WIRELESS PAN

Ashwini Deshmukh

Overview

- It was initially developed by swedish phone maker ERRICSON in 1994 as a way to let laptop computers make calls over a mobile phone.
- Later , over thousands of companies signed on to make bluetooth low power short range wireless standard for a wide range of devices.
- IEEE 802.15 is concerned with the PAN standard that covers Bluetooth

- Bluetooth provides universal short range wireless capabilities
- Uses unlicensed 2.4 GHz ISM band
- Bluetooth devices within 10 m of each other can share up to 720 kbps of capacity
- Bluetooth is intended to support open ended list of applications , including data, audio, graphics and even video

- Some capabilities that bluetooth can provide to customers are
  - Make calls from wireless headset connected remotely to cell phone
  - Eliminating cables linking computers to printers, keyboards and the mouse
  - hookup MP3 players wirelessly to other machines to download music
  - Set up home networks so that one can remotely monitor air conditioner, oven and children's internet surfing
  - Call home from remote location to turn ON/OFF appliances

Bluetooth Applications

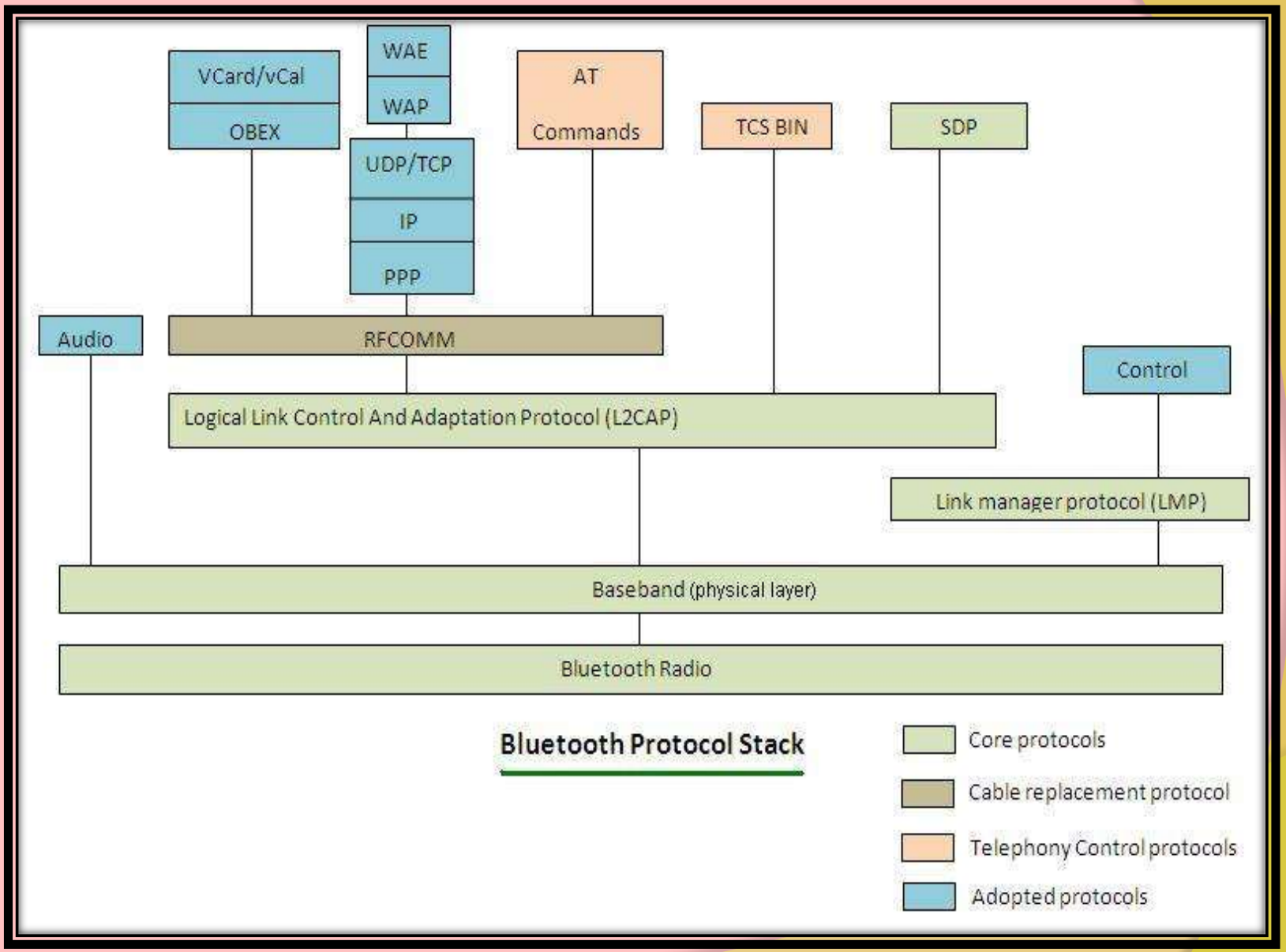
Bluetooth provides support for three general applications areas using short range wireless connectivity

- Data and voice access points : Bluetooth provides real time voice and data transmission by providing effortless connection of portable and stationary devices

- cable replacement : It eliminates the need for numerous cable attachment for connection of practically any kind of communication devise. connections are instant and does not require LOS. Range is 10 m can extend up to 100m with use of amplifiers

- Ad hoc networking: A device equipped with a bluetooth can establish instant connection to another bluetooth radio as soon as it comes into range

Bluetooth Protocol Architecture


VCard/vCal
OBEX
WAE
WAP
UDP/TCP
IP
PPP
AT
Commands
TCS BIN
SDP
Audio
RFCOMM
Control
Logical Link Control And Adaptation Protocol (L2CAP)
Link manager protocol (LMP)
Baseband (physical layer)
Bluetooth Radio
Bluetooth Protocol Stack
Core protocols
Cable replacement protocol
Telephony Control protocols
Adopted protocols

- It is a layered protocol archictecture consisting of-
  - Core protocols
  - Cable replacement and telephony protocols
  - Adopted protocols

- Core protocol is a five-layered stack consisting of

  - Radio : specifies details of air interface, including frequency, the use of frequency hopping , modulation scheme and transmit power

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

- Link Manager Protocol(LMP): responsible for link setup between bluetooth devices and ongoing link management. This includes security aspects such as encryption and authentication

- Logic Link Control and Adaption Protocol(L2CAP): adapts upper layer protocols to the baseband layer. It provides both connection-less and connection oriented services

- ServiCe discovery protocol(SDP): device information, services and the characteristics of the services can be queried to enable the establishment of connection between two or more bluetooth devices

Cable replacement and telephony protocols

- RFCOMM is cable replacement protocol included in bluetooth specifications:
  - It presents a serial port that is designed to make replacement of cable technologies.
  - As serial ports are one of the common types of communication interface, RFCOMM enables replacement of serial port cables with the minimum modification of existing device
  - RFCOMM provides for binary data transport and emulates EIA-232 i.e. RS-232control signals over baseband layer

- Bluetooth specifies a Telephony Control Protocol (TCS):
  - TCS-bin(binary) is a bit oriented protocol that defines call control signals for establishment of speech and data calls between bluetooth devices
  - It also specifies mobility management procedures for handling groups of bluetooth TCS devices

Adopted Protocols

- They are specified by other standard making organizations and included in overall bluetooth architecture

- Bluetooth strategy is to use existing protocols whenever possible and invent only necessary protocols

Adopted protocols include following

- PPP: point to point protocol is a internet standard protocol used to transport IP datagrams over point to point links
- TCP/UDP/IP: they are the foundation protocols of TCP/IP suite
- OBEX: Object exchange protocol is a session level protocol developed by infrared data association(IrDA) for transfer of objects. It provides functionality similar to HTTP but in simpler fashion
- WAE/WAP: bluetooth also incorporates wireless application environment and wireless application protocols

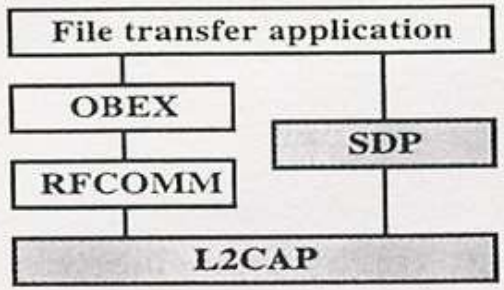
BLUETOOTH Usage Models

Bluetooth usage model is a set of protocols that implements a particular bluetooth baseband application

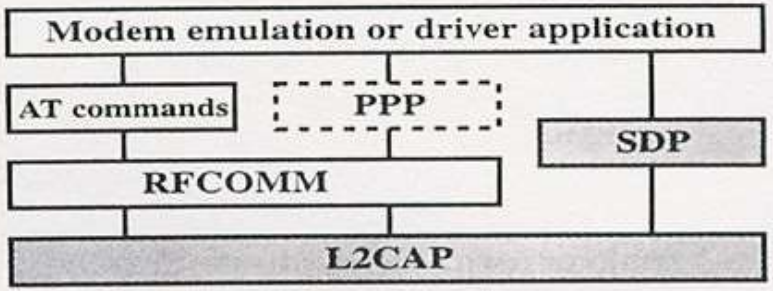
- Following are few highest priority usage models

  - File transfer
    - Support transfer of directories, files, documents, images and streaming media formats.
    - It also include capabilities to browse folder on a remote device.

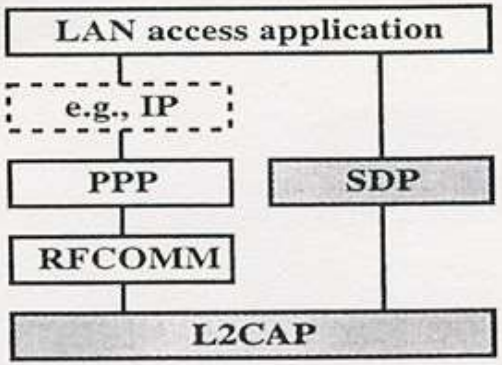
  - Internet bridge
    - With this usage model , a PC is wirelessly connected to mobile phone or cordless modem to provide dial up networking and fax capabilities.
    - For dial up networking AT commands are used to control mobile phone or modem, and another protocol stack like PPP is used for data transfer



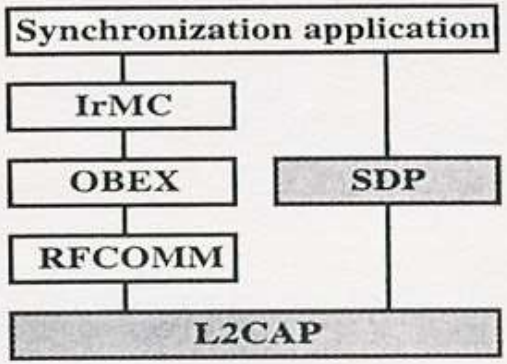
(a) File transfer



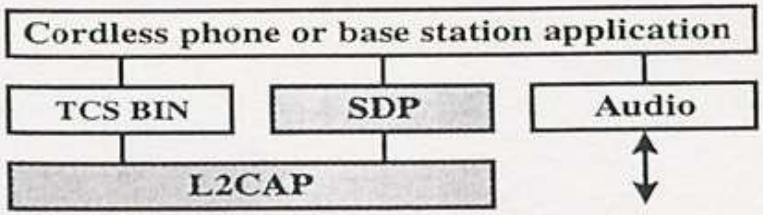
(b) Dial-up networking



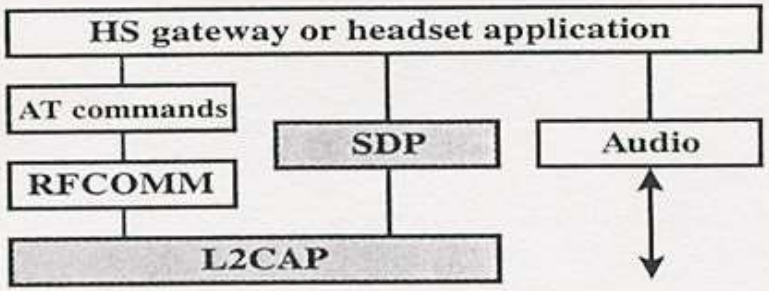
(c) LAN access



(d) Synchronization



(e) Cordless phone and intercom



(f) Headset

- LAN Access:
  - This usage model enables a device on piconet to access LAN

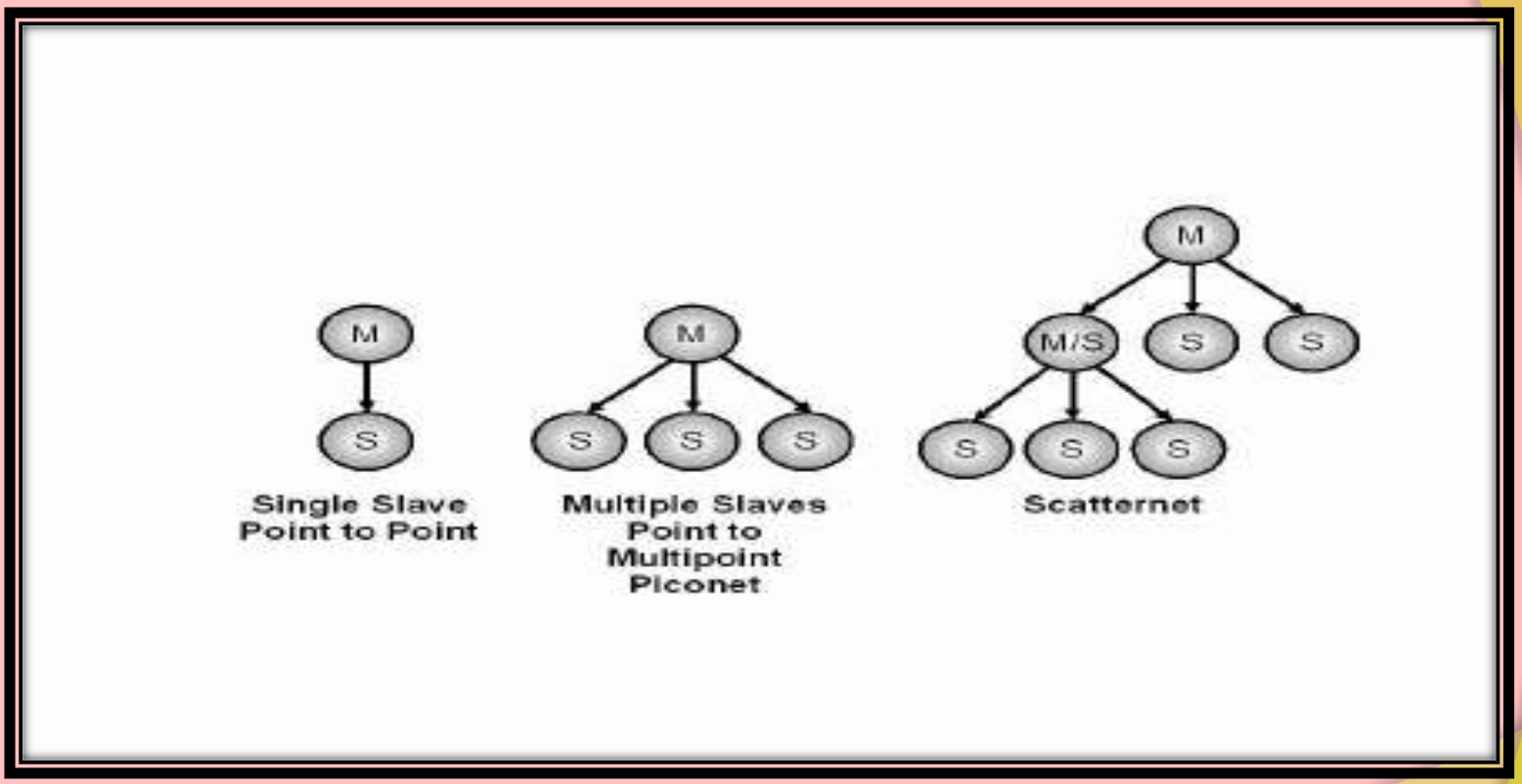
- Synchronization:
  - This Usage model provides device to device synchronization of PIM(personal information management)information such as phone book, calendar, message and note information

  - IrMC (infrared mobile communication) is an IrDA protocol that provides a client/server capability for transferring updated PIM information from one dive to aother

- Three-in-one phone:
  - Telephone handset that implements this usage model may act as a cordless phone connecting to voice base station, as an intercom device for connecting to other telephones and cellular phones
- Headset
  - The headset can act as a remote device's audio input and output interface

Piconets and scatternets

- Basic unit of networking in bluetooth is piconet, cosisting of one
  - One master
  - Seven active slave devices
- Radio designated as master determines-
  - Channel(frequency hopping sequence)
  - Phase(timing offset i.e. when to transmit)
    - These determinations are made on the basis of its own address
- The slave should tune to same cannel and phase as that directed by master
- The slave can communicate only with the master and that too only at the time when permission is granted by master

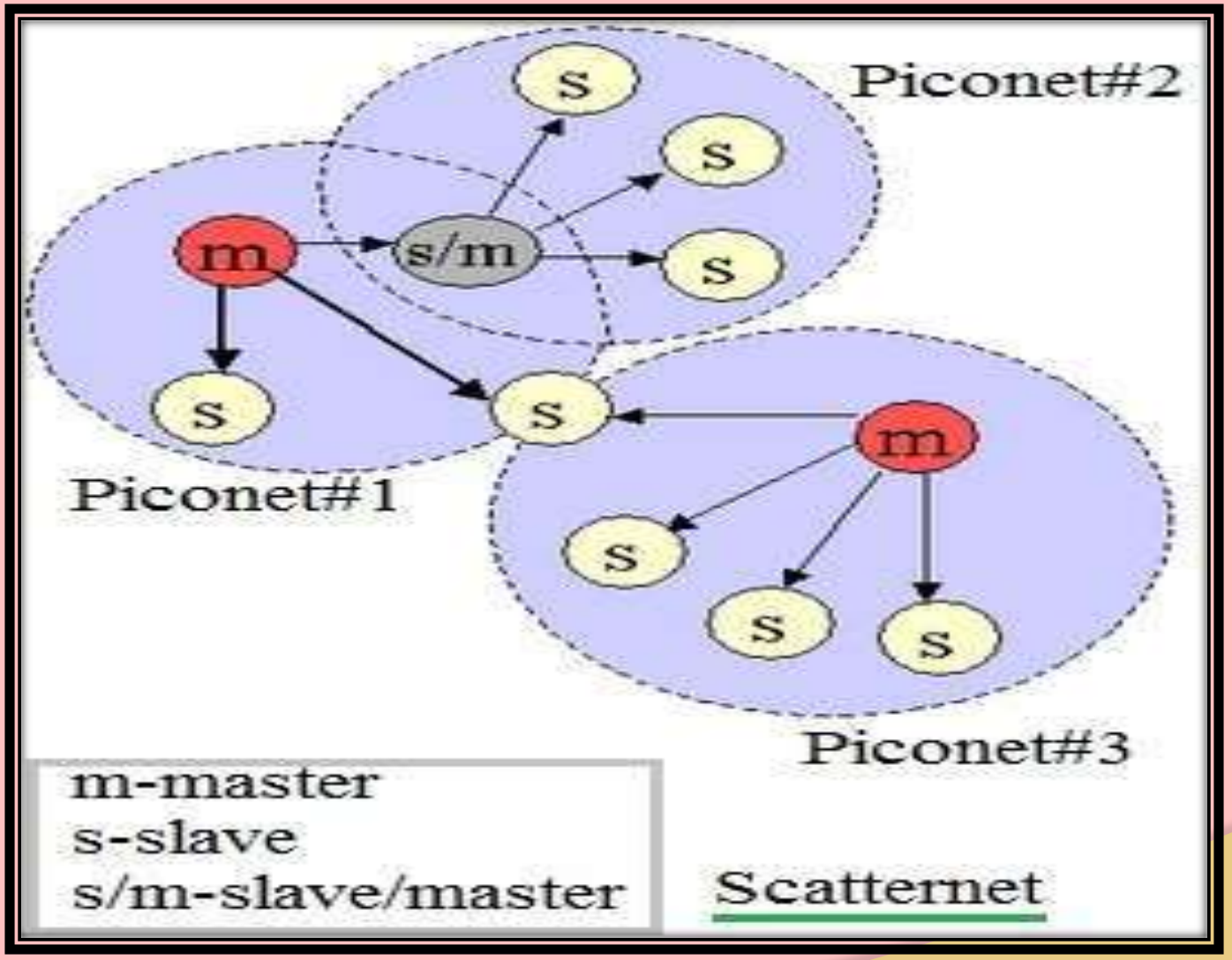

M
S
Single Slave
Point to Point
M
S
S
S
Multiple Slaves
Point to
Multipoint
Piconet
M
M/S
S
S
S
S
S
Scatternet

- A device in one piconet may also exist as a part of another piconet and may function either as master or slave. This form of overlapping is called as scatternet.

- Advantage of piconet/scatternet scheme is that it allows many devices to share the same physical area and make efficient use of BW

- It make use of FH with carrier spacing of 1 MHz and total of such 80 different frequency are used providing total BW of 80MHz

- If FH were not used one channel would have corresponded to single 1 MHz but with FH a logical channel is defined by FH sequence and BW available at any time is 1 MHz.
- Different logical channels can simultaneously share same 80 MHz BW.
- Collision occur when devices in different piconet, on different logical cannels happen to use the same hop frequency at same time
- As number of piconet in area increases no of collisions increases


Piconet#2
s
s
m
s/m
s
s
s
Piconet#1
m
s
s
s
Piconet#3
m-master
s-slave
s/m-slave/master
Scatternet

Radio Specification

- It’s a short document that gives that gives the basic details of radio transmission for bluetooth devices
  - It gives specification for tree classes of transmitters based on output power
    - **Class 1** : outputs 100 mW for maximum range with a minimum of 1 mW. Power control is mandatory. Provides maximum distance
    - **Class 2**: outputs 2.4 mW at maximum with minimum of 0.25 mW. Power control is optional
    - **Class 3** : lowest output of i.e. of only 1 mW

- 2.4 GHz ISM band is used
- It defines 79 1-MHz physical cannels
- Power control is used to keep device from emitting any more RF power than necessary
- Power control algorithm is implemented using link management protocol between master and slave
- Modulation scheme used is Gaussian –FSK: with 1 represented by positive frequency deviation and zero by negative frequency deviation from center frequency. Minimum deviation is 115 KHz

Baseband Specification

- Frequency hopping in bluetooth serves two purpose
  - Provides resistance to interference and multipath effects
  - Provides a form of Multiple Access among co-located devices in different piconets

- Scheme works a follows
  - Total frequency is divided into 1 MHz ,79 physical channels
  - PN sequence is used to hop from one frequency to another
  - Hop rate is 1600 hops per second, so each physical channel is occupied only for a duration of 0.625 msec
  - Each 0.625 msec duration is referred as slot
  - Communication takes place using TDD(time division duplex), which a link transmission technique in which data are transmitted in one direction at time , with transmission altering between two directions
  - Multiple access scheme used is piconet

- Hence piconet access is characterized by FH-TDD-TDMA

Bluetooth radio and baseband parameters

Topology	Upto 7 simultaneous link in logical area
Modulation	GPSk
Peak data rate	1 MBPs
Rf Bandwidth	220 KHz, 1 MHz
RF Band	2.4 GHz , ISM band
RF carriers	23/79
Carrier Spacing	1 MHz
Transmit power	0.1 W
Piconet Access	FH-TDD-TDMA
Frequency Hop Rate	1600 hops/s
Scatternet Access	FH-CDMA

Physical link

- Two types of links can be established
  - Synchronous connected oriented(SCO):
    - Allocates a fixed BW between a point to point connection involving the master and a single slave.
    - The master maintains the SCO link by using reserved slots at regular intervals
    - The basic unit of reservation is two consecutive slots (one in each transmission direction)
    - The master can support up to three simultaneous SCO links while a slave can support two or three SCO links.
    - SCO packets are never retransmitted

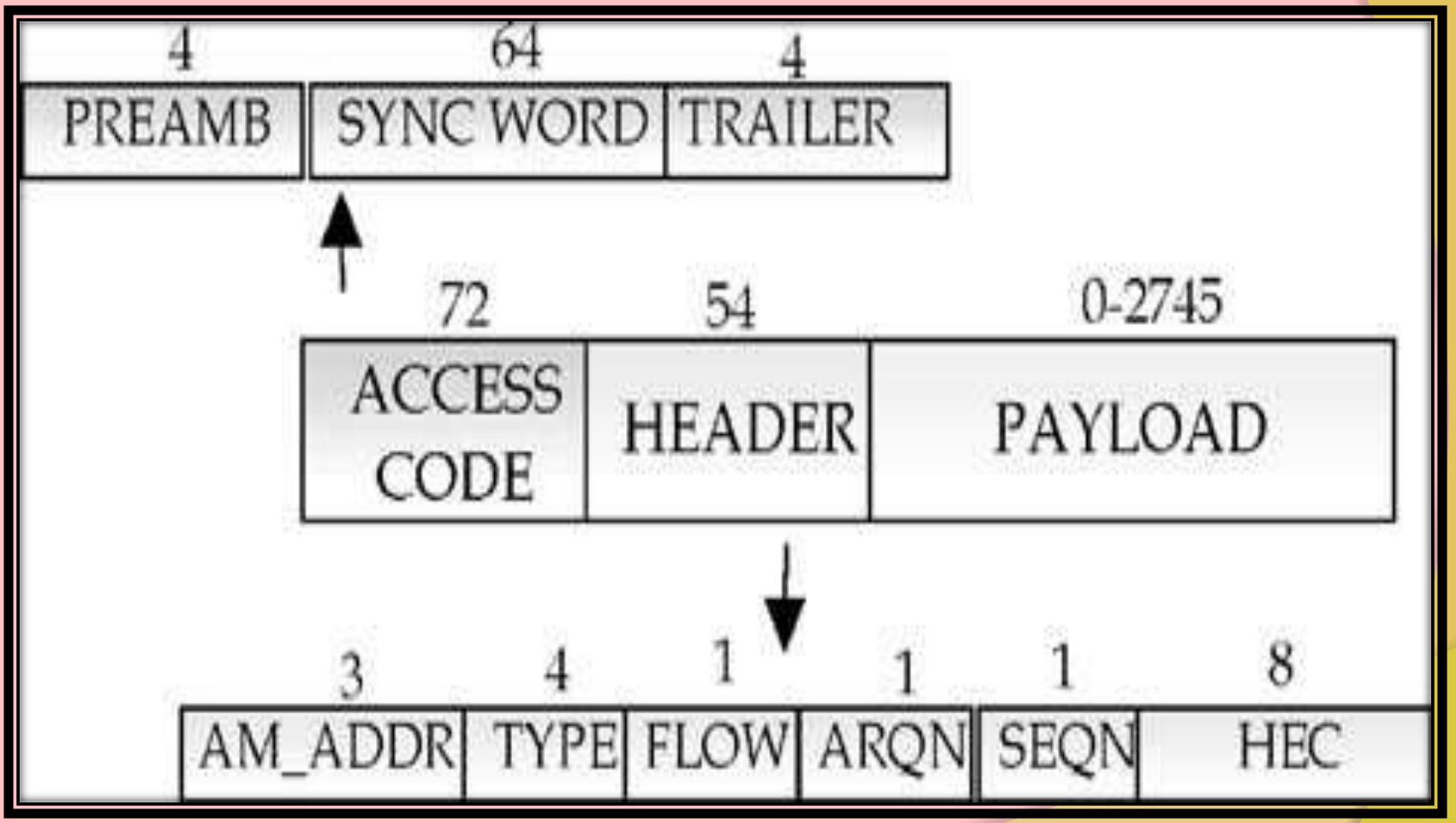
- Asynchronous connection-less(ACL):
  - A point to multipoint link between the master and slaves in the piconet
  - In slots not reserved for SCO links, the master can exchange packets with any slave on a per slot basis, including a slave already engaged in an SCO link
  - Only a single ACL link can exist
  - For most ACL packets, packet retransmission is applied

- SCO links are used primarily to exchange time bounded data requiring guaranteed data rate but without guaranteed delivery

- ACL links provide switched style of connection. No BW reservation is possible and delivery may be guaranteed through error detection and data retransmission

Bluetooth packet format

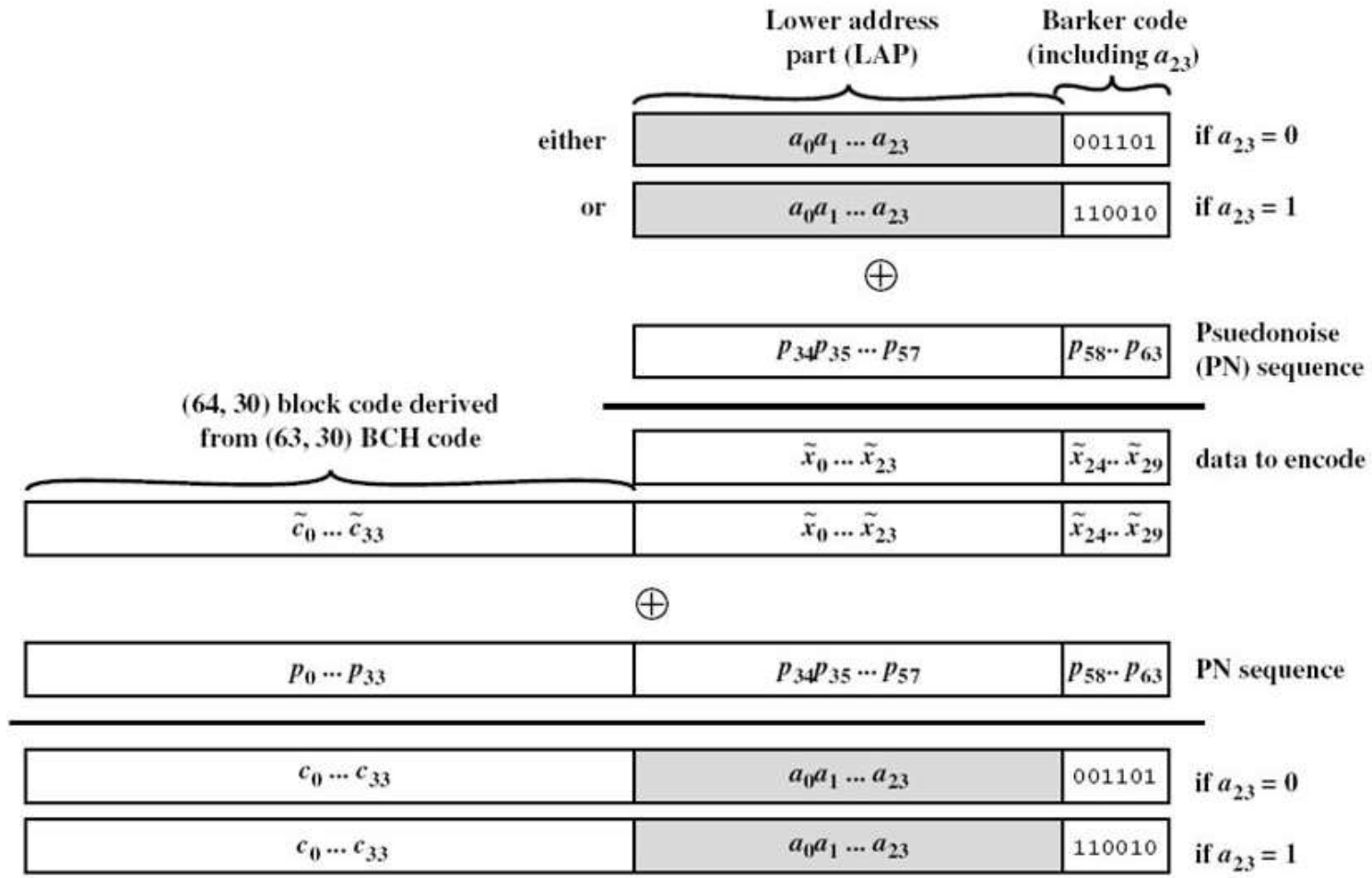
- It consists of three fields
  - Access code : used for timing synchronization, offset compensation, paging and enquiry
  - Header : used to identify the packet type and carry protocol control information
  - Payload : If present, consist of voice or data and, in most cases, a payload header


4
64
4
PREAMB
SYNC WORD
TRAILER
72
54
0-2745
ACCESS CODE
HEADER
PAYLOAD
3
4
1
1
1
8
AM_ADDR
TYPE
FLOW
ARQN
SEQN
HEC

Access code

- It consist of 4 bit preamble, 64 bit sync word and 4 bit trailer
  - The 4 bit preamble contains a pattern 0101 is LSB in sync word is 0 and it contains a pattern 1010 if LSB in sync word is 1
  - Similarly trailer is 0101 if MSB of sync word is 1 and is 1010 is MSB of sync word is zero

64 bit sync word is generated as -



Packet header

- AM_ADDR : this 3 bit field contains active mode address of one of the slave
- Type : identifies the type of packet
- Flow : provide one bit flow control mechanism for ACL only. When this bit is 0 transmission on ACL link is halted, when this bit is 1 transmission is resumed.
- ARQN : provides one bit acknowledgement mechanism for ACL traffic only
- SEQN : provides one bit sequential numbering scheme. Transmitted packets are alternately labeled 1 and 0
- HECN : 8 bits are reserved for header error control. Provides error detection code to protect header

Payload format

- For voice payload no header is defined
- For ACL packets and data portion of SCO DV packets , header is defined
- For data payload, payload format consist of three fields
  - Payload header:8 bit and 16 bit header for single and multi slot packets respectively
  - Payload body: contains user information
  - CRC : 16 bit CRC code is used on all data payloads

- Payload header when present consists of three fields
  - L_CH: identifies the logical channel.
    - 11 : LMP message
    - 10 : Un-fragmented L2CAP message or start of fragmented L2CAP message
    - 01 : continuation of fragmented L2CAP
    - 00 : Other
  - Flow :provide flow control at L2CAP level
  - Length : specifies number of bytes of data in payload excluding header and CRC

Error correction

- Three error correction schemes are used
  - 1/3 rate FEC
  - 2/3 rate FEC
  - ARQ (automatic repeat request)

  - These schemes are designed to satisfy competing requirements. This scheme must be adequate to cope with the inherently unreliable wireless link but must also be streamlined and efficient

1/3 rate FEC

- It is used on the 18 bit packet header and also for voice field in an HV1 packet
- The scheme simply involves ending three copies of each bit.
- A majority logic is used
- Each received triple of bit is mapped into whichever bit is in majaority

2/3 rate FEC

- It is used in DM packets, in data field of DV packet, in FHS packet and in HV2 packet.
- The encoder is a form of hamming code with parameters (15,10)
- In this after 10 bit code word a 5 bit error correcting code is added
- This code can correct up to 1 error and detect up to 2 errors

ARQ

- This is used for DM and DH packets and data field of DV packets
- ARQ scheme has following elements
  - **Error detection** : the destination detects error and discards packets that are in error
  - **Positive acknowledgement** : receiver sends positive acknowledgement to successfully received, error free packets
  - **Retransmission after timeout** : the source retransmits a packet that has not been acknowledged after a predetermined amount of time
  - **Negative acknowledgement and retransmission** : the destination returns a negative acknowledgement to the packets in which error is detected

Logic channels

- five types of logic channels have been defined to carry different types of payload traffic

  - **Link control(LC)** : Used to control the flow of packets over link interface. The channel is mapped onto packet header . It carries low level link information like ARQ, flow control and payload characterization

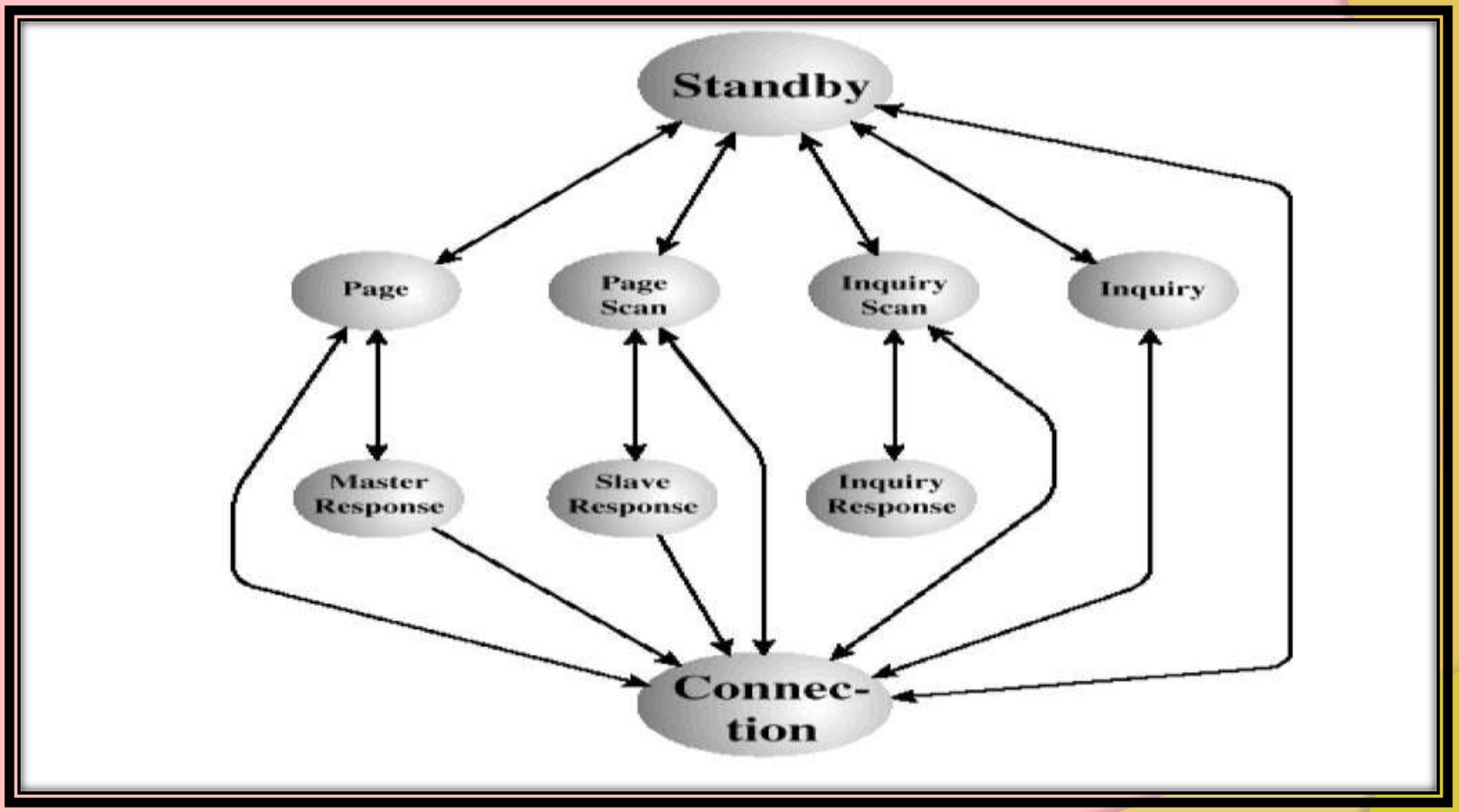
  - **Link manager (LM)** : transport link management information between participating stations. This logical channel supports LMP traffic and can be carried over either an SCO or ACL link

- **user asynchronous(UA):** carries asynchronous user data. It is normally carried over ACL link but may be carried in DV packets on SCO links

- **User isochronous (UI):** carries isochronous user data. It is normally carried over ACL link but may be carried in DV packets on SCO links. At baseband level it is treated the same way as UA cannel

- **User Synchronous (US)** : carries synchronous user data. Carried over sco link

Channel control



- The operation of a piconet can be understood in terms of the states of operation during link establishment and maintenance.

- There are two major states
  - Standby : the default state. This is low power state in which native clock is running.
  - Connection : the device is connected to piconet as a master or a slave.

- In addition there are seven interim substates that are used to add new slaves to the piconet
  - Page : devices has issued a page. It is used by master to activate and connect to the slave. Master sends page message by transmitting slave's device assess code (DAC) in different hop channels
  - Page scan : device is listening for page with its own DAC
  - Master Response : A device acting as a master receives a page response from a slave. The device can now enter the connection state or return to the page state to page for other slaves.
  - Slave Response : A device acting as a slave responds to a page from a master. If connection setup succeeds the device enters the connection state; else returns back to page scan state.

- Inquiry : device has issued an inquiry, to find the identity of device within range
- Inquiry scan : device is listening for an inquiry
- Inquiry response : A device that has issued an inquiry receives an inquiry response.

Link Manager specification

- Manages various aspects of the radio link between a master and a slave
- The protocol involves the exchange of messages in the form of LMP PDU(protocol data unit) between the LMP entities in master and slave
- Messages are always sent as single slot packets with 1-byte payload header that identifies the message type and payload body that contains additional information

- Procedures defined for LMP are grouped into 24 functional areas , each of which involves exchange of one or more messages

1. Two **general response** are accepted and not_accepted which include the opcode for indicating weather the message is accepted or not

LMP supports security services which include

2. **Authentication** involves exchange of two LMP pdu one containing random numbers and one containing signed response

3. **Pairing** allows mutually authenticated users to automatically establish a link encryption key

4. **Change link key:** if two paired devices use a combination key then that key can be changed. One side generates a new key and sends other side the XORed wit old link key. The other side can either accept or reject it

5. **Change current link key:** it can be changed temporarily. Exchange involves use of random numbers and XORed calculation to generate temporary key which is used in single session

6. **Encryption :**parameters include what is the operating encryption mode, the size of key, random seed key used to start a new encryption session, begin and end use of encryption.

LMP provides mechanism for synchronizing the clocks in various piconets

7. **Clock offset request:** when slave receives a FHS packet, difference is calculated between its own clock and the masters clock value included in the payload of the packet. Clock offset value allows the master to know at RF channel the slave wakes up to the page scan after it has left piconet

8. **Slot offset information** : initiating device can transmit a message indicating the time differences between two adjacent piconets

9. **Timing accuracy information request** : used by a device to retrieve the accuracy parameters of another device's timing system

Following two PDU's are used to exchange information about the communicating devices

10. **LMP versions** allows each LMP entity to determine LMP version implemented in the other

11. **Supported features:** the bluetooth radio and link controller may support only s subset of the packet types and features described in the baseband and radio specification. This information is exchanged using the PDU under supported features

Bluetooth has various states and modes that it can occupy. following PDU's help in managing same

12. **Switch master/slave role:** allows a slave to become the master of piconet

13. **Name request:** enables a device to request the text name of another device

14. **Detach:** enables a device to remove itself from connection

15. **Hold mode:** places the link between master and slave in hold mode for specified time

16. **Sniff mode:** allows master and slave to enter in sniff mode after negotiating sniff interval T sniff and a sniff offset , D sniff, which specifies timing of the sniff slot. Sniffing is used for devices that must be continuously in contact with master. sniff mode reduces the power consumption of the device as the receiver can be put on standby between sniff cycles

17. **Park mode:** places slave in park mode

18. **Power control:** used by a device to direct another device to increase or decrease second device's transmit power

19. **Channel quality driven between DH and DM:** a device is configured to use DM, DH packet always or to adjust its packet type according to the quality of the channel. This service allows explicit change among three services

20. **Quality of service:** two parameters define quality of service the poll interval and number of repitions for broadcast packets

21. **Sco link:** used to establish SCO link

22. **Control of multislot packets:** arbitrates the maximum number of time slots a packet can cover. default value is one

23. **Paging scheme:** controls the type of paging scheme to be used between devices on piconet

24. **Link supervision:** controls maximum time a link should wait before declaring a failure

All explained above are shown in following table along with PDU's exchanged

Function	PDUs
General response	accepted, not_accepted
Security Service	
Authentication	au_rand, sres
Pairing	in_rand, au_rand, sres, comb_key, unit_key
Change link key	comb_key
Change current link key	temp_rand, temp_key, use_semi_permanent_key
Encryption	encryption_mode_req, encryption_key_size_req, start_encryption_req, stop_encryption_req
Time/synchronization	
Clock offset request	clkoffset_req, clkoffset_res
Slot offset information	Slot_offset
Timing accuracy information request	timing_accuracy_req, timing_accuracy_res
Station Capability	
LMP version	version_req, version_res
Supported features	features_req, features_res
Mode Control	
Switch master/slave role	Switch_req
Name request	name_req, name_res
Detach	detach
Hold mode	hold, hold_req
Sniff mode	sniff, sniff_req, unsniff_req
Park mode	park_req, park, set_broadcast_window, modify_beacon, unpark_PM_ADDR_req, unpark_BD_ADDR_req
Power control	incr_power_req, decr_power_req, max_power, min_power
Channel quality-driven change between DM and DH	auto_rate, preferred_rate
Quality of service	quality_of_service, quality_of_service_req
SCO links	SCO_link_req, remove_SCO_link_req
Control of multislot packets	max_slot, max_slot_req
Paging scheme	page_mode_req, page_scan_mode_req
Link supervision	supervision_timeout

Reference

- “wireless communication and networks” by william stallings, second edition