Introduction to Bluetooth Networking

Ramiro Liscano

Independent Consultant – Spontaneous Networking

Adjunct Professor at Carleton University

rliscano@ieee.org

Overview

- Where is Bluetooth Positioned in the Wireless World? (5 min.)
- Bluetooth Protocol Stack (25 min.)
- Bluetooth Applications (15 min.)
- The Future of Bluetooth (5 min.)

What is Bluetooth?

- It is a specification that attempts to provide a standard method of wireless communication between various personal devices
- Devices with ranging complexity can utilize Bluetooth technology: from cellular telephones to laptop computers
- Has a complete software framework and its own protocol stack.
- Specifications are driven by a Consortium that was founded in 1998 by Ericsson Microelectronics, Nokia, IBM, Toshiba and Intel. http://www.bluetooth.org

Goals

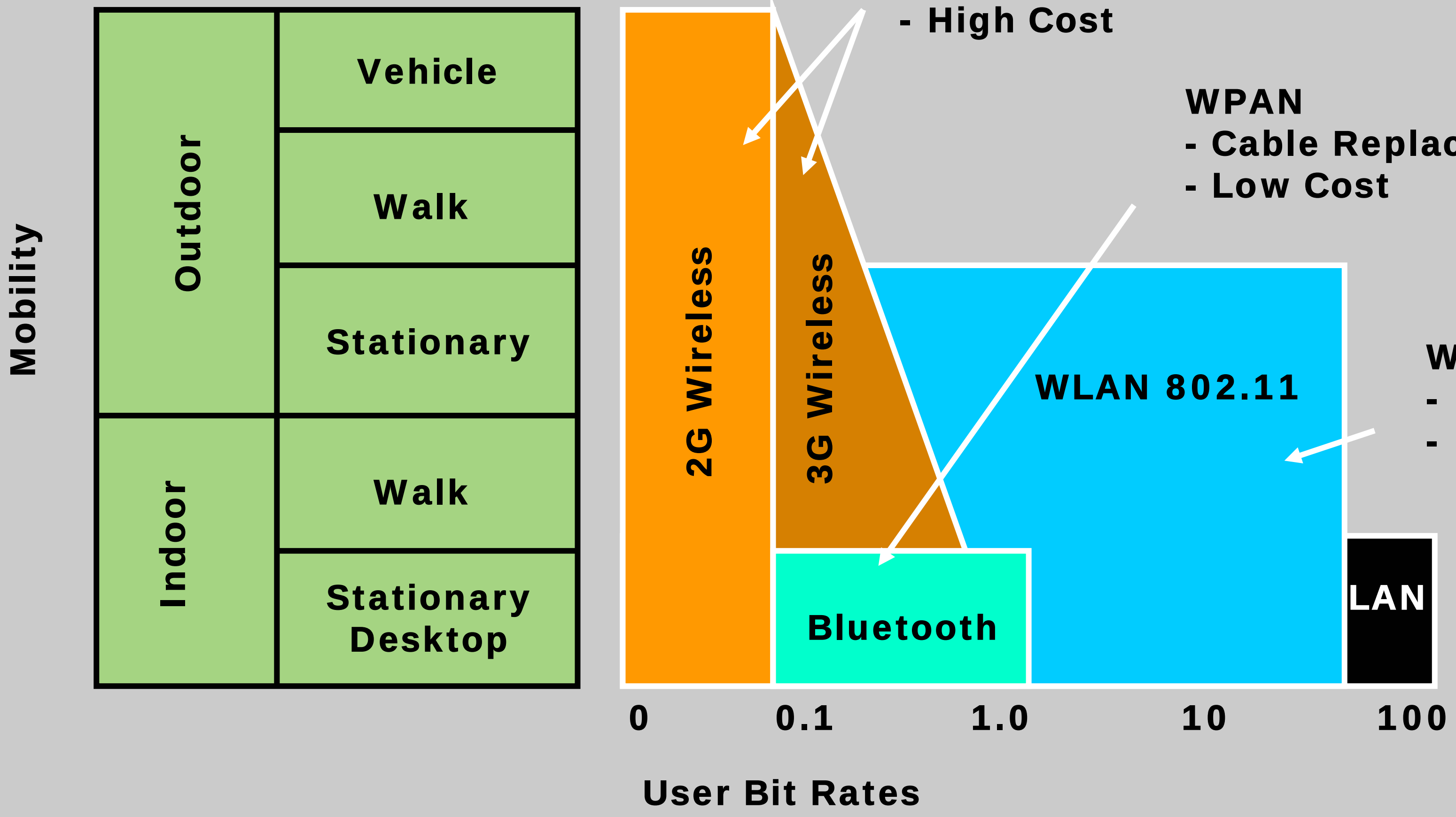
- Cable replacement
- Low Cost (a $5 solution)
- Low Power
- Small Size
- Dynamic networking for devices that are constantly mobile (not in motion)

Ericsson Technology Licensing | Bluetooth Intellectual Property
making Bluetooth Dreams come true

FOR MORE INFO...

Specifications are driven by a Consortium that was founded in 1998 by Ericsson Microelectronics, Nokia, IBM, Toshiba and Intel. http://www.bluetooth.org

Bluetooth and Wireless

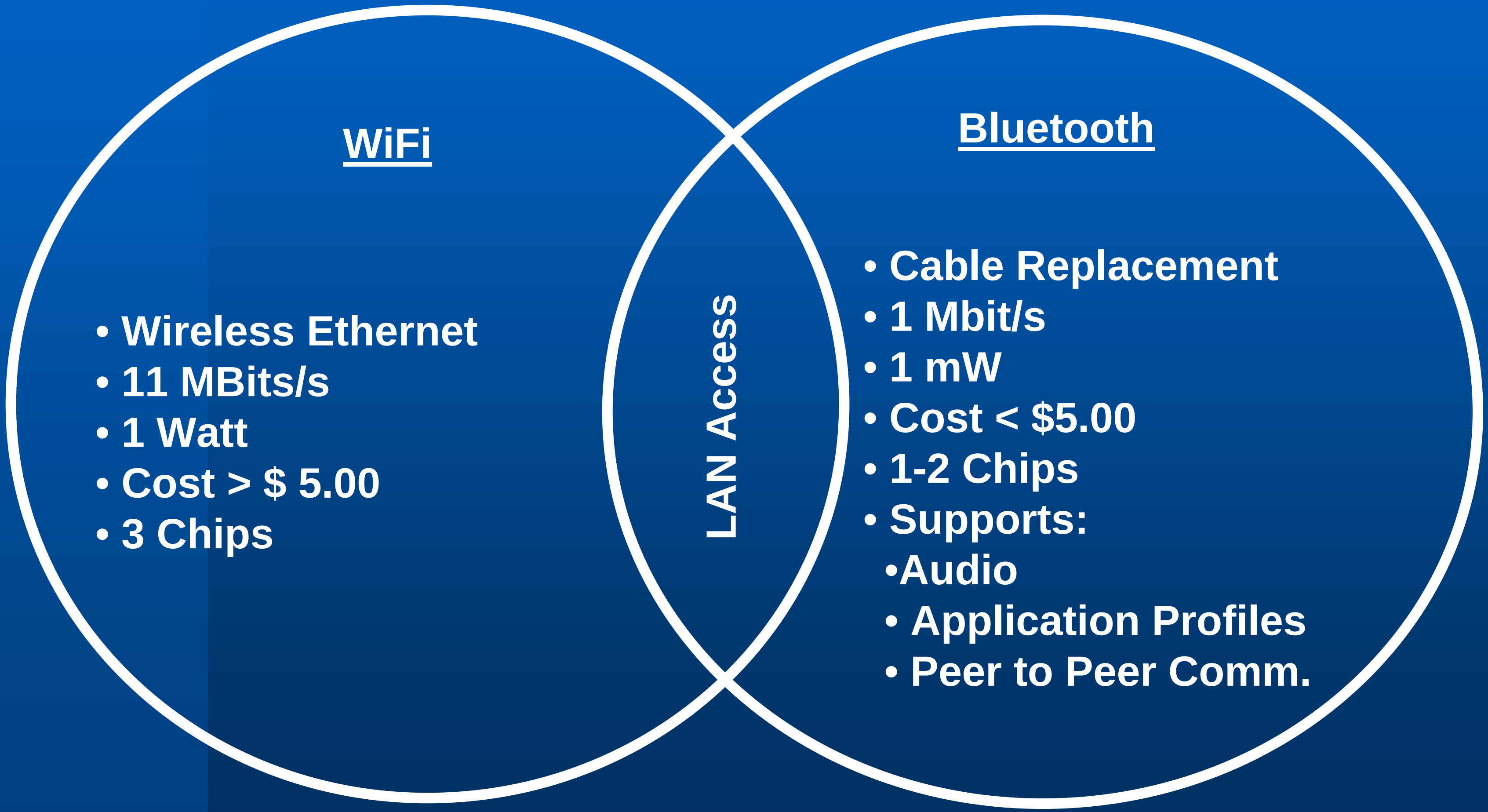


WWAN
- Large Coverage
- High Cost

WPAN
- Cable Replacement
- Low Cost

WLAN
- High Speed
- Moderate Cost

Bluetooth & WiFi



WiFi

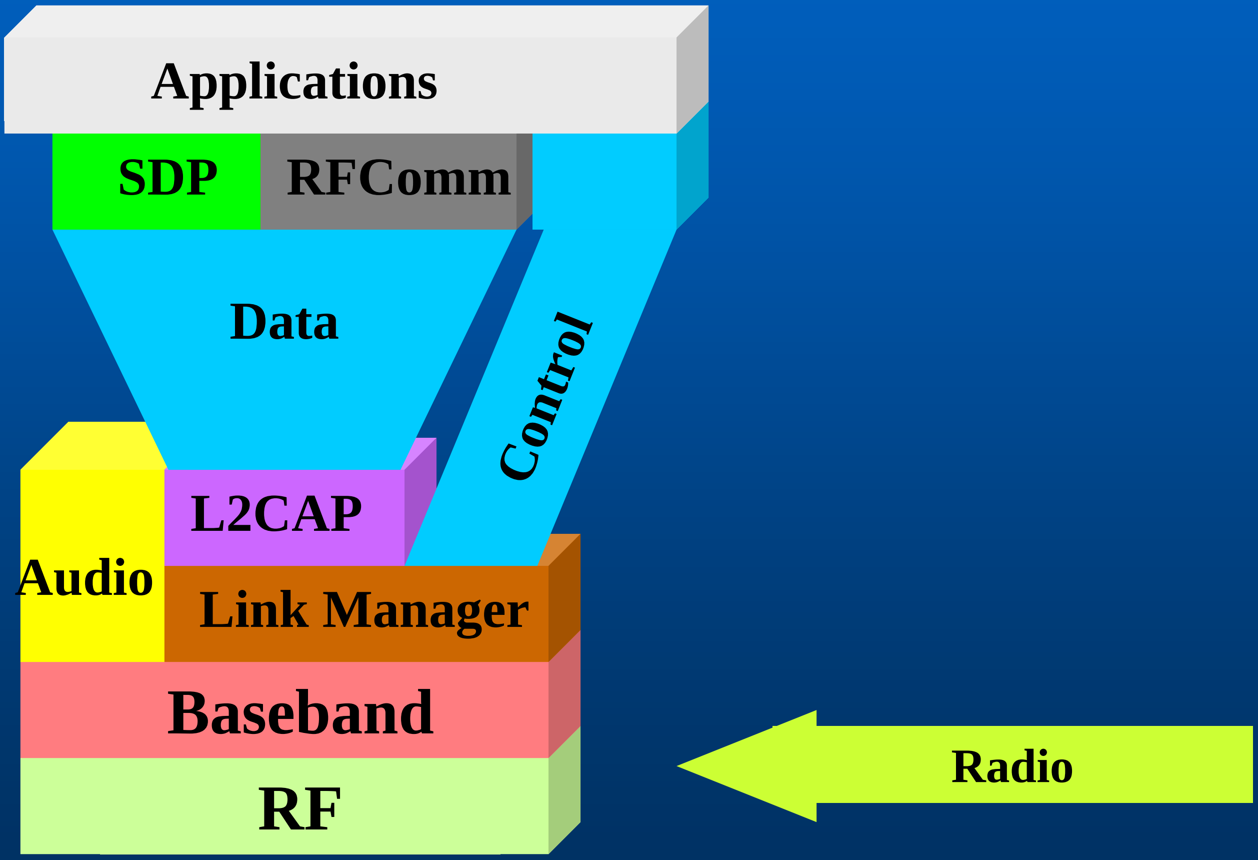
- Wireless Ethernet
- 11 MBits/s
- 1 Watt
- Cost > $ 5.00
- 3 Chips

LAN Access

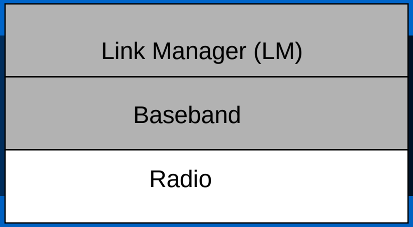
Bluetooth

- Cable Replacement
- 1 Mbit/s
- 1 mW
- Cost < $5.00
- 1-2 Chips
- Supports:
  - Audio
  - Application Profiles
  - Peer to Peer Comm.

Bluetooth Protocol Stack



Technical Specifications

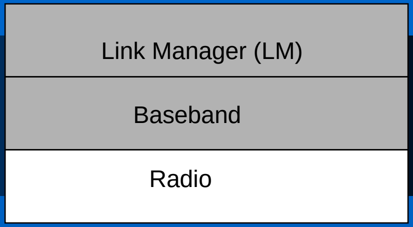

Link Manager (LM)

Baseband

Radio

- Bluetooth devices come in three classes
  - Class 1 (100mW, 100m range)
  - Class 2 (2.5mW, 10m range)
  - Class 3 (1mW, 1m range)
- RF Specs
  - Resides in the unlicensed ISM band between 2.4-2.485GHz
  - Uses frequency hopping over 79 channels, 1600 hops/second
  - 723Kbps throughput (Asymmetrical)
- Current Hardware Solutions
  - Modules that are soldered directly to a USB
  - PCMCIA cards
  - USB and RS232 dongles (SD from Palm)

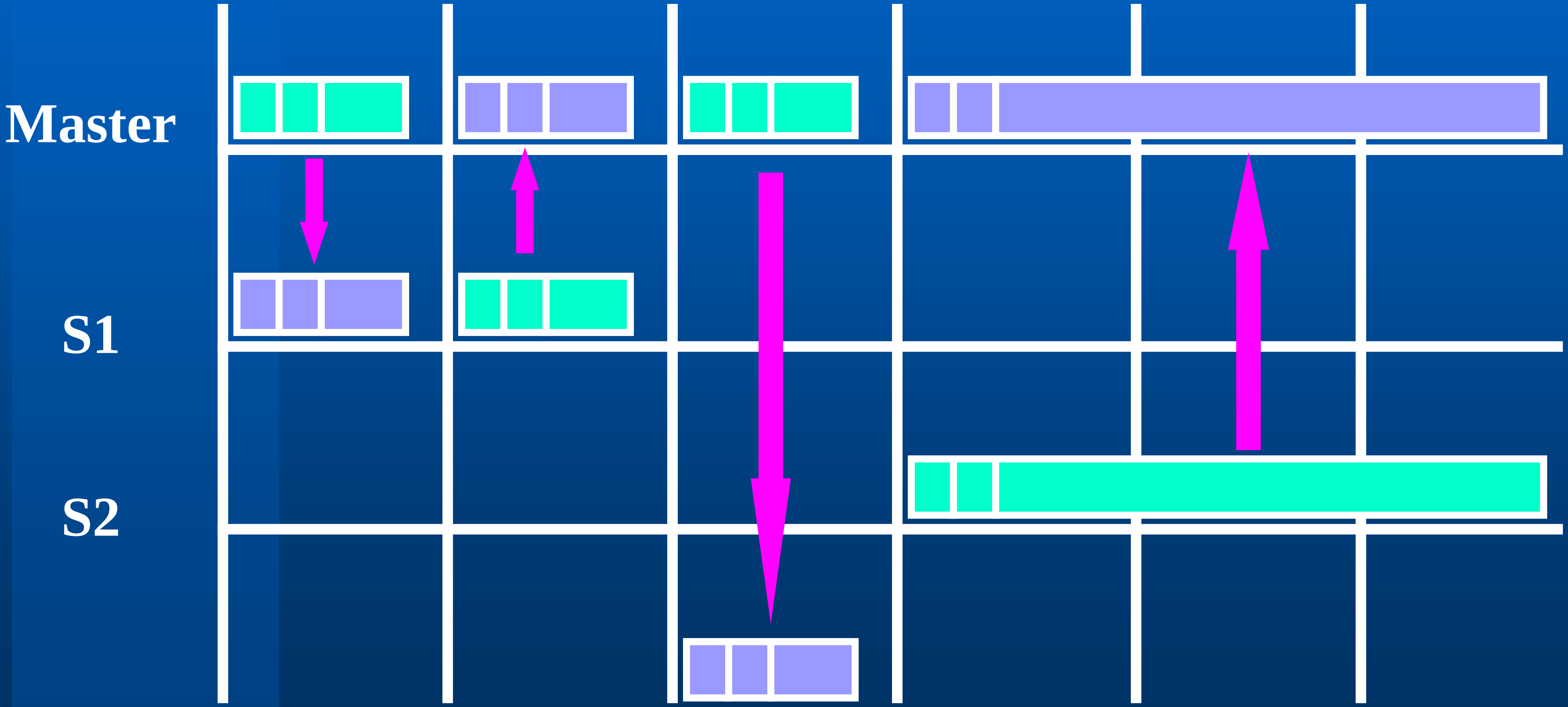
Radio Link Characteristics



Link Manager (LM)

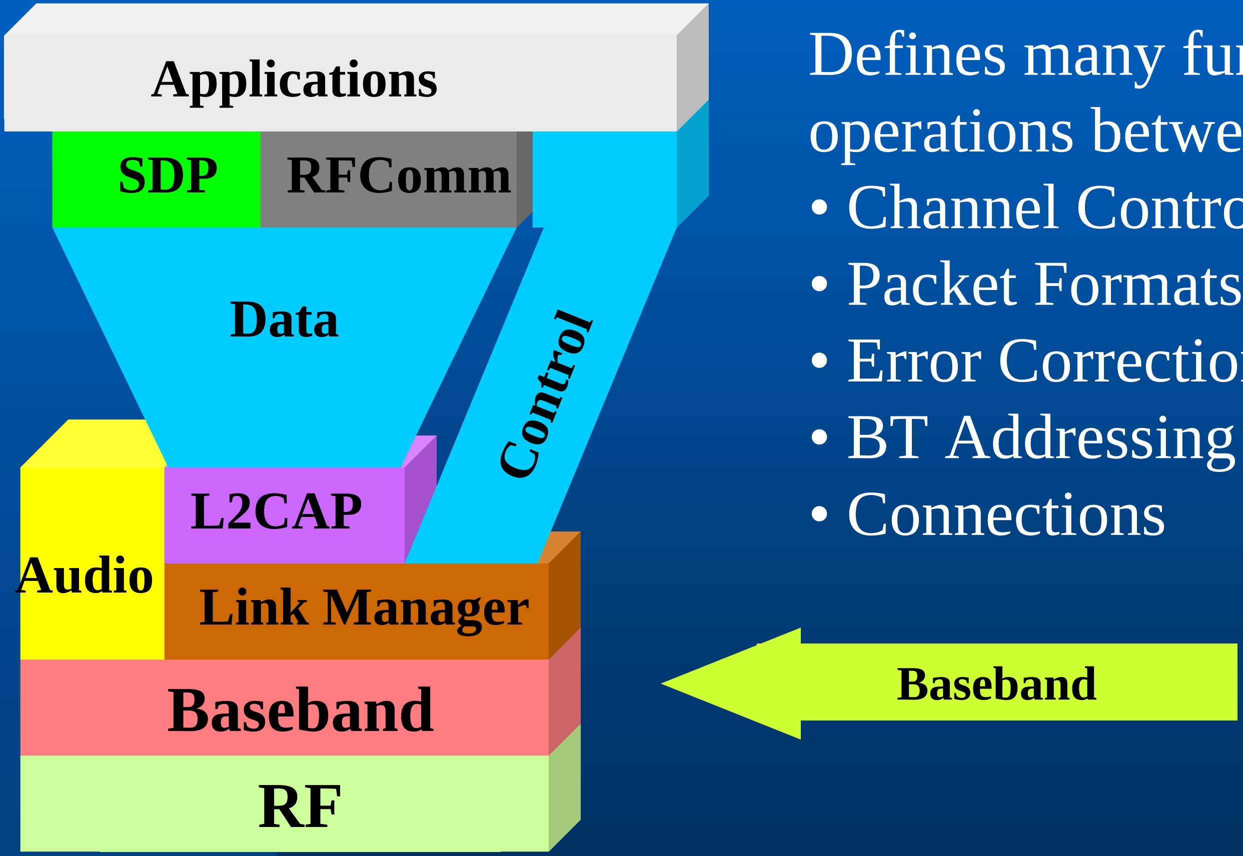
Baseband

Radio



FH: Frequency Hopping **TDD: Time Division Duplex**

Baseband



Defines many fundamental operations between devices

- Channel Control
- Packet Formats
- Error Corrections
- BT Addressing
- Connections

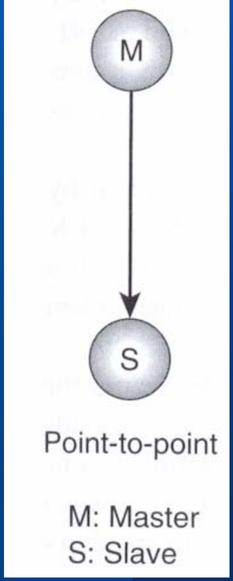
Typical Bluetooth Networks

Link Manager (LM)

Baseband

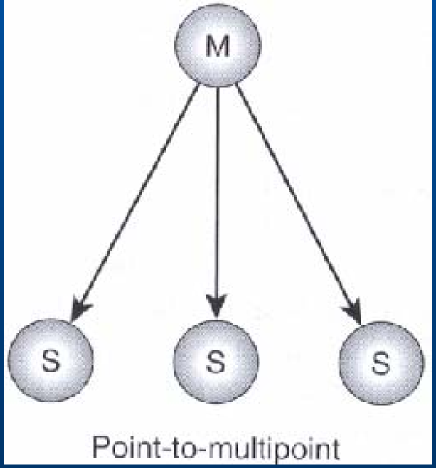
Radio

– Master / Slave Piconet Configurations

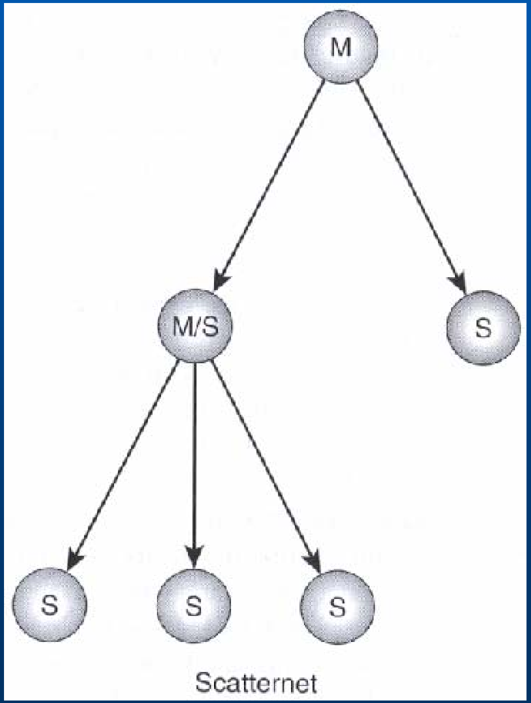


Point-to-point

M: Master
S: Slave

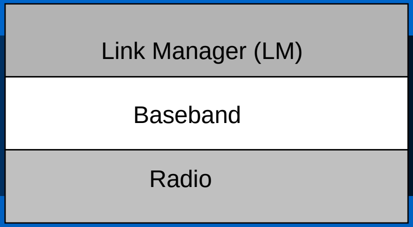


Point-to-multipoint



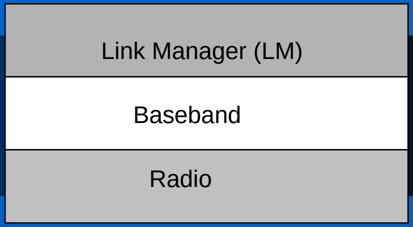
Scatternet

Piconet Characteristics



- Maximum 7 active nodes or 255 parked.
- Everything is controlled by the master.
  - Hopping sequence is unique for a piconet and is determined by the Master’s BT address.
  - The piconet is synchronized by the system clock of the Master.
  - Channel bandwidth.
  - Master can broadcast to slaves.

Connection Modes



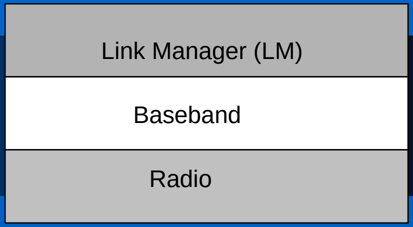
Link Manager (LM)

Baseband

Radio

- Asynchronous Connection-Less (ACL)
  - One ACL connection supported in Slave mode.
  - 761/57.6 Kps or 432.6 Kps both ways.
- Synchronous Connection Oriented (SCO)
  - Point to point connection between a Master and Slave device. Slots are reserved therefore similar to circuit-switch.
  - Up to 3 SCO Links can be supported.
  - 64 Kps, adequate for voice communication.

Device Modes

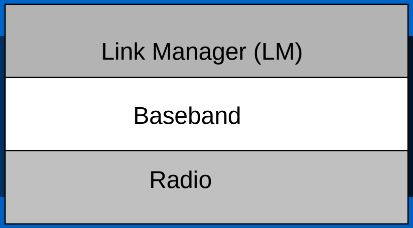

Link Manager (LM)

Baseband

Radio

- **Stand by – Not connected, default state low power mode.**
- **Inquiry – Search for new devices in range. Master operation.**
- **Page – Construct a specific connection to a slave device. Slave address required generally acquired from Inquiry.**
- **Active – Data transmission occurring. Devices are connected.**
- **Sniff – Listening duty cycle is reduced.**
- **Hold- Slave will not support ACL anymore.**
- **Park – Slave no longer active but still synchronized with piconet.**

Inquiry Mode


Link Manager (LM)

Baseband

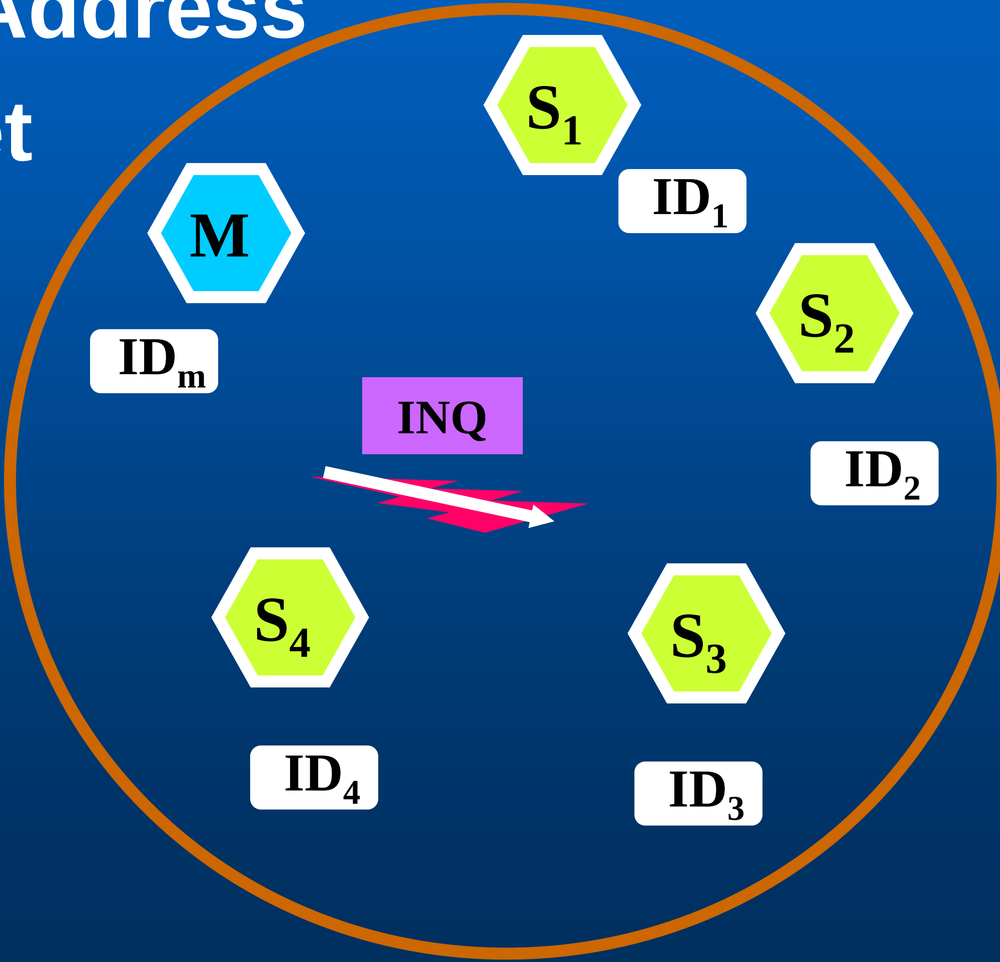
Radio

- Obtain BT Device Address
- Obtain Clock Offset

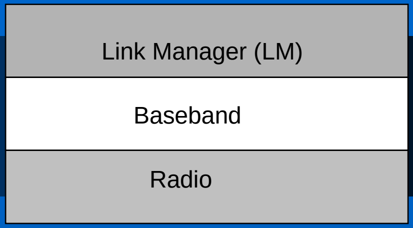
ID_x 24 Bit Device Address

M Wants to find devices

S_x Devices are listening



After Inquiry Mode

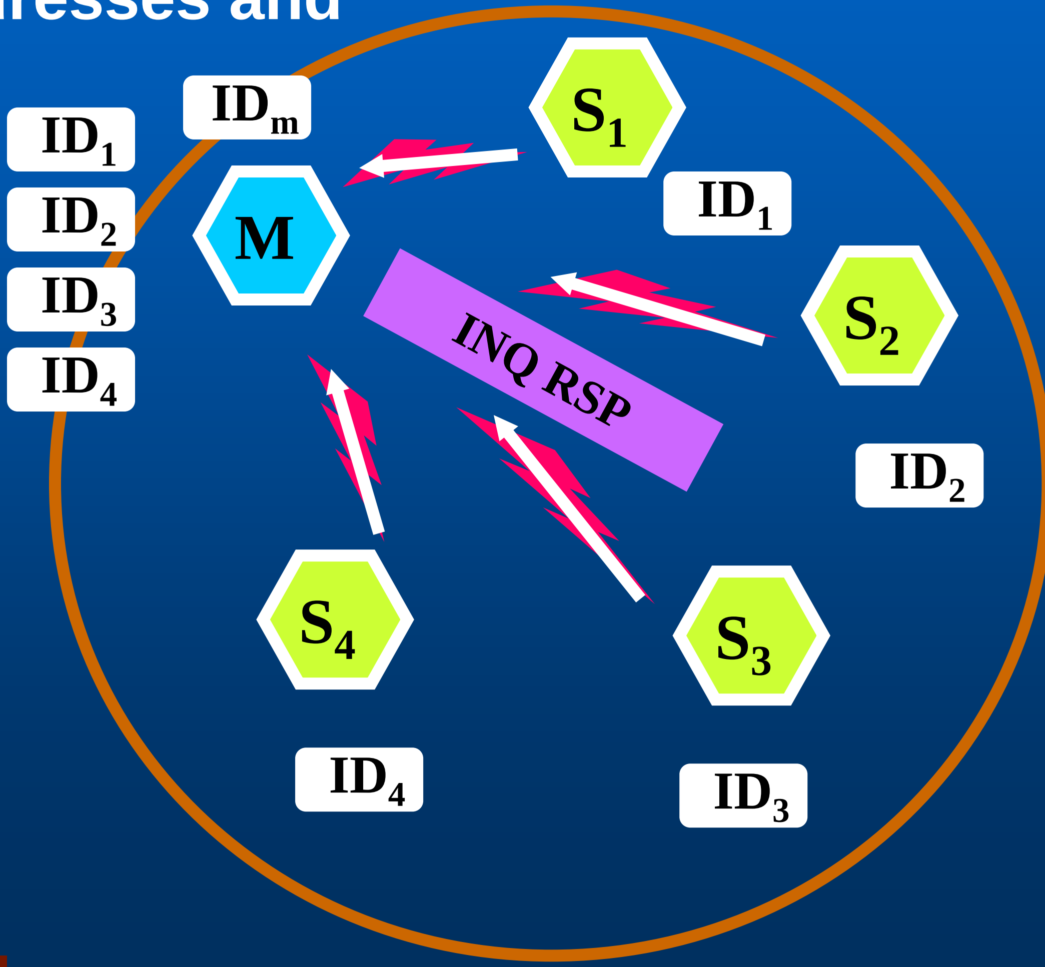


Link Manager (LM)

Baseband

Radio

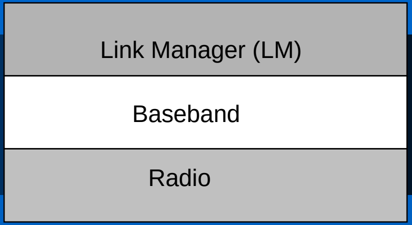
- **Master has all Device Addresses and Clock Offsets**



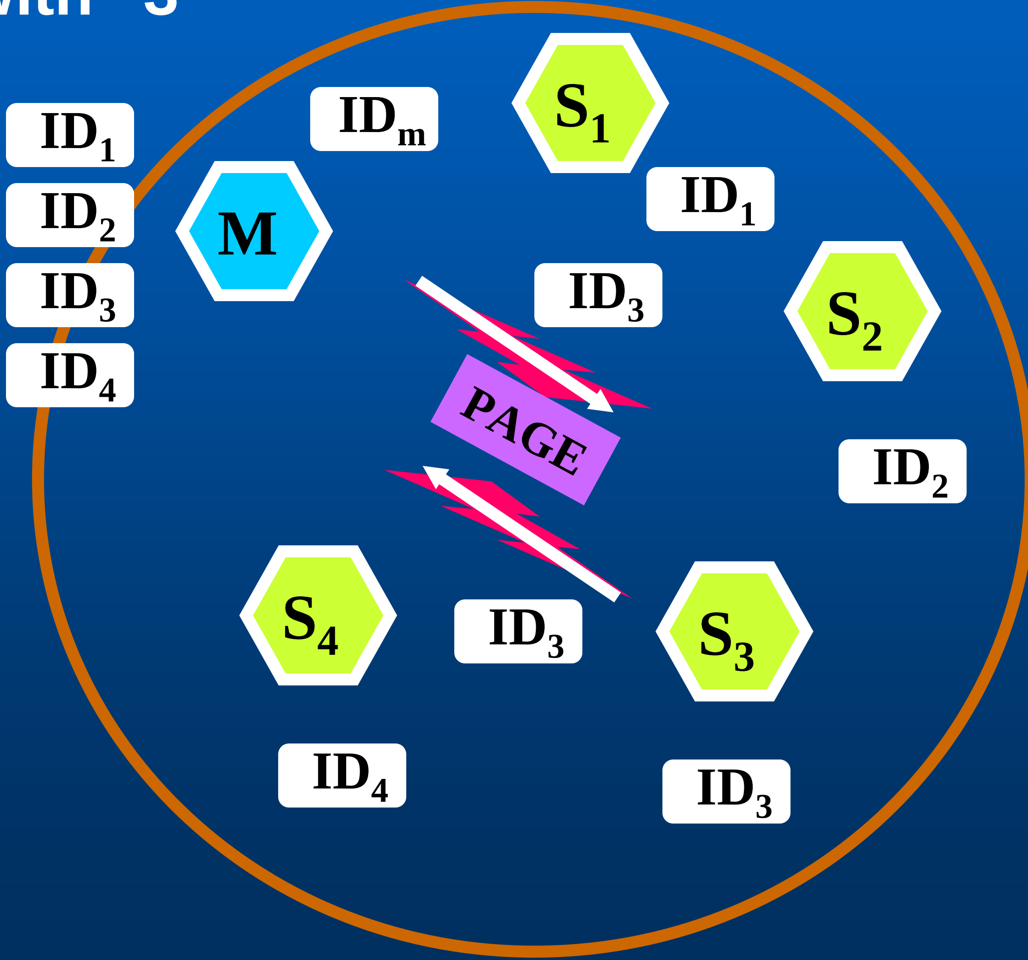
•Radios respond in different slots.

•Master now has device addresses and can start peer to peer connection by paging device

Connection – Paging (1)

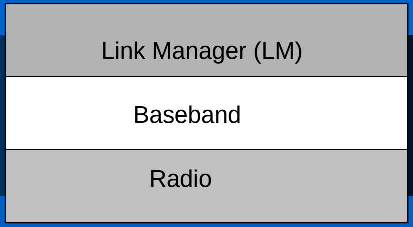


- Master wants to connect with “3”

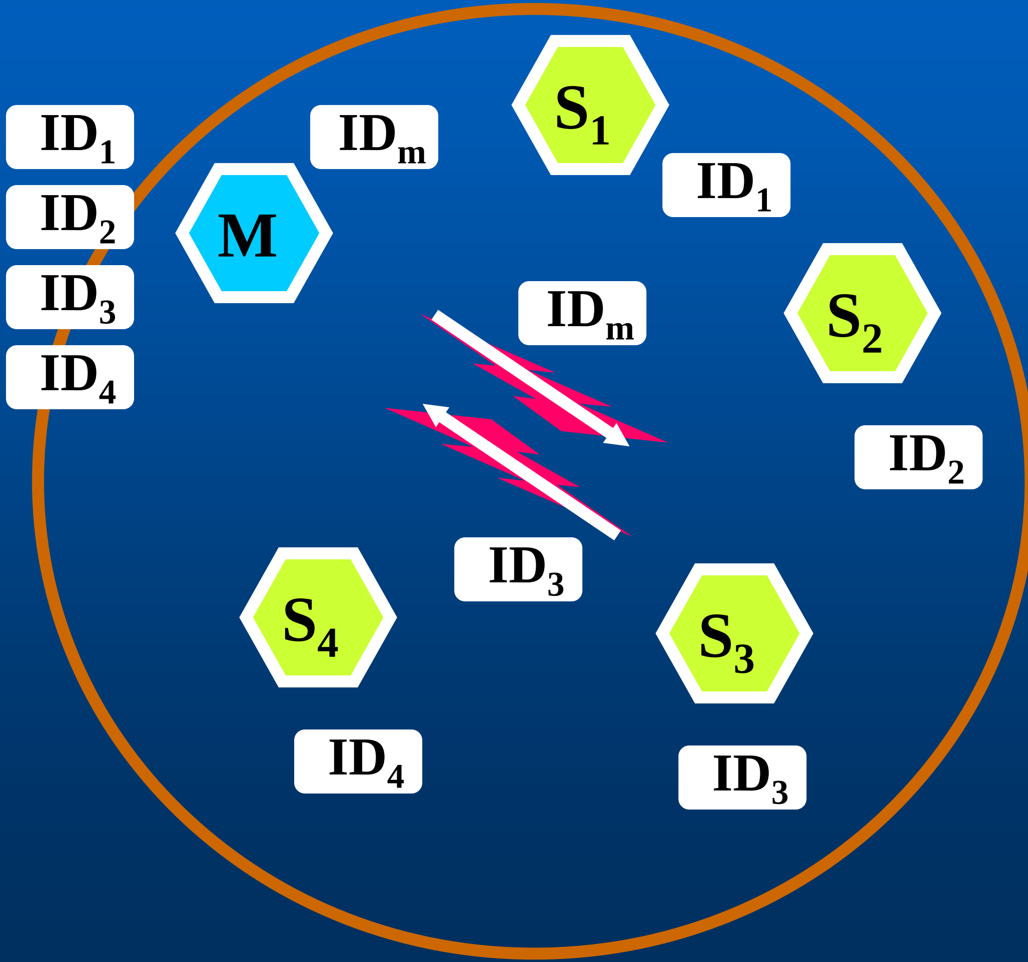


- M pages “3” with ID_3
- S_3 Replies with ID_3

Connection – Paging (2)



- Clocks are synchronized



- M sends “3” its Device ID and clock
- S_3 Can update its clock and change its hopping frequency to match M

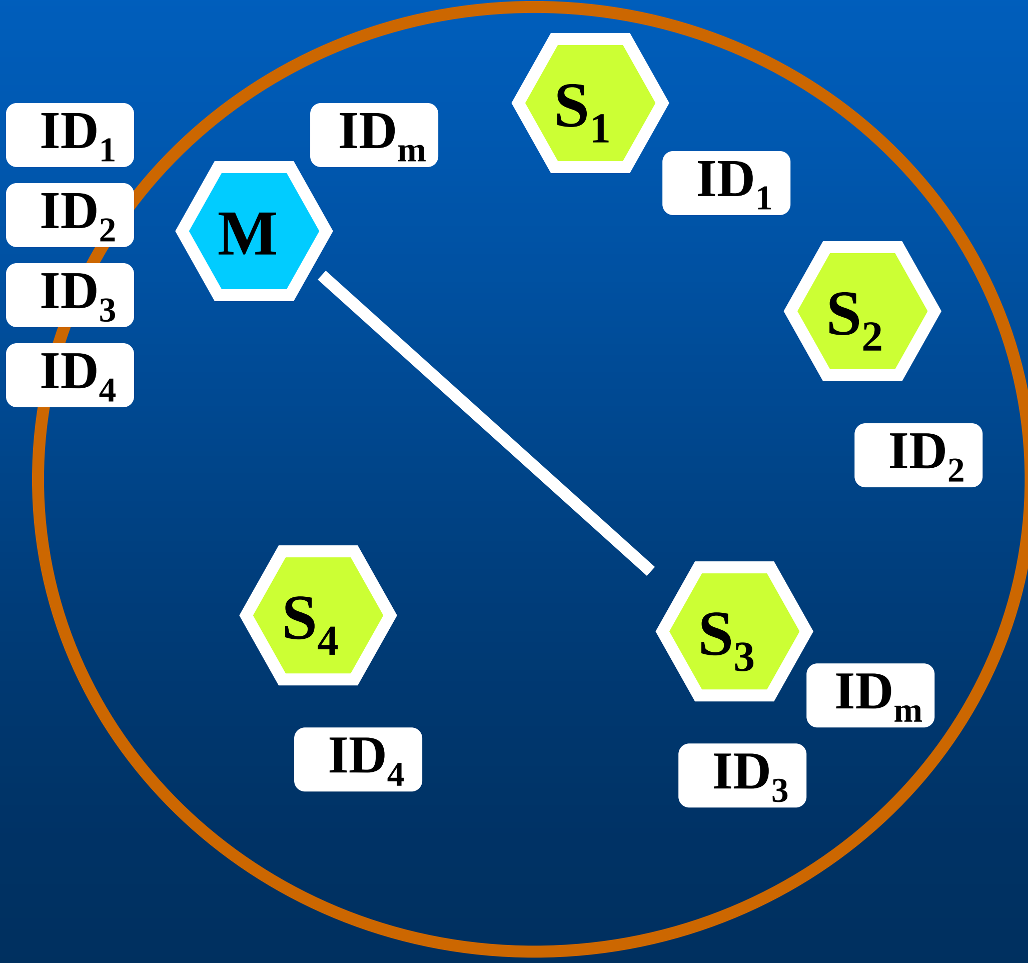
Connection Established

Link Manager (LM)

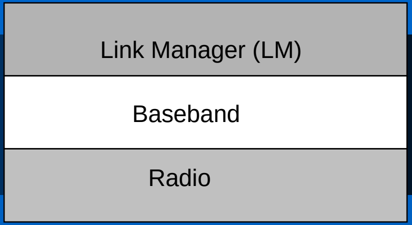
Baseband

Radio

- S_3 is connected to M

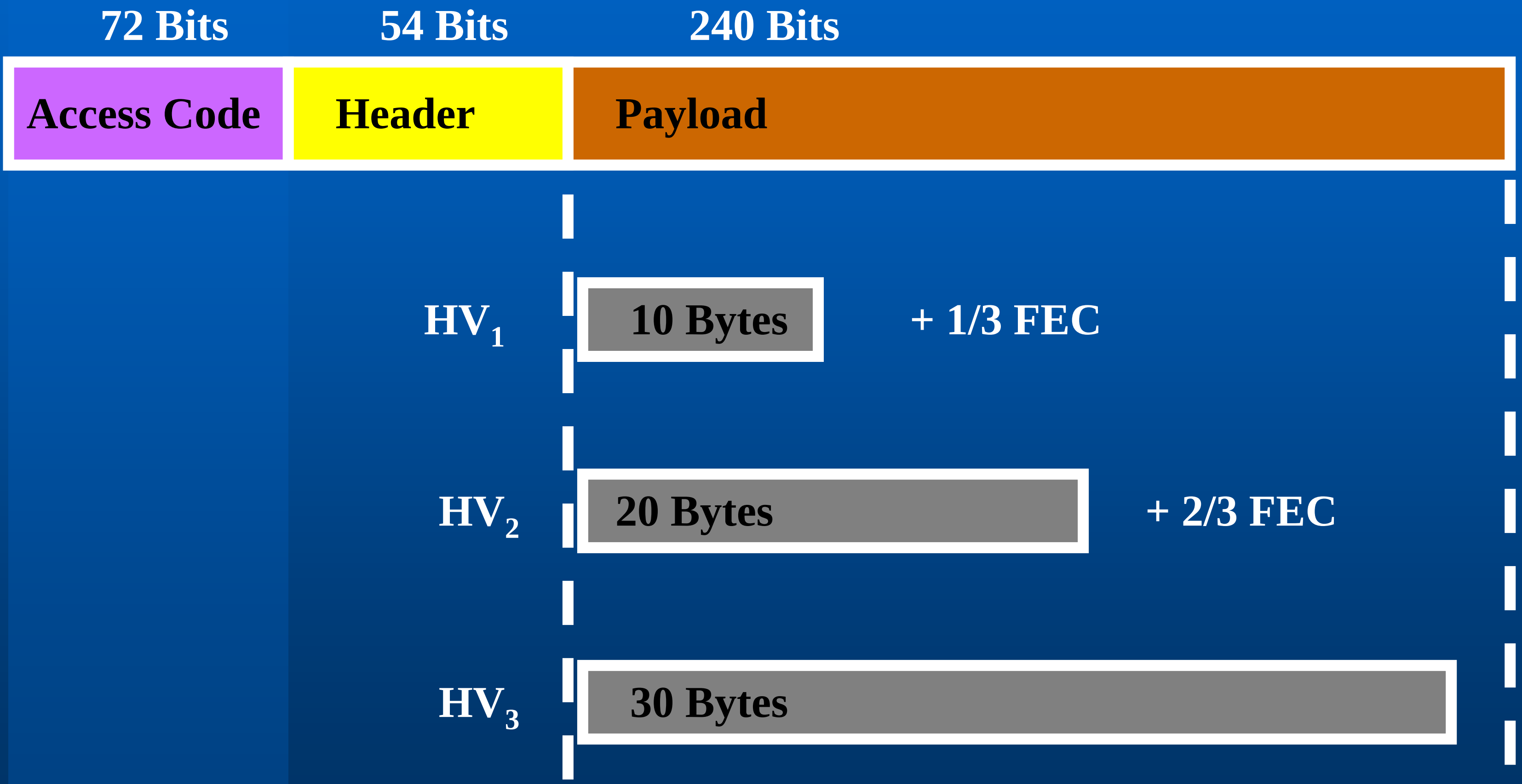


Voice Packet Format


Link Manager (LM)

Baseband

Radio


72 Bits | 54 Bits | 240 Bits

Access Code | Header | Payload

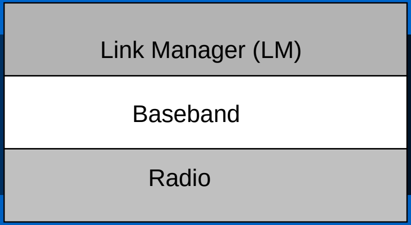
HV_1 10 Bytes + 1/3 FEC

HV_2 20 Bytes + 2/3 FEC

HV_3 30 Bytes

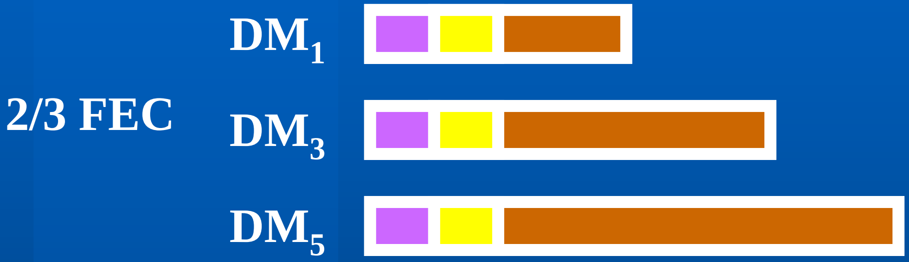
FEC = Forward Error Correction

Data Packet Format

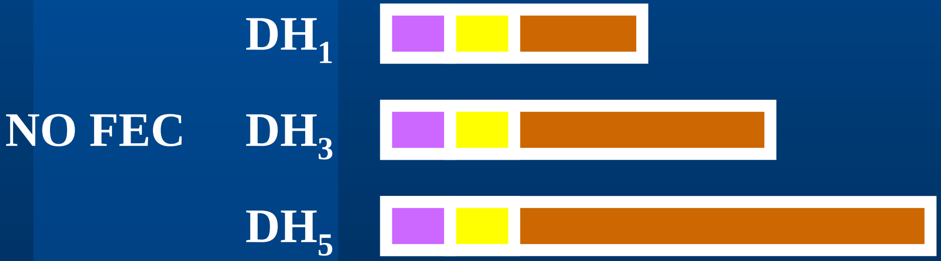

Link Manager (LM)

Baseband

Radio

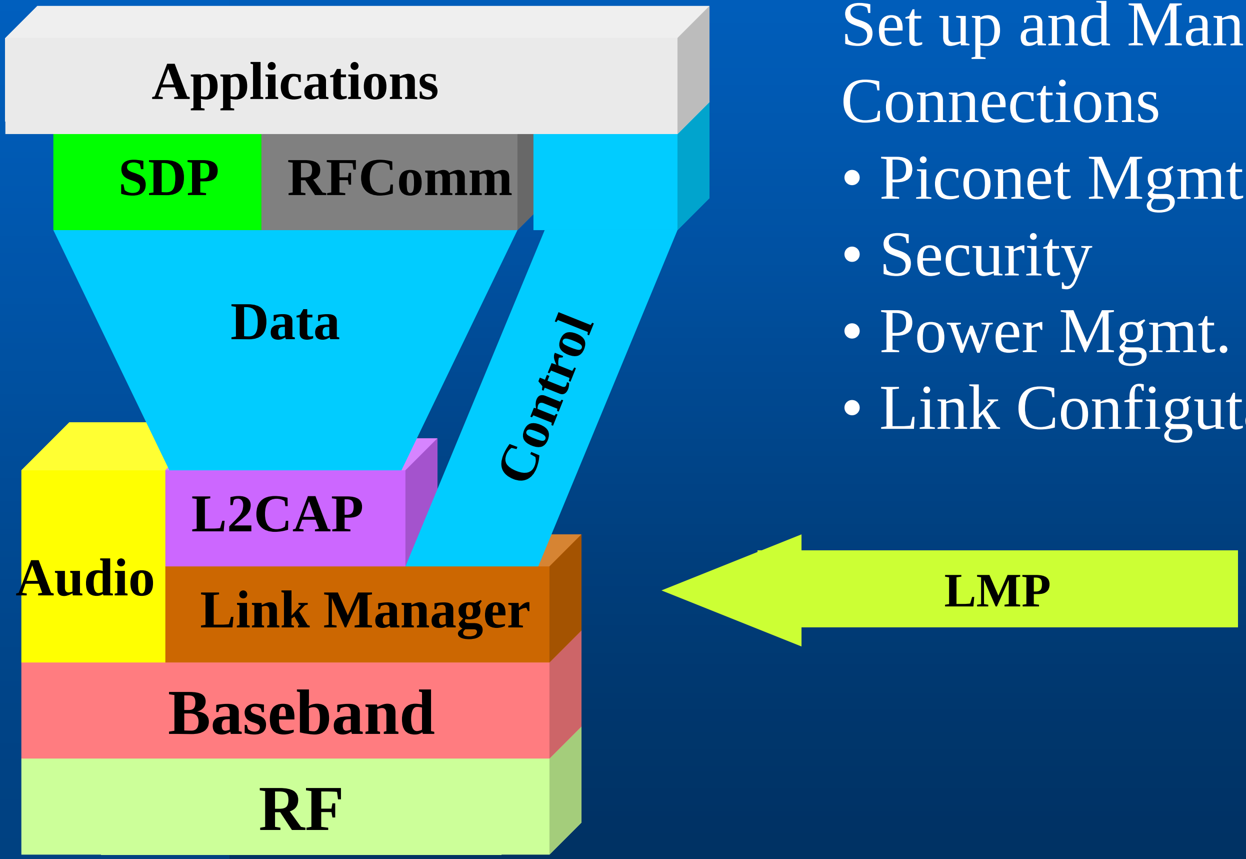


Symmetric	Asymmetric	
108.8	108.8	108.8
258.1	387.2	54.4
286.7	477.8	36.3



Symmetric	Asymmetric	
172.8	172.8	172.8
390.4	585.6	86.4
433.9	723.2	57.6

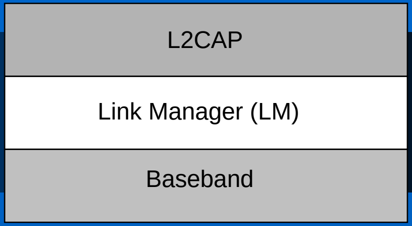
LMP



Set up and Manage Baseband Connections

- Piconet Mgmt.
- Security
- Power Mgmt.
- Link Configutation

Pairing & Authentication

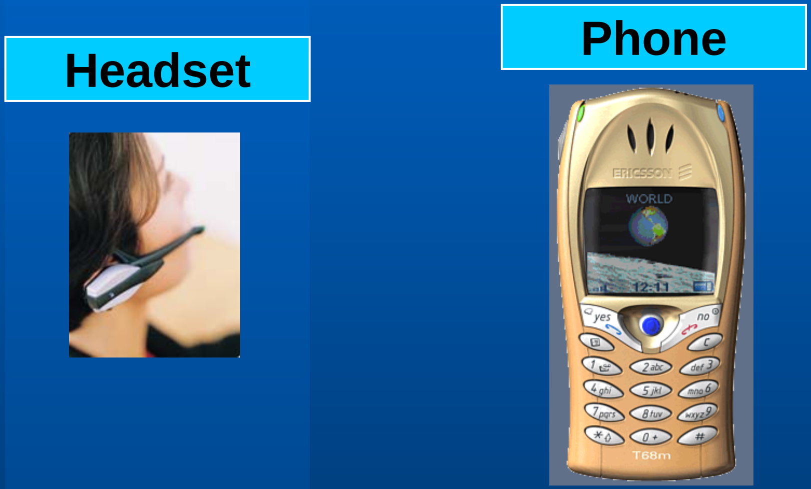


L2CAP

Link Manager (LM)

Baseband

Pairing

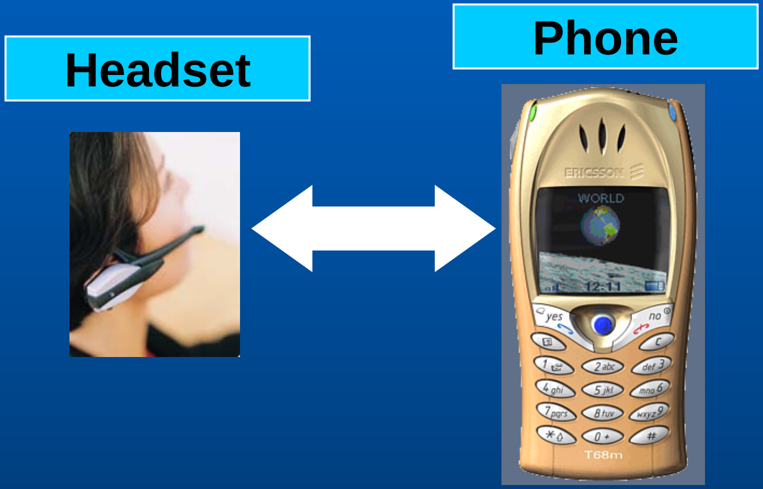


Headset

Phone

- Access to both devices
- Manual PIN entered
- Secret keys generated

Authentication

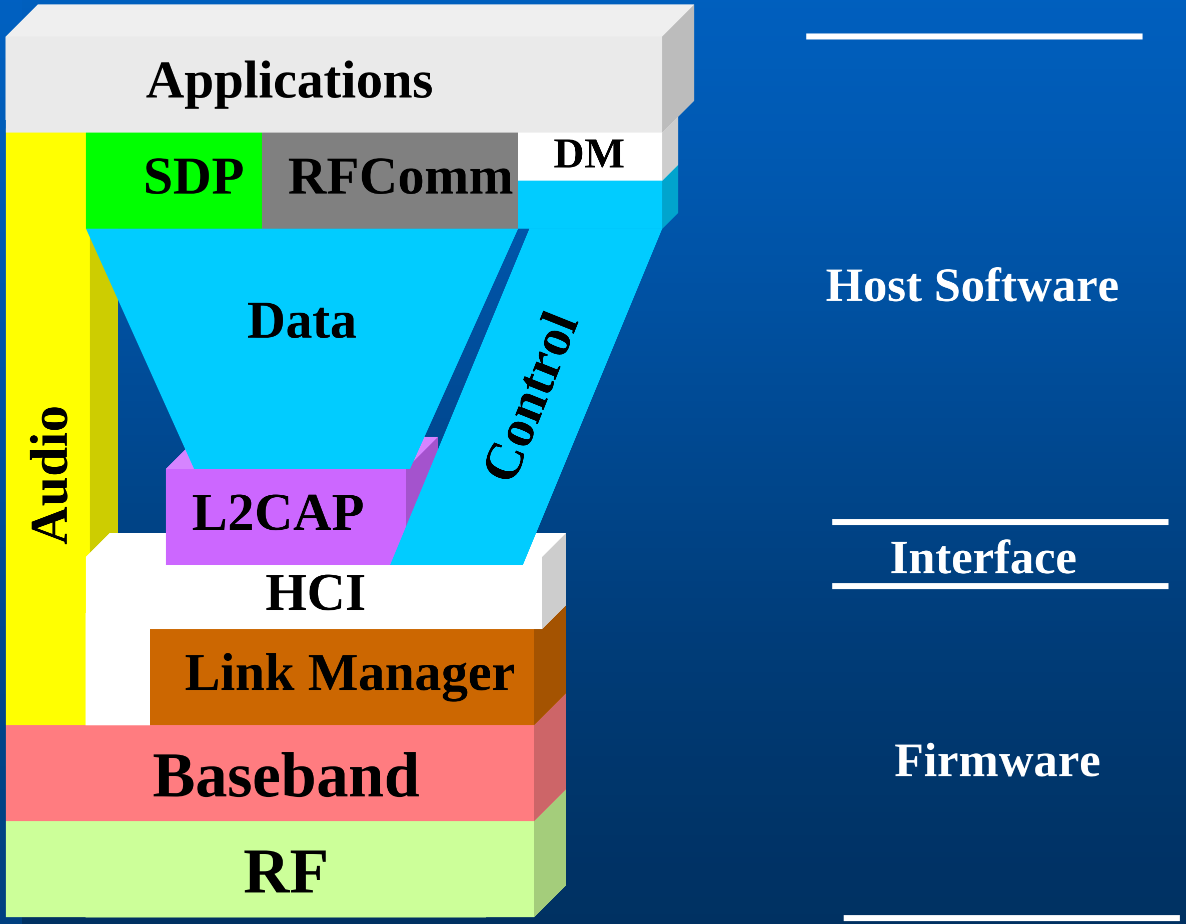


Headset

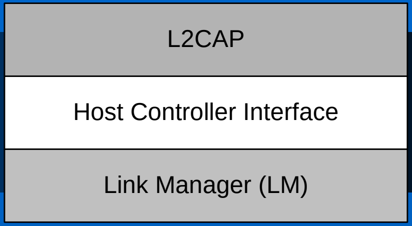
Phone

- Devices connect automatically
- Keys are exchanged
- Authentication based on 128 bit shared key

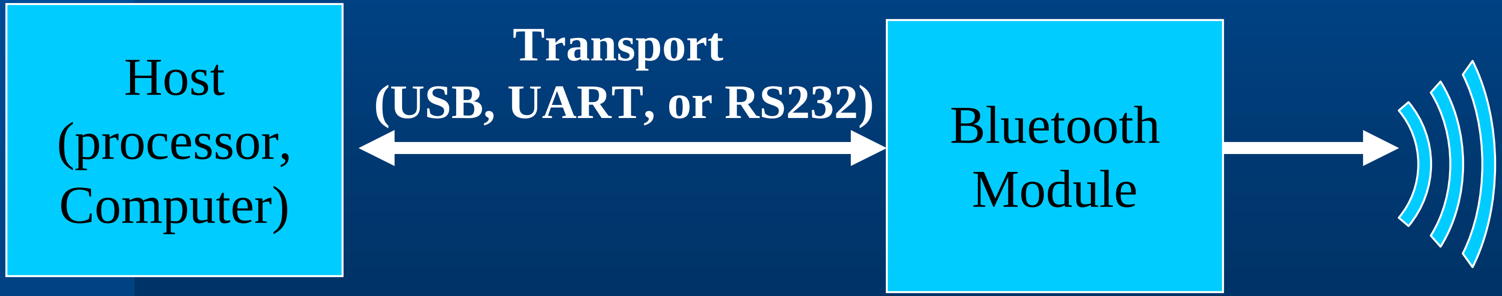
Protocol Stack and HCI



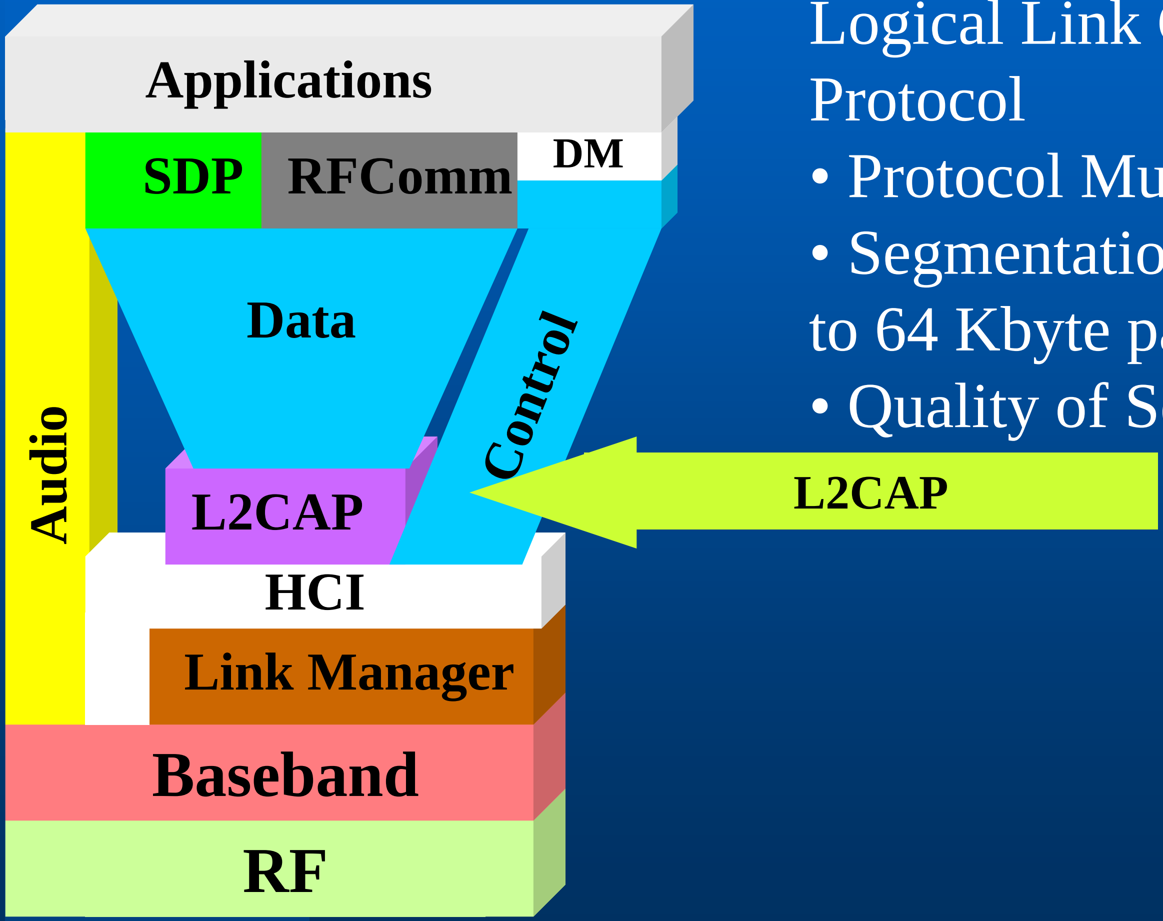
The HCI Layer



- Allows a host device (ie. processor) to perform upper layer stack functions through a physical transport. In other words, allows the stack to be divided between two pieces of hardware
- Three transports defined: UART, USB, and RS232



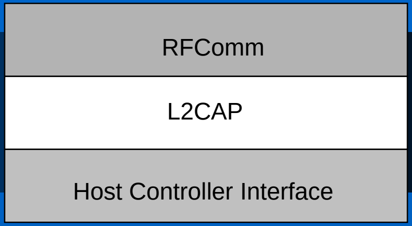
L2CAP



Logical Link Control and Adaptation Protocol

- Protocol Multiplexing
- Segmentation and Reassembly of up to 64 Kbyte packets
- Quality of Service Negotiation

Protocol Architecture

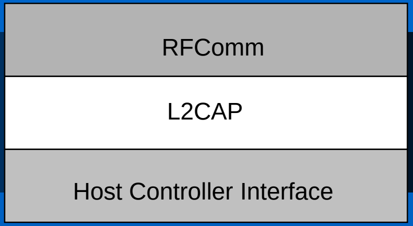

RFComm

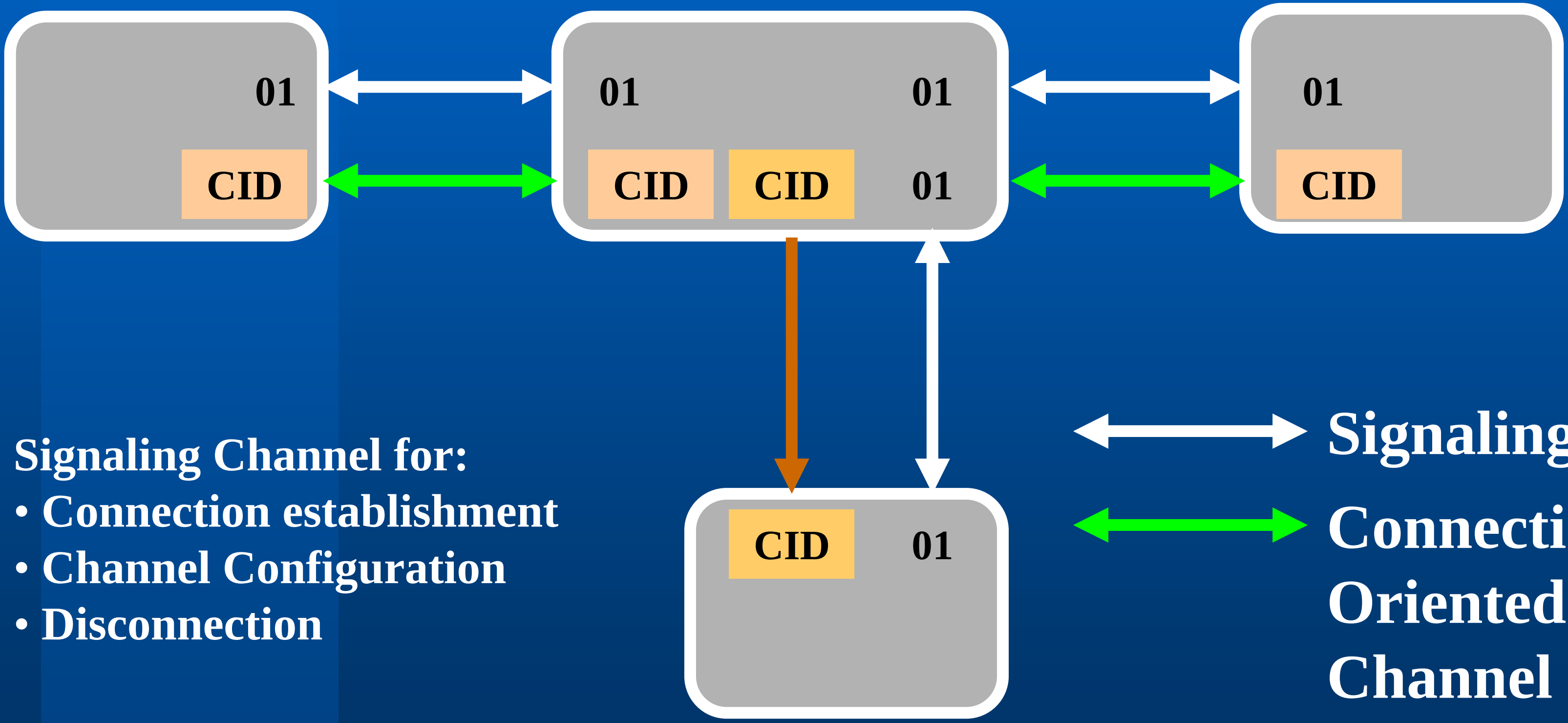
L2CAP

Host Controller Interface

- Creates logical connections with upper layers
  - A channel identifier CID is used to identify the different channels.
  - Channel is assumed to be full duplex.
  - QoS is assigned to each direction of a channel.
  - Connection-oriented, connection-less, and signalling channels can be created.
- Datagram based therefore no streaming of data is possible.
  - Note that audio does not pass through L2CAP.

L2CAP Channels





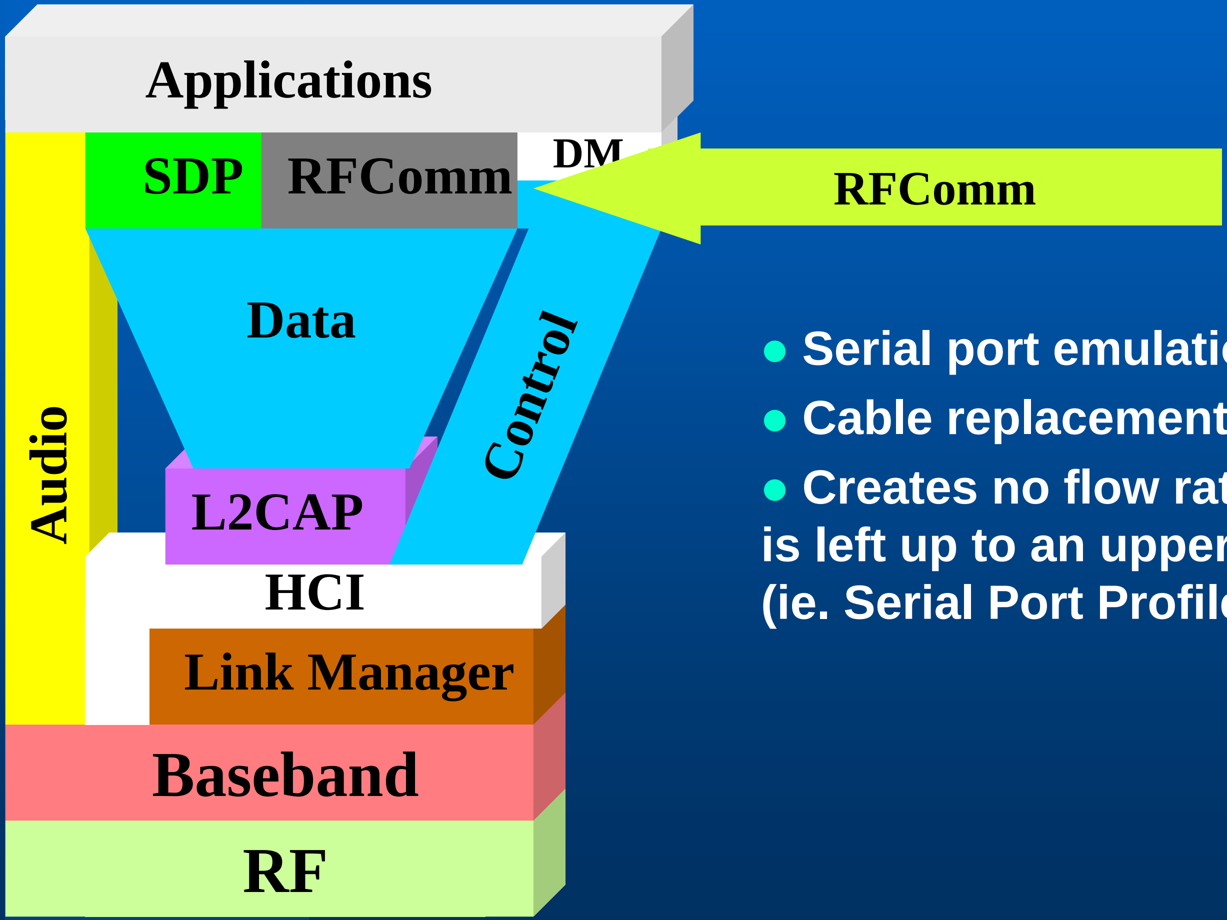
Signaling Channel for:
- Connection establishment
- Channel Configuration
- Disconnection

↔ Signaling Channel

↔ Connection-Oriented Data Channel

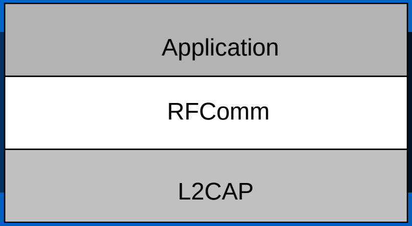
→ Connection-less Channel

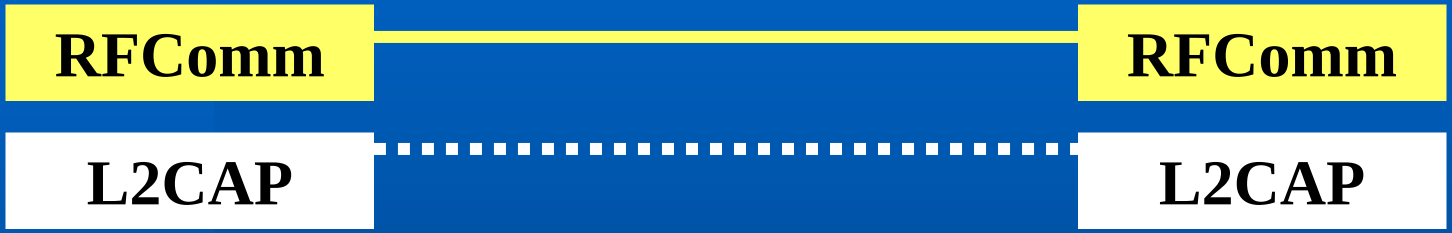
RFComm



- Serial port emulation.
- Cable replacement scenario.
- Creates no flow rate limitations, this is left up to an upper layer application (ie. Serial Port Profile)

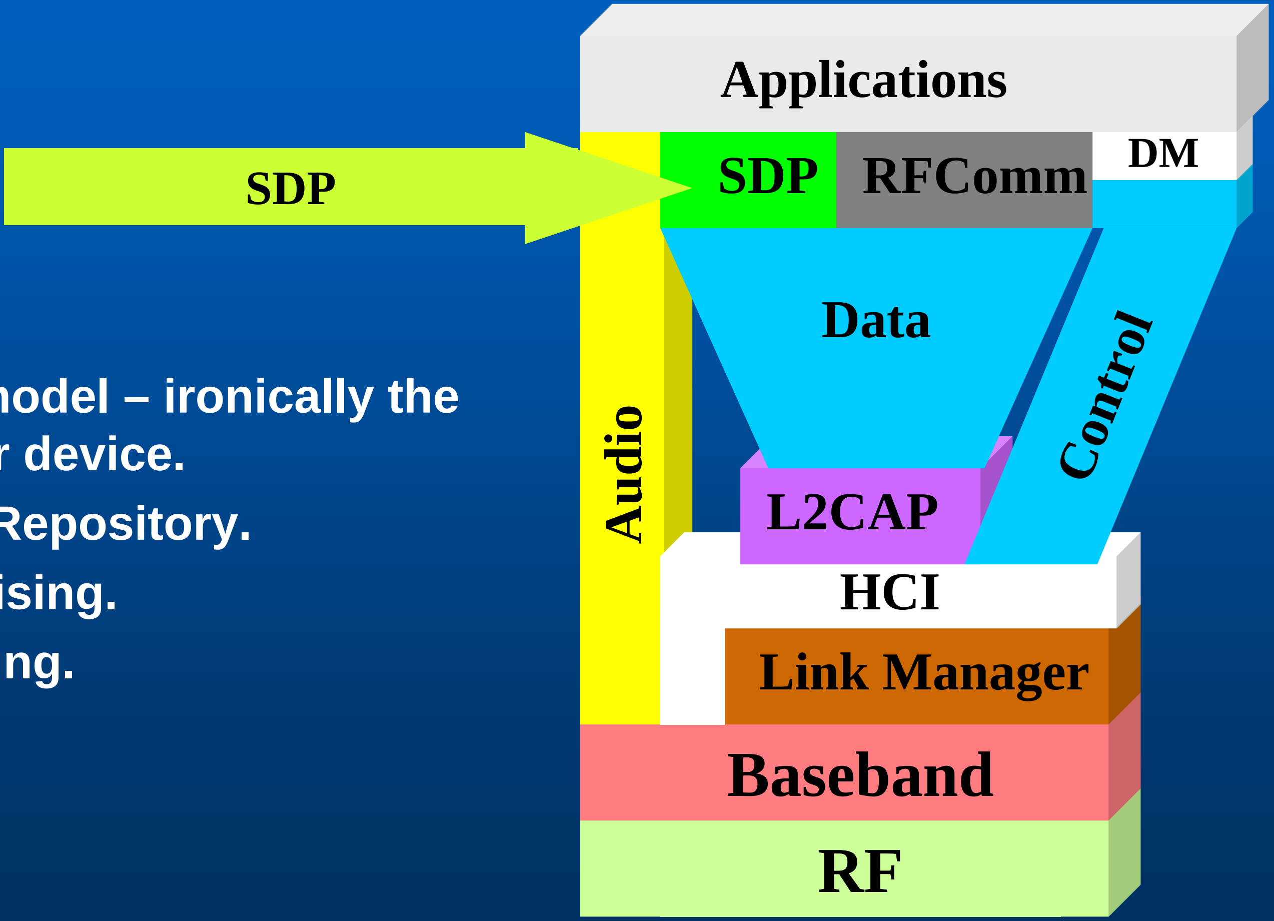
Serial Line Emulation


Application
RFComm
L2CAP


RFComm
RFComm
L2CAP
L2CAP

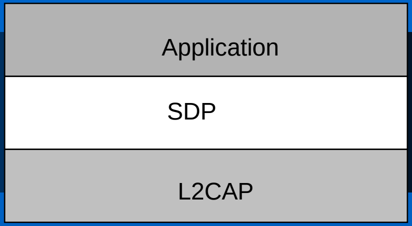
- Design considerations
  - Framing: assemble bit stream into bytes and subsequently into packets.
  - Transport: reliable in-sequence delivery of serial stream.
  - Control signals: RTS, CTS, DTR

Service Discovery Protocol (SDP)



- Client server model – ironically the client is a Master device.
- Local Service Repository.
- Service advertising.
- Service browsing.

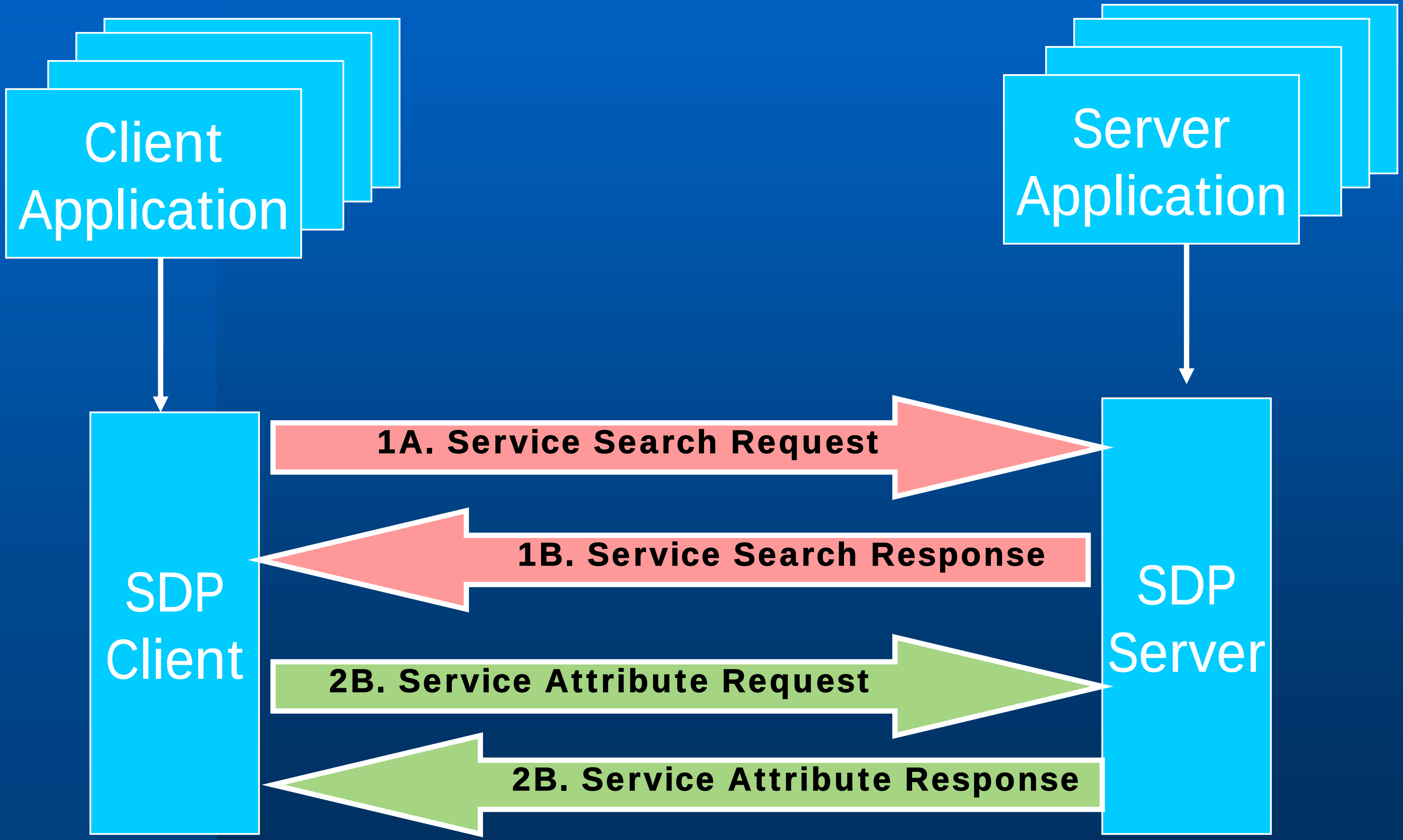
SDP Overview


Application
SDP
L2CAP

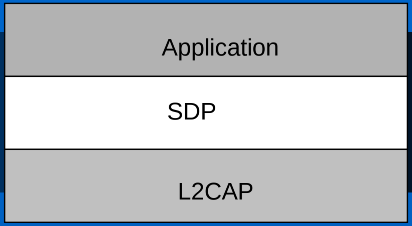
- All devices must provide this capability, it is part of the specification
- Establish L2CAP connection to remote device
- Query for services
  - search for specific class of service, or
  - browse for services
- Retrieve attributes that detail how to connect to the service.
- Establish a separate (non-SDP) connection to use the service.

SDP Transaction

Application
SDP
L2CAP


Client Application
Server Application
SDP Client
SDP Server
1A. Service Search Request
1B. Service Search Response
2B. Service Attribute Request
2B. Service Attribute Response

Service Record


Application

SDP

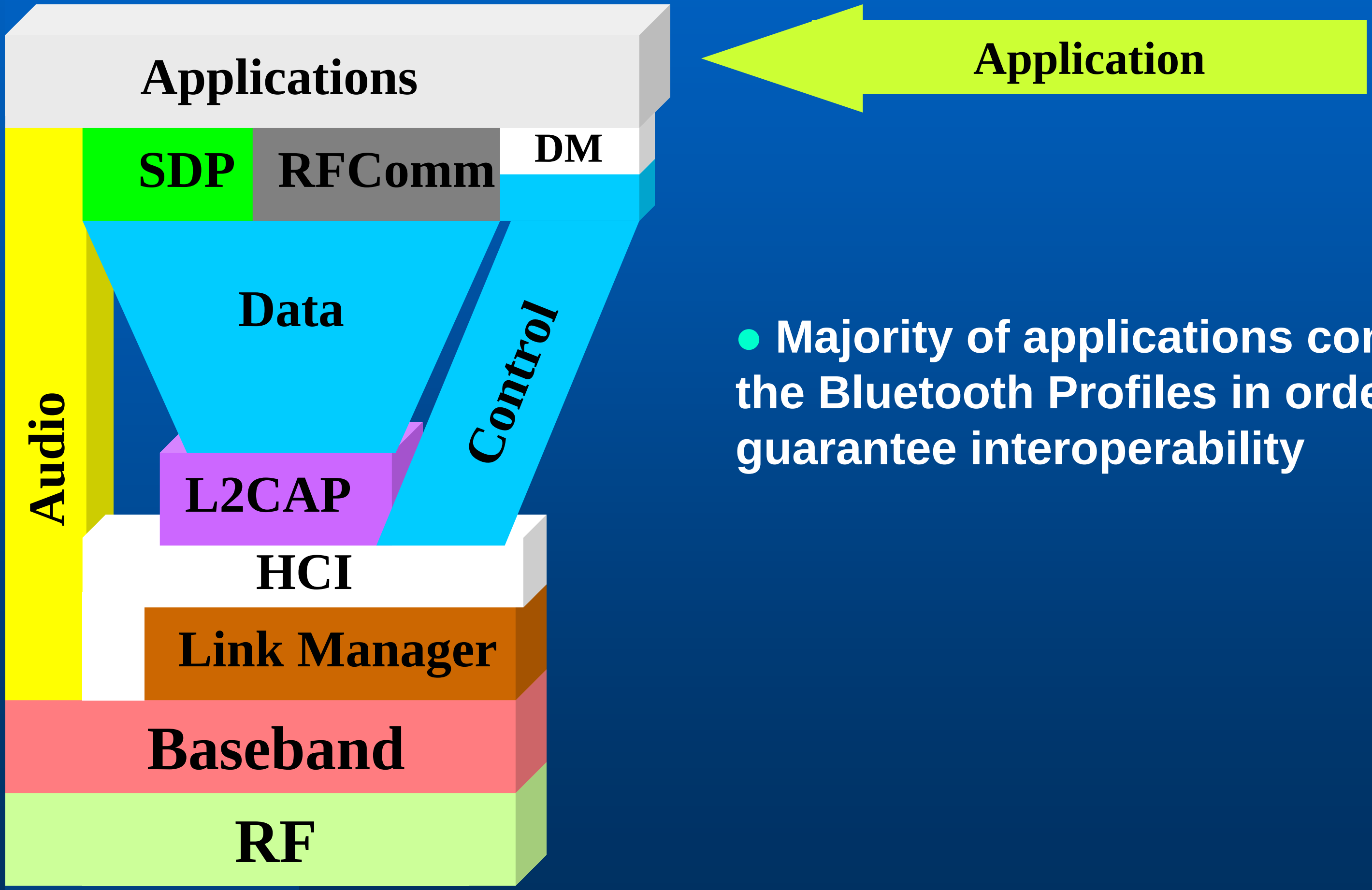
L2CAP

- ServiceClassIDlist
- ServiceID
- ProtocolDescriptorList
- ProviderName
- IconURL
- ServiceName
- ServiceDescription

Service Record

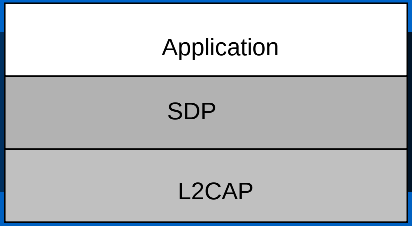
Service Attribute 1
Service Attribute 2
Service Attribute 3
Service Attribute 4
Service Attribute 5
…
…
…

Application



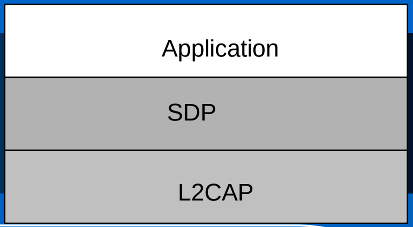
- Majority of applications conform to the Bluetooth Profiles in order to guarantee interoperability

Application Profiles



- Define how devices provide different services in the Bluetooth environment
- There are currently 13 profiles defined by Bluetooth V 1.1
  - Generic Access, Service Discovery Application, Cordless Telephony, Intercom, Serial Port, Headset, Dial-Up Networking, Fax, LAN Access, Generic Object Exchange, Object Push, File Transfer, Synchronization
- 12 Additional Profiles have been defined since V 1.1
  - Advanced Audio Distribution, Advance Video Remote Control, Basic Imaging, Basic Printing, Common ISDN Access, Extended Service Discovery, Hands Free, Hardcopy Cable Replacement, Human Interface Device, Personal Area Networking, SIM Access

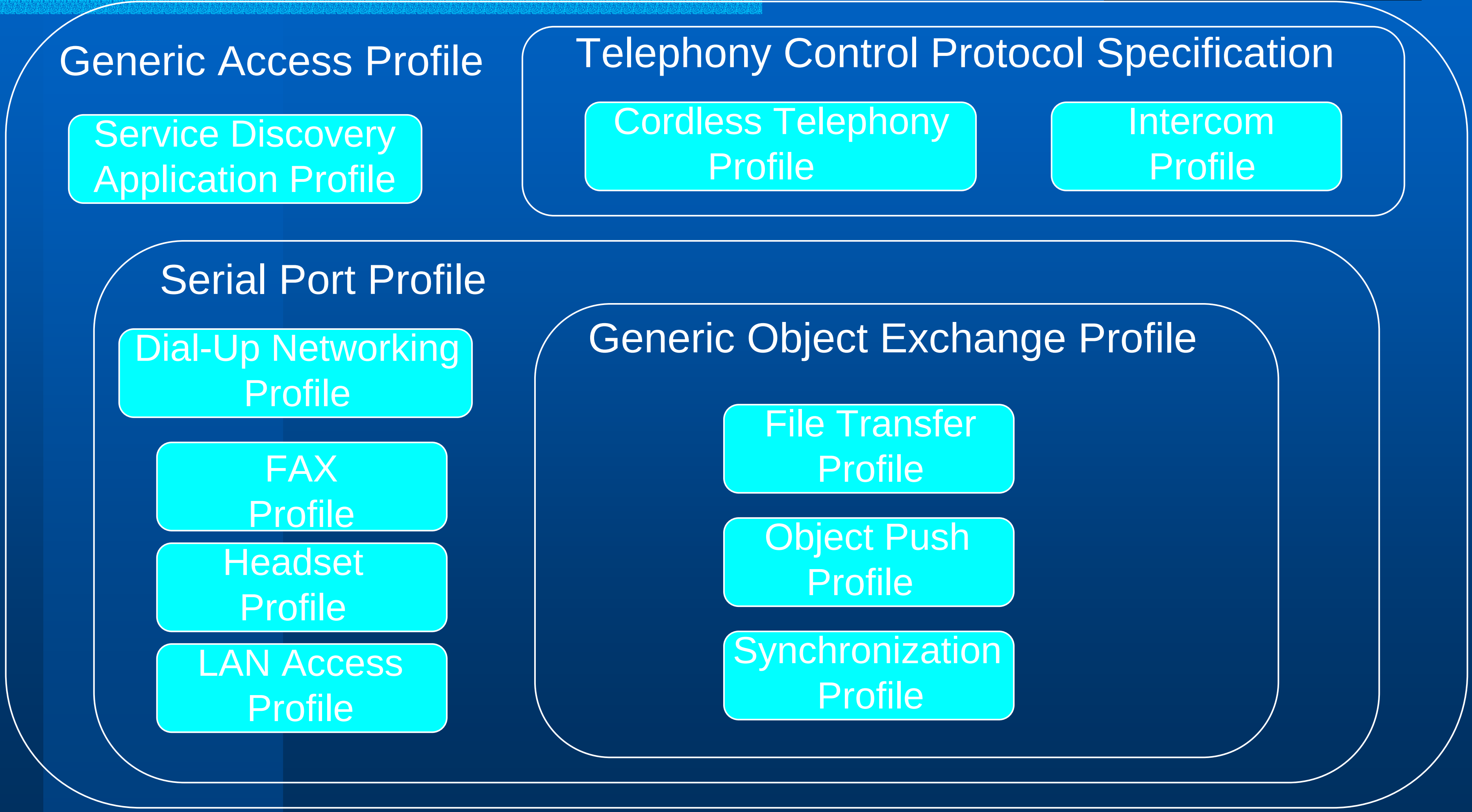
Application Profile Layer



Application

SDP

L2CAP



Generic Access Profile

Service Discovery Application Profile

Telephony Control Protocol Specification

Cordless Telephony Profile

Intercom Profile

Serial Port Profile

Dial-Up Networking Profile

FAX Profile

Headset Profile

LAN Access Profile

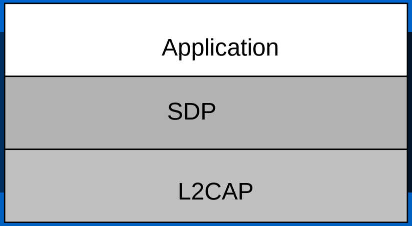
Generic Object Exchange Profile

File Transfer Profile

Object Push Profile

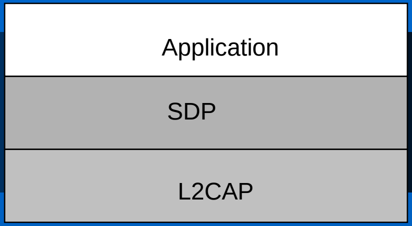
Synchronization Profile

BT Service Profiles (1)



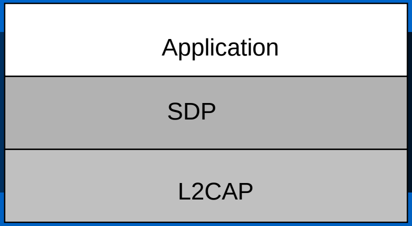
- Provide a clear specification of the protocol and features of a service for a given end-user function.
  - Originated from the ISO/IEC TR 10000
    - Applications share the same features.
    - Parameters are the same.
    - Mechanisms for communicating with other required profiles defined.
    - User interface guidelines are defined.
- Facilitates modular construction of new profiles upon existing profiles.
- Common Look and Feel for Consumers.

BT Service Profiles (2)



- All Profiles are development by the Bluetooth SIG Community.
  - Expensive to Participate.
  - Custom Application Services can be developed but there is no mechanism by which they can be adopted, except the through the Bluetooth SIG.
- The approach is not conducive to “Green” devices. Support for the profile must already exist in the device.
- Difficult to leverage existing services since they do not conform to a BT profile.
- A Service Profile definition is not machine readable, therefore the core work is performed by the developer of a profile in interpreting the profile.

Headset Profile (1)

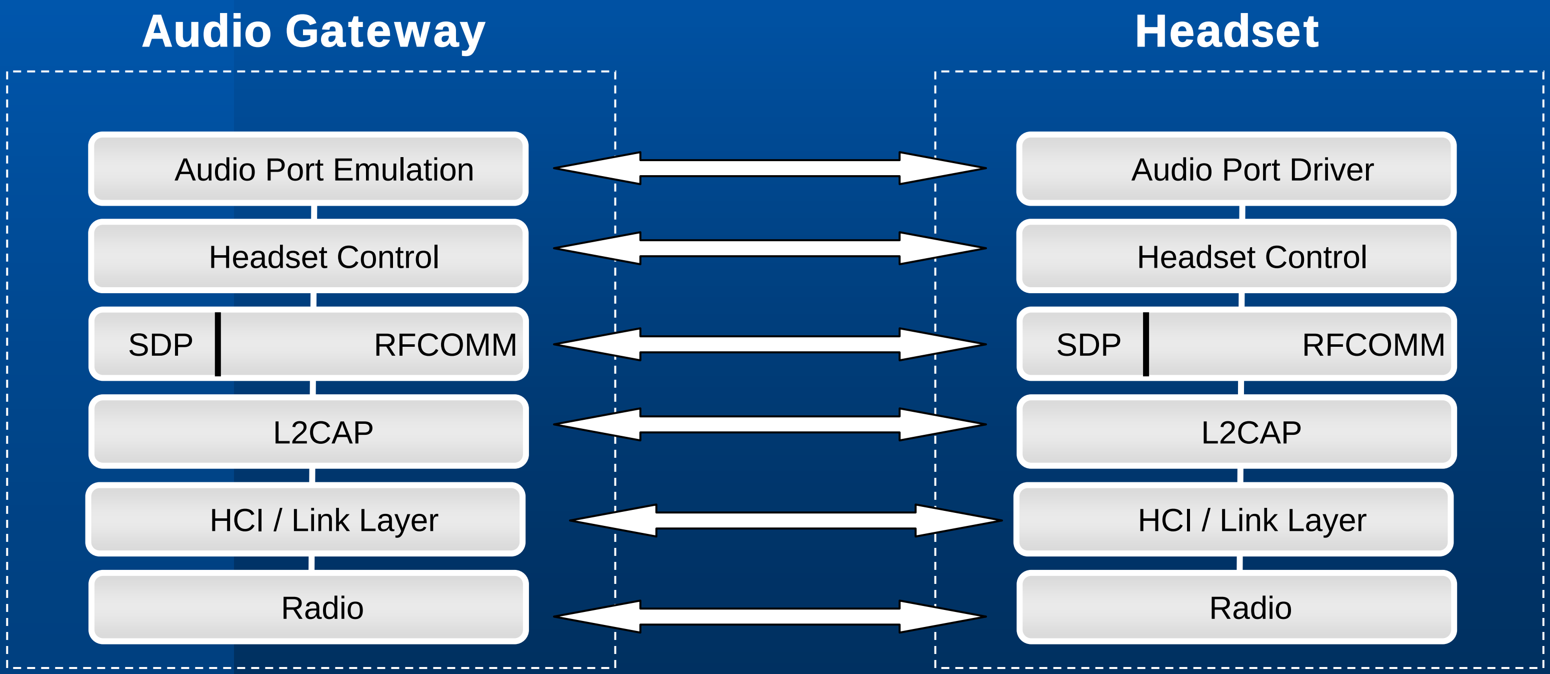


Application

SDP

L2CAP

- Defines 2 Roles
  - Audio Gateway (AG) - Device that is the gateway for the audio channel.
  - Headset (HS) - Device acting as remote mechanism.



Audio Gateway

Audio Port Emulation

Headset Control

SDP | RFCOMM

L2CAP

HCI / Link Layer

Radio

Headset

Audio Port Driver

Headset Control

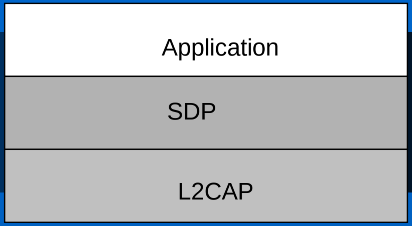
SDP | RFCOMM

L2CAP

HCI / Link Layer

Radio

Headset Profile (2)



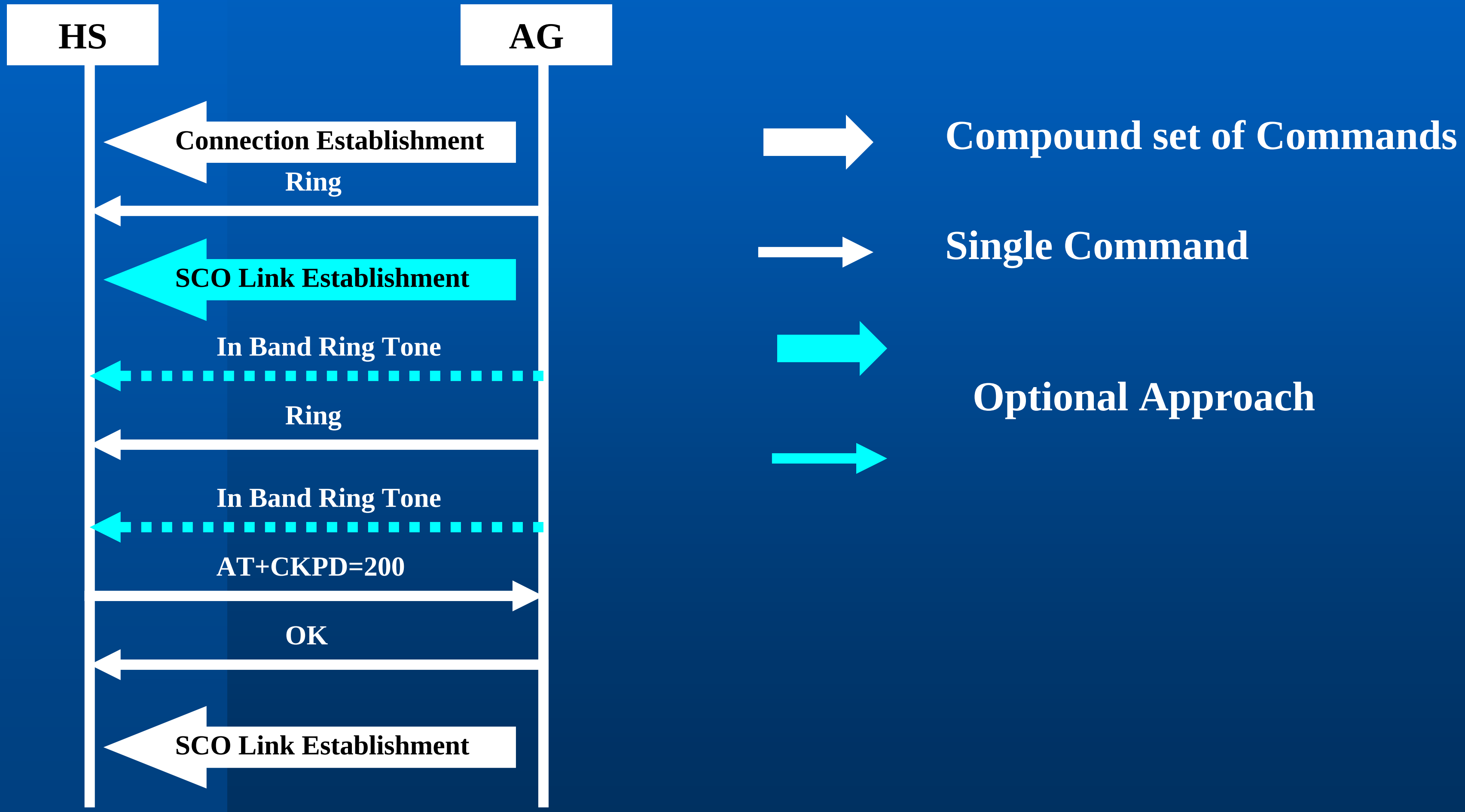
Application

SDP

L2CAP

- Constraints:
  - The profile mandates the usage of CVSD for transmission of audio.
  - Between headset and audio gateway, only one audio connection at a time is supported;
  - The audio gateway controls the SCO link establishment and release.
  - The profile offers only basic interoperability – for example, handling of multiple calls at the audio gateway is not included;
  - The only assumption on the headset’s user interface is the possibility to detect a user initiated action (e.g. pressing a button).

Headset Profile - Incoming Call



HS

AG

Connection Establishment

Ring

SCO Link Establishment

In Band Ring Tone

Ring

In Band Ring Tone

AT+CKPD=200

OK

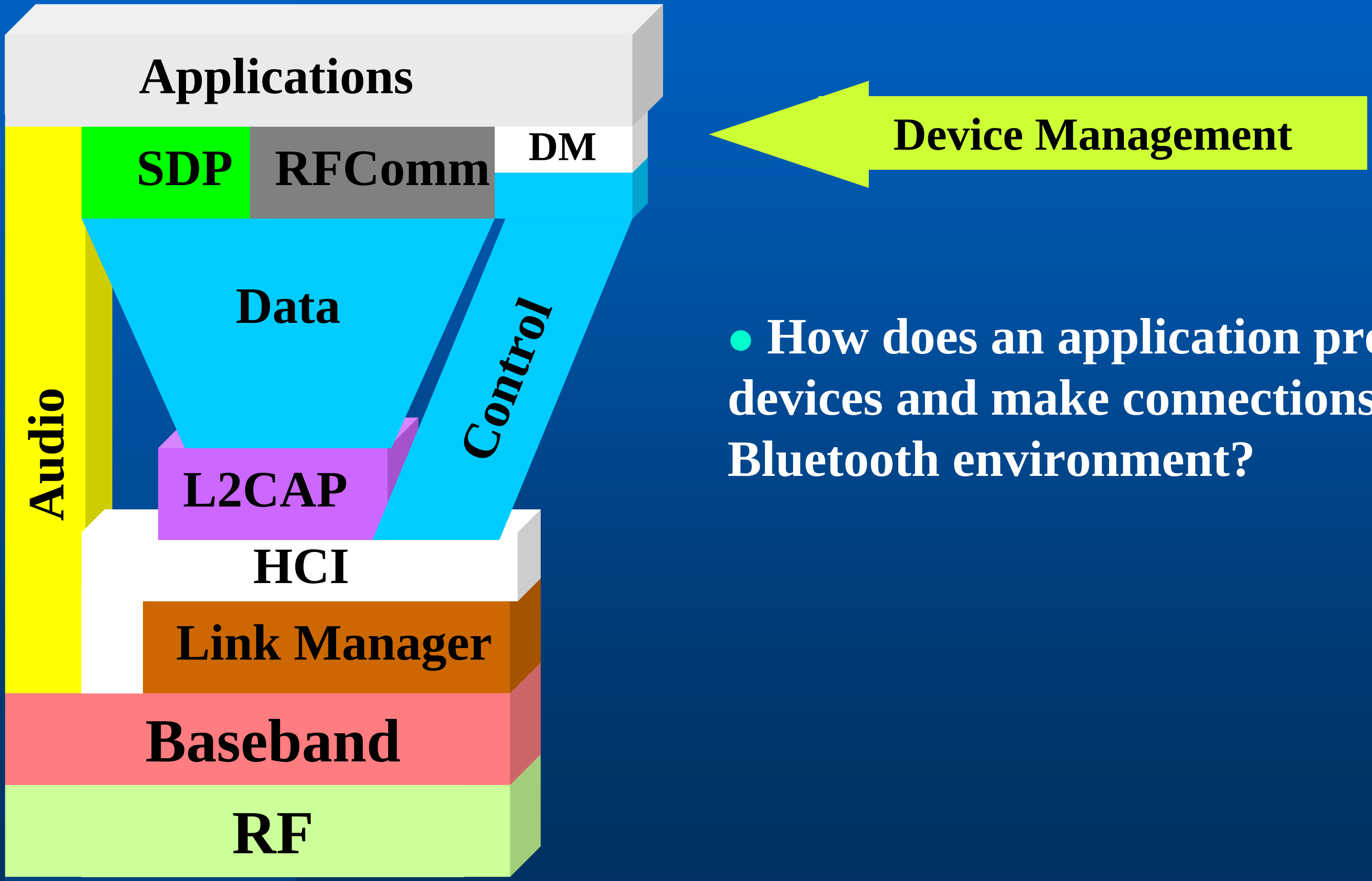
SCO Link Establishment

Compound set of Commands

Single Command

Optional Approach

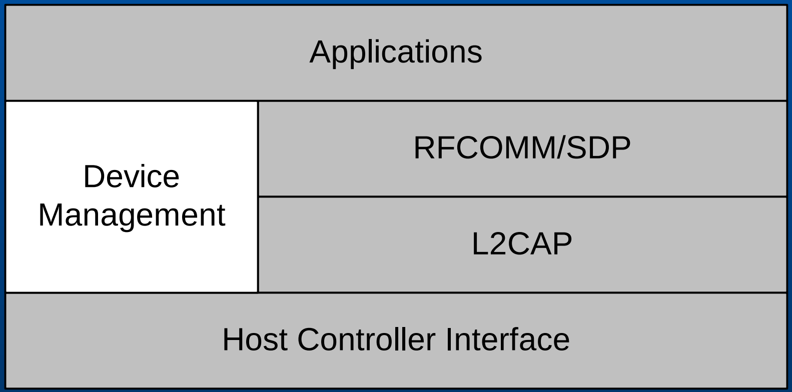
Device Management



- How does an application present devices and make connections in a Bluetooth environment?

Device Management

- **Generally, a solution provider creates a proprietary device management entity that conforms to the Generic Access Profile**



Applications

Device Management

RFCOMM/SDP

L2CAP

Host Controller Interface

New Bluetooth Initiatives

- Scatternets – Ad hoc Bluetooth networks.
  - The problem is one of properly coordinating the Master / Slave roles in order to create the scatternet properly.
- WLAN Profile – IP over Bluetooth.
  - An important profile driven by Microsoft in order to support short range wireless ethernet.
- 802.15 Initiatives
  - High Bandwidth WPAN 802.15.3
- Java APIs for Bluetooth Wireless Technology (JSR-82).
  - Java Open Communities Effort by Motorola.

What is the Future for Bluetooth?

“The future of Bluetooth looks bright because it meets the basic need of connectivity in close proximity.”

References

- Core Bluetooth Specification v1.1, Feb 2001.
- Personal Area Networks over Bluetooth, Presentation, Stefan Mahlknecht, ICT, Tu-Wien.
- Bluetooth Revealed by Brent A. Miller, Chatschik Bisdikian.
- Bluetooth 1.1: Connect Without Cables (2nd Edition), by Jennifer Bray, Charles F. Sturman, Joe Mendolia.
- Bluetooth Profiles, Dean Gratton, 2002.