Bluetooth

Last updated 4/29/21

Bluetooth

- Bluetooth name comes from Danish king Harald Blåtand (Bluetooth), credited with uniting the Scandinavian people during the 10th century.

- The idea was that Bluetooth wireless technology would unite personal computing devices.

Bluetooth

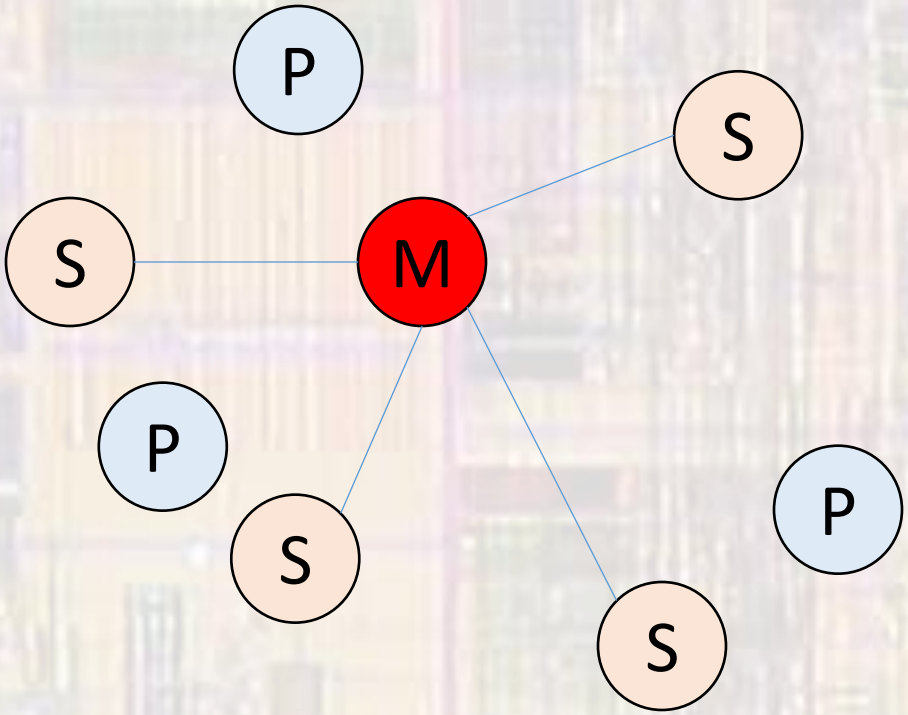
- Bluetooth is a trademark owned by the Bluetooth SIG, Inc., USA.
  - Bluetooth Special Industry Group (SIG) formed in winter of 1998 by Ericsson, IBM, Intel, Nokia, and Toshiba
  - Many additional members
  - Requires testing to be BT compliant
- Goals
  - low cost
  - low power
  - primarily a cable replacement (to connect mobile phones to headsets)
- Uses
  - short-range radio technology
  - ad hoc networking
  - dynamic discovery of other Bluetooth devices & the services they offer

Bluetooth

- Network
  - Piconet
    - Collection of devices connected in an ad hoc fashion
    - One master and the others are slaves for the lifetime of the piconet
    - Each piconet has a unique frequency hopping pattern
      - Master determines frequency hopping pattern
      - Slaves must synchronize
      - Participation in a piconet = synchronization to hopping sequence
    - Each piconet has one master and up to 7 simultaneous slaves
    - Up to 255 Parked slaves
      - Each station gets an 8-bit parked address (255 parked slaves/piconet)

Bluetooth

- Network
  - Piconet
    - Master
    - Slave
    - Parked



Bluetooth

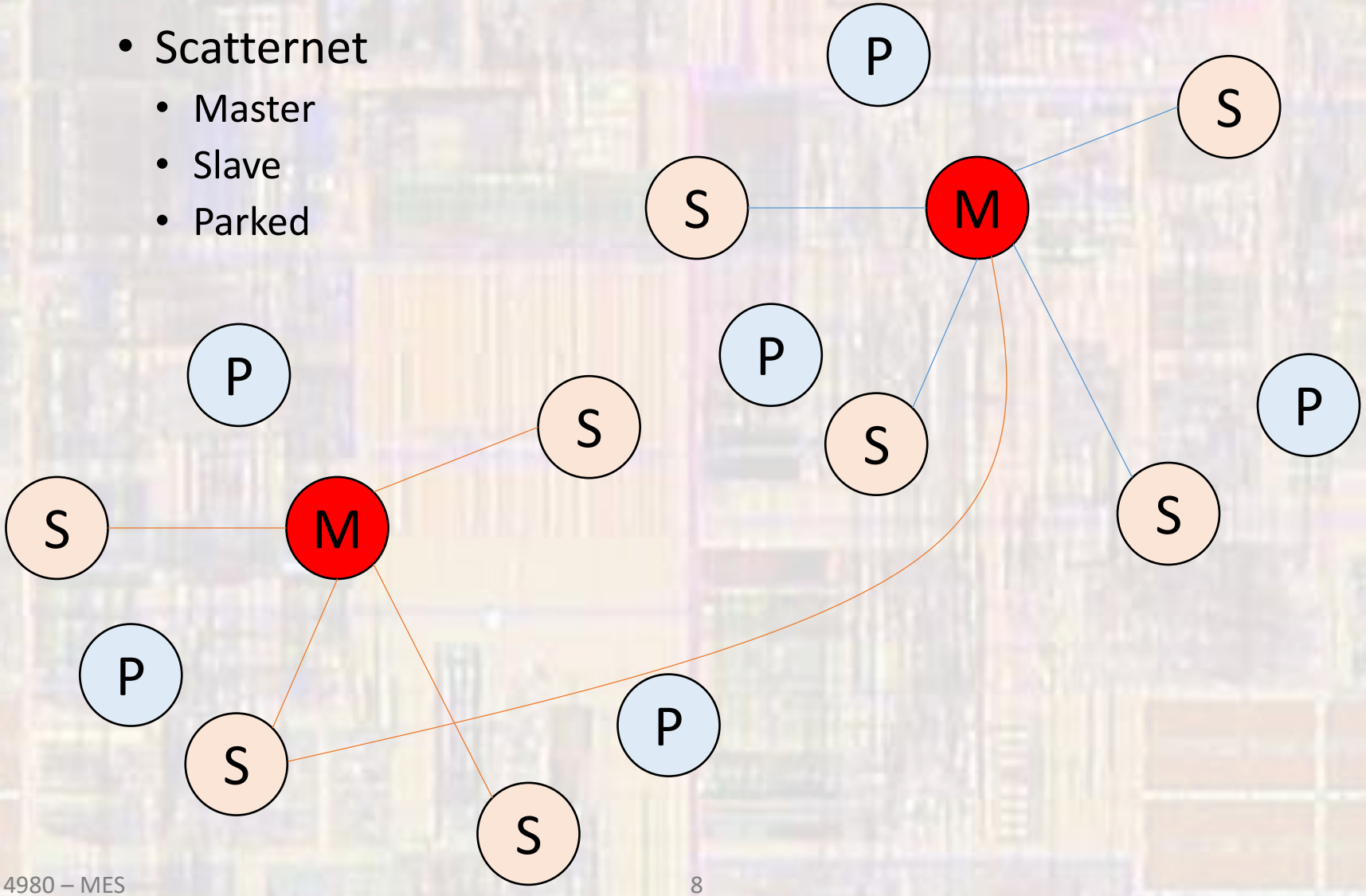
- Network
  - Piconet
    - All devices in a piconet hop together
    - Master gives slaves its clock and device ID
    - Hopping pattern
      - Determined by device ID (48 bit, unique worldwide)
      - Phase in hopping pattern determined by clock
    - Addressing
      - Active Member Address (AMA, 3 bit)
      - Parked Member Address (PMA, 8 bit)

Bluetooth

- Network
  - Scatter net:
    - Linking of multiple co-located piconets through the sharing of common master or slave devices
    - A device can participate in multiple Pico nets
      - Devices can be slave in one piconet and master of another
    - Timeshare
    - Must synchronize to the master of the current piconet
    - Routing protocol not defined

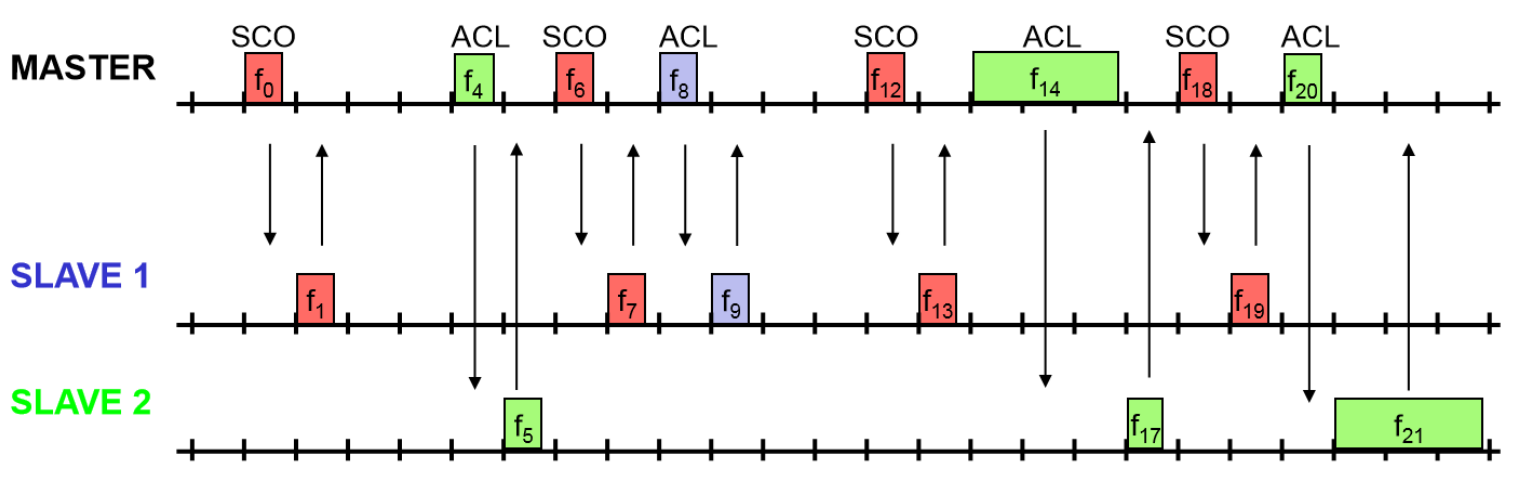
Bluetooth

- Network
  - Scatternet
    - Master
    - Slave
    - Parked



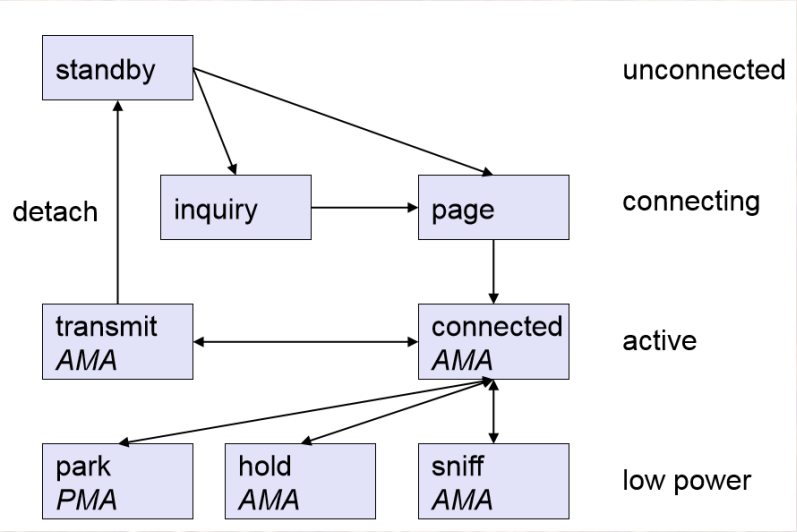
Bluetooth

- Link Types
  - SCO: Synchronous Connection Oriented
    - Synchronous (voice)
    - Point to Point Connection between one master and one slave
  - ACL: Asynchronous Connection Oriented
    - Asynchronous (data)
    - Multipoint connection between one master and one or many slaves

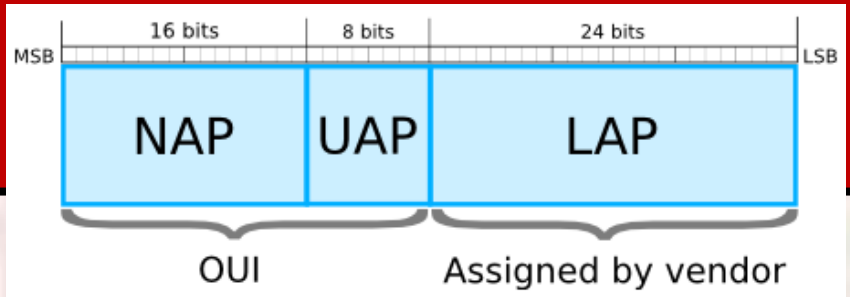


Bluetooth

- Network
  - Network States
    - Standby: do nothing
    - Inquire: search for other devices
    - Page: connect to a specific device
    - Connected: participate in a piconet
    - Transmit: active communication
    - Park: release AMA, get PMA
    - Sniff: listen periodically, not each slot
    - Hold: stop ACL, SCO still possible
      possibly participate in another piconet



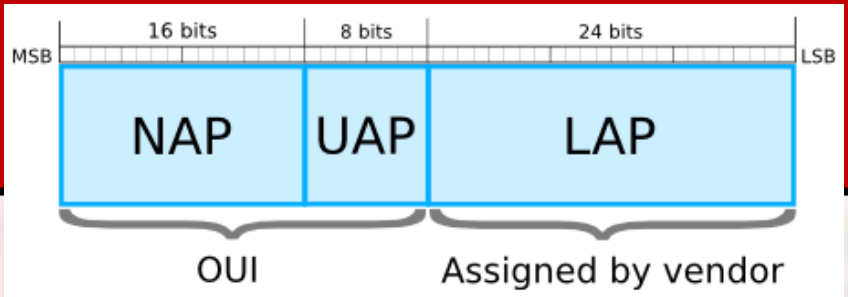
Bluetooth



- Device Address
  - Each Bluetooth device has a unique 48-bit Bluetooth device address (BD_ADDR)
    - 48-bit extended unique identifier (EUI-48)
    - "Universal address" of the IEEE 802-2014 standard
    - Typically written in 1 byte sections 00:11:22:33:FF:EE
  - NAP: Non-significant Address Part
    - Used as part of the frequency hopping algorithm
    - Manufacturer specific
    - Assigned by the IEEE
  - UAP: Upper Address Part.
    - Manufacturer specific
    - Assigned by the IEEE
  - LAP: Lower Address Part.
    - Manufacturer defined
    - Device specific
    - Transmitted with every packet as part of packet header.

Bluetooth

- Device Address



https://macaddresschanger.com/bluetooth-mac-lookup

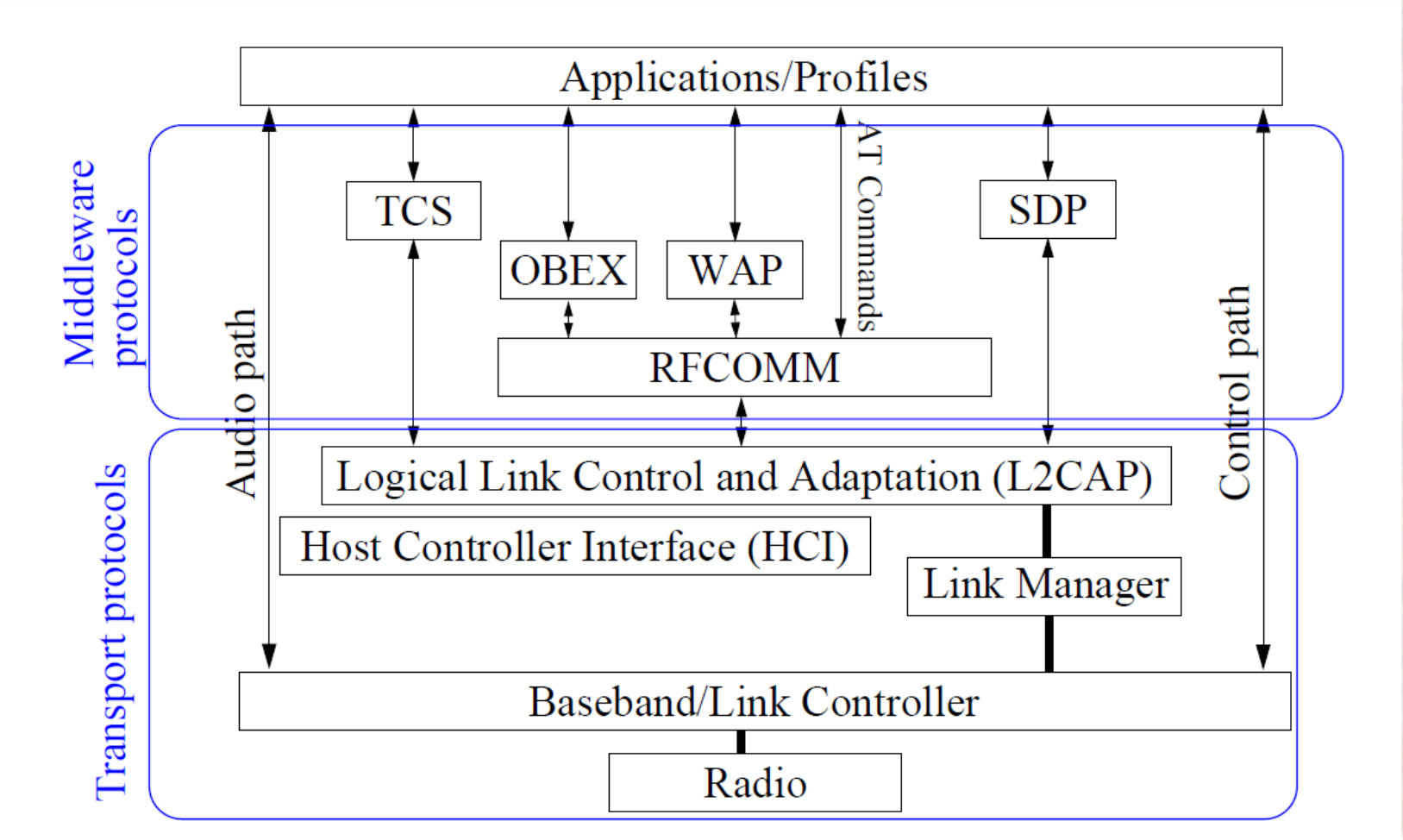
OUI Prefix	Company
00:06:66	Roving Networks

Bluetooth

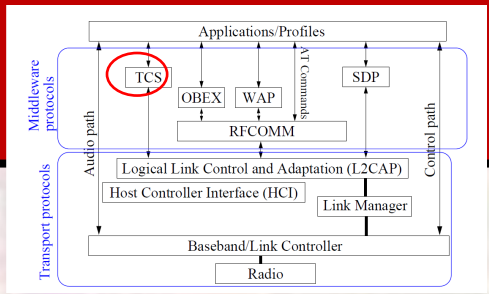
- Bluetooth Profiles
  - Set of rules that allow the technology to complete a particular task
  - Dozens of profiles
    - Advanced Audio Distribution Profile (A2DP)
      - Bluetooth Audio Streaming
      - Characterizes how multimedia audio is streamed from one device to another
    - File Transfer Protocol (FTP)
      - File transfer rules
    - Device ID Profile (DIP)
      - allows product ID, manufacturer, product version and the version of the Device ID to be identified
    - Hands Free Profile
      - duh!
    - Human Interface Device Profile (HID)
      - Rules for keyboards, touch screens, …

Bluetooth

- Bluetooth Protocol Stack

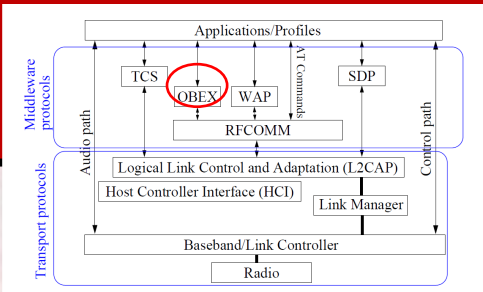


Bluetooth



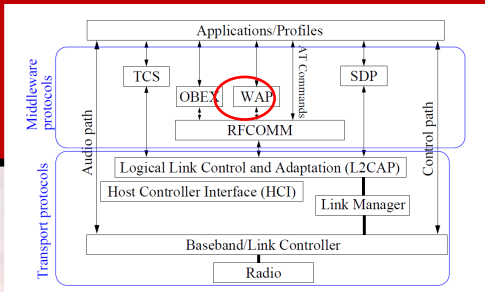
- Telephony Control Signaling (TCS)
  - TCS-AT
    - Telephony control can be performed using the AT command set
    - Uses RFCOMM to send and receive control signaling based on the AT command set (for example to implement a dialer application)
  - TCS-BIN
    - (BIN stands for the binary encoding of information), that runs directly on top of L2CAP;
    - Supports normal telephony control functions
      - placing and terminating a call
      - sensing ringing tones
      - accepting incoming calls
    - Supports point-to-multipoint communications
      - Base station can pass the ringing signal of an incoming call to several cordless headsets associated with the base station.

Bluetooth



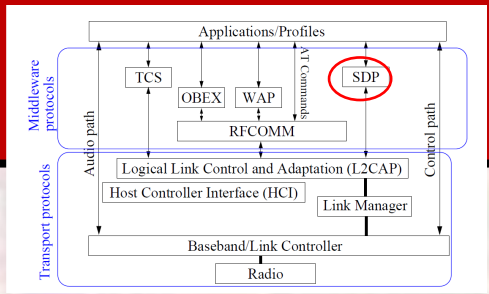
- Object Exchange
  - Uses a binary format for sending data
  - Has rigid transaction parameters
  - Targeted as a resource-sensitive solution
  - Uses a client/server model, in which the requesting device is considered the client device.
    - e.g. exchanging of digital business cards between devices

Bluetooth



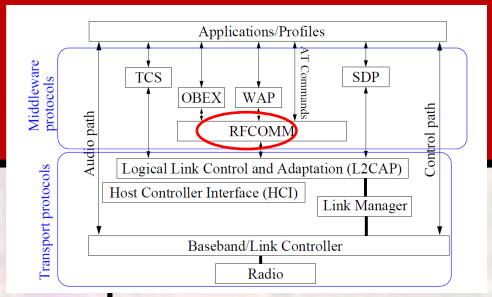
- Wireless Application Protocol (WAP)
  - Wireless protocol that allows mobile devices to use data service and access the Internet
  - No longer in use

Bluetooth



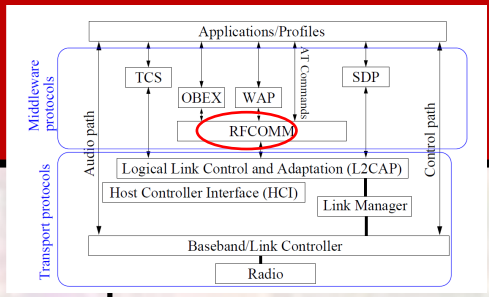
- Service Discovery Protocol (SDP)
  - Provides information about services
    - Does not provide access to these services
  - Optimized for usage by devices with limited capabilities over wireless links
  - Uses binary encoding of information
  - Unique identifiers (UUIDs) describe services and attributes
    - Don’t need a central registration authority for registering services
    - Most UUIDs are 128 bits long
    - 16-bit and 32-bit UUIDs may also be used

Bluetooth



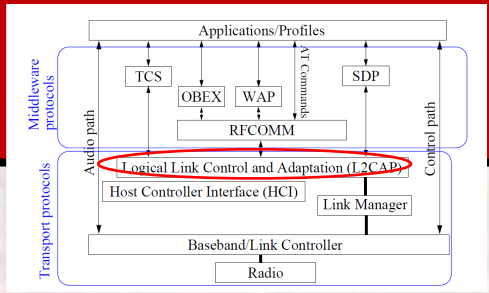
- RFCOMM Protocol
  - Serial interface over the packet-based transport layers
  - Emulates the signals on the nine wires of an RS-232 cable
  - Allows multiplexing (via L2CAP) several serial ports over a single transport
  - Flow control for individual channels
  - Has a reserved Protocol and Service Multiplexer (PSM) value used by L2CAP to identify RFCOMM traffic
  - No error control
  - Enables legacy applications -- written to operate over serial cables – to run without modification

Bluetooth



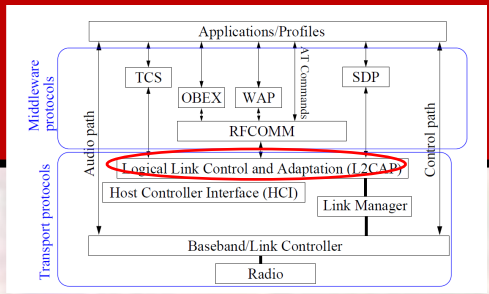
- RFCOMM Protocol
  - Serial interface over the packet-based transport layers
  - Emulates the signals on the nine wires of an RS-232 cable
  - Allows multiplexing (via L2CAP) several serial ports over a single transport
  - Flow control for individual channels
  - Has a reserved Protocol and Service Multiplexer (PSM) value used by L2CAP to identify RFCOMM traffic
  - No error control
  - Enables legacy applications -- written to operate over serial cables – to run without modification

Bluetooth



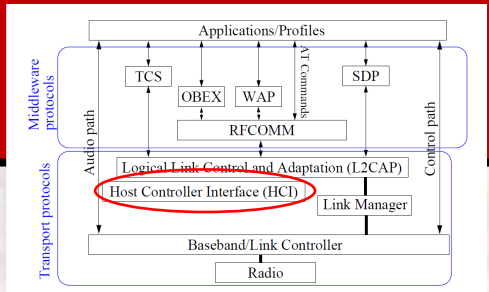
- Logical Link Control and Adaptation Protocol - L2CAP
  - Only data transport path
  - Supports multiplexing to allow several higher layer links to pass across a single ACL connection
  - Disassembly and reassembly to allow transfer of packets larger than lower layers support
  - Quality of Service (QoS) management for higher layer protocols

Bluetooth



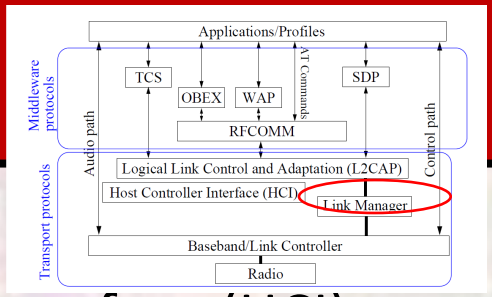
- Logical Link Control and Adaptation Protocol - L2CAP
  - Labels packets with Channel numbers
  - Special channel numbers (control channels) used for connecting, configuring, and disconnecting L2CAP connections
    - More than 1 command can be transmitted per packet
  - Packet configuration
    - length field (2 bytes)
    - channel identifier (2 bytes)
    - data field (0 .. 65535 bytes)

Bluetooth



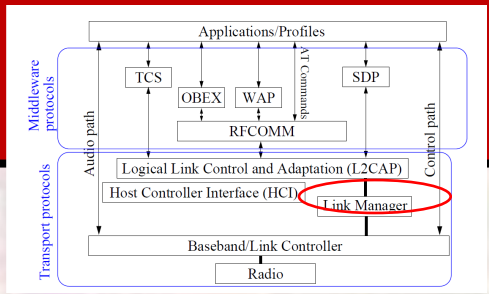
- Host Controller Interface
  - Interface between a host and a Bluetooth module
  - Allows Baseband and Link Manager to run on a processor in the Bluetooth module while higher layers and applications run on the host
  - Bluetooth module can wake the host via a message across this interface
  - 3 message interfaces supported
    - USB Universal Serial Bus
    - RS-232 serial interface with error correction
    - UART Universal Asynchronous Receiver Transmitter

Bluetooth



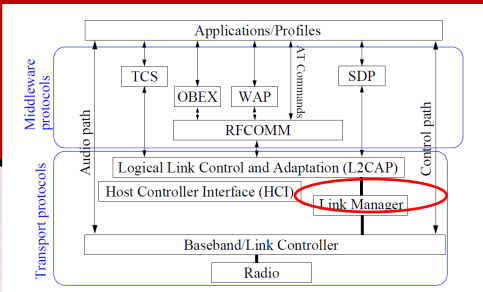
- Link Manager
  - Translates commands from Host Controller Interface (HCI) into operations at baseband level:
    - attaching Slaves to a piconet, and allocating active member addresses (AM addr)
    - tearing down connections when slaves leave piconet
    - configuring links, e.g., controlling Master/Slave switches
    - establishing ACL and SCO links
    - putting connections into one of the low-power modes
  - Communicates with other LMs using the Link Management Protocol (LMP)

Bluetooth



- Link Control Protocol (LCP)
  - Configures and controls baseband
  - Packet level access control
    - determines what packet is going to be sent next
  - High level operations
    - inquiry
    - paging
  - Configures and controls multiple links between devices and piconets
  - Does **not** require its own packets, but uses the (ARQN and SEQN) bits in baseband packets for SCO and ACL links to signal between link controllers - thus forming a logical LC (Link Control) channel

Bluetooth

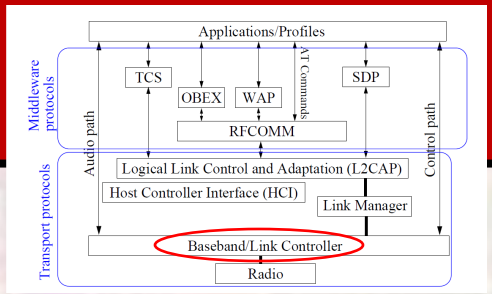


- Link Control Protocol (LCP)

Link Control states

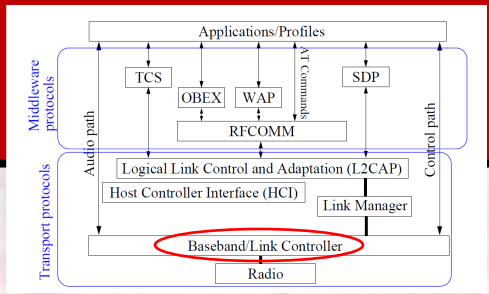
State	Description
Standby	inactive, radio not switched on
Inquiry	device tries to discover all Bluetooth enabled devices in the close vicinity; uses a special fast hopping sequence; FHS packets with device information, such as clock, frequency hop sequence, and BD ADDR, received from available devices; ⇒ a list of all available devices
Inquiry Scan	devices periodically enter the inquiry scan state to make themselves available to inquiring devices; a special slow hopping sequence used
Page	master enters page state and transmits paging messages to slave using access code and timing information which it learned earlier
Page Scan	device periodically enters page state to allow paging devices to establish connections
Connection-Active	Slave synchronizes to master's frequency hop and timing sequence. Master transmits a POLL packet to verify link, Slave sends NULL packet in reply
Connection-Hold	device ceases to support ACL traffic for a period of time, keeps Active Member address (AM_ADDR)
Connection-Sniff	device listens in pre-defined time slots only
Connection-Park	device listens for traffic only occasionally, gives up its AM address

Bluetooth



- Baseband
  - Controls the radio and is responsible for
    - Low level timing
    - Error control
    - Management of the link during a single data packet transfer
  - Packet types:
    - SCO, ACL - carrying payload
    - ID packet consists of access code, used during re-connection
    - NULL packet consists of access code and header, used for flow control or to pass ARQ (automatic repeat request)
    - POLL packet same structure as NULL packet, must be acknowledged
    - FHS (Frequency Hop Synchronization)
    - DV packets have combined data and voice

Bluetooth



- Baseband

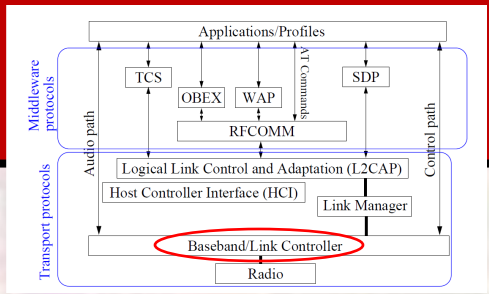
LSB				MSB
ID	AC			
(bit count)	68 or 72			
POLL/NULL	AC	BB_Header		
	68 or 72	54 (1/3 FEC)[a]		
FHS	AC	BB_Heade	FHS payload	
	68 or 72	54 (1/3 FEC)	240 (2/3 FEC)	
ACL/SCO	AC	BB_Heade	ACL or SCO payload	
	68 or 72	54 (1/3 FEC)	0-2744 ({1,2,3[b]}/3 FEC)	
DV	AC	BB_Heade	SCO payload	ACL payload
	68 or 72	54 (1/3 FEC)	80	32-150 (2/3 FEC)

a. 54 bits includes the FEC bits (there are 18 bits of information with each bit repeated 3 times)

b. 3/3 FEC implies no FEC

Bluetooth

- Baseband



Baseband Packet formats

AC	⇒	preamble	sync word		trailer
Access code		4	64		4
BB_Header	⇒	AM_ADDR[a]	PDU_TYPE	Flags[b]	HEC[c]
BaseBand header		3	4	3	8
SCO payload	⇒	SCO Data[d]			
ACL payload	⇒	ACL_pld_hdr[e]	ACL_pld_body		CRC

a. Broadcast packet has address zero

b. Flow (=1 means receive buffer is full), ARQN (ACK represented by ARQN=1 and NAK by ARQN=0), SEQN (alternating bit)

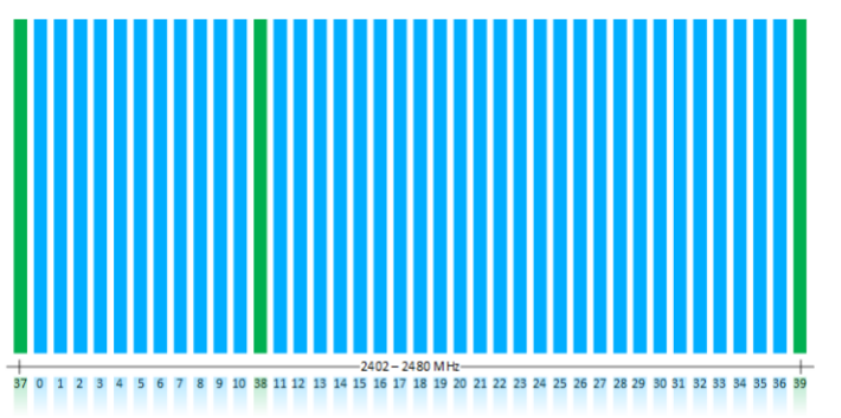
c. Header error check (HEC)

d. 30 bytes (240 bits), error control code with rate 1/3, 2/3, or 1 (no FEC) used for source data size of 10, 20, or 30 bytes; note BB_Header flags for ARQN and SEQN are not used - since there is no flow control or retransmission, similarily the HEC is not used

e. L_CH (Logical CHannel) Field (3 bits) indicates whether payload is start or continuation of message, Flow field (1 bit) controls for data transfer at L2CAP level, Length field (8 bits) indicates the number of data bytes in the payload' header ends with 4 undefined bits

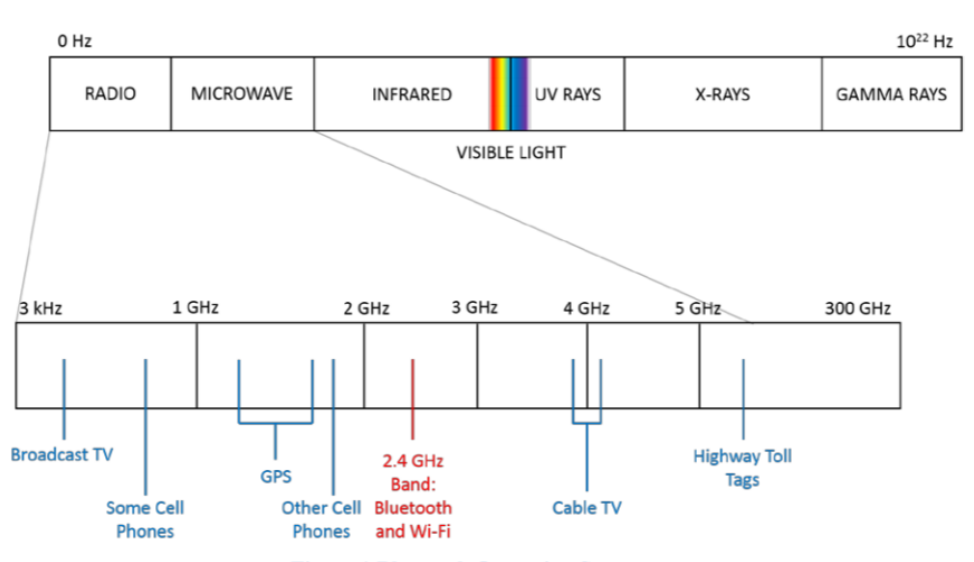
Bluetooth

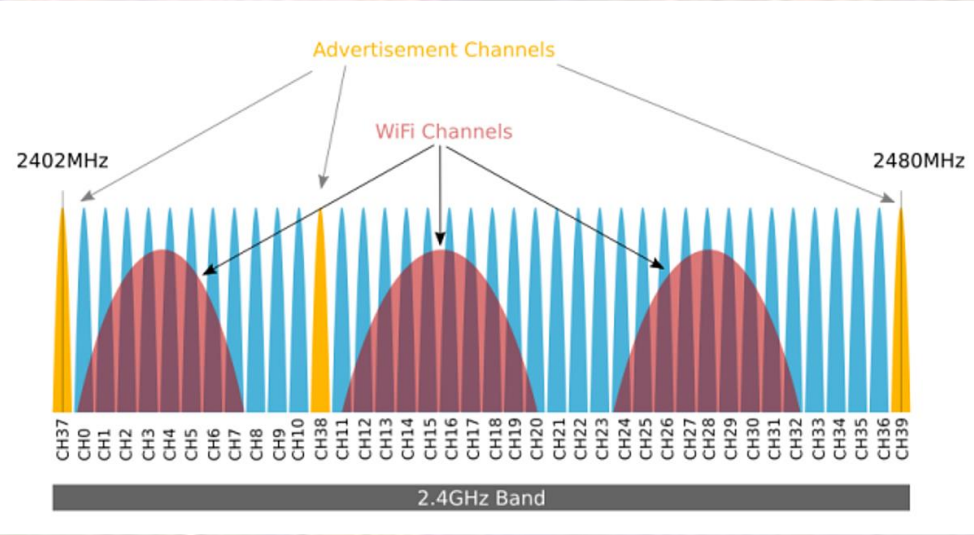
- Radio
  - 2.4 GHz ISM (Industrial Scientific Medical) band
    - License free in most countries
  - 2402 MHz - 2480 MHz
  - 79 channels
    - 1MHz bandwidth
  - 3 advertising channels (LE for sure, ???)
    - Device discovery, connection establishment, and broadcast



Bluetooth

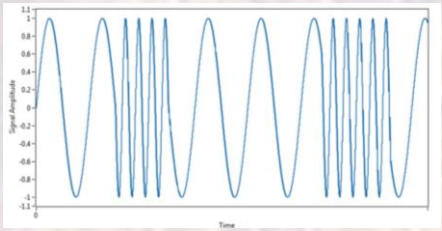
- Radio



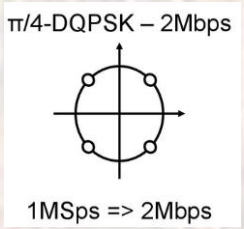


Bluetooth

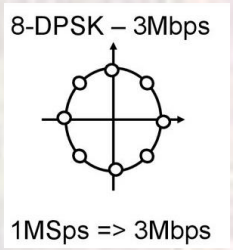
- Radio
  - Modulation
    - GFSK modulation (1Mbit/s)
      - Early versions of Bluetooth
      - +/- 157KHz
      - 1-100 mW transmit power
      - Always used for the header
      - Always used in BT-LE



    - π/4-DQPSK (2Mbit/s)
      - Bluetooth 2.0
      - 2 bits/symbol



    - 8DPSK (3Mbit/s and greater)
      - Bluetooth 2.0+EDR and beyond
      - 3 bits/symbol

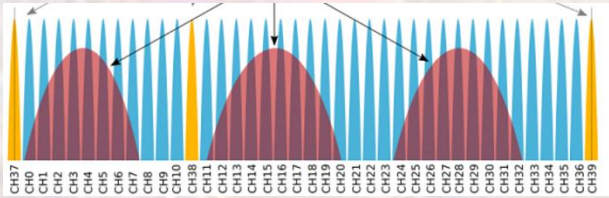


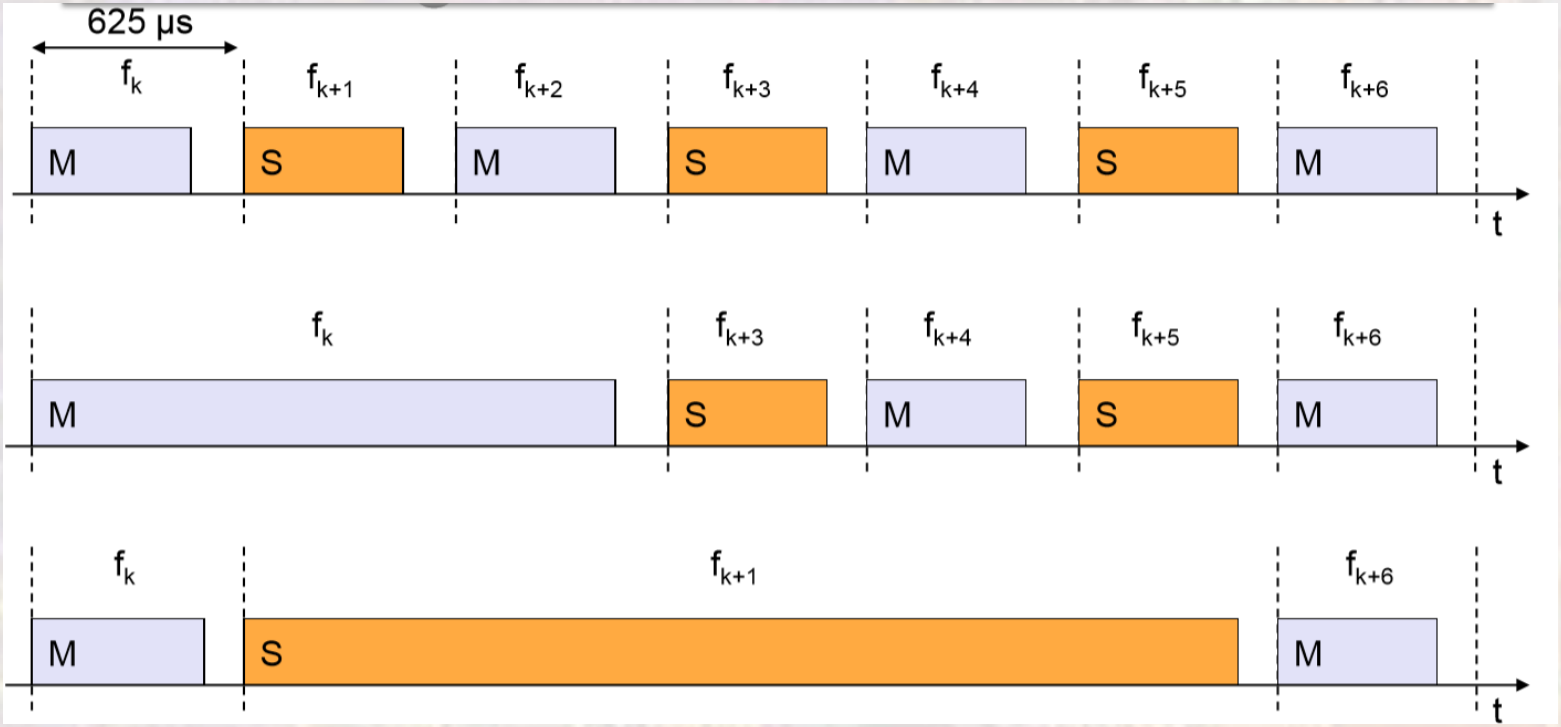
Bluetooth

- Radio – Frequency Hopping
  - 1st two bytes of MAC address (BD_ADDR) used for configuration
  - Each device has a local free-running 28-bit clock that ticks once every 312.5 ms
    - half the residence time in a frequency when the radio hops
  - Nominal hop rate of 1,600 hops/sec
  - Pseudo-random hopping sequence
  - Each slave receives master's address and clock, then uses this to calculate the frequency hop sequence

Bluetooth

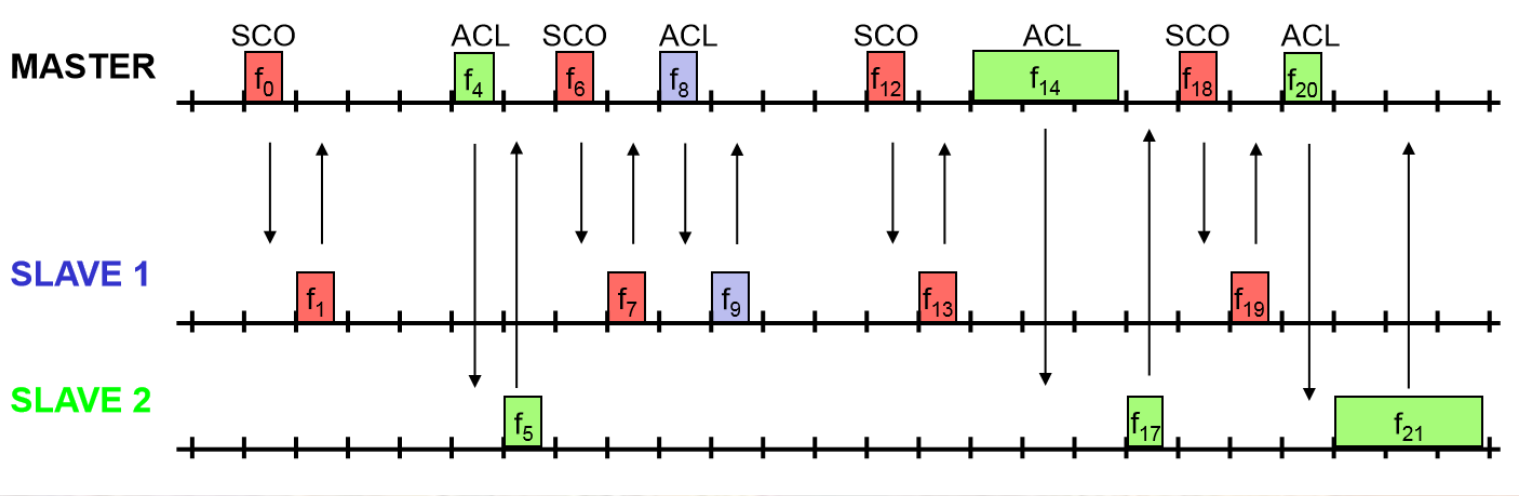
- Radio – Adaptive Frequency Hopping
  - Master / slave alternate in slots
  - Packets can be 1, 3 or 5 slots
  - Hopping is halted for extended hops





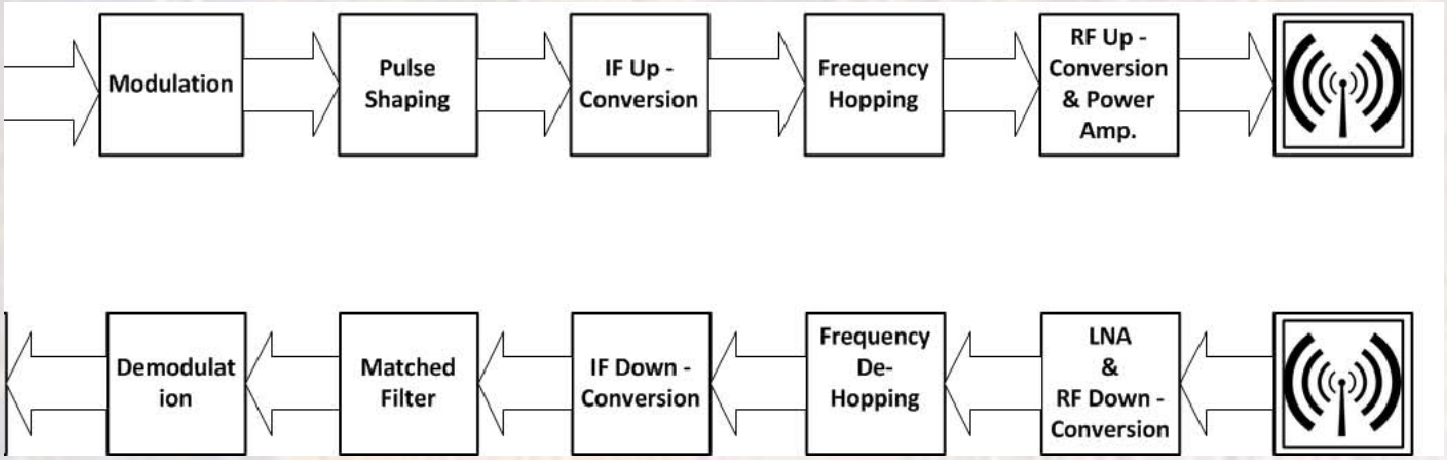
Bluetooth

- Radio – TDM
  - Time Domain Multiplexing
  - Divide the total bandwidth between Bluetooth devices using a given hop sequence
  - Master assigns time slots to slaves
  - Packets are joined together in transmit and receive pairs
  - Master and slaves alternate in time-division duplex (TDD)



Bluetooth

- Radio



Bluetooth

- Performance Summary

Bluetooth version	*Features*	***Speed/Data Rate*** (in theory and without obstacles)	***Range*** (in theory and without obstacles)
V1.0	Basic rate	**1Mbps**	**33ft (10m)**
V2.1	Basic rate SSP – Secure Simple Pairing EDR – Enhanced Data Rate	**3Mbps**	**100ft (30m)**
V3.0	Basic rate EDR SSP HS – High speed Protocol	**24Mbps**	**100ft (30m)**
V4.0, V4.1, V4.2	Basic Rate EDR SSP HS LE – Low Energy Protocol	**24Mbps**	**200ft (60m)**
V5.0	Basic Rate EDR SSP HS LE – Low Energy Protocol IoT – Internet of Things Protocol	**48Mbps**	**800ft (200m)**

HOW?
1MS/s with 8DPSK → 3Mb/s

Bluetooth

- Performance Summary
  - BT 3.0
    - Supports a max of 3Mbps
  - BT 3.0 + HS
    - Use BT to establish connections
    - Use WiFi for data transfer
  - BT 4.x
    - Breaks the standard into 3 pieces
    - Classic – BT2.x equivalent
    - High Speed – BT3.x + HS equivalent
    - Low Energy (LE) – Low energy/limited range version
  - BT 5.x
    - Added a 2MSps capability

Bluetooth

- Performance Summary

Type	Power	Max Power Level	Designed Operating Range	Sample Devices
Class 1	High	100 mW (20 dBm)	Up to 100 m (328 feet)	USB adapters, access points
Class 1.5 (low energy)[7]	Med-High	10 mW (10 dBm)	Up to 30 m (100 feet), but typically 5 m (16 feet)	Beacons, wearable sensors
Class 2	Medium	2.5 mW (4 dBm)	Up to 10 m (33 feet)	Mobile devices, Bluetooth adapters, smart card readers
Class 3	Low	1 mW (0 dBm)	Up to 1 m (3 feet)	Bluetooth adapters