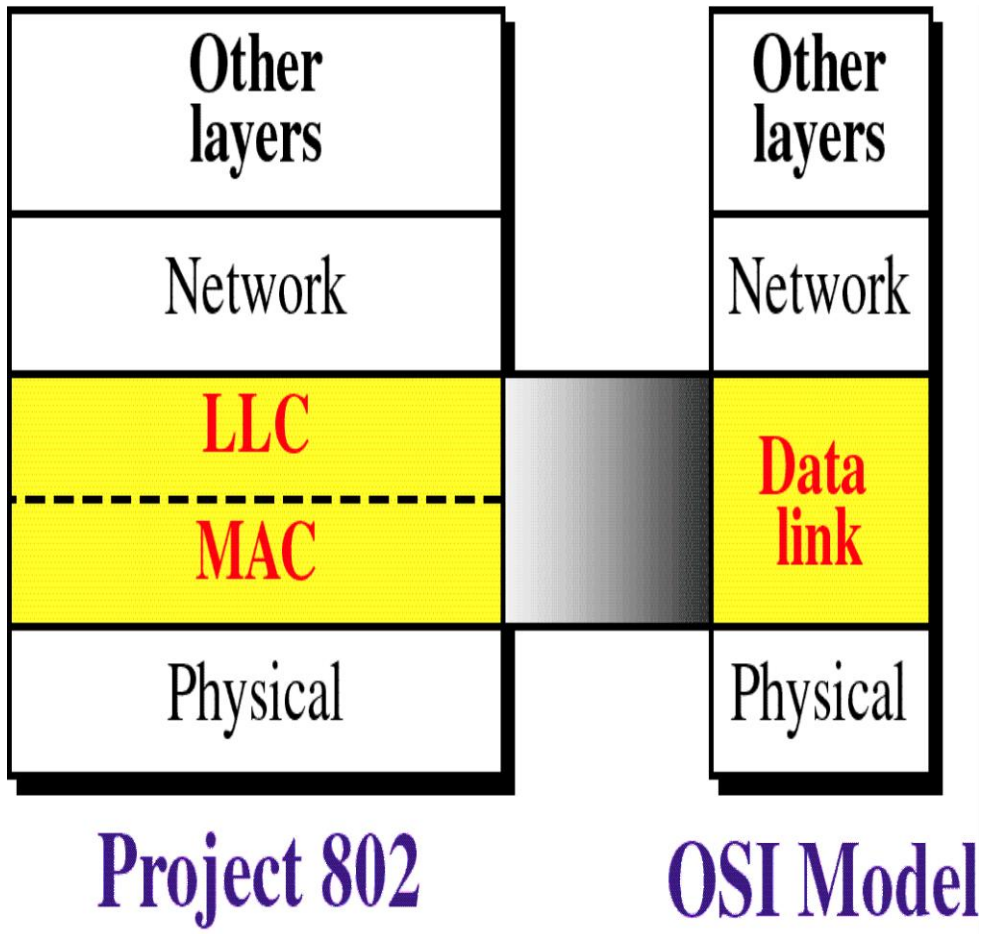
IEEE 802.15 STANDARD FOR WIRELESS PERSONAL AREA NETWORKS

ECE 525E – WIRELESS COMMUNICATION

Tuesday, 07 April 2026

RECAP: WHAT IS IEEE PROJECT 802?

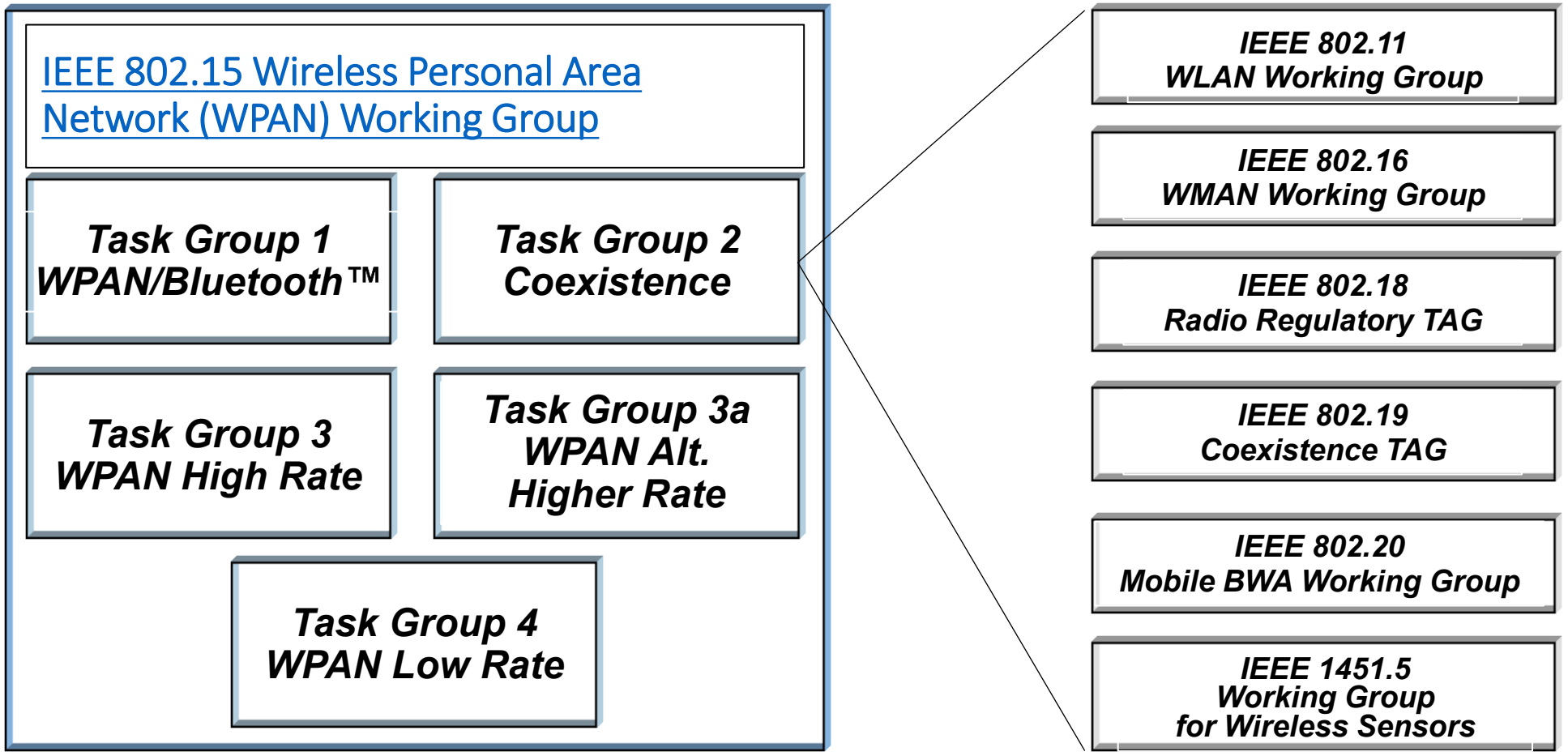
1. **In 1980, the computer society of the IEEE** started the 802 project to set up standards to enable intercommunication between equipment from a variety of manufacturers.
2. **Project 802** does not seek to replace any part of the OSI model but enhances Layer 2.
3. The IEEE has subdivided the data link layer into two sub layers:
   a) Logical link control(LLC)
   b) Medium access control(MAC)



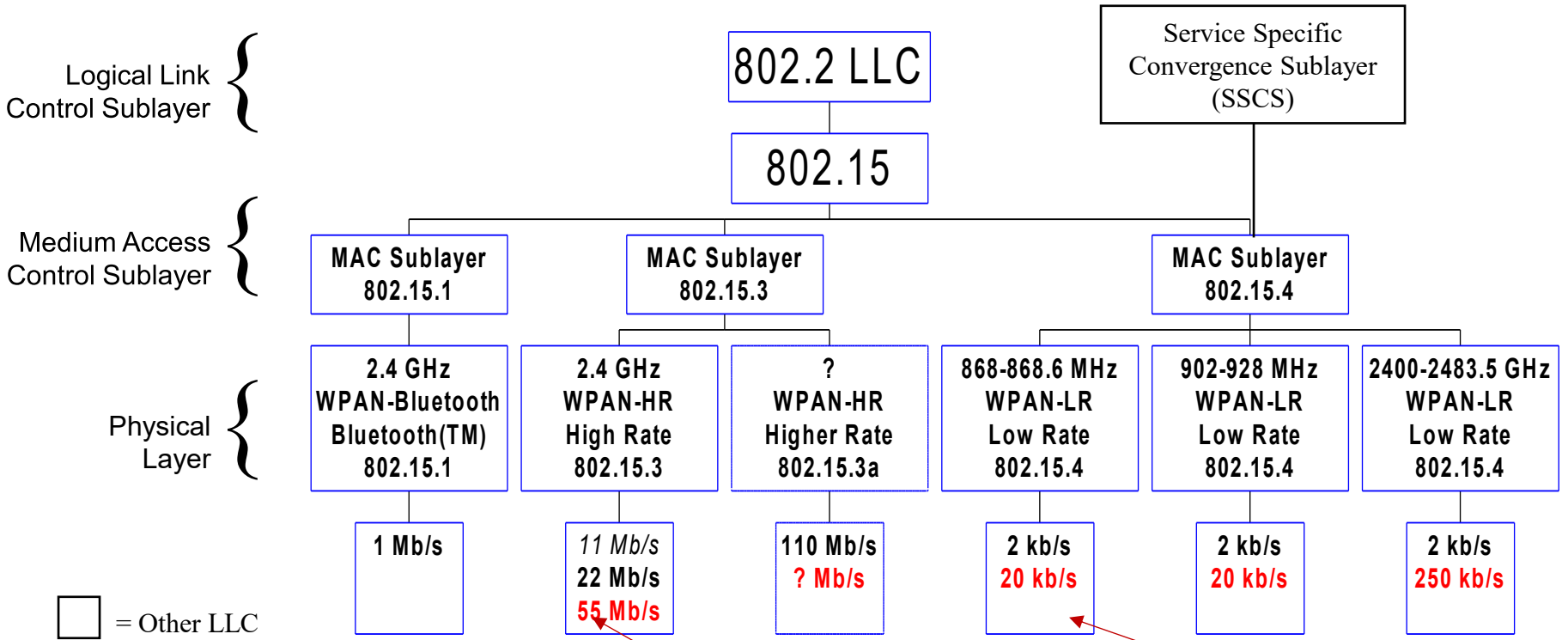
WHAT IS 802.15 WORKING GROUP

1. IEEE 802.15 is the working group under the 802 Project for Wireless personal area networks (WPANs) such as:
   a) Bluetooth
   b) Zigbee
2. These networks find application in the following areas:
   a) Internet of Things networks, mesh networks,
   b) body area networks,
   c) wearables,
   d) visible light communications, among others.

WORKING GROUP 802.15 AND THE OTHER IEEE WIRELESS STANDARDS AREAS



802.15 WORKING GROUP



High-Rate WPANs operate in the unlicensed 2.4 GHz band at data rates up to 55 Mb/s that are commensurate with distribution of high-definition video and high-fidelity audio.

Low-Rate -WPAN is a standard that pertains to the physical layer and the media access control of the data link layer of low-rate wireless personal area networks.

BLUETOOTH

ECE 2115 – WIRELESS COMMUNCATION

Tuesday, 07 April 2026

WHAT IS BLUETOOTH?

1. Bluetooth is a global, RF-based (S-BAND - ISM band: 2.4GHz), short-range, connectivity technology & solution for portable, personal wireless devices
   a) it is not just a radio
   b) create piconets on-the-fly (appr. 1Mbps)
      - piconets may overlap in time and space for high aggregate bandwidth
2. Bluetooth protocol operates at 2.4GHz in the same unlicensed ISM frequency band where RF protocols like ZigBee and WiFi.
3. The Bluetooth specification comprises:
   a) Hardware and software protocol specification
   b) Usage case scenario profiles and interoperability requirements

BLUETOOTH ARCHITECTURE / 01

Communication

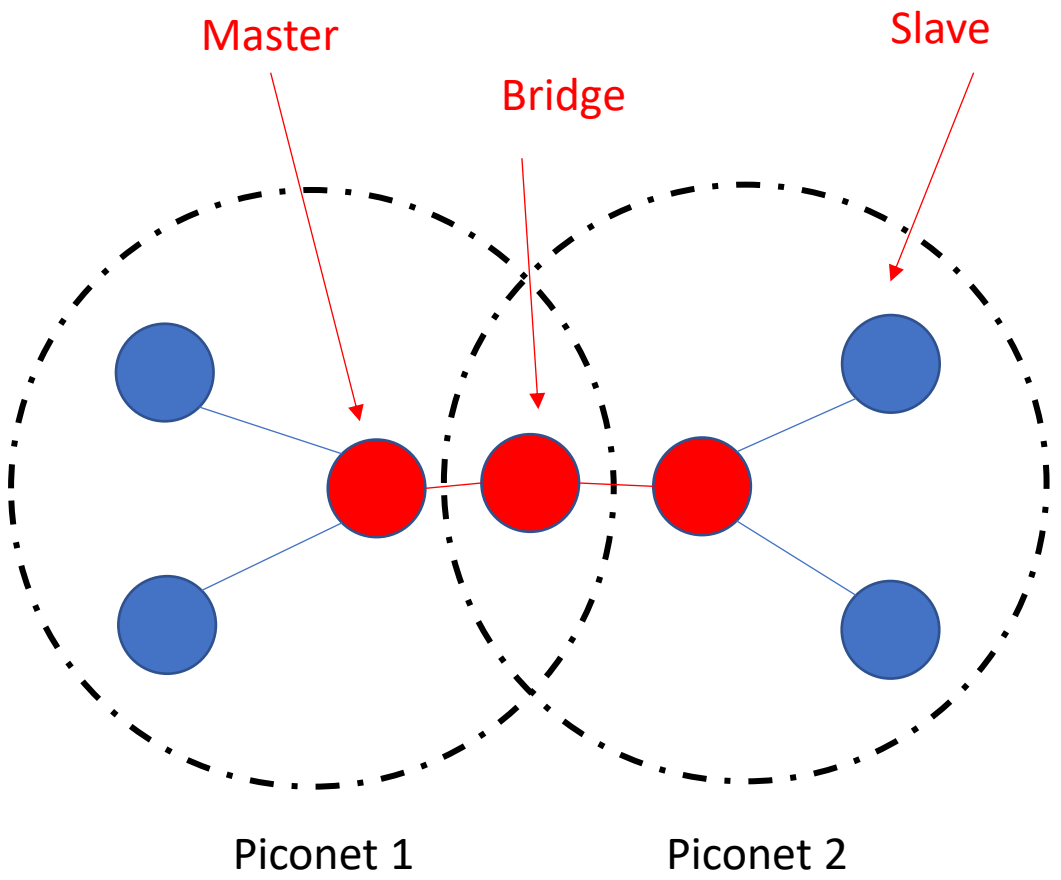
- Bluetooth communication occurs between a master and a slave station. A slave can only connect to one master.
- Bluetooth radios are symmetric in that the same device may operate as a master and also the slave.

Piconets

- Two or more radio devices together form **ad-hoc** networks called piconets.
- All units within a piconet share the same channel.
- Each piconet has one master device and one or more slaves. There may be up to seven active slaves at a time within a piconet.
- A device may be a master in one piconet and a slave in another or a slave in more than one piconet.

Scatternet

- Multiple piconets with overlapping coverage areas form a scatternet.



(a) Scatternet

BLUETOOTH ARCHITECTURE / 02

Radio designation

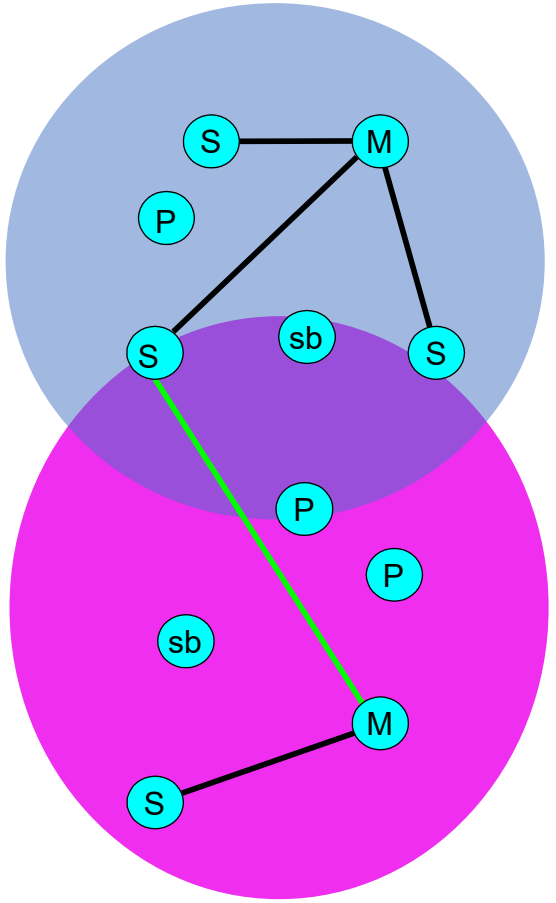
- Connected radios can be master or slave
- Radios are symmetric (same radio can be master or slave)

Piconet

- Master can connect to 7 simultaneous or 200+ inactive (parked) slaves per piconet
- Each piconet has maximum channel capacity of 1 Mbps.
- Unique hopping pattern/ID

Scatternet

- High-capacity system
- Minimal impact with up to 10 piconets within range

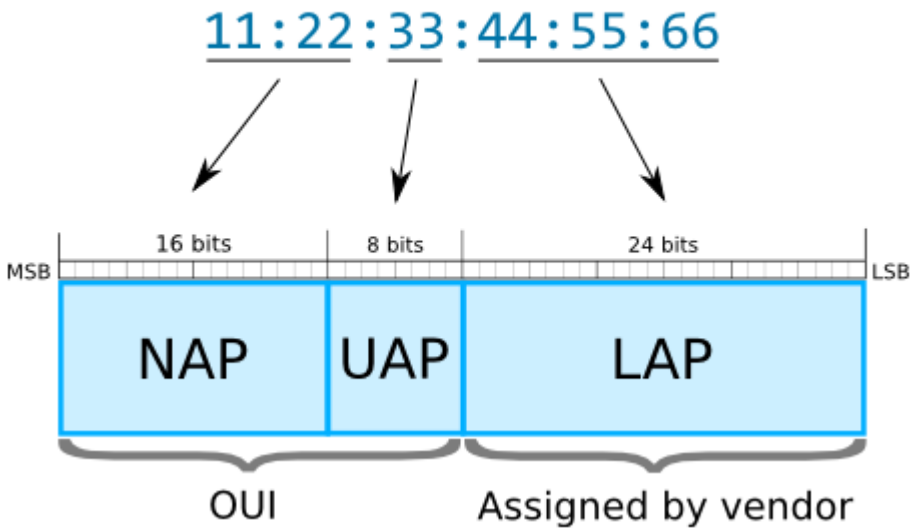


BLUETOOTH PICONET

1. All devices in a piconet hop in frequency together
   To form a piconet: master gives slaves its *clock* and *device ID*
   Hopping pattern determined by *device ID* (48-bit)
2. Phase in hopping pattern determined by *Clock*
   Non-piconet devices are in standby
3. Piconet Addressing
   a) **A**ctive **M**ember **A**ddress (AMA, 3-bits), i.e Master and 2^3-1 = 7 slave devices
   b) **P**arked **M**ember **A**ddress (PMA, 8-bits), i.e Master + 2^8-1 = 255 Parked devices

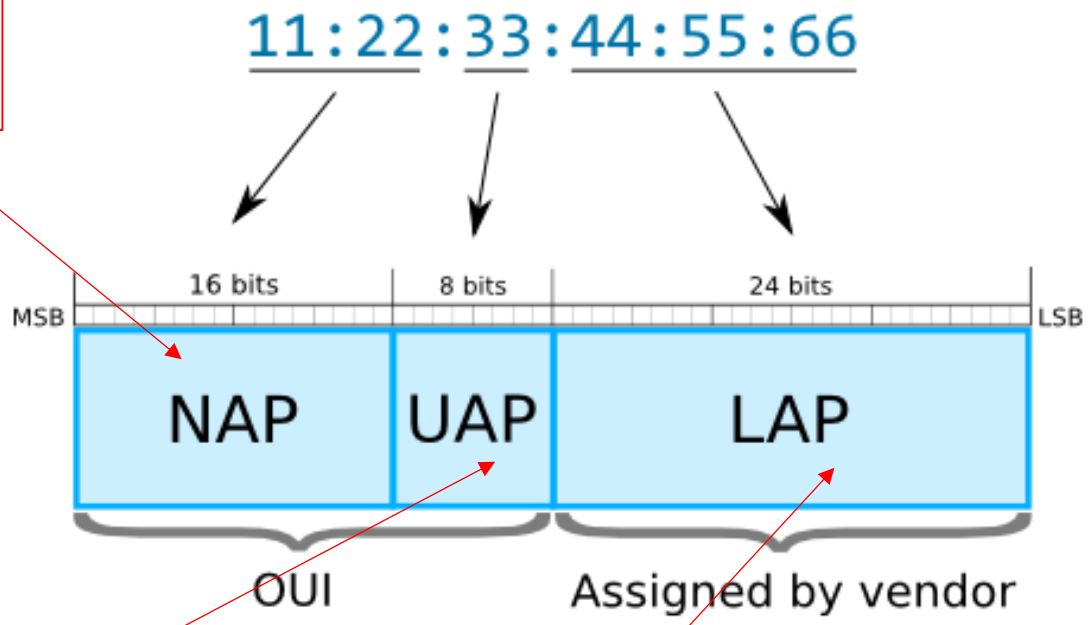
BLUETOOTH NAMES & ADDRESSES

- Every single Bluetooth device has a unique 48-bit address, commonly abbreviated BD_ADDR.
- BD_ADDR is usually displayed as 6 bytes written in hexadecimal and separated by colons e.g. 00:11:22:33:FF:EE.
- The most-significant half (24 bits) of the address is an **Organization Unique Identifier (OUI),** which identifies the manufacturer and are assigned by IEEE.
- The lower 24-bits are the more unique part of the address.



BLUETOOTH ADDRESSING (BD_ADDR)

NAP
Non-significant **A**ddress **P**art (2 bytes). Contains first 16 bits of the OUI. The NAP value is used in Frequency Hopping Synchronization frames



UAP
Upper **A**ddress **P**art (1 byte) is used for seeding in various Bluetooth specification algorithms.

LAP
Lower **A**ddress **P**art (3 bytes) uniquely identifies a Bluetooth device as part of the Access Code in every transmitted frame.

MAC ADDRESS OF BLUETOOTH DEVICES

- Most Bluetooth devices have the MAC address clearly labeled.
- For example, on this RN-42 Bluetooth Module, the address printed next to "MAC NO." is 00066666628BE:

Bluetooth SMD Module - RN-42 (v6.15)

WRL-12574 ROHS

3

$18.95

Shipping outside of the US?
Click here for info

Notify Me We do not currently have an estimate of when this product will be back in stock.

- 1 +

BACKORDER

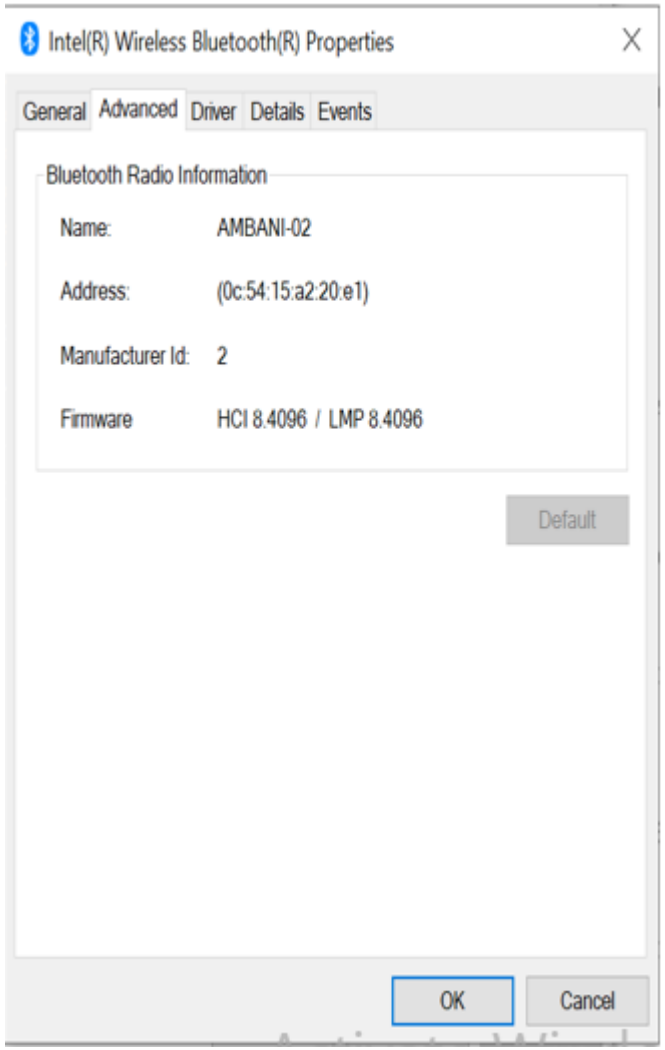
Stock availability

BLUETOOTH USER FRIENDLY NAMES

1. Bluetooth devices also have user-friendly names given to them for easy identification.

2. The rules for device names are less stringent.

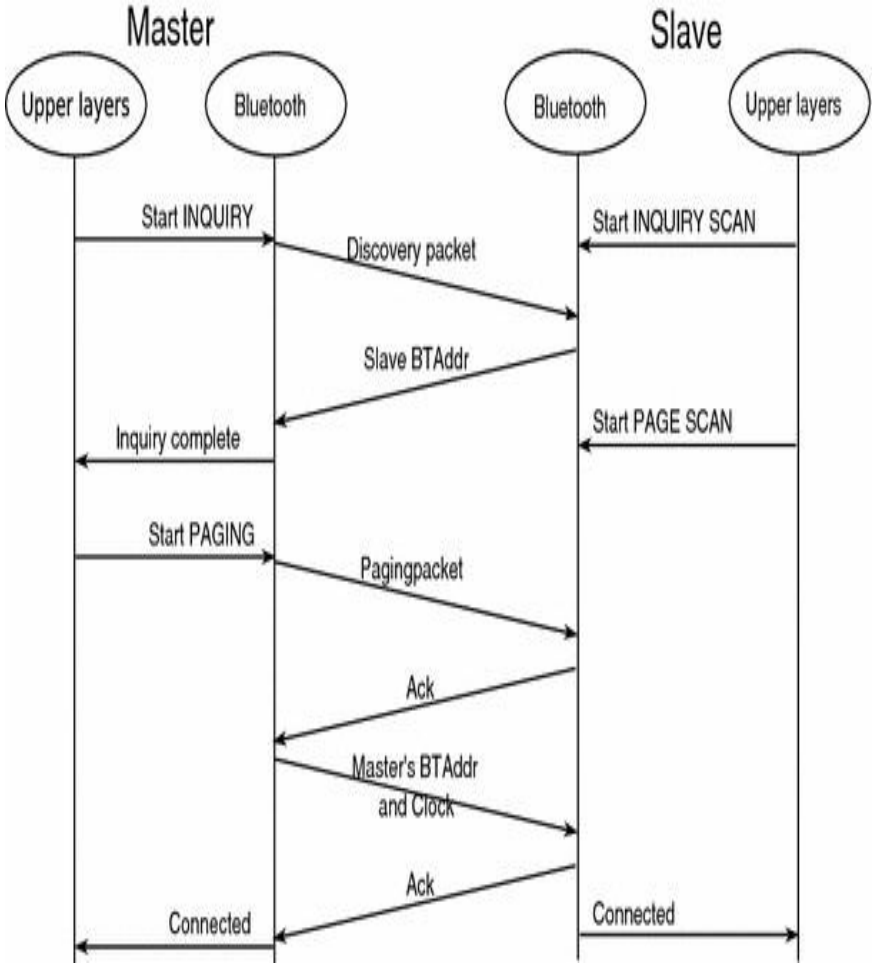
3. They can be up to 248 bytes long.
4. Two devices can share the same name.



BLUETOOTH CONNECTION PROCESS

Creating a Bluetooth connection between two devices is a multi-step process involving three progressive states:

1. **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.
2. **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).
3. **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



BLUETOOTH CONNECTION MODES

While connected, a device can either be actively participating or it can be put into a low power sleep mode.

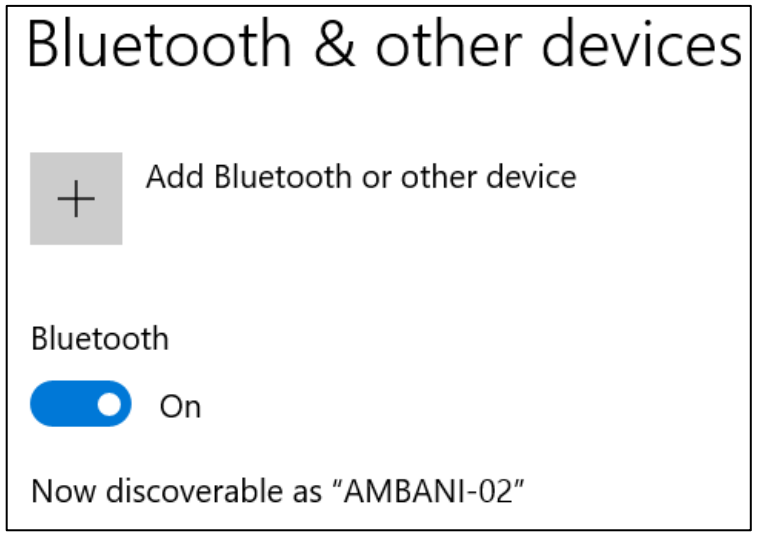
1. **Active Mode:** Regular connected mode, where the device is actively transmitting or receiving data.
2. **Sniff Mode:** Power-saving mode, where the device is less active. It'll sleep and only listen for transmissions at a set interval (e.g. every 100ms).
3. **Hold Mode:** A temporary, power-saving mode where a device sleeps for a defined period and then returns back to active mode after some interval. The master can command a slave device to hold.
4. **Park Mode:** 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.

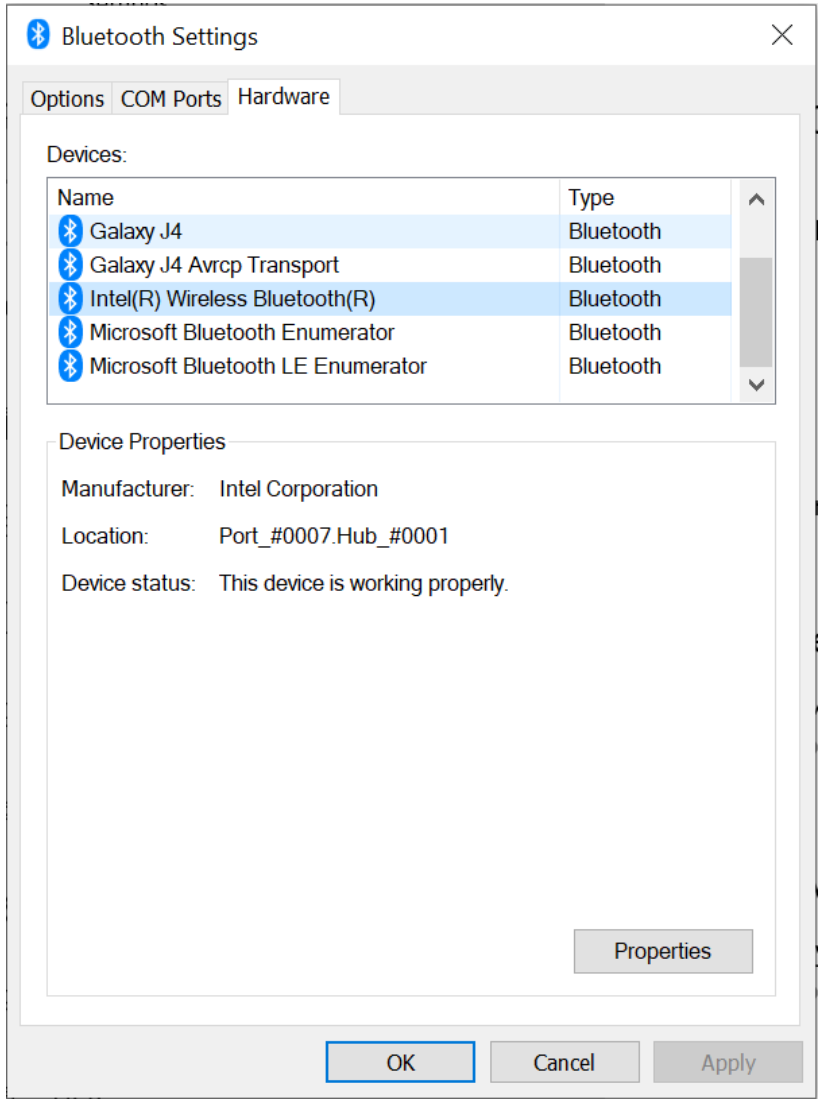
HOW TO FIND BLUETOOTH BD_ADDR IN WINDOWS /01

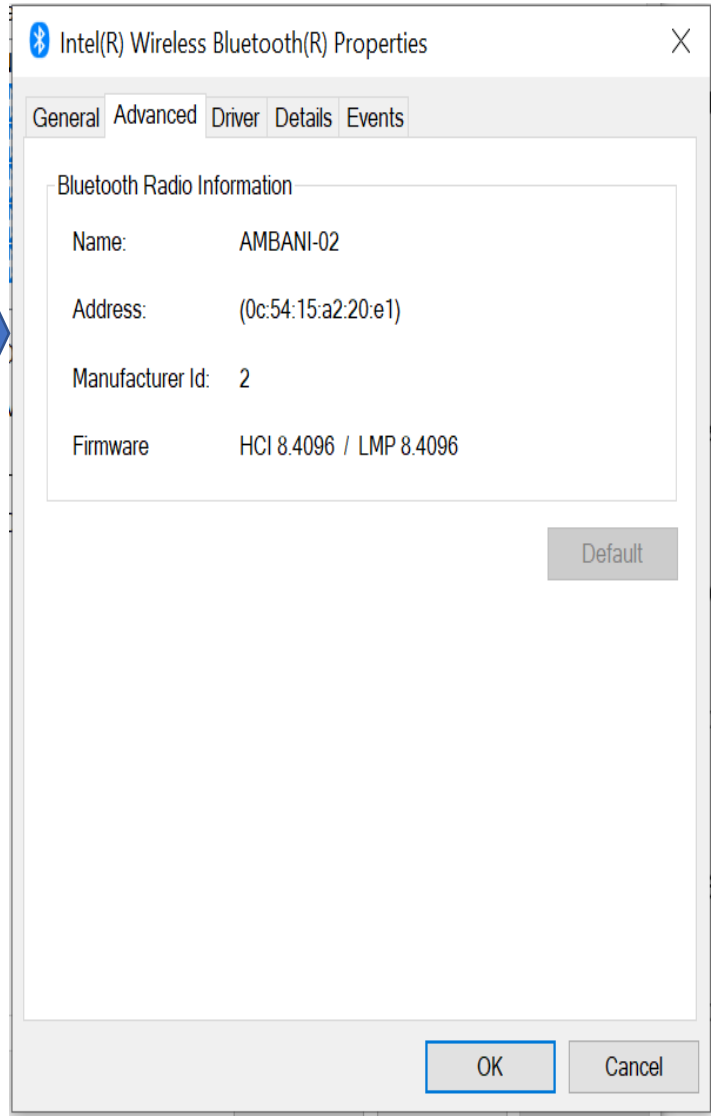
Follow the following steps to find Bluetooth MAC Address in Windows:

1. Click the Bluetooth icon in the system tray and select "Open Settings".
2. Select "Bluetooth and Other Devices"
3. Select “More Bluetooth Options".
4. In the "Bluetooth Radio Properties" form go to "Advanced" tab.

HOW TO FIND BLUETOOTH BD_ADDR IN WINDOWS /02

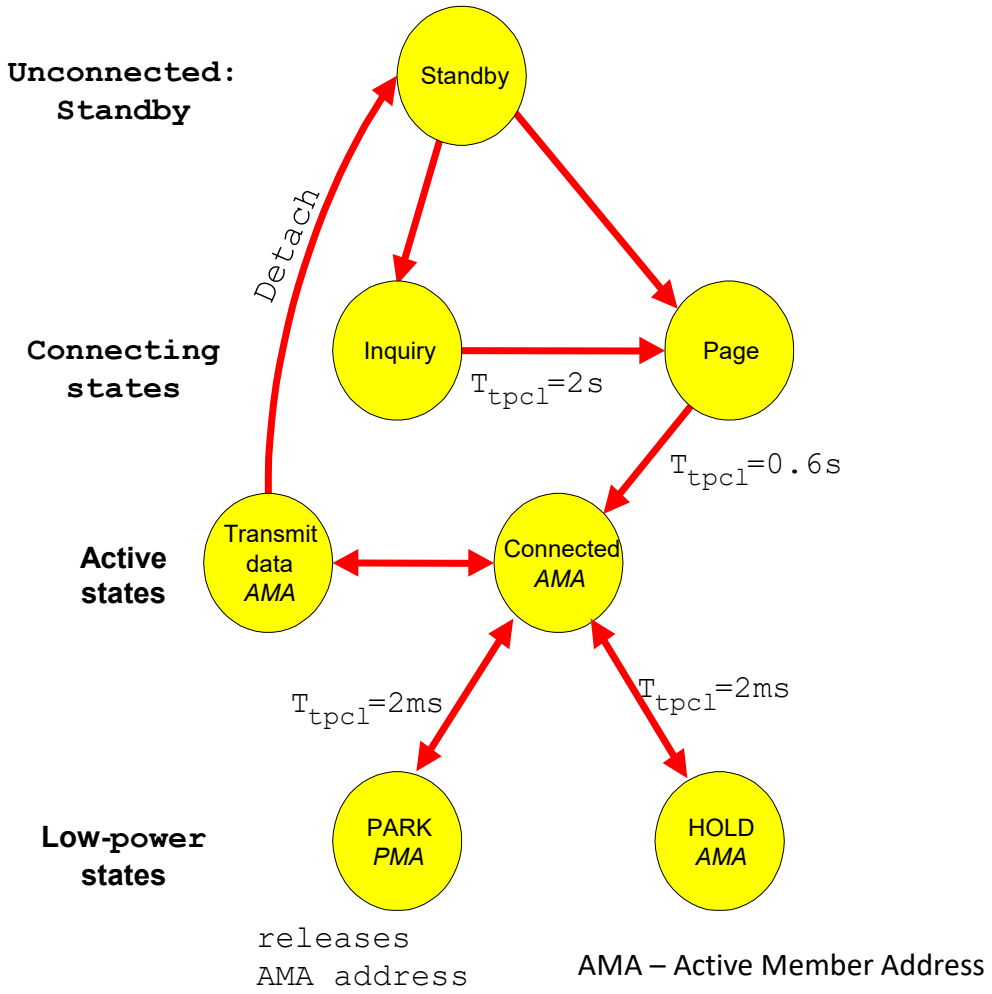






BLUETOOTH BASESBAND PROTOCOL

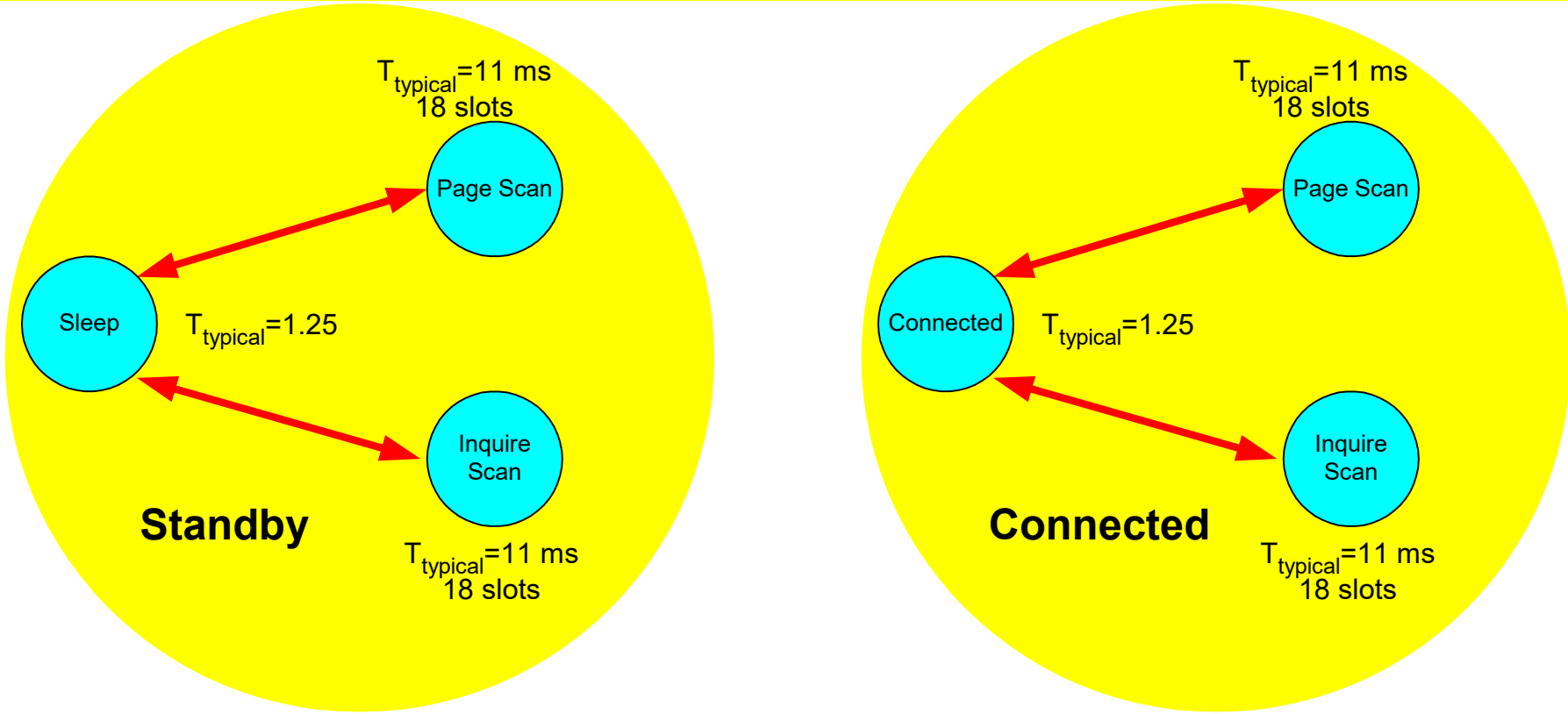
- Standby
  - Waiting to join a piconet
- Inquire
  - Ask about radios to connect to
- Page
  - Connect to a specific radio
- Connected
  - Actively on a piconet (master or slave)
- Park/Hold
  - Low-power connected states



BLUETOOTH INQUIRE PROCEDURE

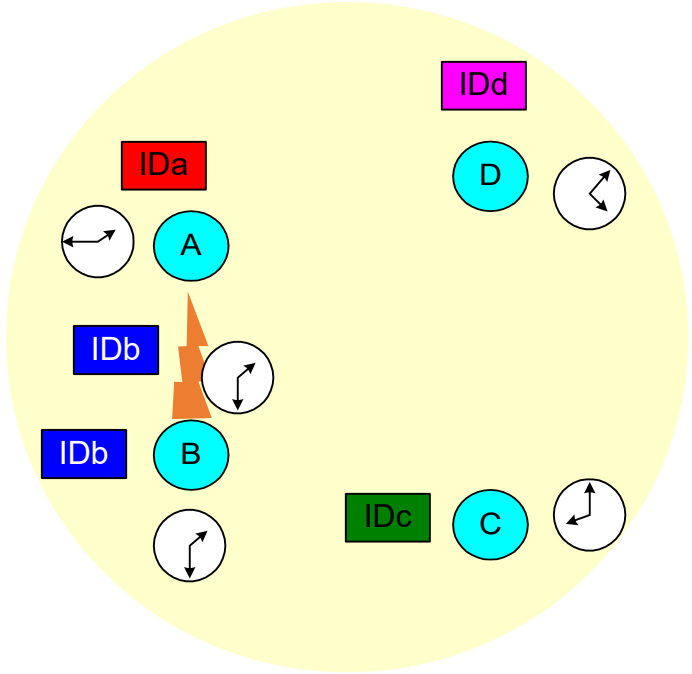
1. Paging radio issues page packet with Inquire ID
2. Any radio doing an Inquire scan will respond with an FHS packet
   a) FHS packet gives Inquiring radio information to page
      I. Device ID
      II. Clock
   b) If there is a collision then radios wait a random number of slots before responding to the page inquire
3. After process is done, Inquiring radio has *Device IDs* and *Clocks speeds* of all radios in range

PAGE AND INQUIRE SCANS



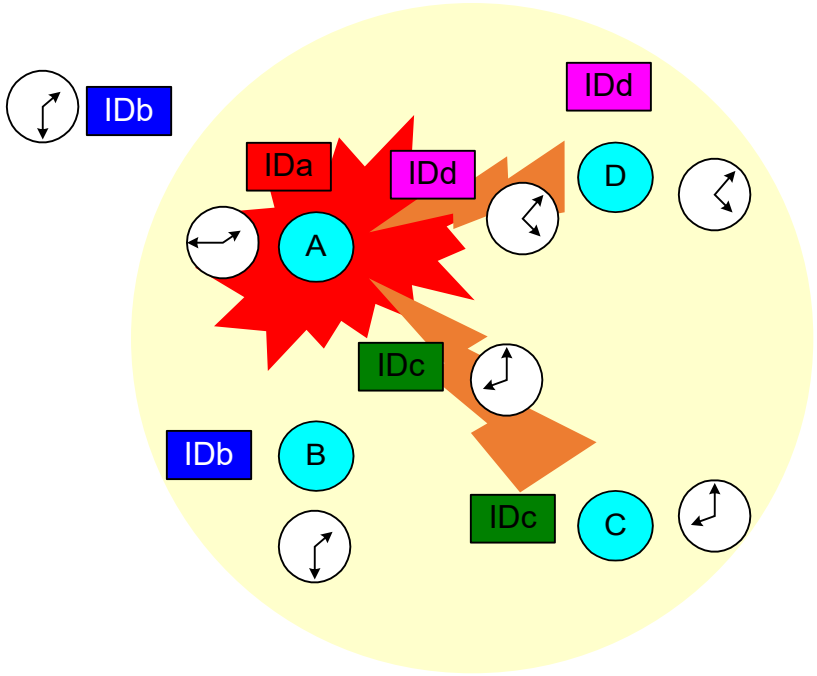
- A radio must be enabled to accept pages or inquires
  - Consumes 18 slots every 1.25 s (or so) for each scan
    - slot is 0.625 ms

INQUIRING FOR RADIOS / 01



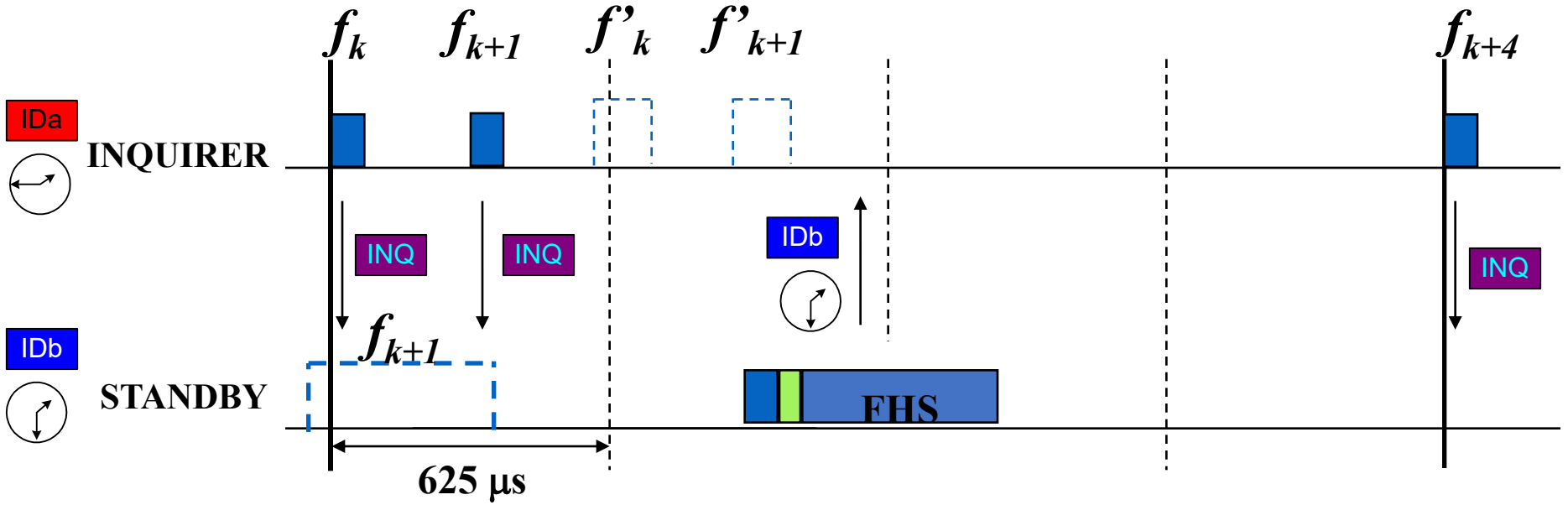
- Radio Wants to find other radios in the area
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing a Inquire Scan
  - Radio B recognizes Inquire and responds with an FHS packet
    - Has slave's ***Device ID*** and ***Clock***

INQUIRING FOR RADIOS / 02



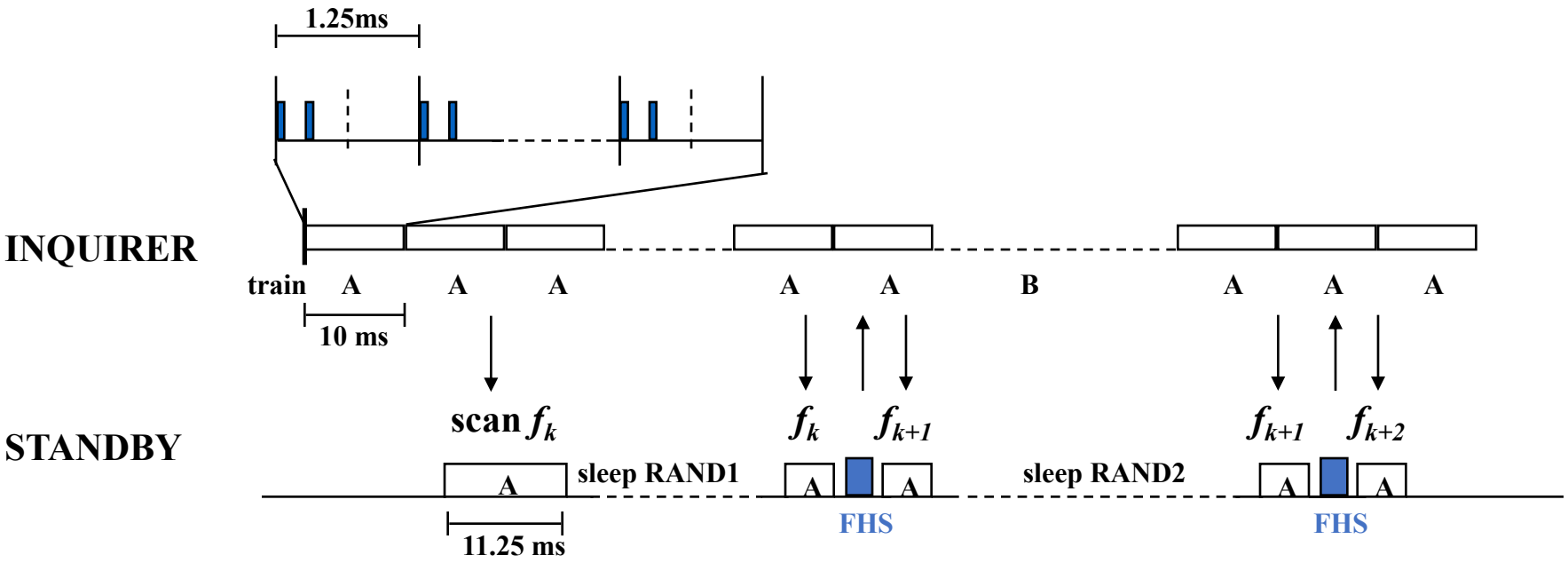
- Radio Wants to find other radios in the area
  - Radio A Issues an Inquire (again)
  - Radios C and D respond with FHS packets
    - As radios C & D respond simultaneously packets are corrupted and Radio A won't respond
    - Each radio waits a random number of slots and listens

INQUIRY PROCEDURE



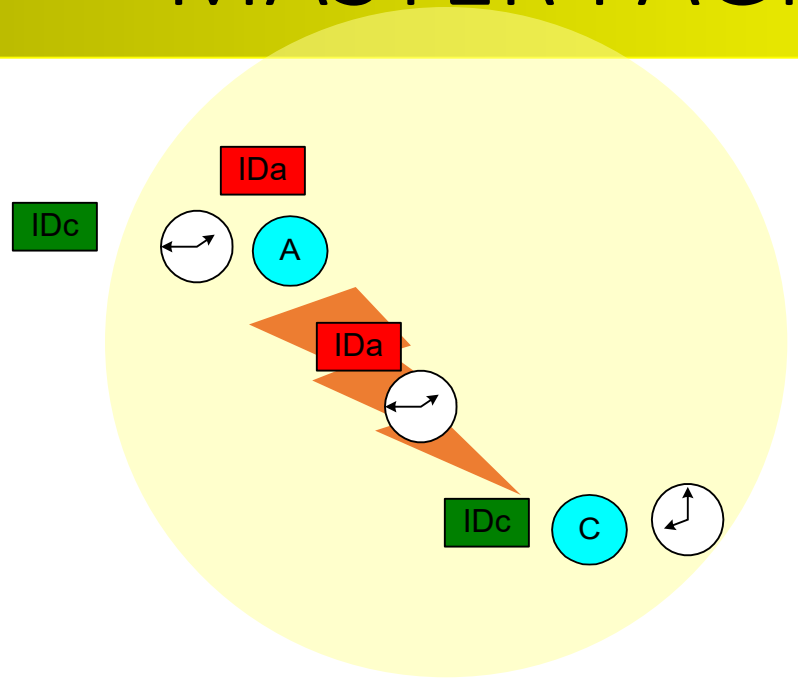
- Inquiry has unique device address (all BT radio use)
  - Unique set of “Inquiry” hop frequencies
- Any device can inquire by paging the Inquiry address
- Correlater hit causes slave to respond with FHS packet
  - ***Device ID***
  - ***Clock***

INQUIRY PROCEDURE



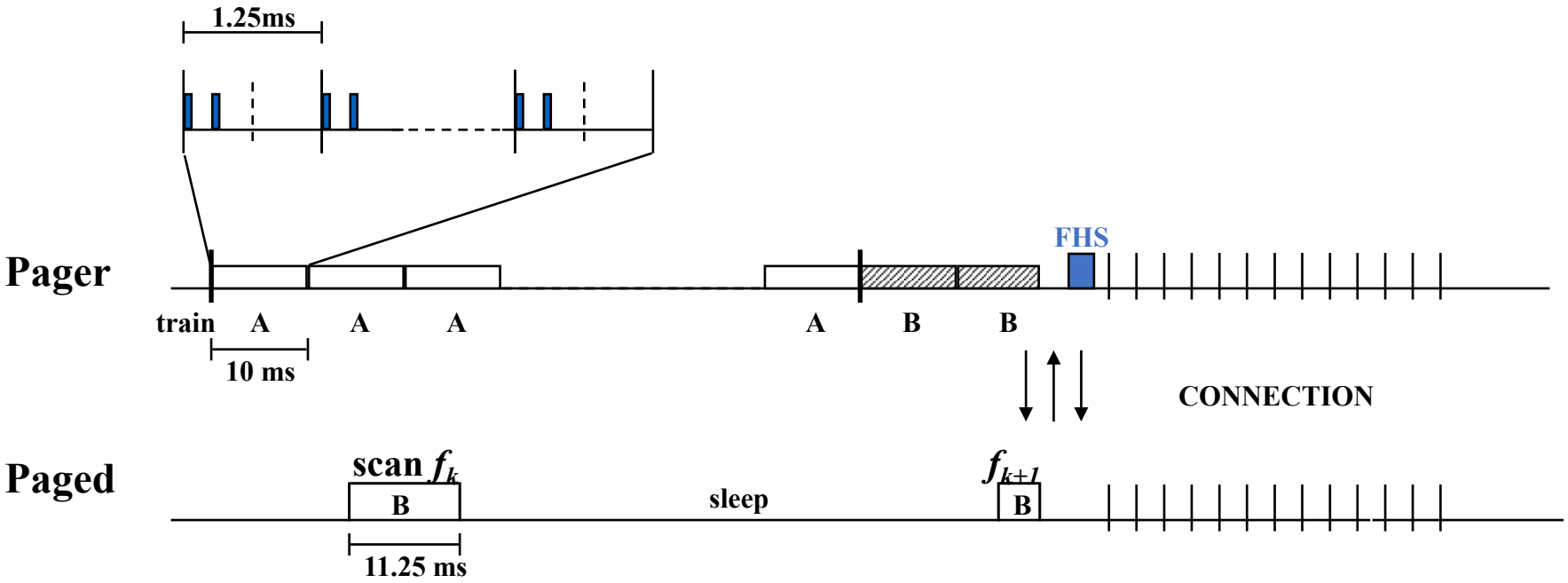
- Multiple slaves are expected to respond
  - Correlater hit causes slave to
    - respond with FHS packet
    - Wait a random number of slots
    - Wait for another Inquiry page and repeat
- Master should end up with a list of slave FHS packets in area

MASTER PAGING A SLAVE



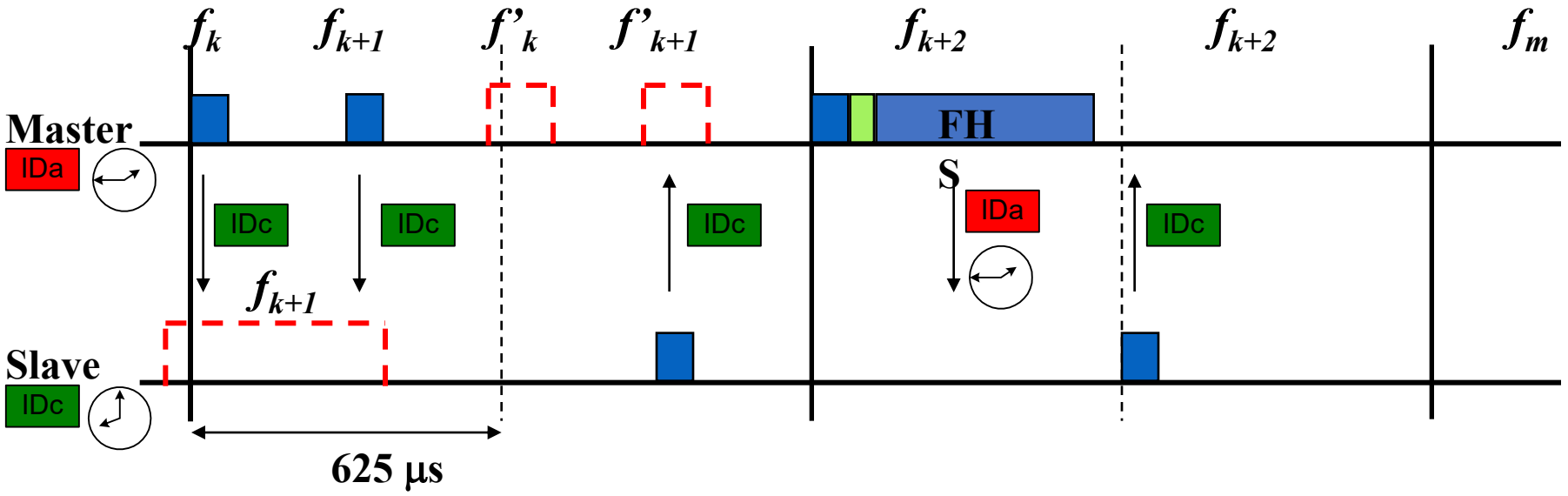
- Paging assumes master has slaves *Device ID* and an idea of its *Clock*
  - A pages C with C's ***Device ID***
  - C Replies to A with C's ***Device ID***
  - A sends C its ***Device ID*** and ***Clock*** (FHS packet)

PAGING PROCEDURE



- Each slave page scans on unique sequence of 32 channels f_k
  - Master pages 16 most likely channels for entire sleep period (nominally 1.25 seconds)
- If clocks are off, then second train sent on last 16 frequencies for entire sleep period

MASTER PAGING A SLAVE



- Master pages slave (packet has slave ID) at slave page frequency (1 of 32)
  - Master sends page train of 16 most likely frequencies in slave hop set
    - Slave ID sent twice a transmit slot on slave page frequency
    - Master listens twice at receive slot for a response
  - If misses, master sends second train on remaining 16 frequencies
- Slave listens for 11 ms (page scan)
  - If correlater triggers, slave wakes-up and relays packet at response frequency
  - Master responds with FHS packet (provides master's ***Device ID*** and ***Clock***)
  - Slave joins piconet

BLUETOOTH RADIO INTERFACE

- frequency synthesis: frequency hopping
  - 2.402 + k MHz, k=0, …, 78
  - 1,600 hops per second
- conversion bits into symbols: modulation
  - GFSK (BT = 0.5; 0.28 < h < 0.35);
  - 1 MSymbols/s
- transmit power
  - 0 dbm to 20dbm with power control
- receiver sensitivity
  - -70dBm @ 0.1% BER

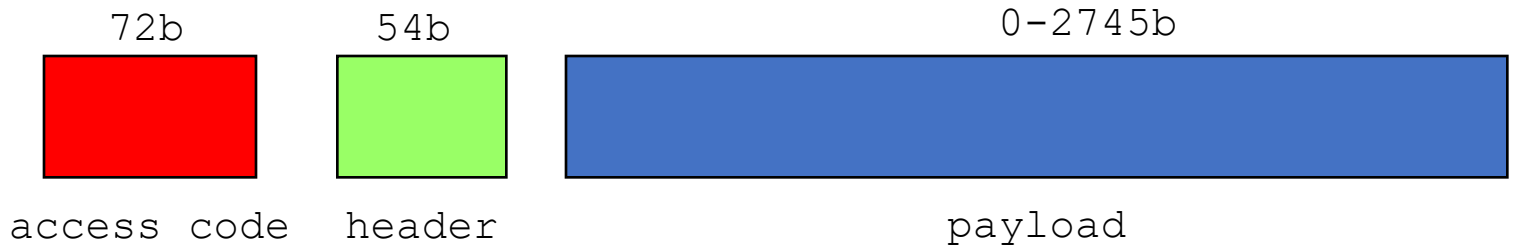
BLUETOOTH FREQUENCY HOPPING

- Spread spectrum frequency hopping radio
  - 79/23 one MHz channels
  - Hops every packet
    - Packets are 1, 3 or 5 slots long
  - Frame consists of two packets
    - Transmit followed by receive
  - Nominally hops at 1600 times a second (1 slot packets)

BASEBAND LINK TYPES

- Polling-based packet transmissions
  - 1 slot: 0.625msec (max 1600 slots/sec)
  - master/slave slots (even-/odd-numbered slots)
  - polling: master always “polls” slaves
- Synchronous connection-oriented (SCO) link
  - “circuit-switched”
    - periodic single-slot packet assignment
  - symmetric 64Kbps full-duplex
- Asynchronous connection-less (ACL) link
  - packet switching
  - asymmetric bandwidth
    - variable packet size (1-5 slots)
      - max. 721 kbps (57.6 kbps return channel)
      - 108.8 - 432.6 kbps (symmetric)

ERROR HANDLING



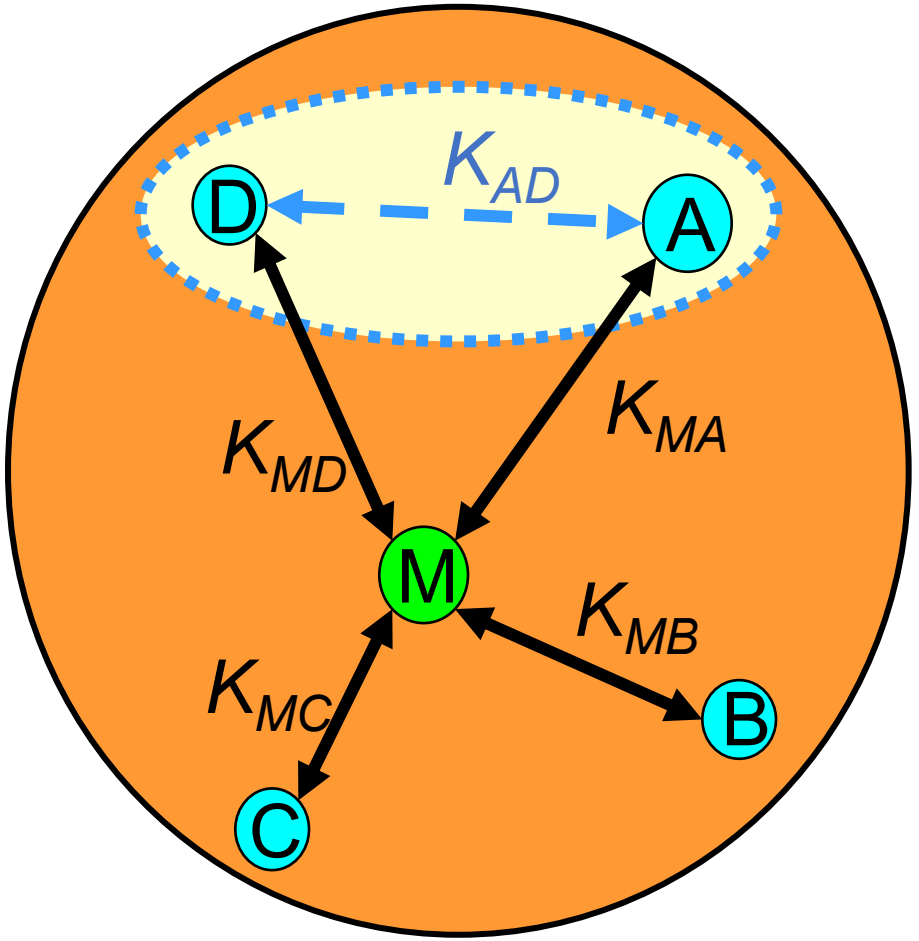
- Forward-error correction (FEC)
  - Headers are protected with 1/3 rate FEC and HEC
  - Payloads may be FEC protected
    - 1/3 rate: simple bit repetition (SCO packets only)
    - 2/3 rate: (10,15) shortened Hamming code
    - 3/3 rate: no FEC
- ARQ (ACL packets only)
  - 16-bit CRC (CRC-CCITT) & 1-bit ACK/NACK
  - 1-bit sequence number

BLUETOOTH SECURITY FEATURES / 01

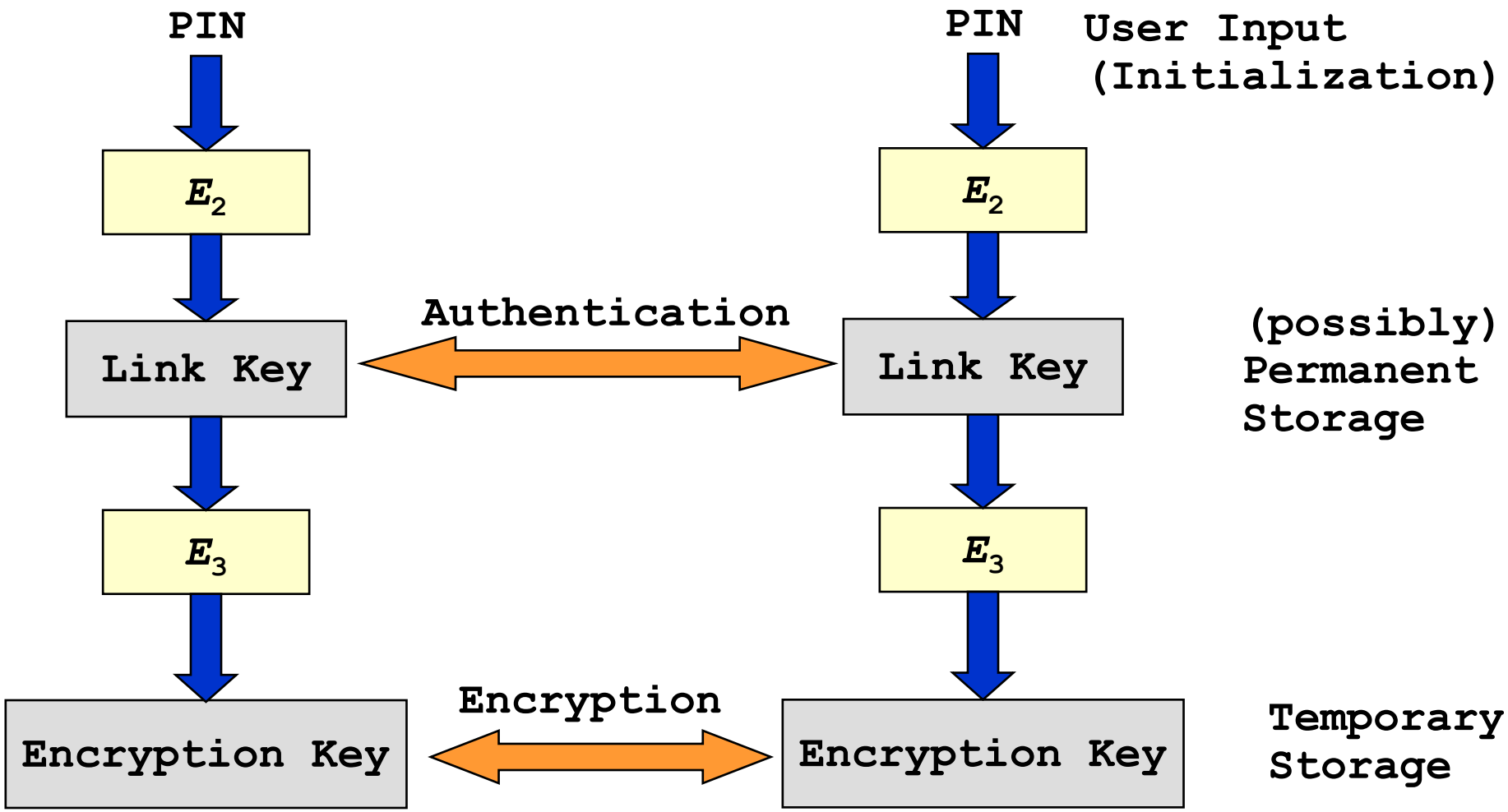
- Fast frequency hopping (79 channels)
- Low transmit power (range <= 10m)
- Authentication of remote device
  - based on link key (128 Bit)
  - May be performed in both directions
- Encryption of payload data
  - Stream cipher algorithm ($\leq$ 128 Bit)
  - Affects all traffic on a link
- Authentication/Initialization by user
  - PIN entry by user

BLUETOOTH SECURITY FEATURES / 02

- Link keys are generated via a PIN entry
- A different link key for each pair of devices is allowed
- Authentication:
  - Challenge-Response Scheme
- Permanent storage of link keys



KEY GENERATION & USAGE



APPLICATION LEVEL SECURITY

- Builds on-top of link-level security
  - creates trusted device groups
- Security levels for services
  - authorization required
  - authentication required
  - encryption required
- Different or higher security requirements could be added:
  - Personal authentication
  - Higher security level
  - Public key

BLUETOOTH POWER MANAGEMENT

- Standby current < 0.3 mA
  - 3 months(*)
- Voice mode 8-30 mA
  - 75 hours
- Data mode average 5 mA
  (0.3-30mA, 20 kbps, 25%)
  - 120 hours
- Low-power architecture
  - Programmable data length (else radio sleeps)
  - Hold and Park modes: 60 µA
    - Devices connected but not participating
    - Hold retains Active Member AMA address (AMA), Park releases AMA, gets PMA address
    - Device can participate within 2 ms

(*)Estimates calculated with 600 mAh battery and internal amplifier, power will vary with implementation

BLUETOOTH POWER CLASSES

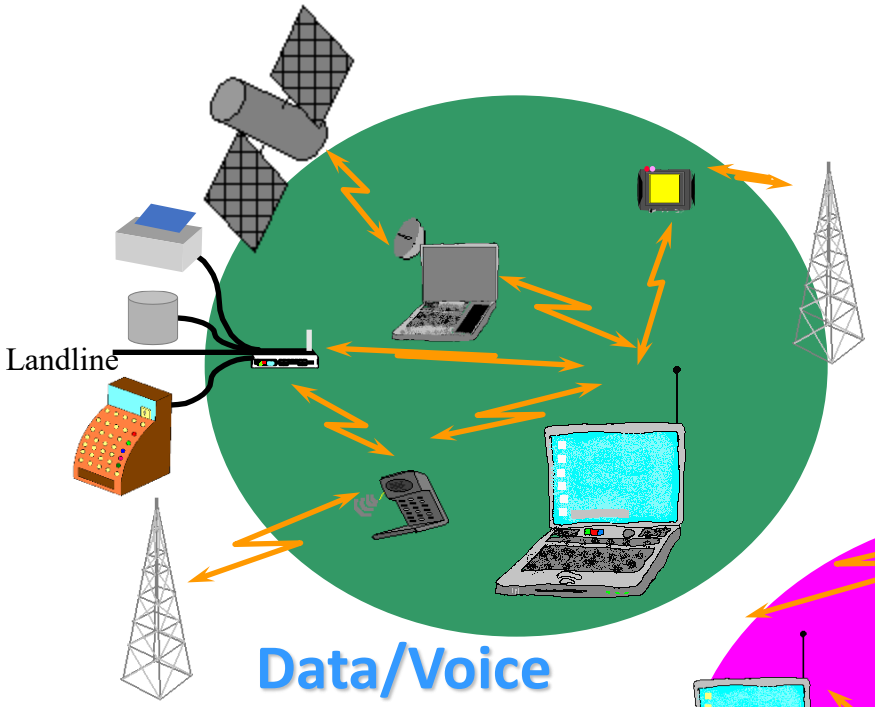
1. Different applications of Bluetooth require different power levels which also affects the range.
2. The transmit power, and by extension range, of a Bluetooth module is defined by its power class.
3. There are three defined classes of Bluetooth power:

Class Number	Max Output Power (dBm)	Max Output Power (mW)	Max Range
Class 1	20 dBm	100 mW	100 m
Class 2	4 dBm	2.5 mW	10 m
Class 3	0 dBm	1 mW	10 m

GENERAL FEATURES OF BLUETOOTH

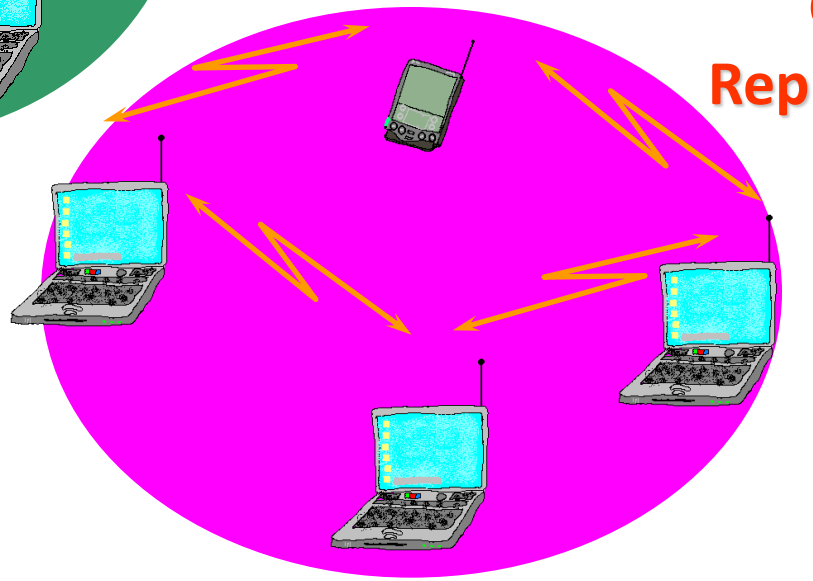
Topology	Supports up to 7 simultaneous links	Each link requires another cable
Flexibility	Goes through walls, bodies, cloths...	Line of sight or modified environment
Data rate	1 MSPS, 720 Kbps	Varies with use and cost
Power	0.1 watts active power	0.05 watts active power or higher
Size/Weight	25 mm x 13 mm x 2 mm, several grams	Size is equal to range. Typically 1-2 meters. Weight varies with length (ounces to pounds)
Cost	Long-term $5 per endpoint	~ $3-$100/meter (end user cost)
Range	10 meters or less Up to 100 meters with PA	Range equal to size. Typically 1-2 meters
Universal	Intended to work anywhere in the world	Cables vary with local customs
Security	Very, link layer security, SS radio	Secure (its a cable)

BLUETOOTH APPLICATIONS



Data/Voice
Access Points

Cable
Replacement



Personal Ad-hoc Networks