Wireless Technology Applications

Bluetooth Technology Part II

Melvyn U Myint Oo
T16620
68790688
melvyn_oo@sp.edu.sg

At the end of this lecture, you should be able to:

Explain Bluetooth technology

1. Bluetooth Link Manager Layer

2. Bluetooth Security

3. Bluetooth Link Controller State Diagram

4. Bluetooth Connection Procedure

5. Bluetooth Power Usage

6. Other Layers and Functions

7. Bluetooth Profile

8. Bluetooth Applications

9. WPAN Applications

Bluetooth Link Manager Layer

The duties of the Link Manager layer in the Bluetooth stack

- – managing the piconet
- – performing security
- – Error Correction
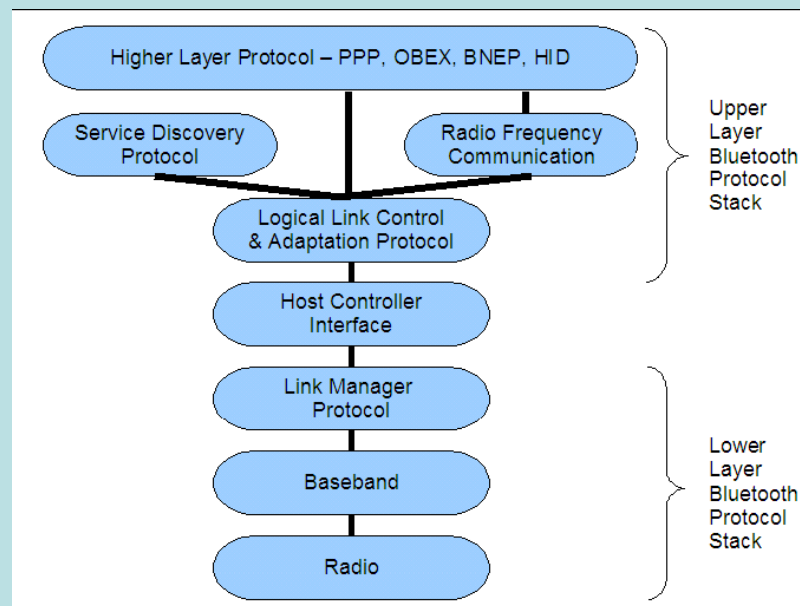
Bluetooth Link Manager Layer

Error Correction

- 1/3 rate Forward Error Correction (FEC)

- 2/3 rate Forward Error Correction and

- automatic retransmission request

1/3 rate Forward Error Correction (FEC)

- – Repeats every bit three times for redundancy. The maximum data rate is effectively divided by 3, hence the term 1/3 rate

# Bluetooth Link Manager Layer

Error Correction

2/3 rate FEC

- – Adds extra bits to data sent for error correction. These extra bits are examined by the receiving device to determine in an error took place in the transmission.

- – For example, if 8 bits of data were to be sent, they would be expanded into 12 bits, which includes the error correction data. The extra bits reduce the maximum data rate that can be achieved for a transmission, but allows the receiver to detect multiple bits errors and correct single bits errors, preventing retransmission of the data.

Official (Open), Non-sensitive

Bluetooth Link Manager Layer

Automatic retransmission request (ARQ)

- Continuously retransmits the data fields of a data-only or a data-voice packet until an acknowledgment is received or

- a timeout value is exceeded.

Automatic Retransmission
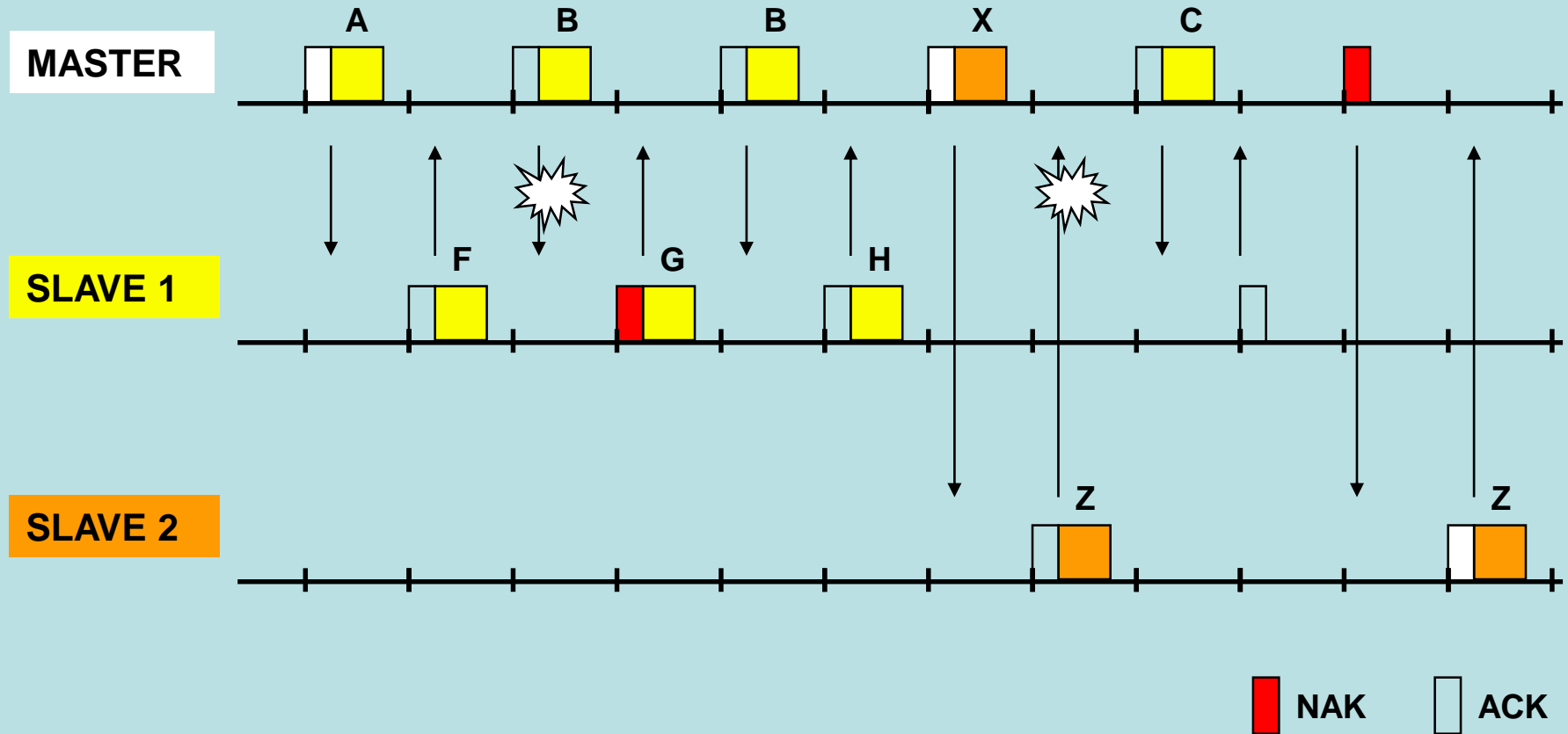
Bluetooth Security

~~Three~~(Four) security modes

- Mode 1 (nonsecure) does not enforce any security.

- Mode 2 (service level enforced security) enforces security when an L2CAP channel is established for the required service.

- Mode 3 (link level enforced security) enforces security when baseband ACL link is established

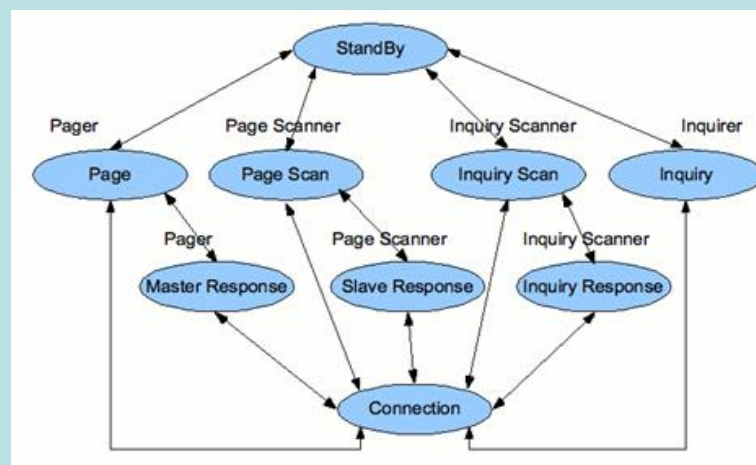- Mode 4: service level enforced security with encrypted key exchange (Bluetooth version 2.1 + EDR)

Link controller state and function

Standby

- Default state.

- When a Bluetooth-enabled device is not connected, it is in a **StandBy** state.

- It is a low-power state in which the native clock is running.

Connection

- The device is connected to a piconet as a master or slave.

Link controller state and function

- To discover other Bluetooth-enabled devices within its RF range, *the* **inquirer** *has to be in* **Inquiry** *state*.

- To allow other Bluetooth-enabled devices to discover its existence, *the* **inquiry scanner** *has to be in the* **Inquiry Scan** *state.*

- To response to an inquiry, *the* **inquiry scanner** *has to be in the* **Inquiry Response** *state to transmit an FHS (Frequency Hopping Synchronization) packet.*
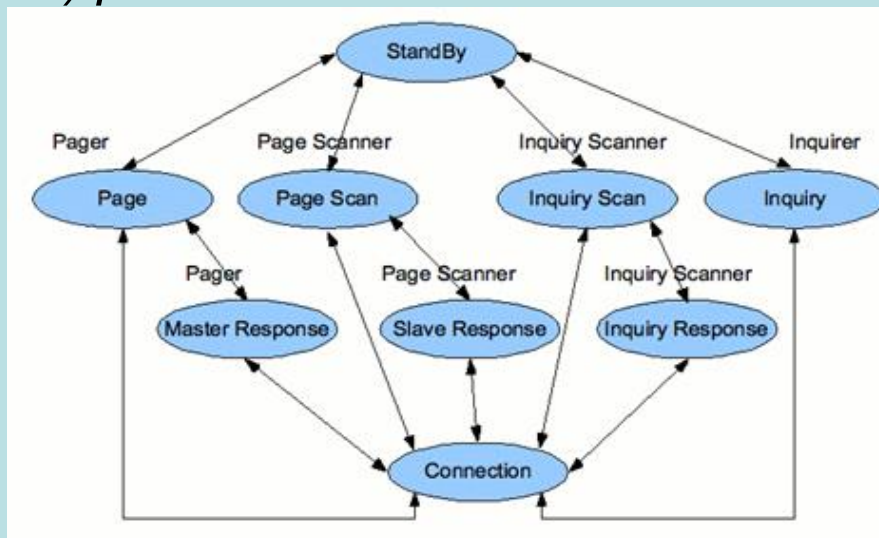
Bluetooth Connection Procedure

- The three procedures involves in establishing a connections are:
    - Inquiry procedure
    - Page procedure
    - Connection procedure

How do two Bluetooth devices get connected in the first place?
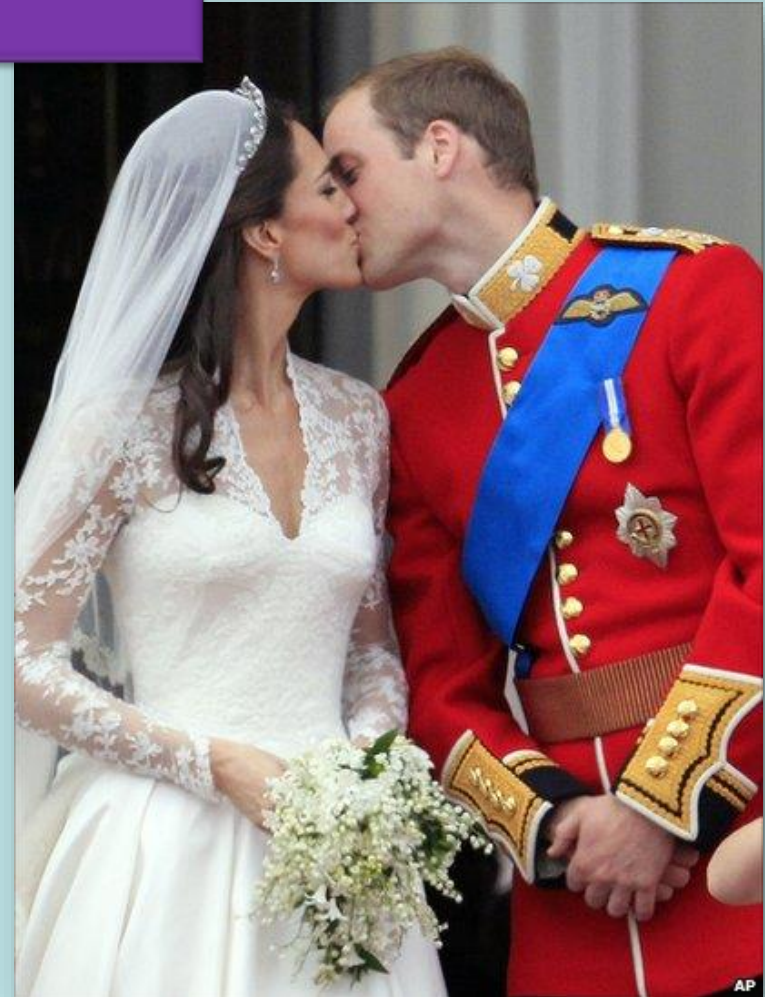
Three important procedures

Procedure 1: Inquiry

Procedure 1: Inquiry

- **Inquiry** is to discover other Bluetooth-enabled devices in range
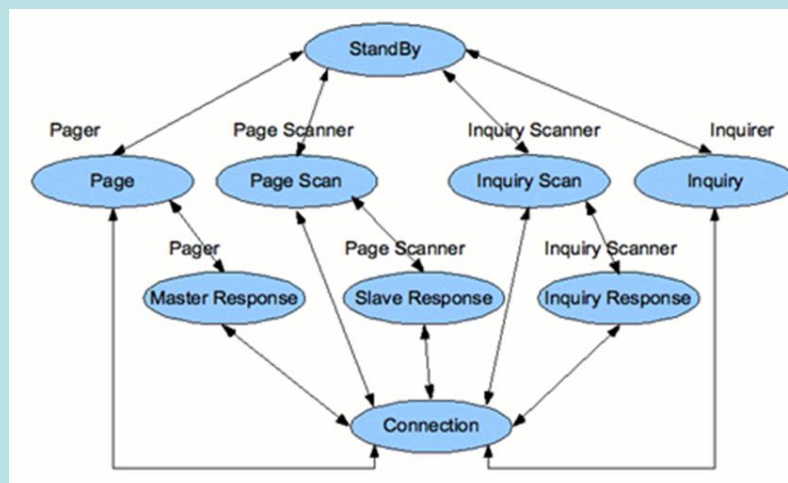
Bluetooth Connection Procedure

Inquiry Procedure

- It is the first step in establishing a piconet

- Potential Master identify devices in range that wish to participate in the piconet.
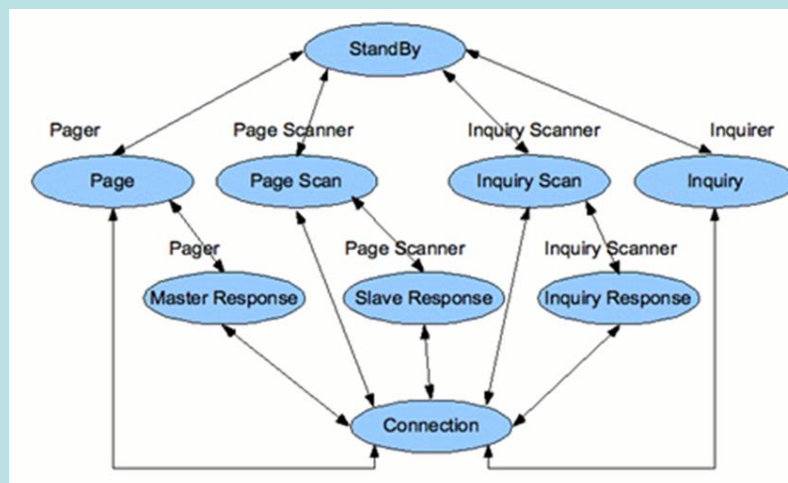
Procedure 2: Page

- Page is to connect the pair of Bluetooth-enabled devices

Bluetooth Connection Procedure

Paging Procedure

- Once the master has founds devices within it's range, it can establish a connection by paging the devices.

Procedure 3: Connection
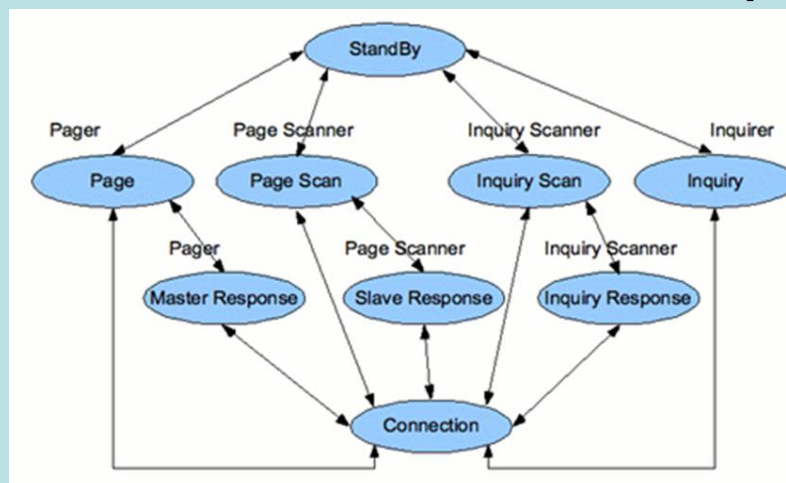
Bluetooth Connection Procedure

Connection procedure

- The connection states starts when the slave is switch to the master timing.

- Once the slaves in the Connection states, it can be in one of the four modes operation.
  - **Active**
  - **Sniff**
  - **Hold**
  - **Park**

Official (Open), Non-sensitive

Bluetooth Power Usage

- Battery powered

- conserving power is essential for Bluetooth

- Voice Transmission: 5 hrs

- Data Transmission: 120 hrs

- Idle or waiting for communication (low power mode): 3 months

Bluetooth Power Usage

- Active mode

  - the Bluetooth device actively participates on the channel

  - consumes an amount of power that corresponds to the type of data that is being transmitted

  - Example: Over a period of time this amount of power averages out to 2.5 mW or 4 dBm in a Power Class 2 device.

Bluetooth Power Usage

- Sniff mode
  - a slave device listens to the piconet master at a reduced rate so that it uses less power
  - The interval is programmable and depends on the application.

Bluetooth Power Usage

- Hold mode
  - slave units into **HOLD** mode demand
  - only an internal timer is running
  - Data transfer restarts instantly whenever the slave moves from hold mode back to active mode, but power consumption is kept to a minimum while it is not transmitting
  - Is used when connecting several piconets or managing a low power device such as a temperature sensor.

Bluetooth Power Usage

- Park mode
  - the most efficient of power-saving modes
  - In park mode, a device is still synchronized to the piconet but it does not participate in any traffic.
  - occasionally listen to the traffic of their master in order to resynchronize and check on broadcast messages
  - Power consumption in this mode is mere 0.3 mA.

Other Layers and Functions

- Logical Link Control Adaptation Protocol (L2CAP)

    – responsible for segmenting and reassembling data packets

TCP/IP Packet – 1500 bytes

- RFCOMM

    – provides serial port emulation for Bluetooth computer's standard serial port
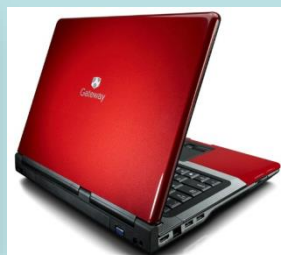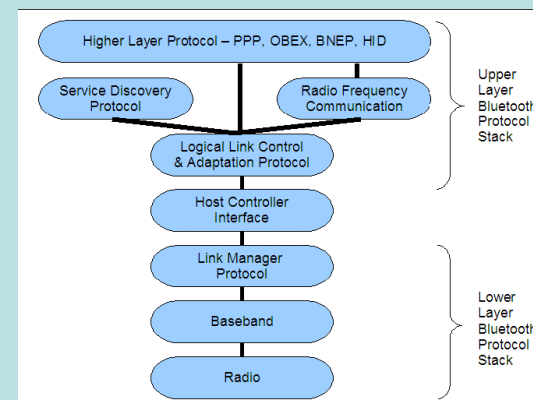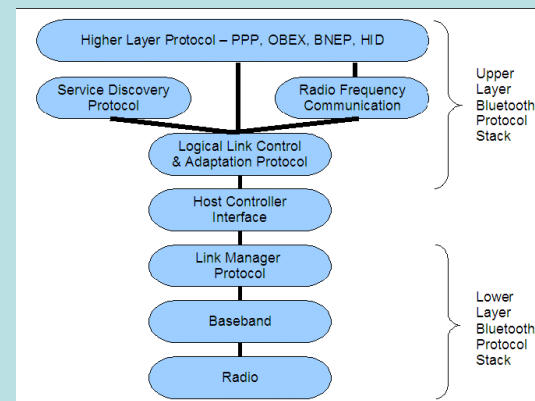
Other Layers and Functions

- ## Service Discovery Protocol (SDP)

  – to query device information, services and characteristics

  – select which services to be connected to

Bluetooth Profile

- Bluetooth specification

- **Protocol** – definition of protocol layers like radio, baseband, LMP, HCI, L2CAP, SDP and RFCOMM
- **Profile** – services that can be used in Bluetooth

- Why do we need Bluetooth Profile specification?

- Vision is to be the de-facto wireless technology to integrate devices from consumer electronics, telecommunications, computer and networking, automobiles, health care services

Bluetooth Profile

- Two foundation profiles
- Generic Access Profile (GAP)
- Service Discovery Application Profile (SDAP)

- Other foundation profiles
- Serial Port Profile (SPP) is pre-requisite for DUN, FAX, HSP, HFP, SAP and GOEP
- Generic Object Exchange Profile (GOEP) is prerequisite for FTP, OPP, SYNCH and BPP

Bluetooth Profile
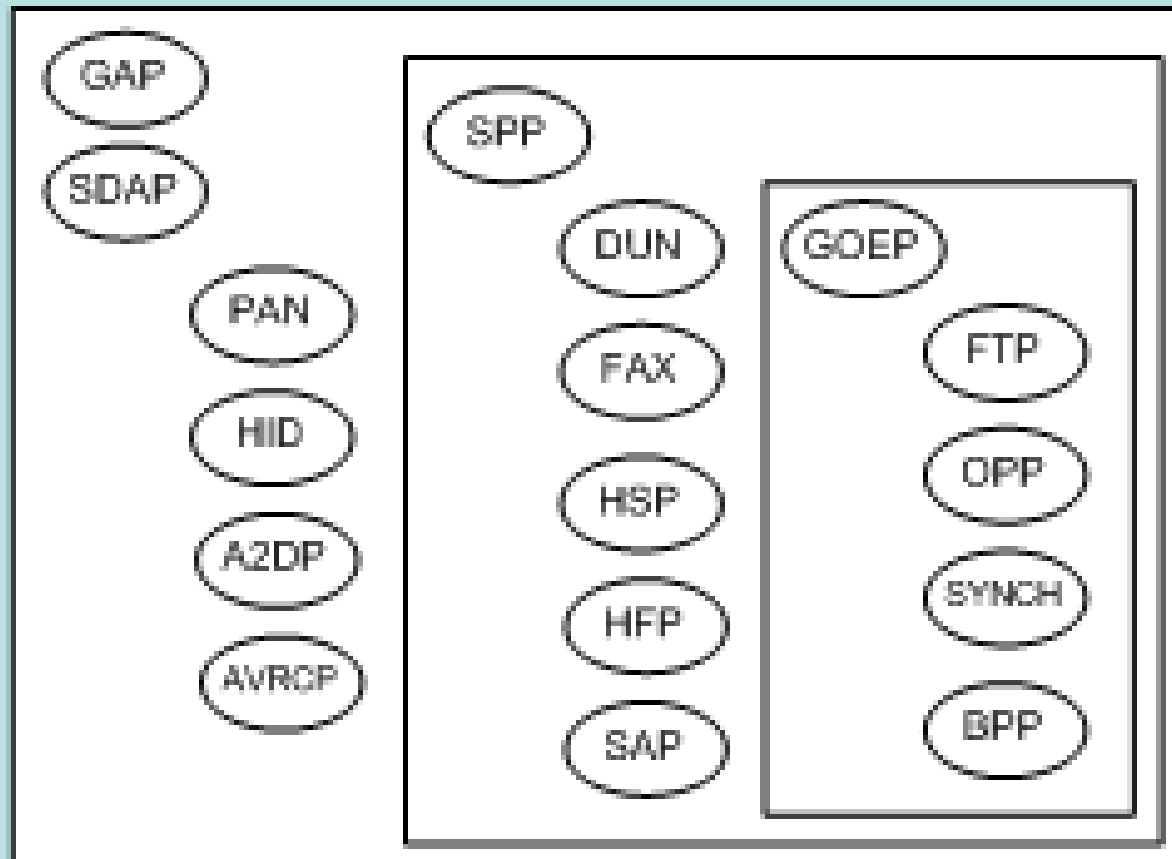
Relationship among Bluetooth Profiles

Bluetooth Profile

- ## GAP (Generic Access Profile)
- Discoverability – governs the use of inquiry scan
- Nondiscoverable
- Limited discoverability
- General discoverability
- Connectability – governs the use of page scan
- Pairability – governs the LMP pairing facilities
- ## SDAP(Service Discovery Application Profile)
- Governs the use of SDP for browsing services
- ## SPP (Serial Port Profile)
- RS-232 serial cable emulation
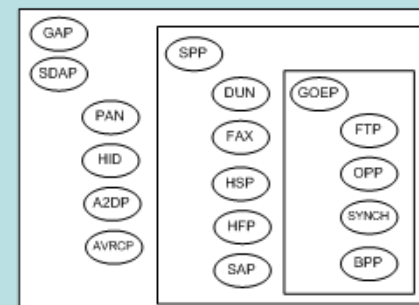
Relationship among Bluetooth Profiles

Bluetooth Profile

- DUN (Dial Up Networking Profile)
- Support AT command and PPP to allow Bluetooth communication device to act as an Internet bridge
- FAX
- To provide fax facilities (Class 1, 2.0 Service Class 2) in Bluetooth communication device
- HSP (Headset Profile)
- Audio gateway on mobile phone for mono voice
- Headset on Bluetooth-enabled headsets
- HFP (Hands-Free profile)
- Similar to HSP and able to connect to multiple devices
- SAP (SIM Access Profile)
- To allow Bluetooth communication device to access the SIM card in mobile phones
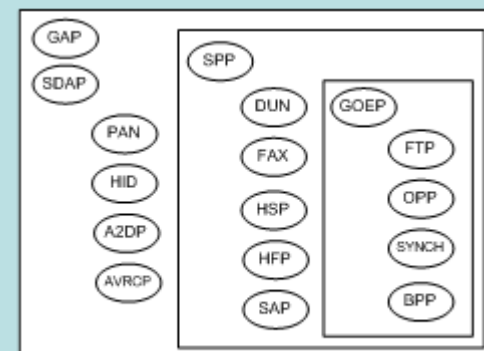
Relationship among Bluetooth Profiles

Bluetooth Profile

- GOEP (Generic Object Exchange Profile)
- Support OBEX layer defined in IrDA
- FTP (File Transfer Profile)
- Data transfer using Bluetooth links
- OPP (Object Push Profile)
- Similar to FTP except for business card exchange and uses Bluetooth authentication
- SYNCH (Synchronization profile)
- Synchronize personal data
- BPP (Basic Printing Profile)
- Provide printing service without the need of a dedicated printer driver
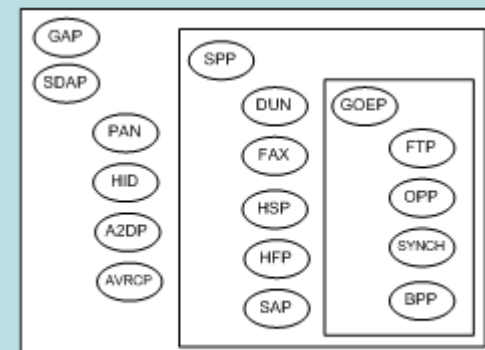
Relationship among Bluetooth Profiles

Bluetooth Profile

- ## PAN

- Support BNEP to encapsulate Ethernet packets in L2CAP payload

- ## HID

- Support HID protocol from USB

- ## A2DP

- Distribute high-quality audio content in mono or stereo using ACL channels

- ## AVRCP

- Provide audio/video control functions in audio/video equipment
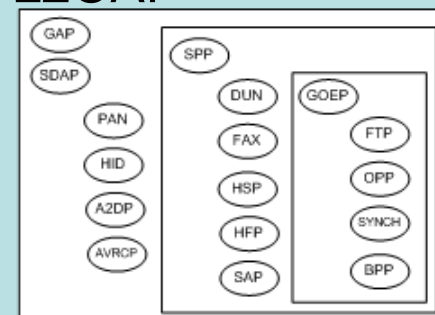
Relationship among Bluetooth Profiles

Additional Profiles for Bluetooth Low Energy (Bluetooth 4.0)

Low energy application profiles are based on the generic attribute profile, or GATT

Health care profiles

- HTP — for medical temperature measurement devices
- GLP — for blood glucose monitors
- BLP — for blood pressure measurement

Additional Profiles for Bluetooth Low Energy (Bluetooth 4.0)

Sports and fitness profiles

- HRP — for devices which measure heart rate
- CSCP — for sensors attached to a bicycle or exercise bike to measure cadence and wheel speed
- RSCP — running speed and cadence profile
- CPP — cycling power profile
- LNP — location and navigation profile

Additional Profiles for Bluetooth Low Energy (Bluetooth 4.0)

Proximity sensing

- FMP — the "find me" profile — allows one device to issue an alert on a second misplaced device.

- PXP — the proximity profile — allows a proximity monitor to detect whether a proximity reporter is within a close range. Physical proximity can be estimated using the radio receiver's RSSI value, although this does not have absolute calibration of distances. Typically, an alarm may be sounded when the distance between the devices exceeds a set threshold.

Additional Profiles for Bluetooth Low Energy (Bluetooth 4.0)

Alerts and time profiles

- ANP - The phone alert status profile and alert notification profile allow a client device to receive notifications such as incoming call alerts from another device.

- TIP - The time profile allows current time and time zone information on a client device to be set from a server device, such as between a wristwatch and a mobile phone's network time.

Comparison between Classic Bluetooth and Bluetooth Low Energy

Technical Specification	Classic Bluetooth technology	Bluetooth low energy technology
Distance/Range (theoretical max.)	100 m (330 ft)	50 m (160 ft)
Over the air data rate	1–3 Mbit/s	1 Mbit/s
Application throughput	0.7–2.1 Mbit/s	0.27 Mbit/s
Active slaves	7	Not defined; implementation dependent
Security	56/128-bit and application layer user defined	128-bit AES with Counter Mode CBC-MAC and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive frequency hopping, Lazy Acknowledgement, 24-bit CRC, 32-bit Message Integrity Check
Latency (from a non-connected state)	Typically 100 ms	6 ms
Total time to send data (det. battery life)	100 ms	3 ms , <3 ms
Voice capable	Yes	No
Network topology	Piconet, Scatternet	Star

Comparison between Classic Bluetooth and Bluetooth Low Energy

Technical Specification	Classic Bluetooth technology	Bluetooth low energy technology
Power consumption	1 as the reference	0.01 to 0.5 (depending on use case)
Peak current consumption	<30 mA	<15 mA
Service discovery	Yes	Yes
Profile concept	Yes	Yes
Primary use cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, security, proximity, healthcare, sports & fitness, etc.	Mobile phones, gaming, PCs, watches, sports and fitness, healthcare, security & proximity, automotive, home electronics, automation, Industrial, etc.
Frequency channel	79 channels with 1-MHz BW	40 channels with 2-MHz BW
Maximum Transmit Power	100 mW (20 dBm)	10 mW (10 dBm)
Modulation techniques	GFSK, 4PSK, 8PSK	GFSK

Bluetooth Applications

- Currently, 5 million Bluetooth chipsets are produced weekly.

- Bluetooth applications

- Voice signal from mobile phone to headset (HSP,HFP)

- Voice signal from mobile phone to car kits (HFP, SAP)

- Images from mobile phone to laptop (FTP)

- Music signal from MP3 player to stereo headphones (A2DP, AVRCP)

- Internet access from laptop through mobile phone (DUN, PAN)

- Mouse and keyboard to computers (HID)

- Business card exchange between mobile phones (OPP)

- Synchronize data between PDA and laptop (SYNCH)

- Printing from laptop to printer (BPP)

WPAN Applications

- Bluetooth/ZigBee/UWB/RFID
  - Current and future applications for WPAN technology include
  - Synchronisation PDAs, cellular and Smartphones, cameras and so on
  - Home control systems (smart-home)
  - Cordless telephones
  - Portable device data exchange
  - Industrial control systems

WPAN Applications

- Bluetooth/ZigBee/UWB/RFID
  - Location –smart tags used to locate people at home or at the office
  - Security systems
  - Interactive toys
  - Inventory tracking
  - Health care and elder care
  - Energy monitoring and control (Smart grid) Applications