Personal Area Network (PAN)
Bluetooth
(IEEE – 802.15.1)

Bhupendra Pratap Singh

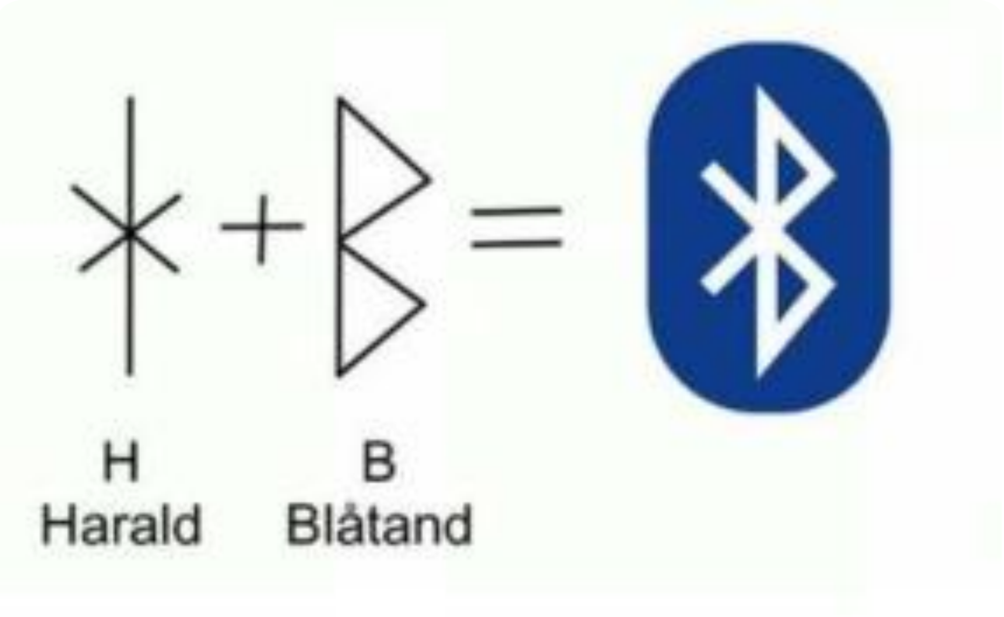
Bluetooth : What/Where

- One of the most popular short-range wireless communication standard
- Known as IEEE 802.15.1, now maintained by SIG (Special Interest Group)

Bluetooth is everywhere

- How many Bluetooth devices are there in the room?
- Cellphones, wireless mouse/keyboard, smart watch/bracelet, earphone,ibeacon,

Bluetooth: The Name



The name: Bluetooth

- Harald Gormsson
- Aka. Harald Blåtand (Harald Bluetooth)
- Likes to eat blueberries
- King of Denmark and Norway
- Unites the Norway, Sweden and Den mark
- Eloquent, good at communication

Bluetooth: How it all started

Invention

- 1994
- Erission
- a wireless alternative to RS-232 cable

Development

- 1997-1998
- Erission, Nokia, Toshiba, IBM, Intel
- Ver 0.7, 0.8 proposed

Publish

- 1999
- SIG (Special Interest Group) is founded
- Microsoft, Motorola, Samsung, Lucent with SIG
- Bluetooth 1.0 published

What is Bluetooth

- Facilitates voice and data transfers
- Allows users to connect a wide range of computing and telecommunications devices without cables
- Provides on-the-fly connections between devices
  - – Offers the possibility of ad hoc networks
- Delivers synchronicity between personal devices
- Packet based two-way communication
- Low power devices
- Small size
- Low cost (USD $5)

Bluetooth: The chronicle

Bluetooth 1.0

1998.10 – 2003. 11
“Base Rate”

- 1Mbps data rate
- V1.0 - Draft
- V1.0A - published on 1999.7
- V1.0B Enhanced the Interoperability
- V1.1 - IEEE 802.15.1
- V1.2 Enhanced the compatibility

Bluetooth 2.0 + EDR

2004. 11 – 2007. 7
“Enhanced Data Rate”

- Higher ordered modulation for data payload
- 2Mbps or 3Mbps physical data rate

- V2.0
- V2.1

Bluetooth 3.0 + HS

2009. 4
“HS Mode”

- AMP Alternative MAC/PHY
- Implement high data rate by using 802.11 protocols.
- Facing the Challenge from Wi-Fi

- V3.0

Bluetooth 4.0

2010. 6 – 2014. 12
“Low Energy”

- Facing the IoT application
- Changed the protocol greatly, almost a new technology

- V4.0
- V4.1
- V4.2

Bluetooth Scenario

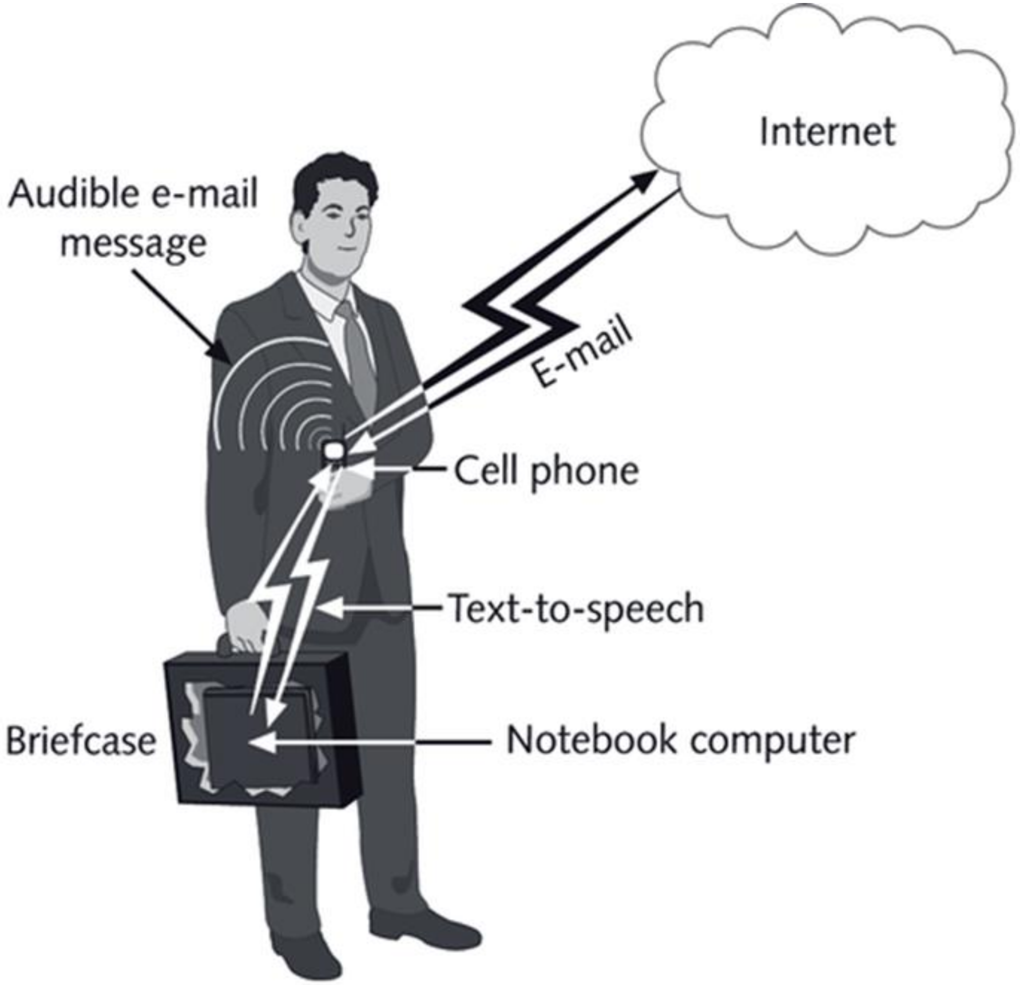


Figure 5-1 Bluetooth scenario

Bluetooth Specifications

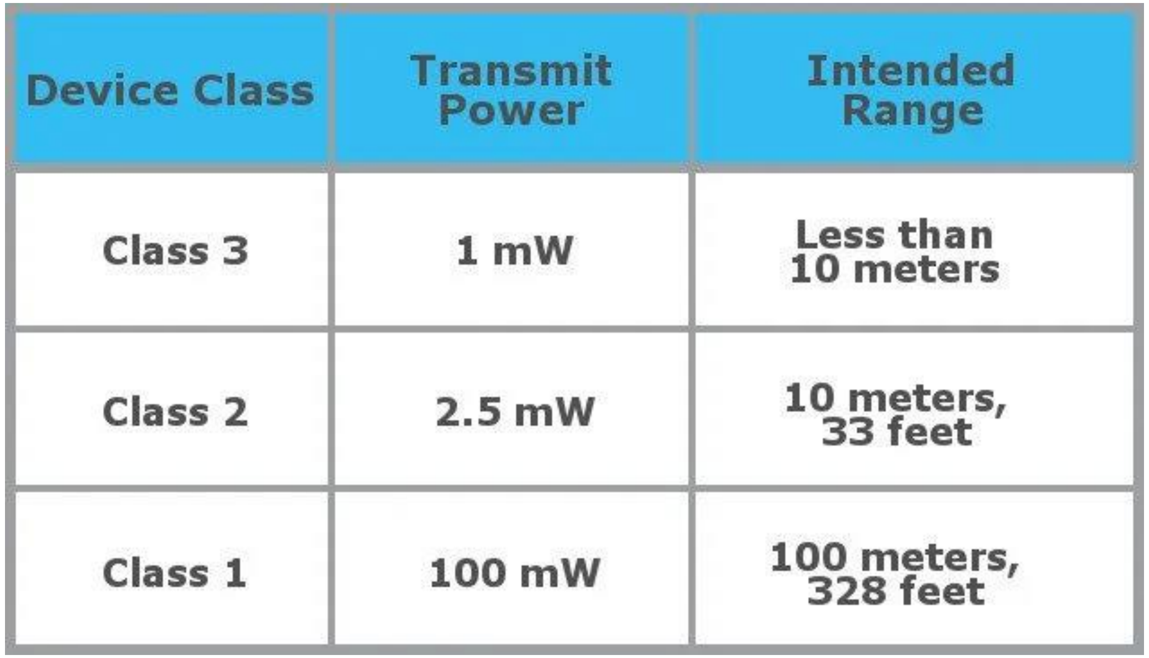
- Specification contains both link layer and application layer definitions, for data and voice applications
- Operates in the unlicensed industrial, scientific and medical (ISM) band at 2.4 to 2.485 GHz,
- Uses spread spectrum, frequency hopping, full-duplex signal at a nominal rate of 1600 hops/sec.
- Uses adaptive frequency hopping (AFH) to reduce interference between wireless technologies sharing the 2.4 GHz spectrum.

Cont…

The operating range depends on the device class:

- **Class 3 radios** – have a range of up to 1 meter
- **Class 2 radios** – most commonly found in mobile devices – have a range of 10 meters
- **Class 1 radios** – used primarily in industrial use cases – have a range of 100 meters
- **The most commonly used radio Class 2 uses 2.5 mW of power.**
- **radios are powered down when inactive**
- **Data Rate**
- 1 Mbps for Version 1.2
- Up to 3 Mbps supported for Version 2.0

Power Transmitted vs Range



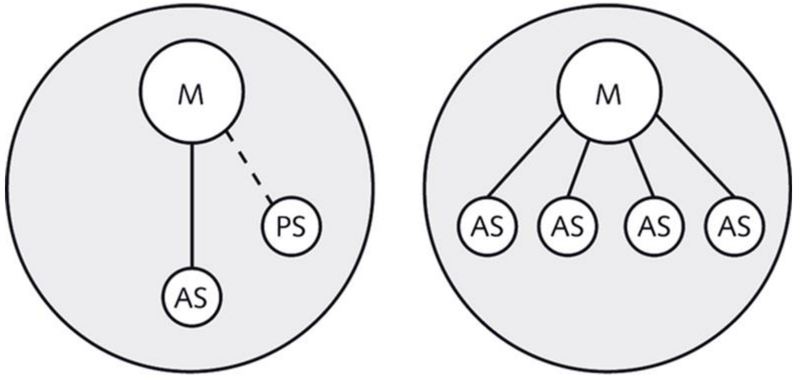
Device Class	Transmit Power	Intended Range
Class 3	1 mW	Less than 10 meters
Class 2	2.5 mW	10 meters, 33 feet
Class 1	100 mW	100 meters, 328 feet

Architecture & Operations

- During typical operation, a physical radio channel is shared by a group of devices
- Synchronized to a common clock and frequency hopping pattern.
- One device provides the synchronization reference and is known as the master.
- All other devices are known as slaves.
- A group of devices synchronized in this fashion form a **Piconet**.

Piconet

- One master and at least one slave using the same channel
- An active slave is sending transmissions
- A passive slave is not actually participating.
- 7-member address space (3 bits, with zero reserved for broadcast), which limits the maximum size of a Piconet to 8 device



M = Master
AS = Active slave
PS = Parked slave

Figure 5-9 Piconets

- **A Piconet can contain up to seven slaves clustered around a single master.**
- **The device that initializes establishment of the Piconet becomes the master**
- **One Master, 7 Slave Devices (Max 255 Devices, but other than 8 should be in parked mode/standby mode**

Scatternet

- Multiple Piconet can cover same area with different master and hop sequences
- Device can be a member of two or more overlaying Piconet
- **Group of Piconet connected is called a Scatternet**
- Communication among Piconet occurs using master device address and clock for each Piconet
- Bluetooth device can be a slave in several Piconet, but master in only one

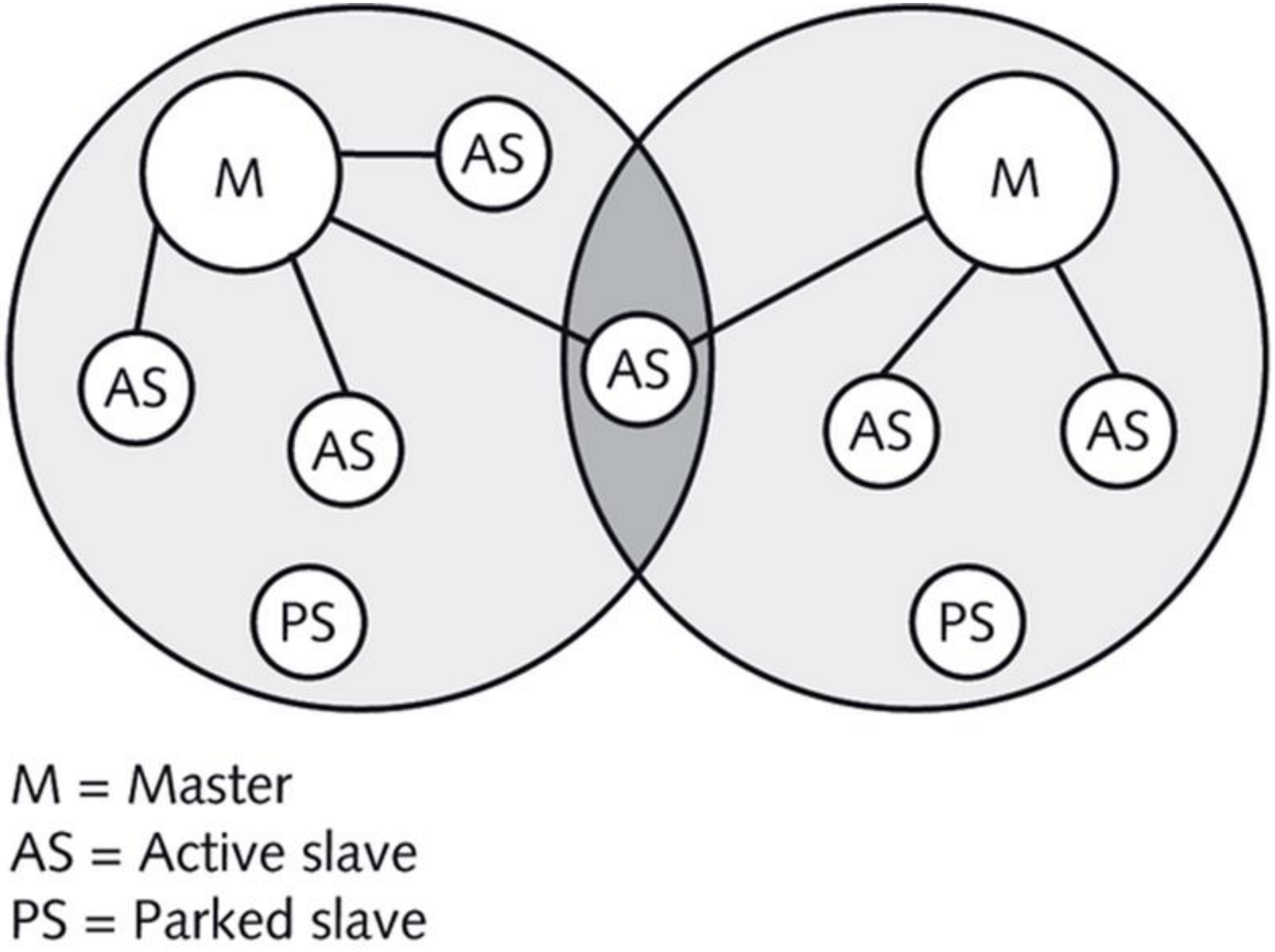


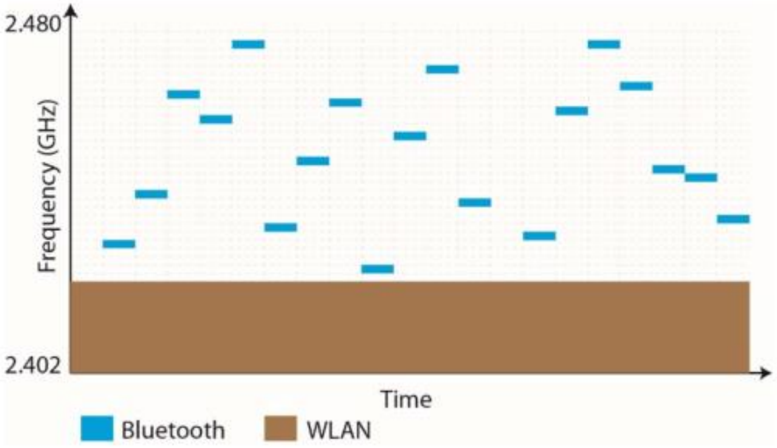
Figure 5-16 Scatternet

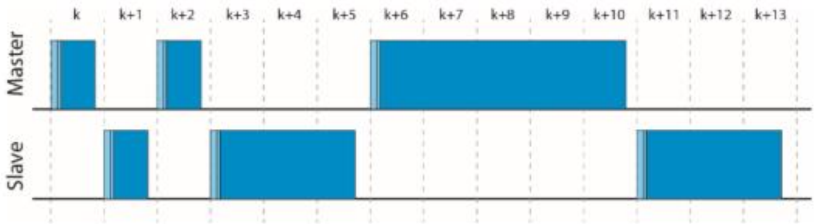
Frequency Hopping : A visit

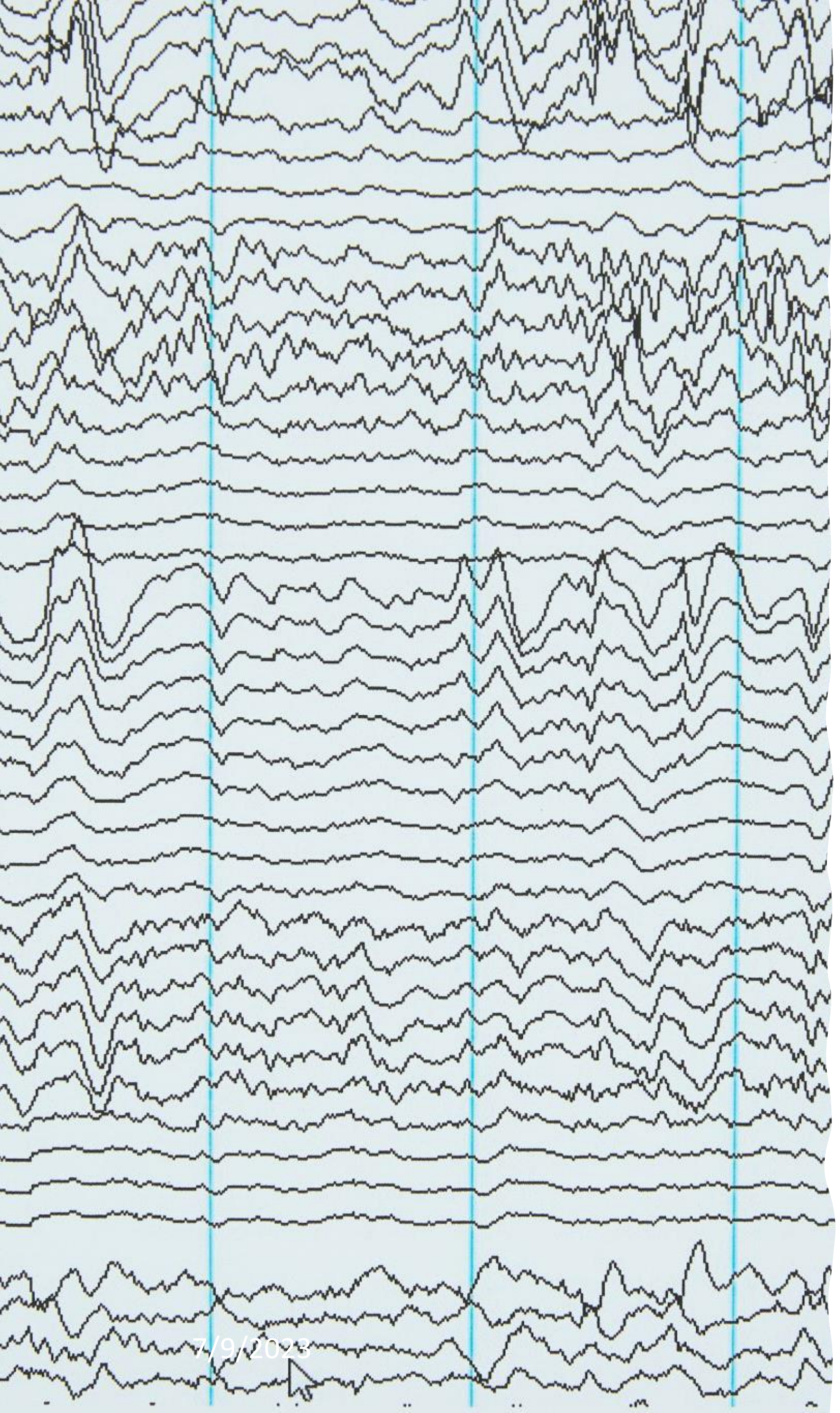
- A technology that spreads its signal over rapidly changing carrier frequencies
- (Hedy Lamarr (1914 – 2000) -
  (Movie Star and Inventor)
- Made an auto piano with her husband
- Received a patent in 1942 on Frequency Hopping“ Secret Communication System”
  Patent No. 2,292,387
- The patent expired in 1959
  but no one used FH until 1962

Bluetooth and Frequency Hopping

- Frequency Hopping and Time slots
  - Fast. 1600 times / sec = 625us / slot
  - FH and AFH (Adaptive Frequency Hopping)
  - “Frequency Selection Kernel” Complicated algorithm, sometimes treated as a Black Box
  - FH sequence based on the “Bluetooth CLK” and “Bluetooth Address” of the Master device
  - Single-slot Packet and multi-slot packets







Hopping Pattern

- Devices in a Piconet use a specific frequency hopping pattern
- Pattern is algorithmically determined by certain fields address and clock of the master.
- It is a pseudo-random ordering of the 79 frequencies in the ISM band.
- The hopping pattern may be adapted to exclude a portion of the frequencies that are used by interfering devices.
- Improves co-existence with static (non-hopping) ISM systems when these are co-located

Data Transmission

- The physical channel is sub-divided into time units known as slots.
- Data is transmitted between devices in packets that are positioned in these slots.
- At times, a few consecutive slots may be allocated to a single packet.
- Frequency hopping takes place between the transmission or reception of packets.
- Effect of full duplex transmission using a time-division duplex (TDD) scheme.

Time division duplex (TDD) refers to duplex communication links where uplink is separated from downlink by the allocation of different time slots in the same frequency band. It is a transmission scheme that allows asymmetric flow for uplink and downlink data transmission

Data Transmission cont….

Bluetooth is a packet-based protocol with a master- slave structure.

One master may communicate with up to 7 slaves in a Piconet

The master switches rapidly from one device to another in a round-robin fashion.

Simultaneous transmission from the master to multiple other devices is possible via broadcast mode, but not used much.

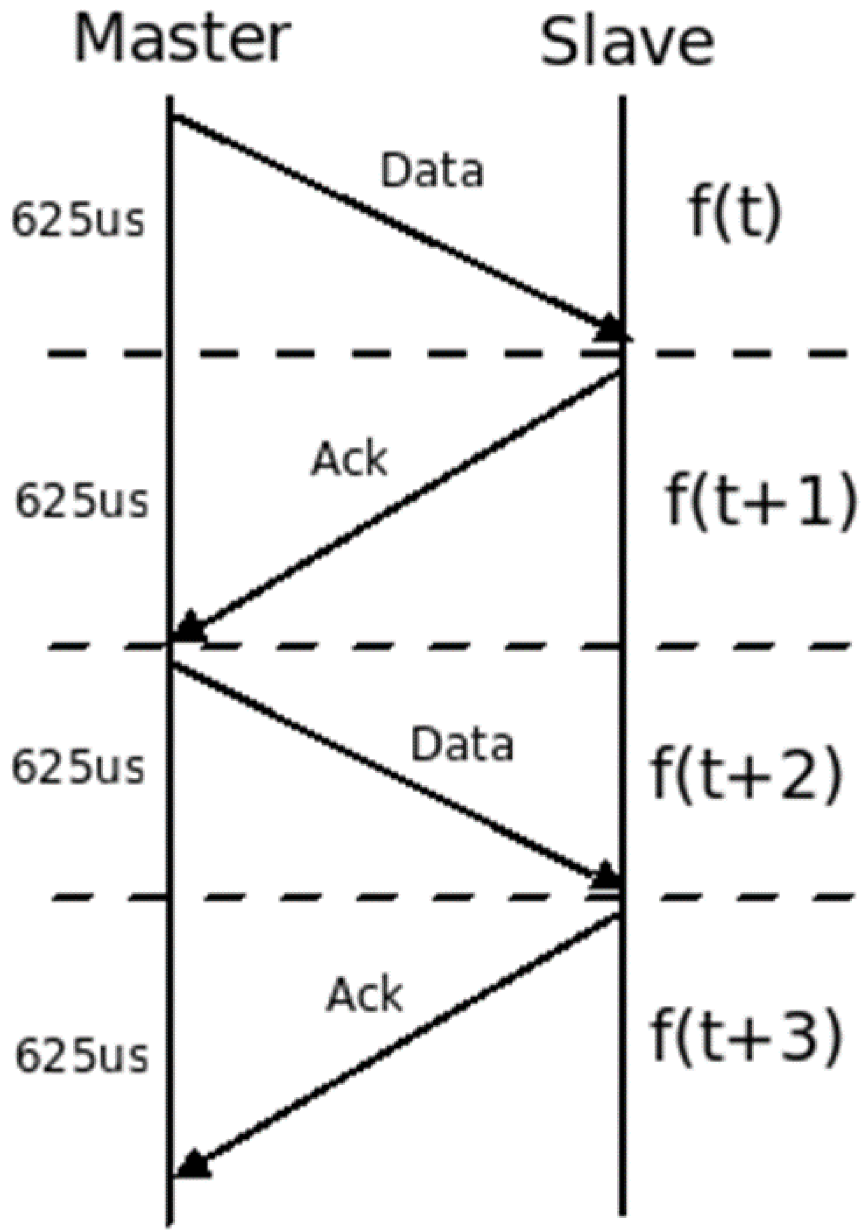
All devices share the master's clock.

Packet exchange is based on the basic clock, defined by the master, which ticks at 312.5 µs intervals.

Data Transmission cont….

- Two clock ticks make up a slot of 625 µs
  - two slots make up a slot pair of 1250 µs.
- In the simple case of single-slot packets the master transmits in even slots and receives in odd slots
  - the slave, conversely, receives in even slots and transmits in odd slots.
- Packets may be 1, 3 or 5 slots long
- but in all cases the master transmit will begin in even slots and the slave transmit in odd slots.

Bluetooth Sending Data



Bluetooth Protocol Stack

A view with Hardware and software stack perspective

What Is Bluetooth?

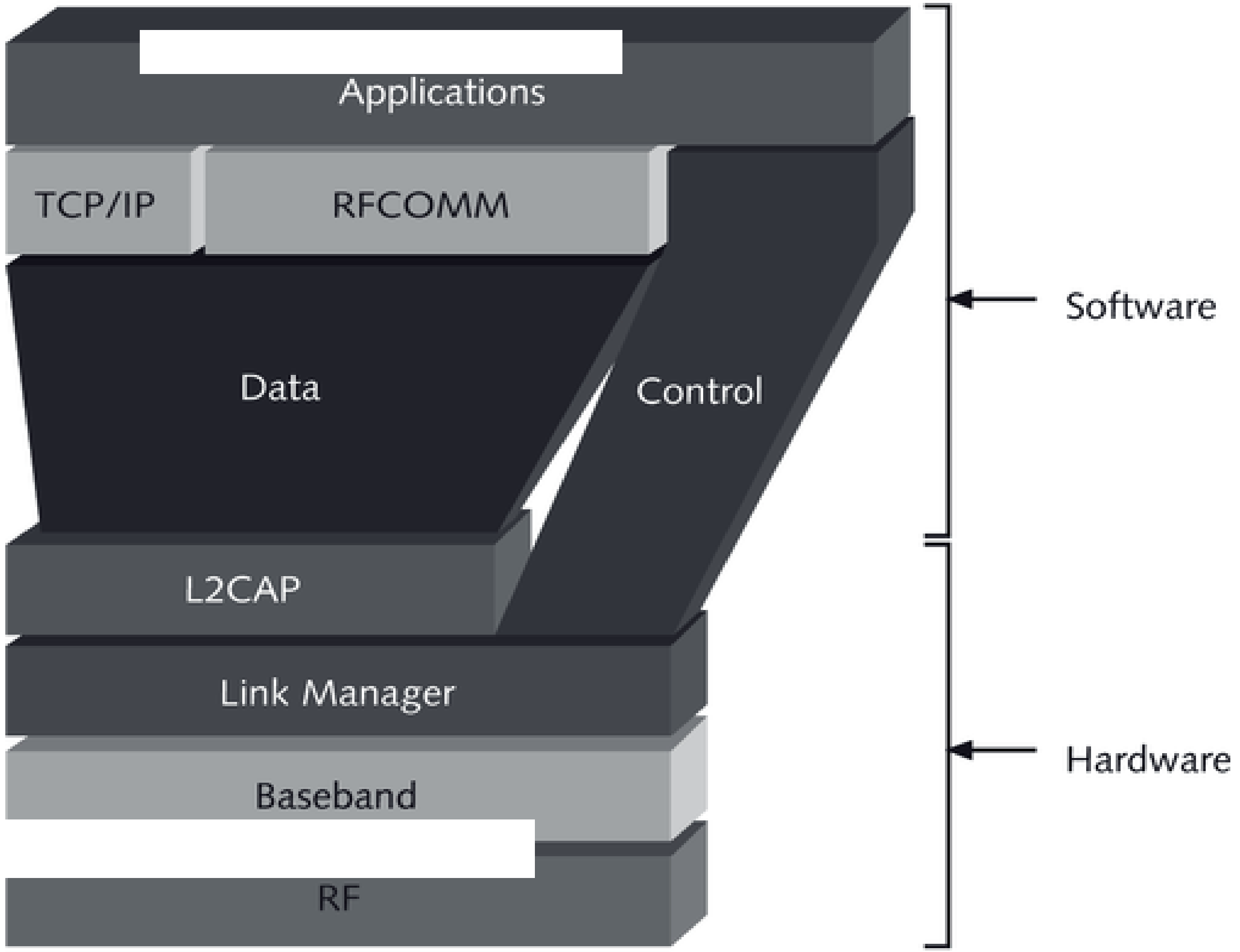
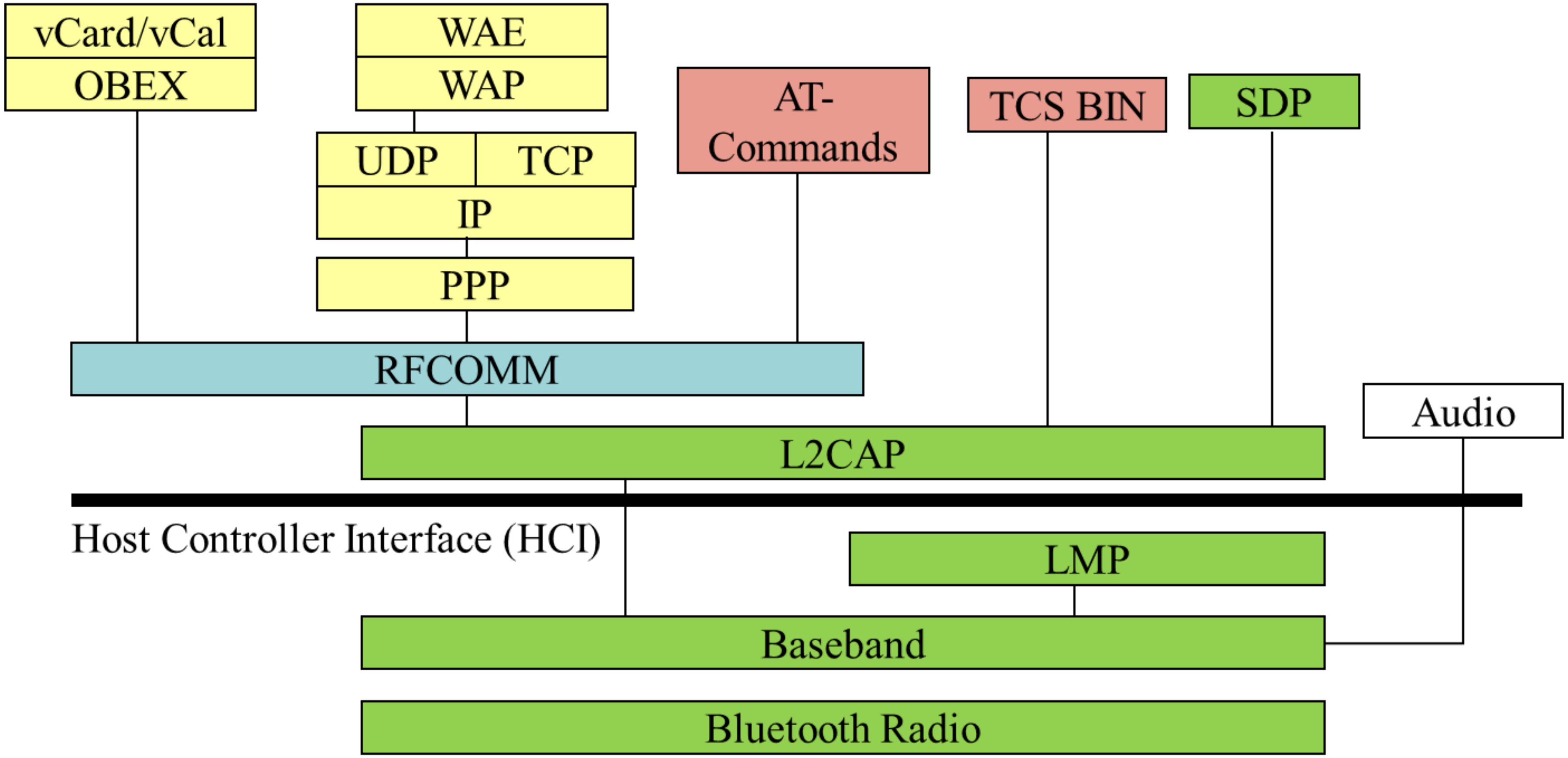


Figure 5-4 Bluetooth protocol stack

Bluetooth Protocol Stack



vCard/vCal

OBEX

WAE

WAP

UDP

TCP

IP

PPP

AT-Commands

TCS BIN

SDP

RFCOMM

L2CAP

Audio

Host Controller Interface (HCI)

LMP

Baseband

Bluetooth Radio

🟩 Bluetooth Core Protocol

🟦 Cable Replacement Protocol

🟨 Adopted Protocol

🟥 Telephony Protocol

Bluetooth Protocol Stack

- **Bluetooth Radio** : specifics details of the air interface, including frequency, frequency hopping, modulation scheme, and transmission power.

- **Baseband**: concerned with connection establishment within a piconet, addressing, packet format, timing and power control.

- **Link manager protocol (LMP)**: establishes the link setup between Bluetooth devices and manages ongoing links, including security aspects (e.g. authentication and encryption), and control and negotiation of baseband packet size

Bluetooth Protocol Stack

- **Logical link control and adaptation protocol (L2CAP)**: adapts upper layer protocols to the baseband layer. Provides both connectionless and connection-oriented services.

- **Service discovery protocol (SDP)**: handles device information, services, and queries for service characteristics between two or more Bluetooth devices.

- **Host Controller Interface (HCI):** provides an interface method for accessing the Bluetooth hardware capabilities. It contains a command interface, which acts between the Baseband controller and link manager

Bluetooth Protocol Stack

- **TCS BIN (Telephony Control Service)**: bit-oriented protocol that defines the call control signaling for the establishment of voice and data calls between Bluetooth devices.
- **OBEX(Object Exchange)** : Session-layer protocol for the exchange of objects, providing a model for object and operation representation.
- **RFCOMM**: a reliable transport protocol, which provides emulation of RS232 serial ports over the L2CAP protocol.
- **PPP** : is used to provide a method to transport datagrams over this emulated serial link(RFCOMM).
- **WAE/WAP**: Bluetooth incorporates the wireless application environment and the wireless application protocol into its architecture.

*WAP (Wireless Application Protocol) & WAE – Wireless Application Environment

Connection Establishment States

- **Standby**
  - State in which Bluetooth device is inactive, radio not switched on, enable low power operation.
- **Page**
  - Master enters page state and starts transmitting paging messages to Slave using earlier gained access code and timing information.
- **Page Scan**
  - Device periodically enters page state to allow paging devices to establish connections.

Connection Establishment States

Inquiry

State in which device tries to discover all Bluetooth enabled devices in the close vicinity.

Inquiry scan

Most devices periodically enter the inquiry scan state to make themselves available to inquiring devices.

Connection Establishment Process

- Inquiry -- If two Bluetooth devices know absolutely nothing about each other, one must run an inquiry to try to discover the other. One device sends out the inquiry request, and any device listening for such a request will respond with its address, and possibly its name and other information.
- Paging (Connecting) -- Paging is the process of forming a connection between two Bluetooth devices. Before this connection can be initiated, each device needs to know the address of the other (found in the inquiry process).
- Connection -- After a device has completed the paging process, it enters the connection state. While connected, a device can either be actively participating or it can be put into a low power sleep mode.
- Active Mode -- This is the regular connected mode, where the device is actively transmitting or receiving data.
- Sniff Mode -- This is a power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (e.g. every 100ms).
- Hold Mode -- Hold mode is a temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode when that interval has passed. The master can command a slave device to hold.
- Park Mode -- Park is the deepest of sleep modes. A master can command a slave to "park", and that slave will become inactive until the master tells it to wake back up.

Layers

- The protocol architecture of the bluetooth consists of following in a bluetooth protocol stack.
- Core protocols consisting 5-layer protocol stack viz.
  - radio
  - baseband
  - link manager protocol,
  - L2CAP-logical link control and adaptation protocol
  - service discovery protocol.

Physical Channel and links

- Within a physical channel, a physical link is formed between any two devices that transmit packets in either direction between them.
- In a piconet physical channel there are restrictions on which devices may form a physical link.
  - There is a physical link between each slave and the master.
  - Physical links are not formed directly between the slaves in a piconet.

Physical links

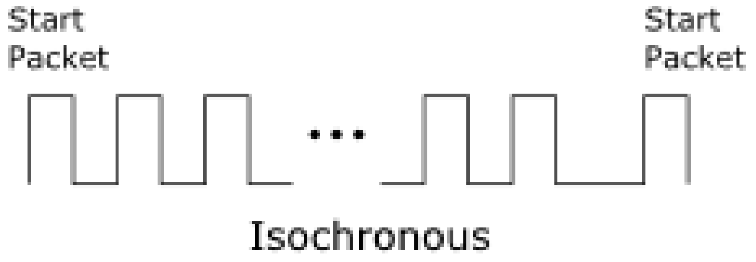
- Synchronous Connection Oriented (SCO)
    - Support symmetrical, circuit-switched, point-to-point connections
    - Typically used for voice traffic.
    - Data rate is 64 kbit/s.
- Asynchronous Connection-Less (ACL)
    - Support symmetrical and asymmetrical, packet-switched, point-to-multipoint connections.
    - Typically used for data transmission .
    - Up to 433.9 kbit/s in symmetric or 723.2/57.6 kbit/s in asymmetric

Logical Transport

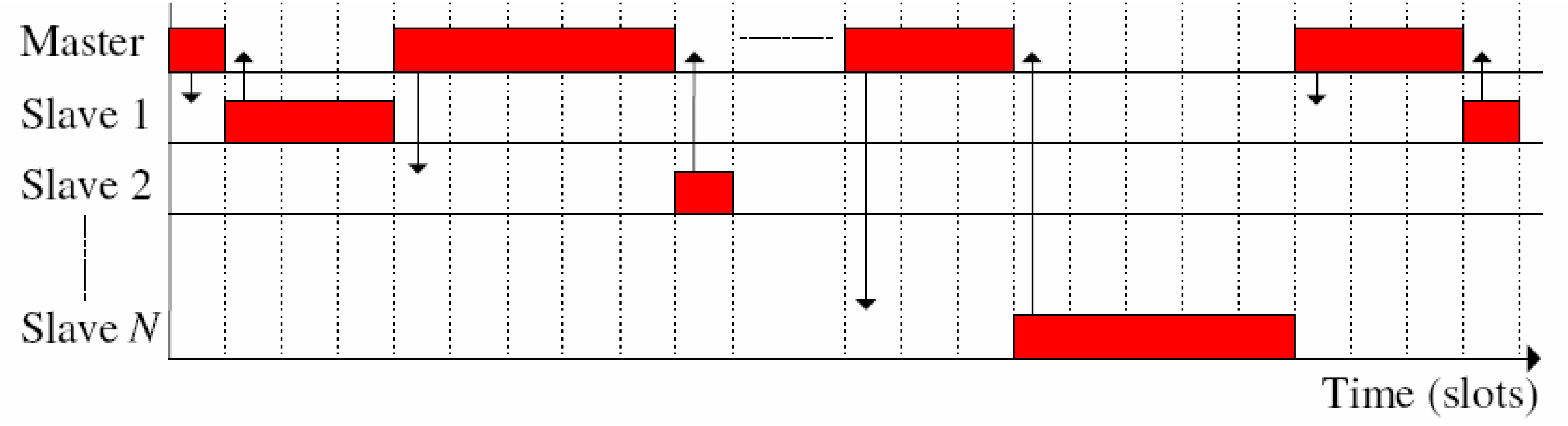
- The physical link is used as a transport for one or more logical links that support
  - unicast synchronous,
  - asynchronous and isochronous traffic,
  - broadcast traffic
- Traffic on logical links is multiplexed onto the physical link by occupying slots assigned by a scheduling function in the resource manager
- A control protocol, Link Manager Protocol (LMP) is carried over logical links in addition to user data.

Revisiting isochronous data Transfer

- An isochronous data transfer system combines the features of an asynchronous and synchronous data transfer system. An isochronous data transfer system sends blocks of data asynchronously, in other words the data stream can be transferred at random intervals. Each transmission begins with a start packet.



Time Division Duplexing



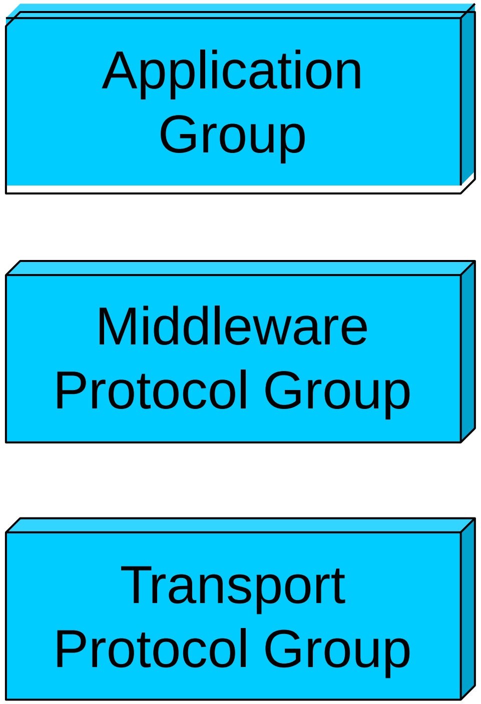
SCO Link- Voice

- Synchronous connected-oriented (SCO) link is used primarily for voice transmission at a speed of 64 Kbps
- It is a Symmetrical point-to-point connection between a master and a single slave
- A master can support up to three simultaneous SCO links while slaves can support two or three SCO links

ACL- Data

- Asynchronous connection-less Link (ACL) is used for transmission of data
- Packet-switched link from one master to all slaves Also called point-to-multipoint link
- Only one ACL link can exist.
- The default ACL logical transport is created whenever a device joins a piconet.

High Level View of Bluetooth stack



Application Group

Middleware Protocol Group

Transport Protocol Group

Transport Protocol Group

- To allow devices to locate each other
- To create, configure and manage Physical and Logical links
  - To allow higher layers to pass data through this layer
- Protocols in this group are
  - RF, baseband
  - Link Manager Protocol(LMP)
  - L2CAP

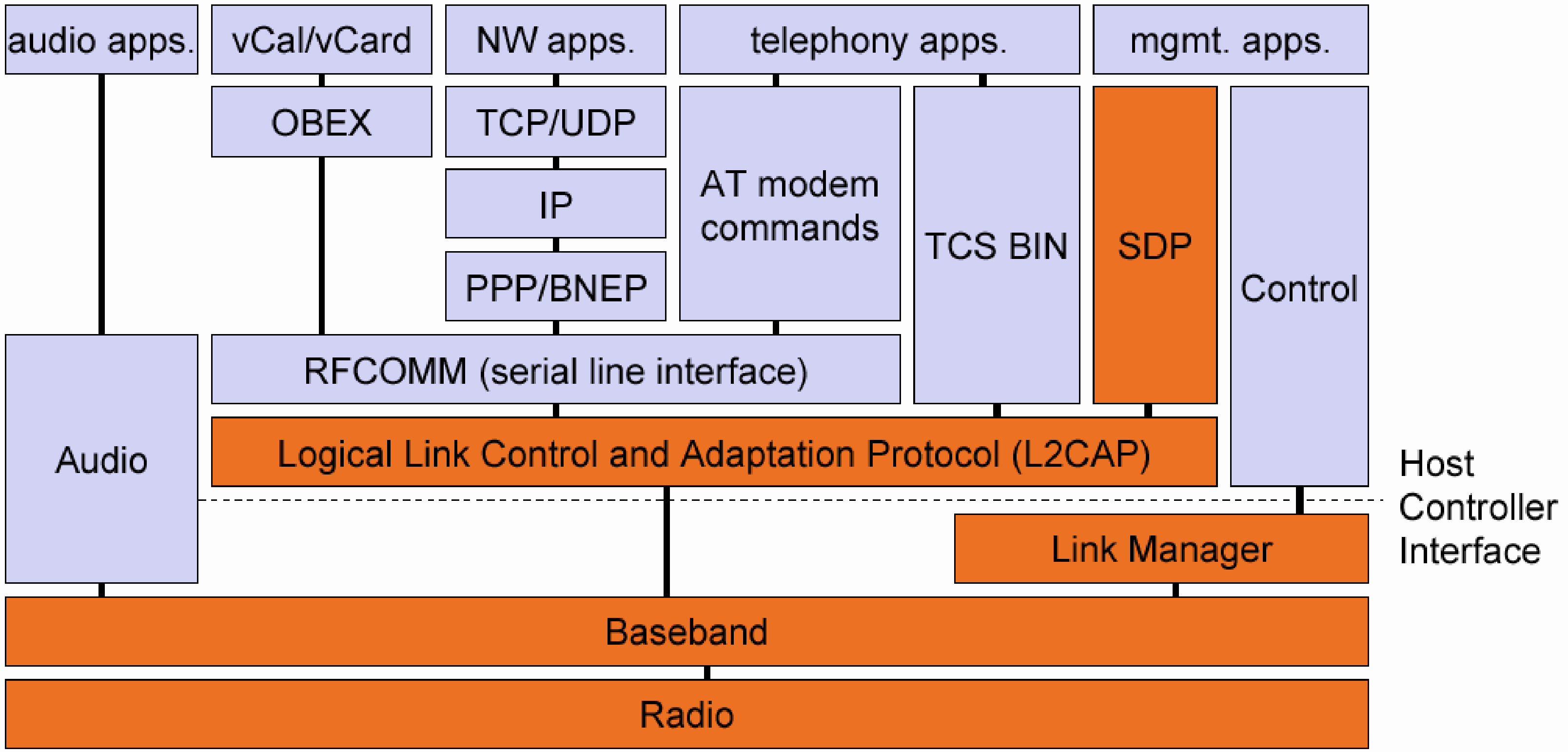
Middleware Protocol Group

- Includes transport protocols required for existing and new applications to operate over bluetooth
- They can be adopted
  - IP, PPP, OBEX, etc.
- They can be Bluetooth specific
  - RFCOMM, TCS-BIN, SDP, etc

Application Group

- Includes actual applications that make use of bluetooth links
- This could be legacy, unaware of bluetooth transports
  - Modem dialer
  - Web browser
- This could be bluetooth aware
  - One that uses TCS for controlling telephony equipment

Bluetooth protocol stack



AT: attention sequence
OBEX: object exchange
TCS BIN: telephony control protocol specification – binary
BNEP: Bluetooth network encapsulation protocol

SDP: service discovery protocol
RFCOMM: radio frequency comm.

Transport Protocol Group

Link Manager Protocol

- Link mangers in each device negotiate the properties of the air-interface between them using LMP
- Properties include bandwidth allocation to support
  - desired grade of service for data
  - periodic bandwidth reservation for audio traffic
- Other functions
  - Supervise device pairing, Authentication, Encryption, Power control

L2CAP

- Traffic from data applications is routed via L2CAP
- Supports protocol multiplexing
- Enables of segmentation of large packets and subsequent reassembly at receiving end
- Facilitates maintenance of desired level of service through negotiation with L2CAP on peer

Middleware Protocol Group

RFCOMM

- Legacy applications that use serial port
  - Peer to peer file and object transfer
  - Data synchronization
  - Dial up networking
- Provides abstraction for a serial port
- Makes migration of applications modeled for cabled serial communication, easy
- Modelled on ESTI TS07.10 standard, with adaptations for bluetooth

Service Discovery Protocol (SDP)

- Bluetooth usage model can be viewed as making use of some set of services
- In traditional LAN, these services are provided by servers which are statically configured
- In ad-hoc network, static configurations do not work, hence locating services becomes important
- Once communication channel is established, next logical step is to find out services available
- Service Discovery Protocol (SDP) defines a method to discover and learn about services offered by other devices and vice-versa

Telephony control Protocol (TCS)

- Telephony Control Specification layer is designed to support telephony functions
- It includes
  - Call control functions
  - Group management functions
  - Exchange of call signaling information

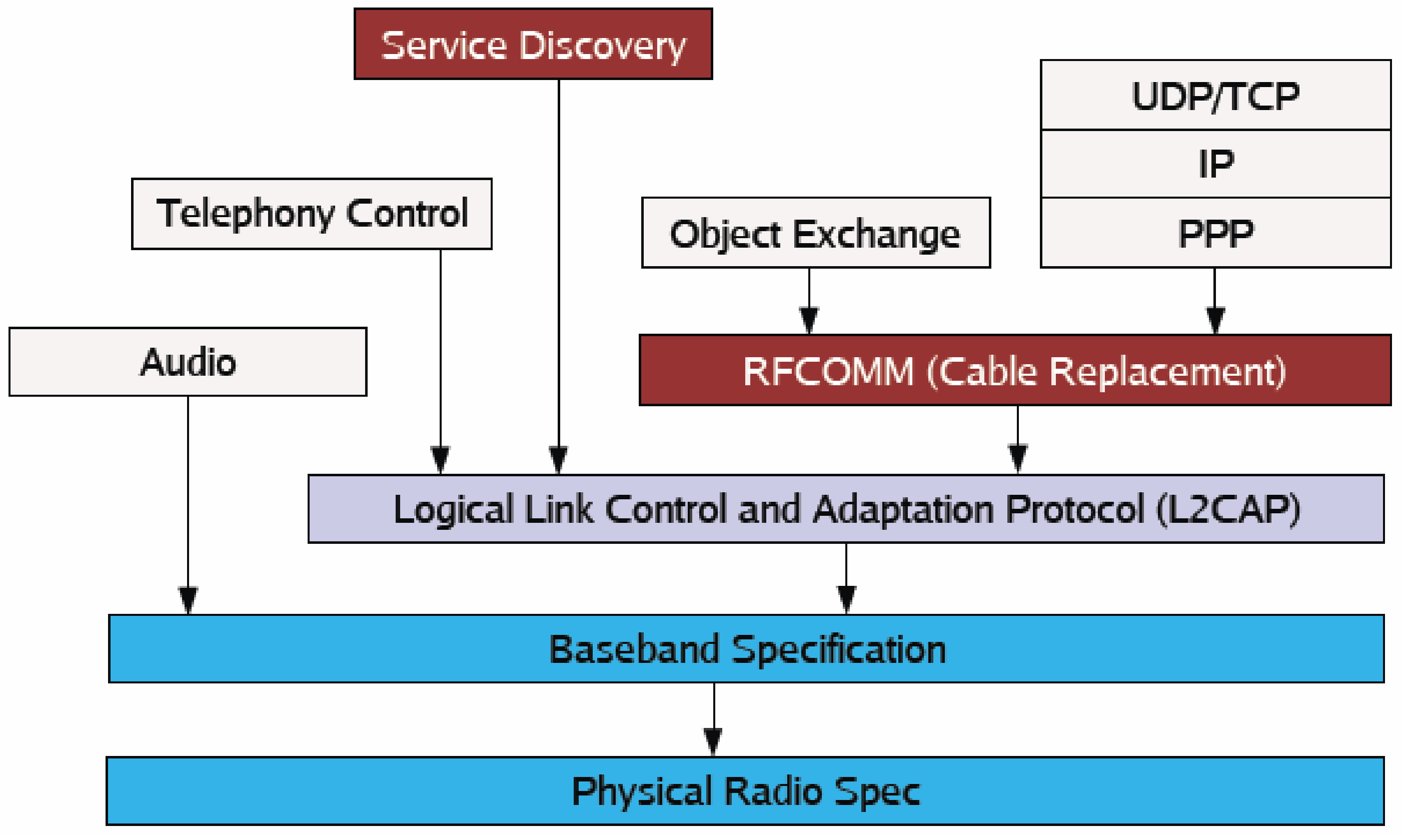
Audio

- Since Audio traffic is ischronous, it is directly routed to the baseband
- SCO packets are defined for use with audio traffic
- Rate is 64kbps and 8 bit logarithmic PCM or CVSD modulation
- In addition to voice, the channel can also other forms

  of audio like music or short audio clips

Continuously variable slope delta modulation (CVSD or CVSDM) is a voice coding method. It is a delta modulation with variable step size (i.e., special case of adaptive delta modulation)

Protocol Architecture



Bluetooth Profiles

- A Bluetooth profile is a specification regarding an aspect of Bluetooth-based wireless communication between devices.
- In order to use Bluetooth technology, a device must be compatible with the subset of Bluetooth profiles necessary to use the desired services.
- A Bluetooth profile resides on top of the Bluetooth Core Specification and (optionally) additional protocols.

Bluetooth Profiles(contd.)

- The profiles provide standards which manufacturers follow to allow devices to use Bluetooth in the intended manner

Eg. BH-505 supports

Advanced Audio Distribution Profile (A2DP) Audio/Video
Remote Control Profile (AVRCP)
Hands Free Profile(HFP) Headset
Profile (HSP)

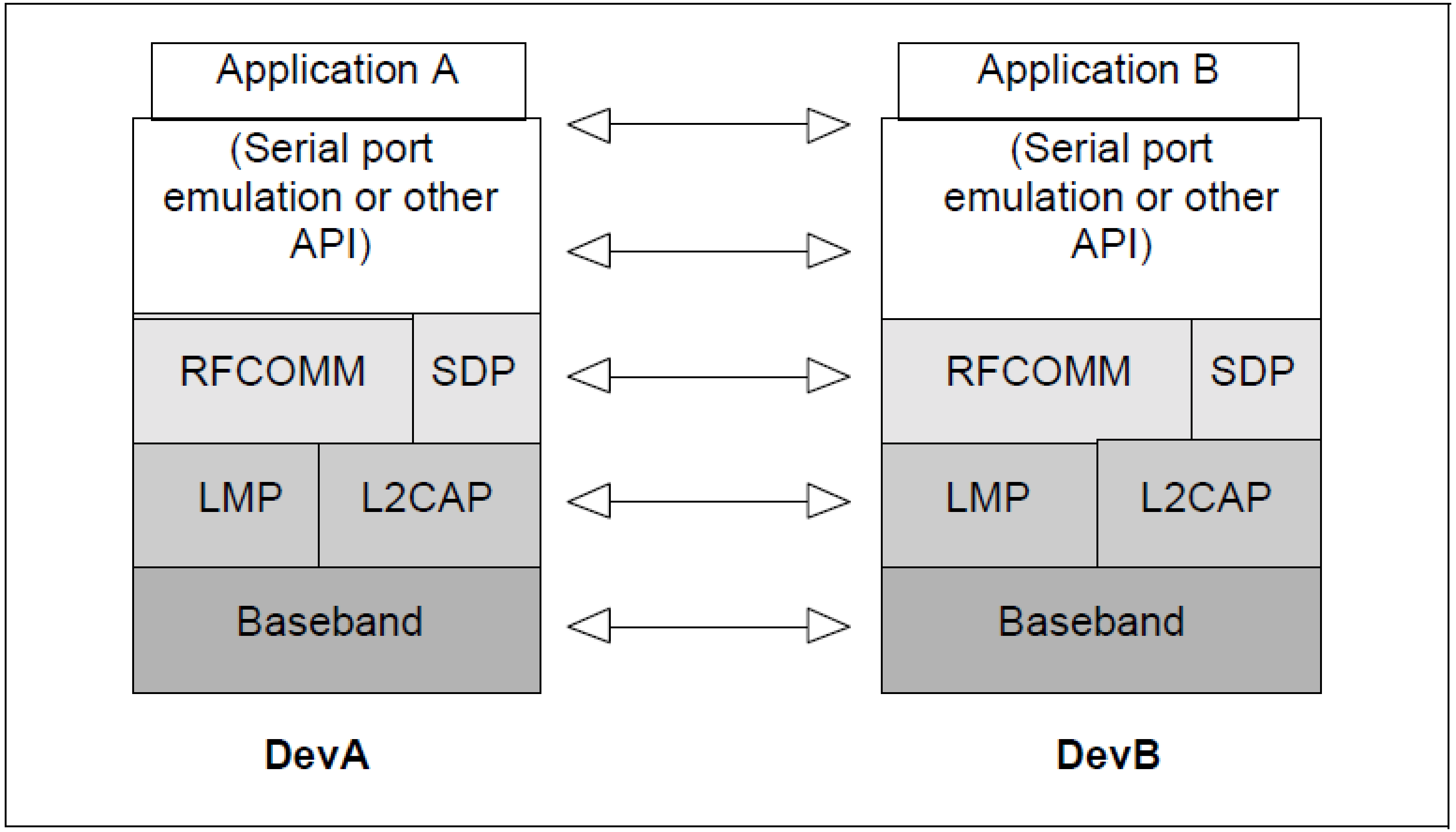
Bluetooth Profiles

- Generic
  - GAP Generic Access Profile
  - SDAP Service Discovery Application Profile
- Serial
  - SPP Serial Port Profile
  - GOEP Generic Object Exchange Profile
  - OPP Object Push Profile
  - FTP File Transfer Profile
  - SP Synchronization Profile

Bluetooth Profiles

- Telephony
  - CTP Cordless Telephony Profile
  - IP Intercom Profile
  - HS Headset Profile
- Networking
  - DNP Dial-up Networking Profile
  - FP Fax Profile
  - LAP LAN (Local Area Network) Access Profile

Serial Port Profile



Typical Applications

- Wireless control of and communication between mobile phone and hands-free headset.
  - –This was one of the earliest applications to become popular.

- Wireless networking between PCs in a confined space and where little bandwidth is required.
- Wireless communication of PC input/output devices
  - The common ones- mouse, keyboard and printer.
- Replacement of traditional wired serial communications
  - test equipment, GPS receivers, medical equipment, bar code scanners, traffic control devices.

Typical Applications(contd.)

- For controls where infrared was traditionally used.
- For low bandwidth applications where higher USB bandwidth is not required and cable-free connection desired.
- Wireless bridge between two Industrial Ethernet (e.g.,

PROFINET) networks.

- Game consoles like Nintendo Wii Sony's PlayStation 3, PSP G for respective wireless controllers.
- Short range transmission of health sensor data from medical devices to mobile phone, set-top box or dedicated telehealth device

Thank you !!