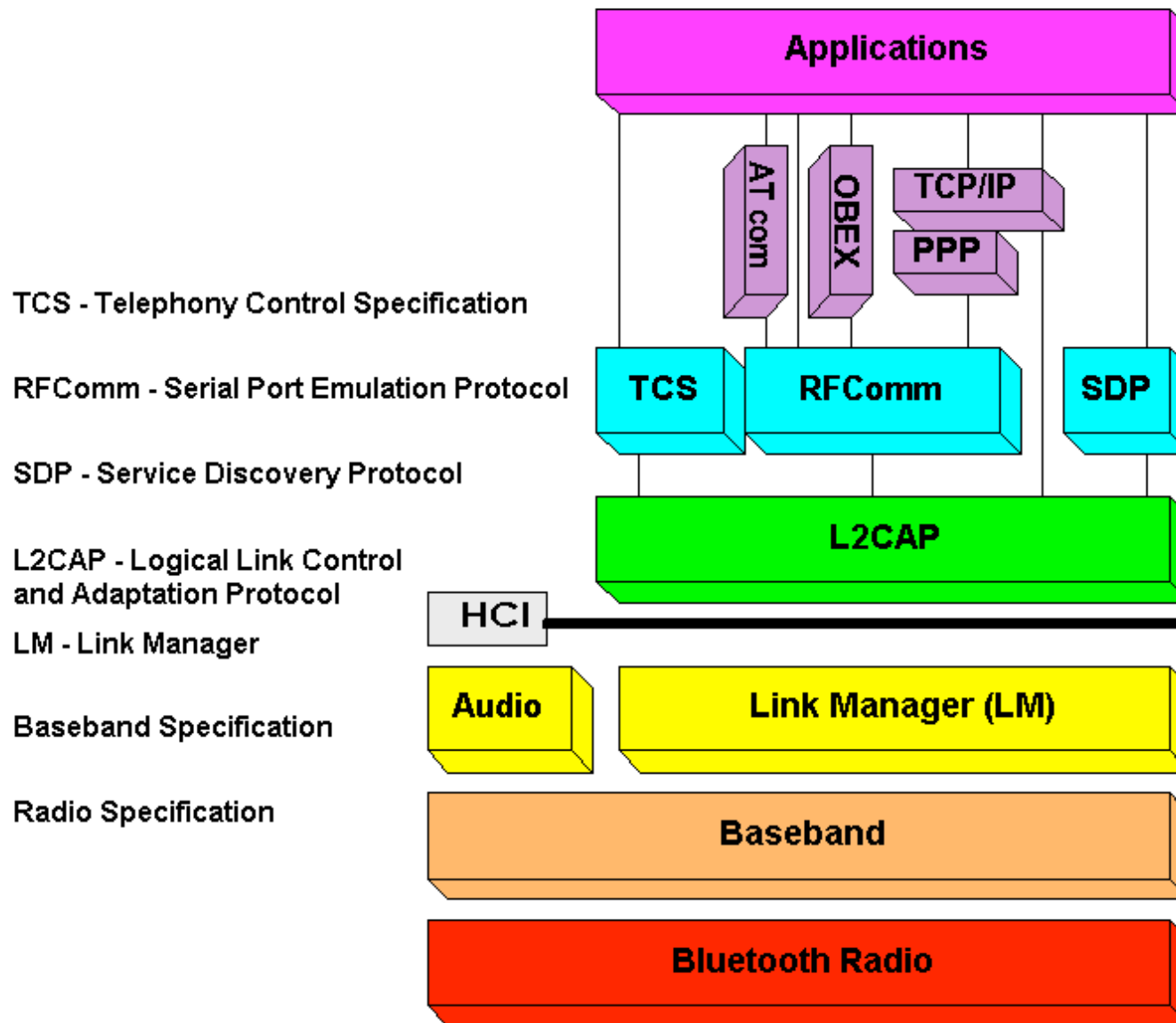
Protocol Stack



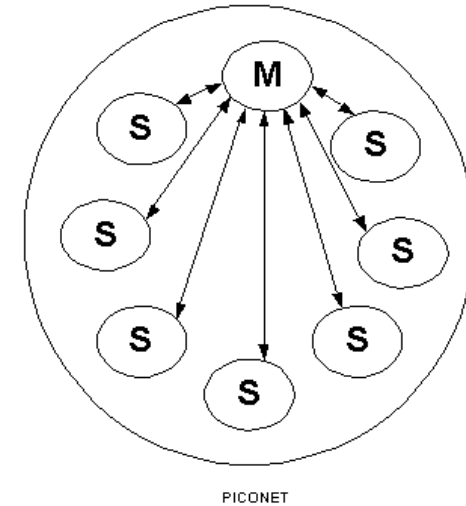
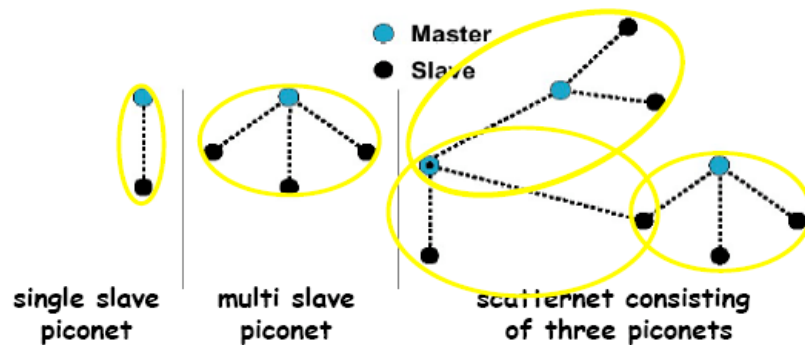
-  Core protocols
-  Cable replacement protocols

-  Telephony control protocols
-  Adopted protocols

Bluetooth Core Protocols



Piconet

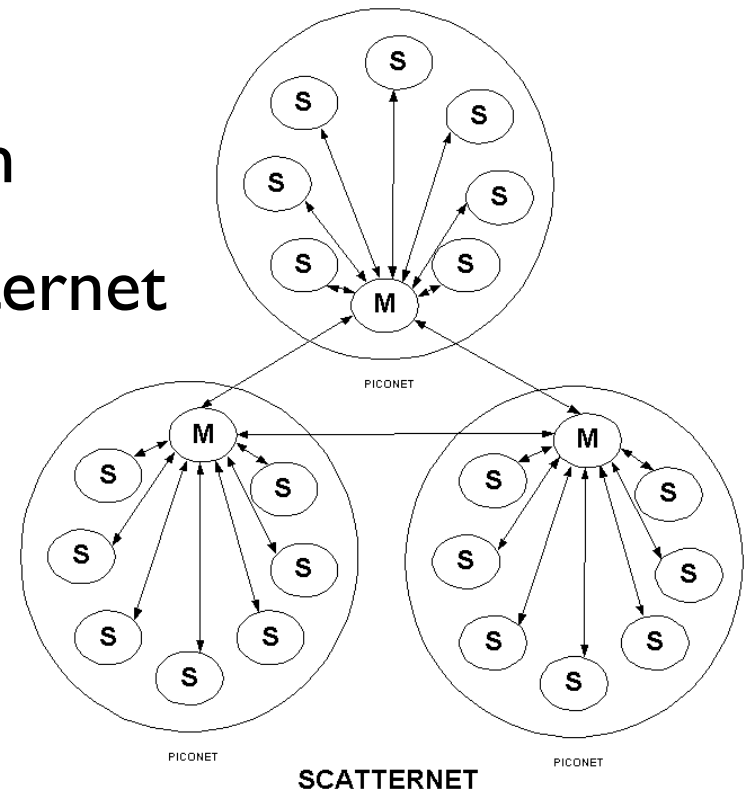


- 8 active devices (master & 7 slaves)
- All hop together
- Master ID and clock determines hop
 - pseudo-random, need seed and start



Scatternet

- inter-piconet communication
- can be 10 piconets in a scatternet
- ad-hoc, P2P network
- (rarely used these days)



The Link Manager

- Responsible for establishing, supervising and tear down connections and logical links.
- Link controller states introduced to carry out these tasks.
- States:
 - Standby
 - Inquiry / Inquiry Scan
 - Page / Page Scan
 - Connection

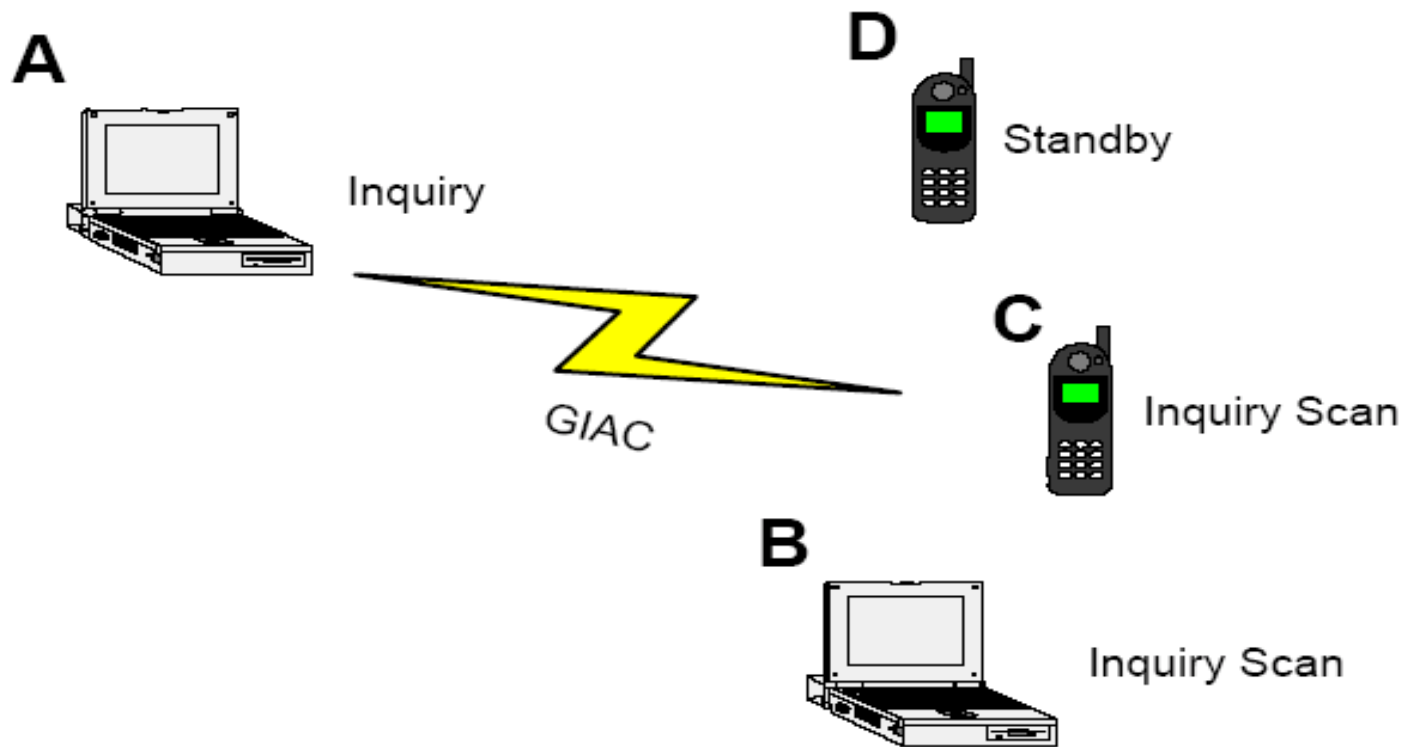


The Link Manager

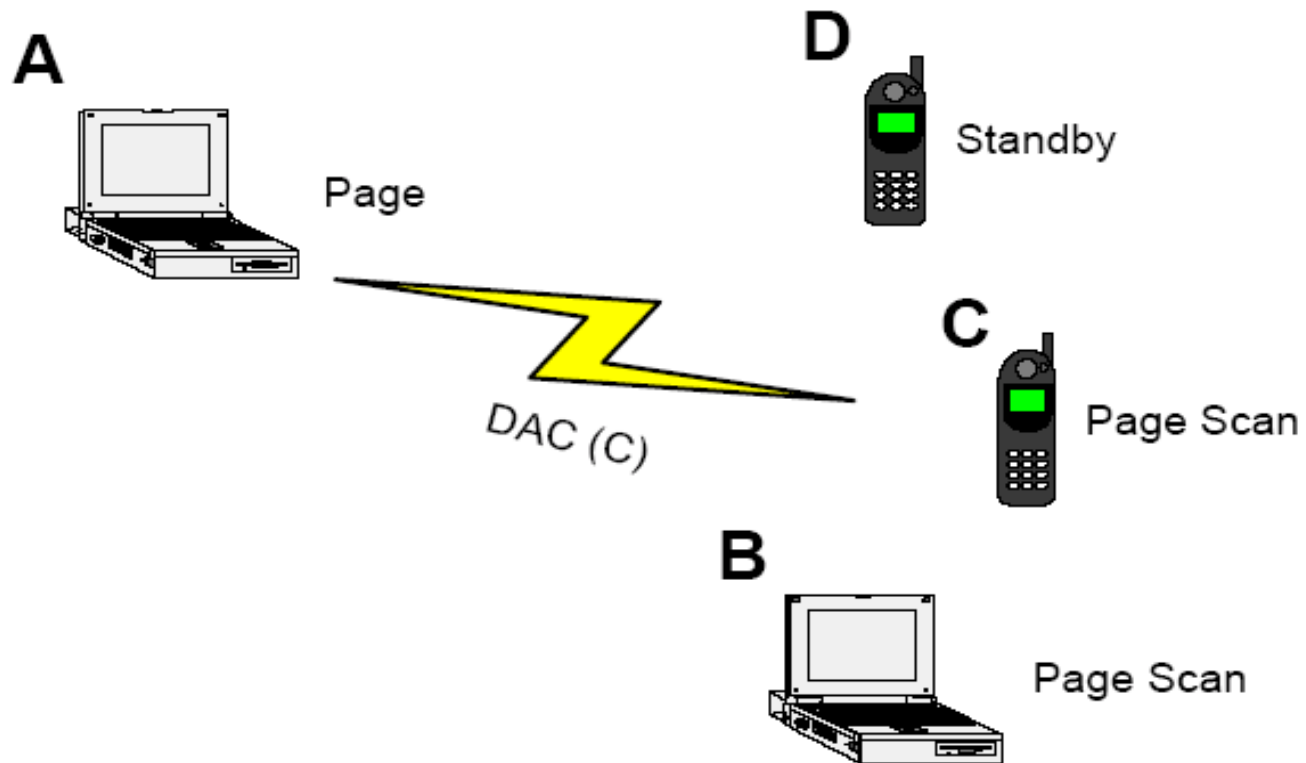
(cont.)

- Inquiry
 - Used to detect all devices in an unknown environment.
- Page / Page Scan
 - Describes how connection is established.
 - Have to know the address of the other devices. Is usually achieved through inquiry.
- Connection
 - Master and slaves are synchronized.
 - Connection is established.

Inquiry / Inquiry Scan



Page / Page Scan



Host Controller Interface (HCI)

- Provided to ease the partition of the Bluetooth Stack across two processors.
- Some systems will implement the baseband and link manager on the Bluetooth device and higher levels on the host processor.
- The HCI is provided as an interface between these parts.



Logical Link Control and Adaption (L2CAP)

- Deals with
 - multiplexing of different services
 - segmentation
 - reassembling of packets
 - Quality of Service

Profiles

- Provide interoperability between devices from different manufacturers for specific services and use cases.
- A profile defines
 - a selection of messages and procedures
 - gives an unambiguous description of communication between two devices.



Bluetooth in ad hoc networks

- Bluetooth network infrastructure is of dynamic ad-hoc type.
- It is constantly changing and depending on the movement of the devices.

Bluetooth in ad hoc networks (cont.)

- Temporary networks.
- Connect "on-the-fly".
- Small wireless network called "personal area network" (PAN).
- Provide voice, data, eliminate cables, bridge networks.
- Supports PDAs, mobile phones, printers, faxes, microphones.



Security

- Bluetooth provides security only over the radio link, from each device to all other devices.
- Three security specifications:
 - Confidentiality
 - Authentication
 - Authorization



Barbie Bluetooth Headset



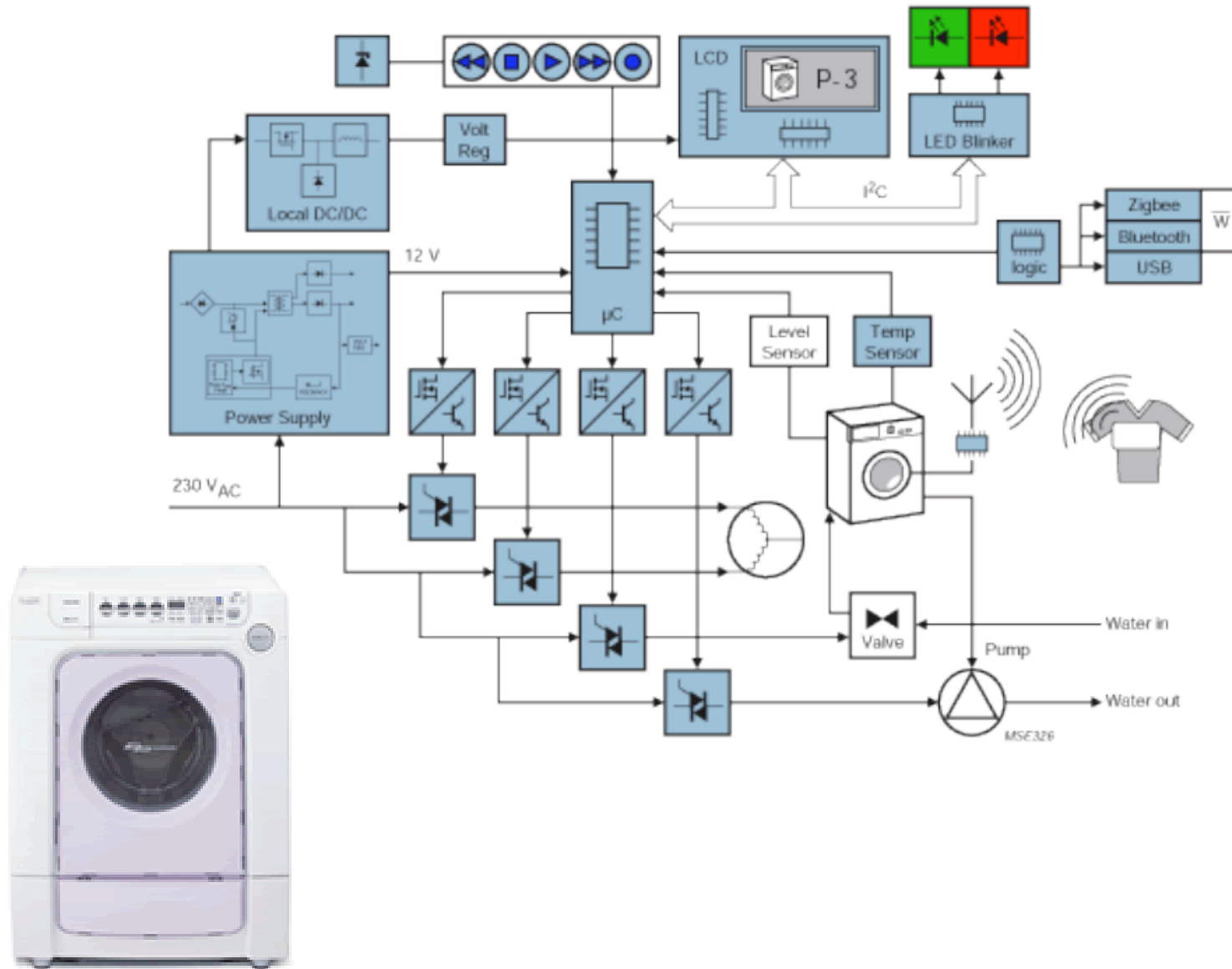
Found this on the gizmodo site:

“Some die-hard Trekkie would probably love to get his hands on this. A guy from New Zealand modeled this Barbie doll to a) look like a Star Trek crew member, and b) act as a Bluetooth handsfree headset. Yes, that’s right, it’s embedded with a Bluetooth headset. According to Ms. Barbie herself:”

You can use me to make and receive calls with Bluetooth 1.1 compatible mobile phones. I have no wires. I work within a 10 meter radius of your phone so you can leave your mobile in your pocket or a bag. You turn me on/off, receive calls, make calls and pair me with other devices by pressing in the small of my back.



Intelligent washing machine



Our focus

- What we don't care about
 - bluetooth headsets, keyboards, ovens
 - how to blast advertisements at users
- What we do care about
 - how to send data between bluetooth devices using python code
- But in this lecture, will give a foundation to let you discover more



Programming Concepts

- Choose a communication partner
- Desired type of communication
- Connection
 - initiate outgoing or accept incoming
- Send & Receive data



Choosing Partner

- Every device has a bluetooth address
 - unlike TCP, same address at all layers
 - 48-bit mac address (unique)
 - could be changed by software
- Devices have bluetooth name
 - User supplied, not unique
 - “My Phone” is a common name

Common protocols

- RFCOMM
 - com port (rs232) replacement, streaming
 - only 30 ports available
 - reliable
- L2CAP
 - connection oriented, customizable reliability
 - reserved ports: 1 -- 4095 (odd numbered)
 - unreserved: 4097 -- 32765 (odd numbered)



Service ID

- Every service has a 128 bit (supposedly) unique identifier -- UUID
 - some reserved, developers registered
- Service class ID
- Service Description -- human readable
- Protocol Descriptor -- which prot. used
- Profile Descriptor -- which ones, e.g. mouse



Bluetooth Freq Hopping

- Designed for BT device rich environments
- Lots of radio interference
- Divide spectrum into 72 slices
- Frequency hop between slice
 - pseudo-random hopping
 - hard to track without knowing seed
- Why pairing / discovery takes so long



HCI Tools

- hcitool scan
- hcitool bind
- hcitool connect

