ITMC412 PAN
شبكات المنطقة الشخصية

Bluetooth - IEEE802.15.1
L4

By: Dr. Abdussalam Nuri Baryun
abaryun.teaching@gmail.com
abaryun.classhub@gmail.com

IEEE Standards for PAN

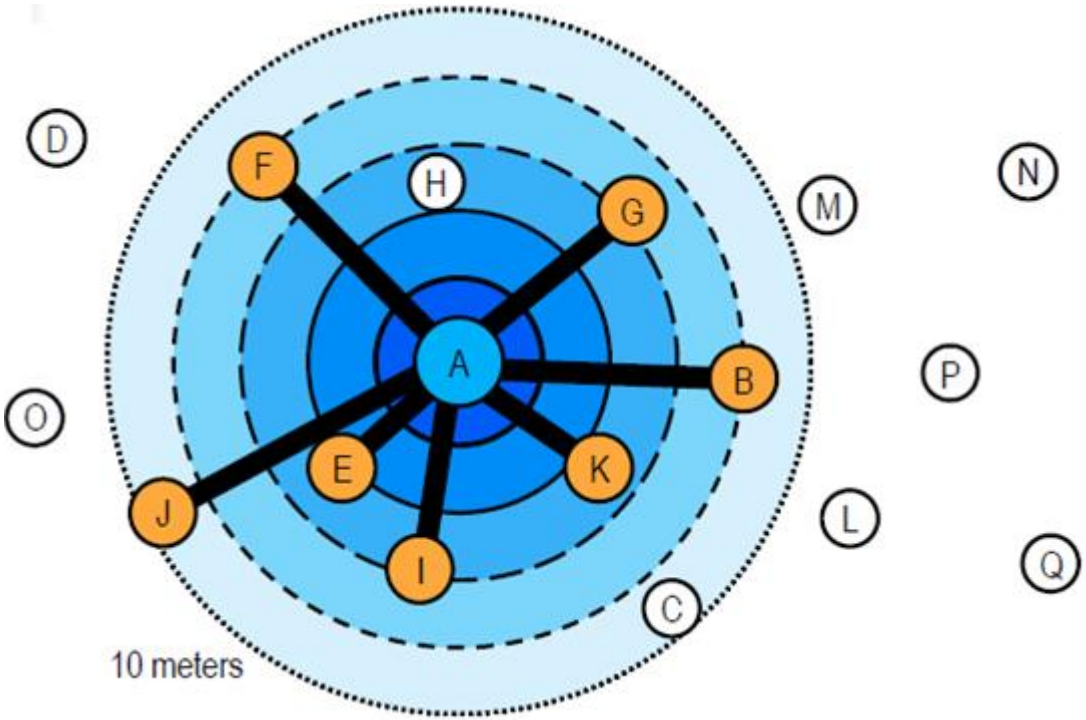
- **IEEE 802.15.1 :** Bluetooth
- **IEEE 802.15.2 :** Interoperability
- **IEEE 802.15.3 :** High data rate WPAN (WiMedia)
- **IEEE 802.15.4 :** Low data rate WPAN (ZigBee)

Bluetooth uses: the Master-Slave Scheme

- The basic piconet physical channel is defined by the master of the piconet. The master controls the traffic on the piconet physical channel by a polling scheme.
- By definition, the device that initiates a connection by paging is the master. Once a piconet has been established, master-slave roles may be exchanged.

Network Architecture: Piconets & Scatternets

- One master attached with slaves up to 7 is a piconet



Scatternet

- Bluetooth devices participate in multiple piconet, making scatternet.

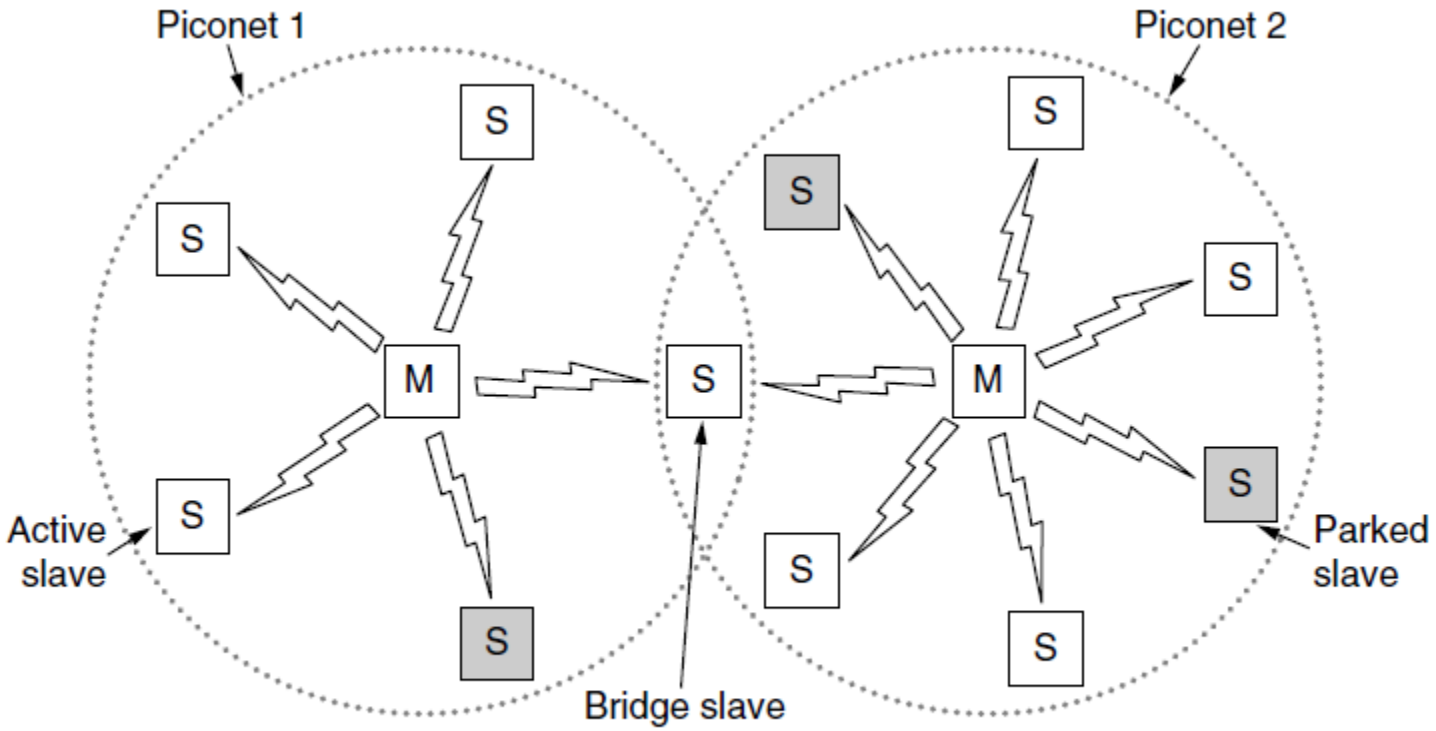
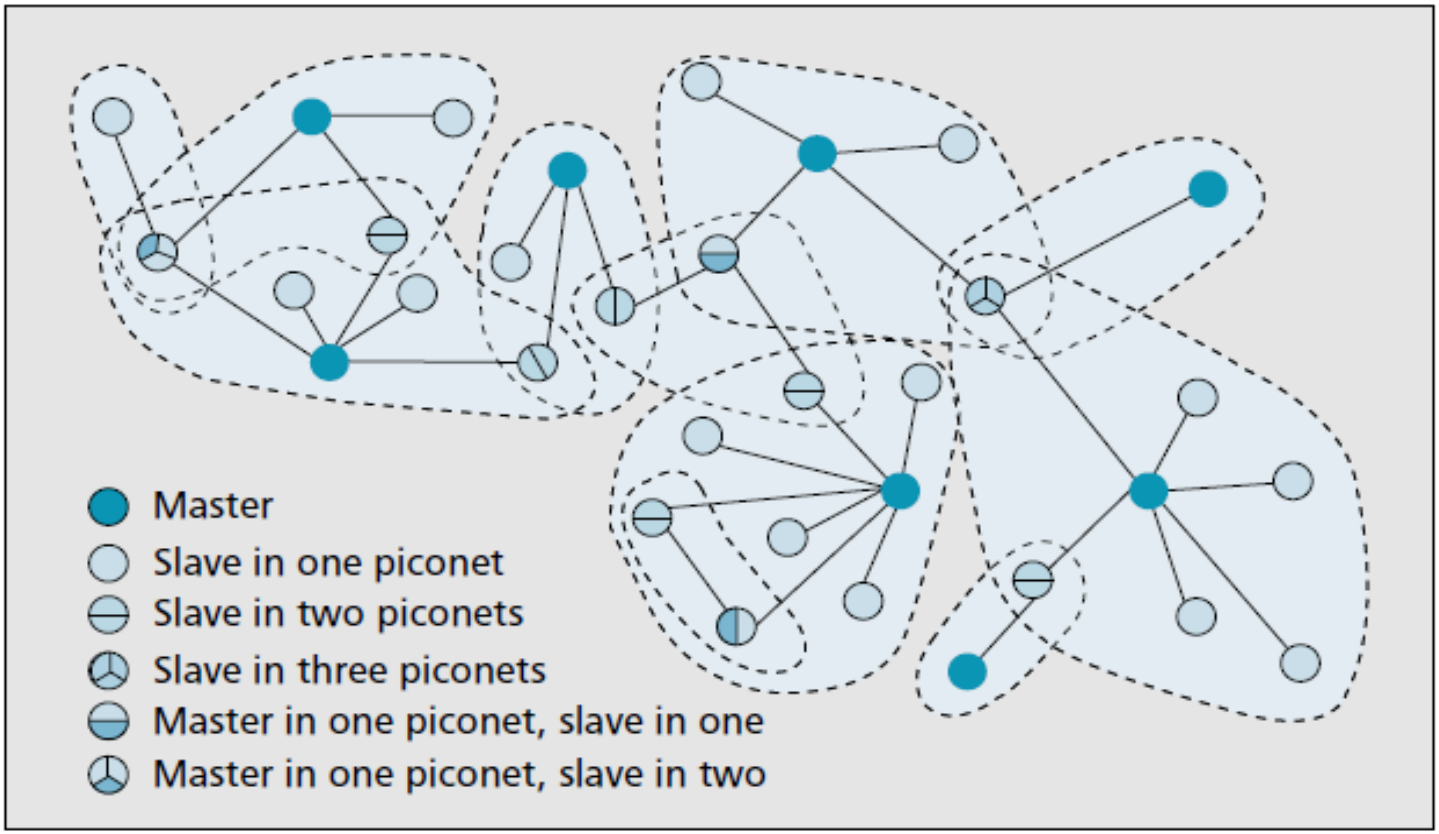


Figure 4-34. Two piconets can be connected to form a scatternet. **Reference [1]**

Scatternet

- A slave participates in max 3 piconet. A master in one piconet can participate as slave in other two piconets.



Reference [3]

Definition

- **scatternet:** Two or more piconets that include one or more devices participating in more than one piconet.
- **piconet master:** The device in a piconet whose clock and device address are used to define the piconet physical channel characteristics.
- **piconet slave:** Any device in a piconet that is not the piconet master, but is connected to the piconet master, and that controls piconet timing and access by its transmissions to slaves.

- **Bluetooth Device Address (BD_ADDR):** The address used to identify a device conforming to this standard.

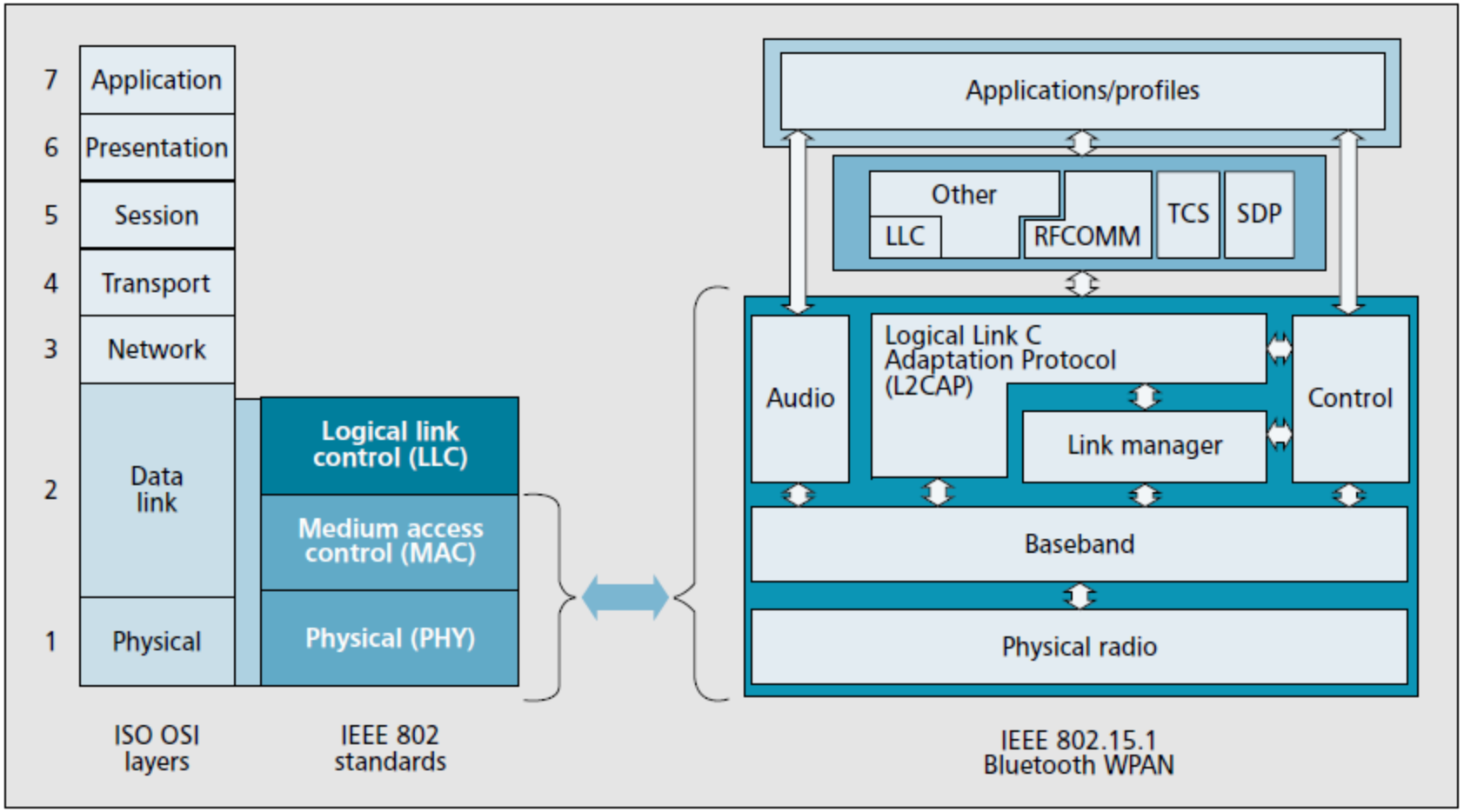
  - The device address: A 48-bit address used to identify each device.

- **coverage area:** The area where two devices can exchange messages with acceptable quality and performance.

- **personal identification number (PIN):** A user-friendly number that can be used to authenticate connections to a device before pairing has taken place.
- **participant in multiple piconets:** A device that is concurrently a member of more than one piconet. It achieves this status using time division multiplexing (TDM) to interleave its activity on each piconet physical channel.

- This standard defines physical layer (PHY) and medium access control (MAC) specifications for wireless connectivity with fixed, portable, and moving devices within or entering a personal operating space (POS).
- A POS is the space about a person or object that typically extends up to 10 m in all directions and envelops the person whether stationary or in motion.

System Architecture



Reference [3]

Core specifications: defines the layers of the Bluetooth protocol architecture:

- Radio : air interface, tx-power, modulation, FH
- Baseband : power control, addressing, timing, connections.
- Link manager protocol (LMP) : link setup & mgmt, incl. authentication, encryption, …
- Logical link control and adaptation protocol (L2CAP): adapts upper layer to baseband
- Service discovery protocol (SDP) : device info, services and characteristics.

Bluetooth Transmission vs others

- A Bluetooth device has a built-in short-range radio transmitter. The current data rate is 1 Mbps with a 2.4-GHz bandwidth. This means that there is a possibility of interference between the IEEE 802.11b wireless LANs and Bluetooth PANs.

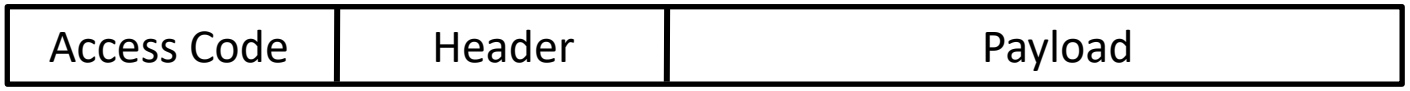
Bluetooth PAN Communications

- **All piconet communication is with the master**
- Master with up to 7 active slaves
  - Slaves only communicate with master
  - Slaves must wait for permission from master
- Master picks radio parameters
  - Channel, hopping sequence, timing, …
- Scatternets can be used to build larger networks
  - A slave in one piconet can also be part of another piconet
  - Either as a master or as a slave
  - If master, it can link the piconets

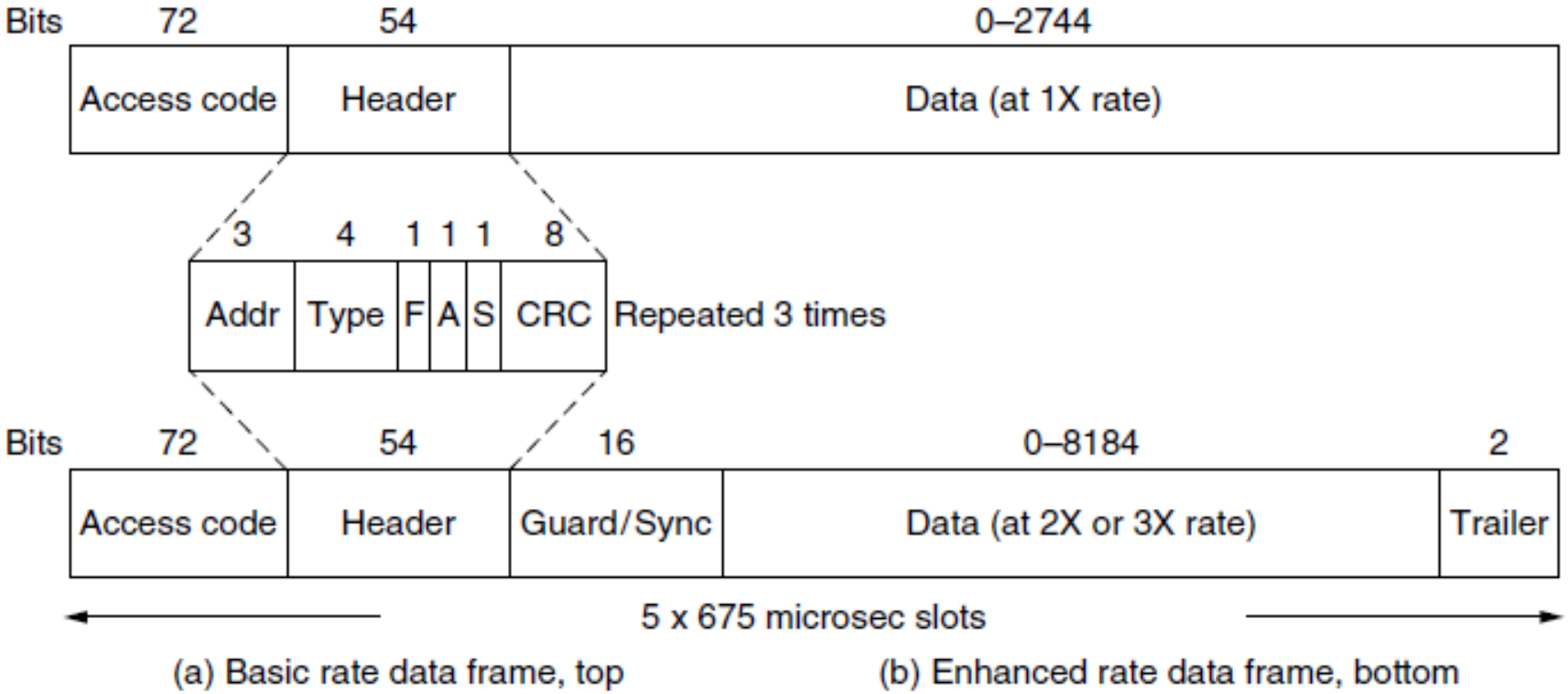
Packet General format

- The access code is 72 or 68 bits, and the header is 54 bits. The payload ranges from zero to a maximum of 2745 bits. Different packet types have been defined. Packet may consist of the following:

  — The shortened access code only
  — The access code and the packet header
  — The access code, the packet header, and the payload



Bluetooth Frames/Packets



Typical Bluetooth data frame at (a) basic and (b) enhanced, data rates.

Reference [1]

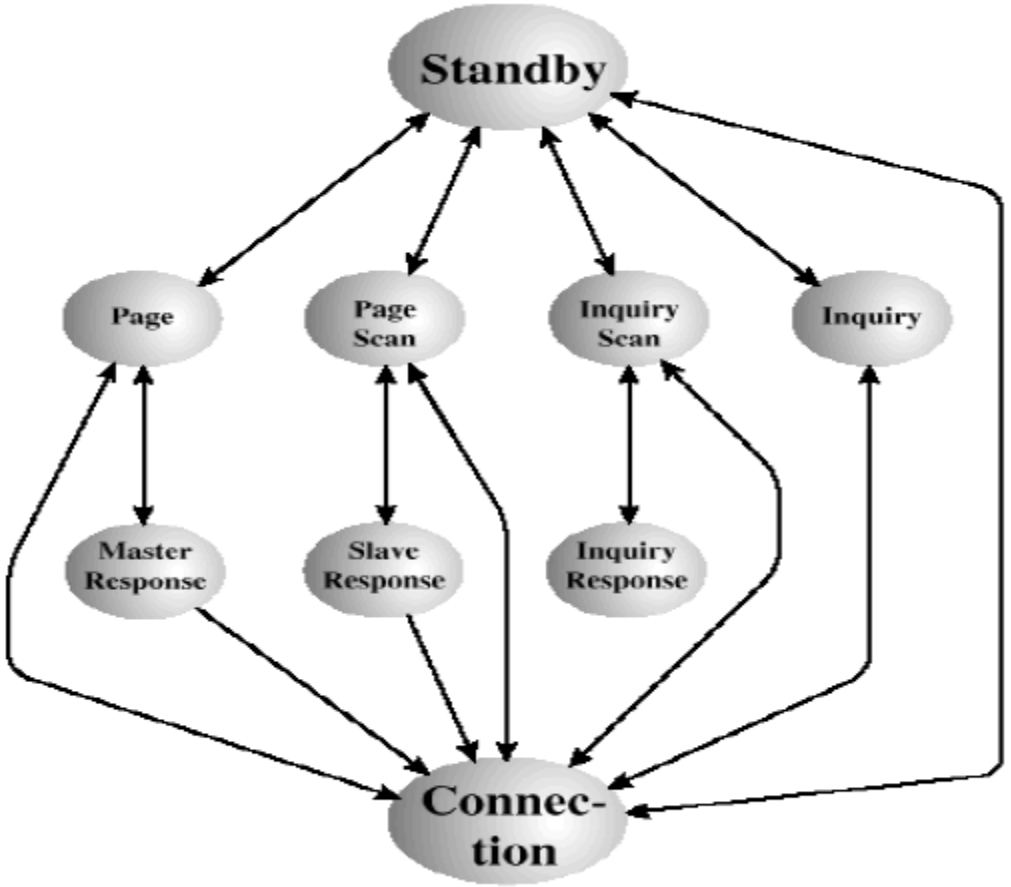
Five Common Packet types for Bluetooth

- **ID packet** (Access code only without packet header)
- **NULL packet** (has header without payload)
  - Does not need acknowledgement.
- **POLL packet** (without payload but is sent by master node only).
  - Needs acknowledgement from slave node.
- **FHS packet** (Frequency Hop Synchronization)
- **DM1 packet** (Data-Medium rate, for transport)
- There are other bluetooth packets which are

Frequency Hopping (FH)

- FH occurs by jumping from one channel to another in pseudorandom sequence. The Hopping sequence shared with all devices on piconet
- Provides resistance to interference and multipath effects.
- Provides a form of multiple access among colocated devices in different piconets
- The total bandwidth is divided into 79 physical channels each has 1MHz.

PAN Node States [2]



Joining Piconet Procedures

- Devices not connected to a piconet are in **STANDBY** mode, using low power.
- A connection is made by either 1) a **PAGE** command if the address is known or 2) by the **INQUIRY** command followed by a **PAGE.**
  - An INQUIRY is a discovery command to identify nearby radios
  - PAGE is used to connect to a known device
- When a radio sends an INQUIRE command, all the listening radios respond with their FHS packets, which tells the inquiring radio of all the radios in the area.
- All listening radios perform a page scan and/or an inquiry scan every 1.25 seconds.
- The master radio sends an FHS to the paged radio.

Inquiry Procedure

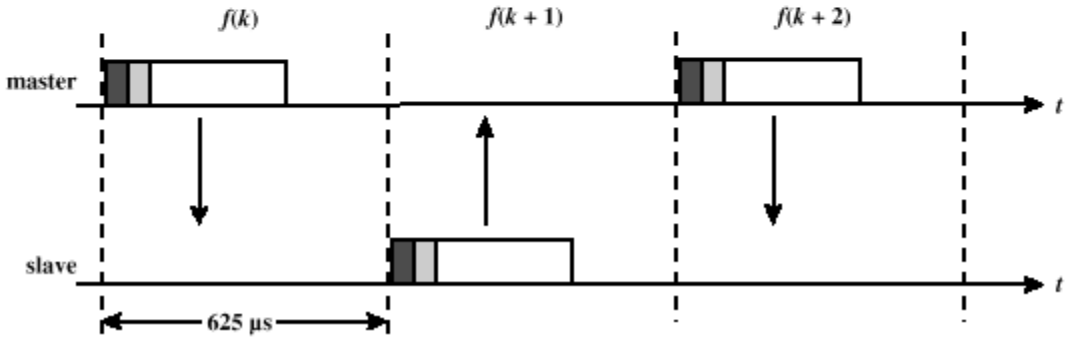
- Potential master identifies devices in range that wish to participate:
  - Transmits ID packet with inquiry access code (IAC)
  - Occurs in Inquiry state
  - On 32 wake-up carriers (out of 79)
- Device receives inquiry:
  - Enter Inquiry Response state
  - Returns FHS packet with address and timing information
  - Moves to page scan state

Page Procedure

- Master uses device address to calculate a page frequency-hopping sequence
- Master pages with ID packet and device access code (DAC) of specific slave
- Slave responds with DAC ID packet
- Master responds with its FHS packet
- Slave confirms receipt with DAC ID
- Slaves moves to Connection state

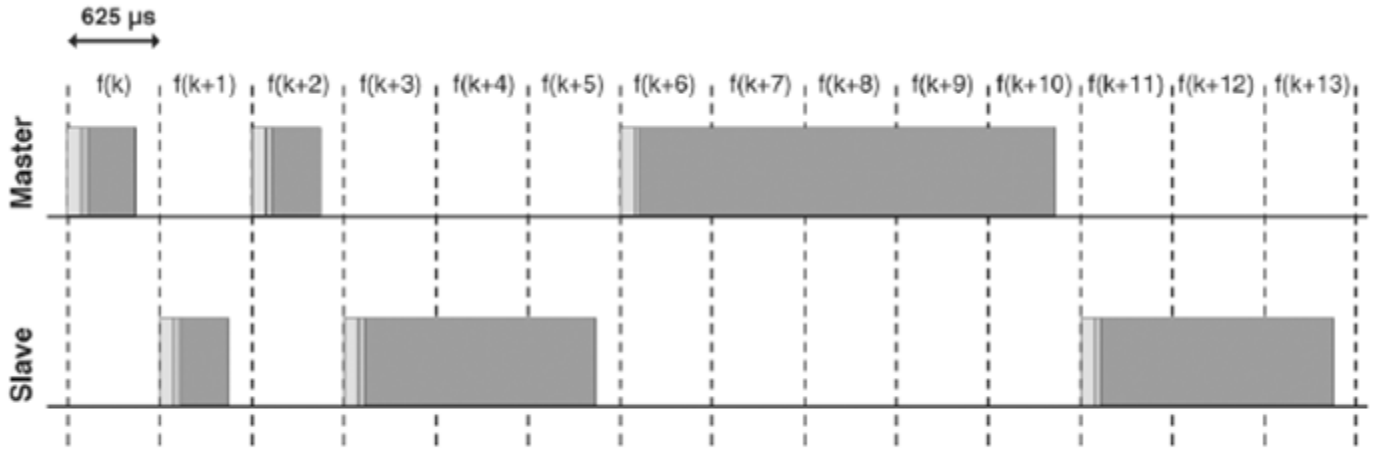
FH-TDD-TDMA [2]

- Bluetooth devices use time division duplex (TDD)
- Access technique is TDMA
- FH-TDD-TDMA

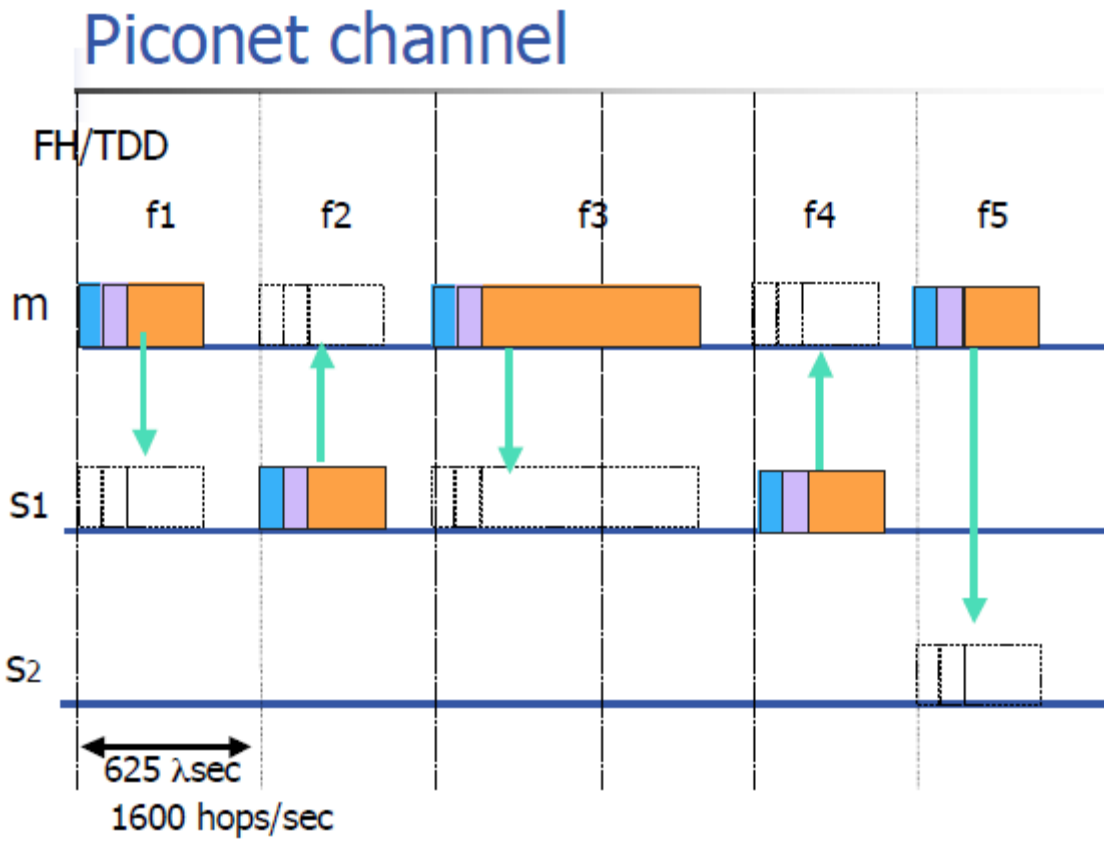


Multislot packets

- Due to packet types that cover more than a single slot, master transmission may continue in odd-numbered slots, and slave transmission may continue in even-numbered slots



Multislot packets


Piconet channel
FH/TDD
f1
f2
f3
f4
f5
m
S1
S2
625 λsec
1600 hops/sec

Reference [2]

PHY Links in Bluetooth

- **Synchronous connection oriented (SCO)**

- Allocates fixed bandwidth between point to-point connection of master and slave

- Master maintains link using reserved slots

- Master can support three simultaneous links

- **Asynchronous connectionless (ACL)**
  - Point-to-multipoint link between master and all slaves
  - Only single ACL link can exist

Packet Exchange in ACL

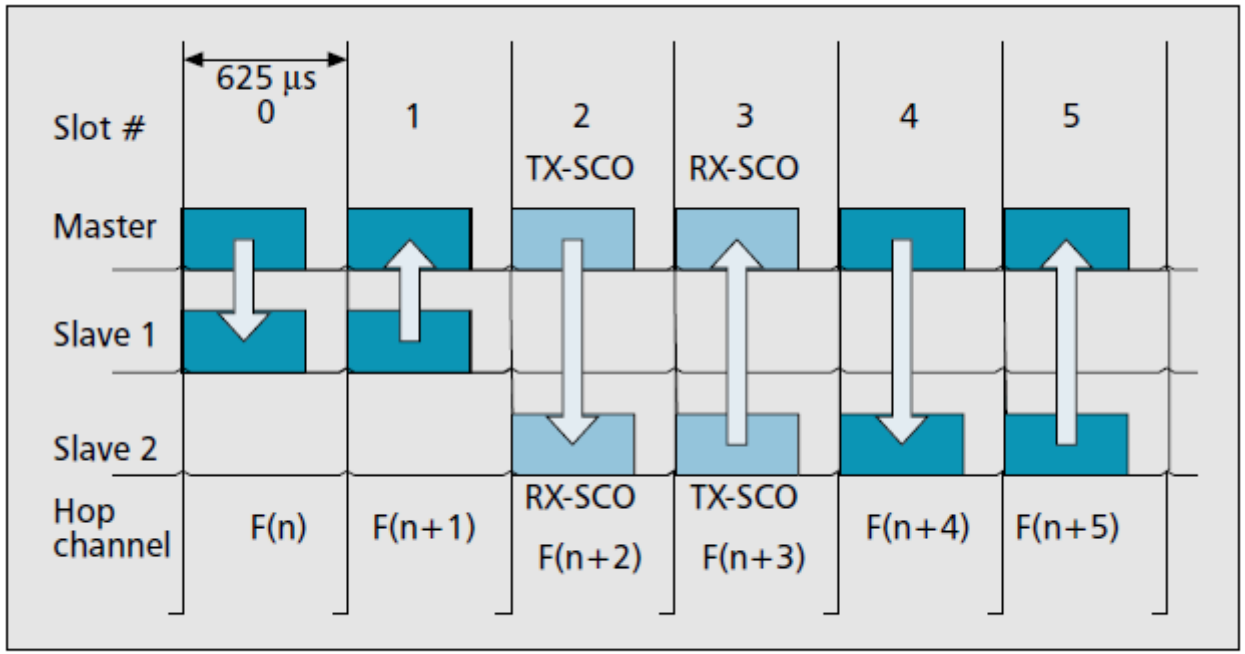
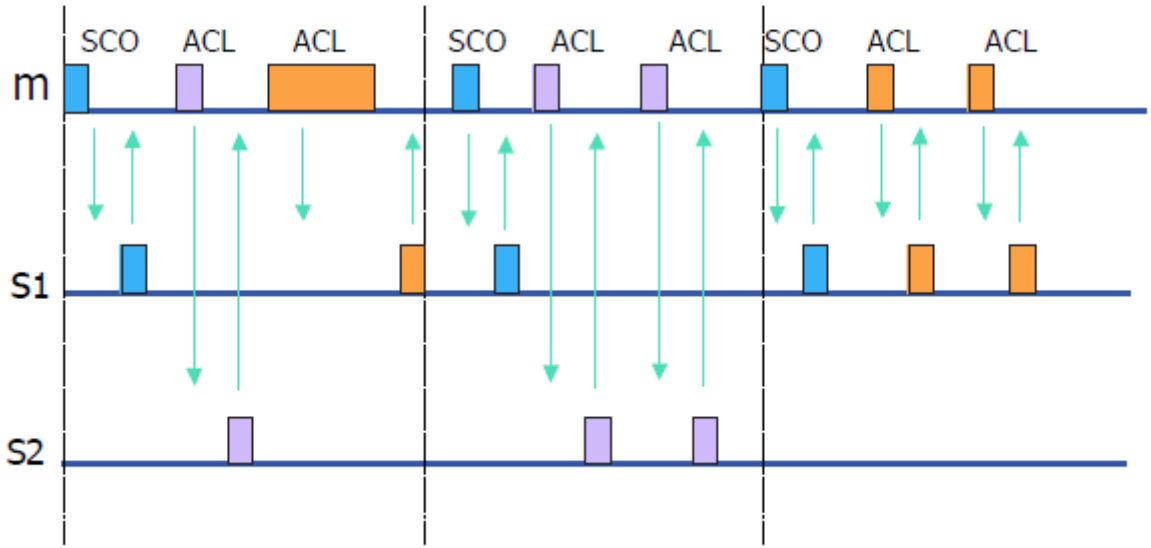


Figure 4. *An example of packet exchange: dark packets belong to ACL links.*

Reference [3]

SCO/ACL Mixed Link Example



Reference [2]

Logical Link Control and Adaptation Protocol (L2CAP)

- Provides a link-layer protocol between entities with a number of services.
- Relies on lower layer for flow and error control.
- Makes use of ACL links, does not support SCO links.
- Provides two alternative services to upper-layer protocols: Connectionless and connection-oriented services.

L2CAP Logical Channels

- **Connectionless**
  - Supports connectionless service
  - Each channel is unidirectional
  - Used from master to multiple slaves
- **Connection-oriented**
  - Supports connection-oriented service
  - Each channel is bidirectional with QoS on each direction
- **Signaling**
  - Provides for exchange of signaling
  - messages between L2CAP entities

Power Management

Two main states are defined for Bluetooth devices:

- **Standby:** No data are exchanged, only the clock is running.
- **Connection:** Each device is connected with the master of the piconet.

Four substates of connection are possible:

- Active mode: The device is active in the piconet.
- Sniff mode: This is a low-power-consumption state as the listening activity is working during sniff slots only.
- Hold mode: The ACL traffic of a device is stopped for a certain period.
- Park mode: The device is no longer a member of the piconet, but remains synchronized with the master of the piconet; this is the lowest power- consuming state.

Access Code

- In IEEE 802.15.1, all transmissions over the physical channel begin with an access code.
- Three different access codes are defined :

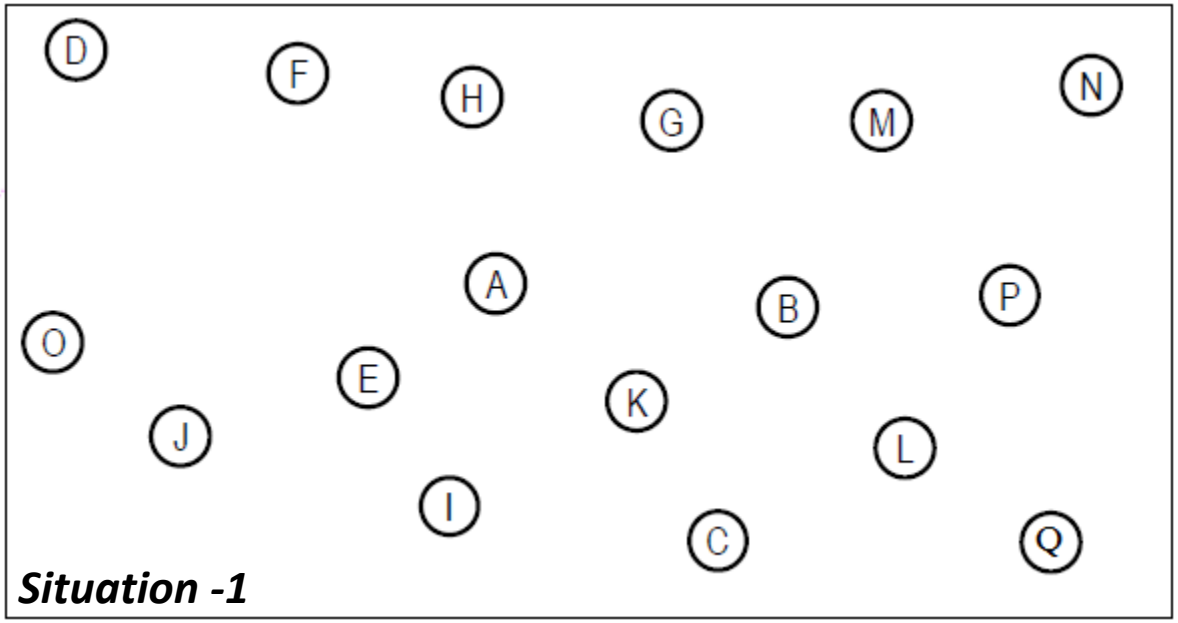
— Device access code (DAC), used during the **page scan**

— Channel access code (CAC), used in the CONNECTION state

— Inquiry access code (IAC), used in the **inquiry substate.**

Piconet Creation Scenario

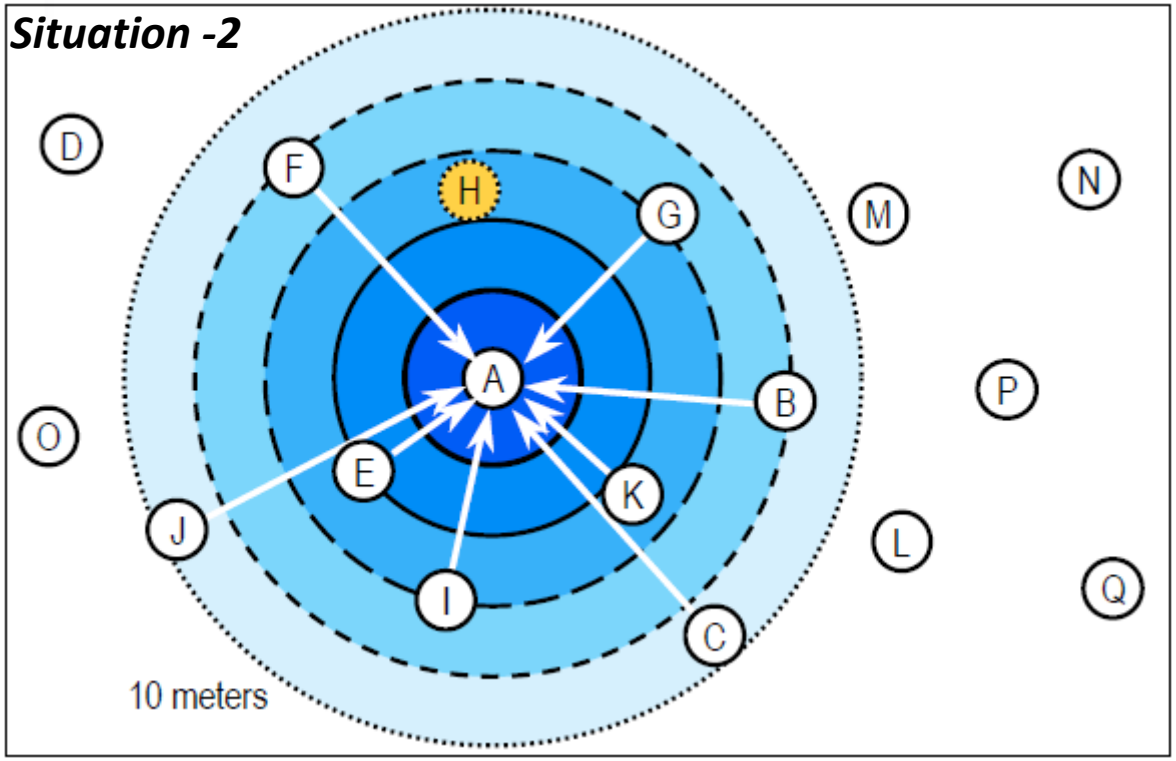
- Initially Bluetooth devices only know about themselves.
- Everyone passively monitors in Standby mode
- No devices are synchronized



Situation -1

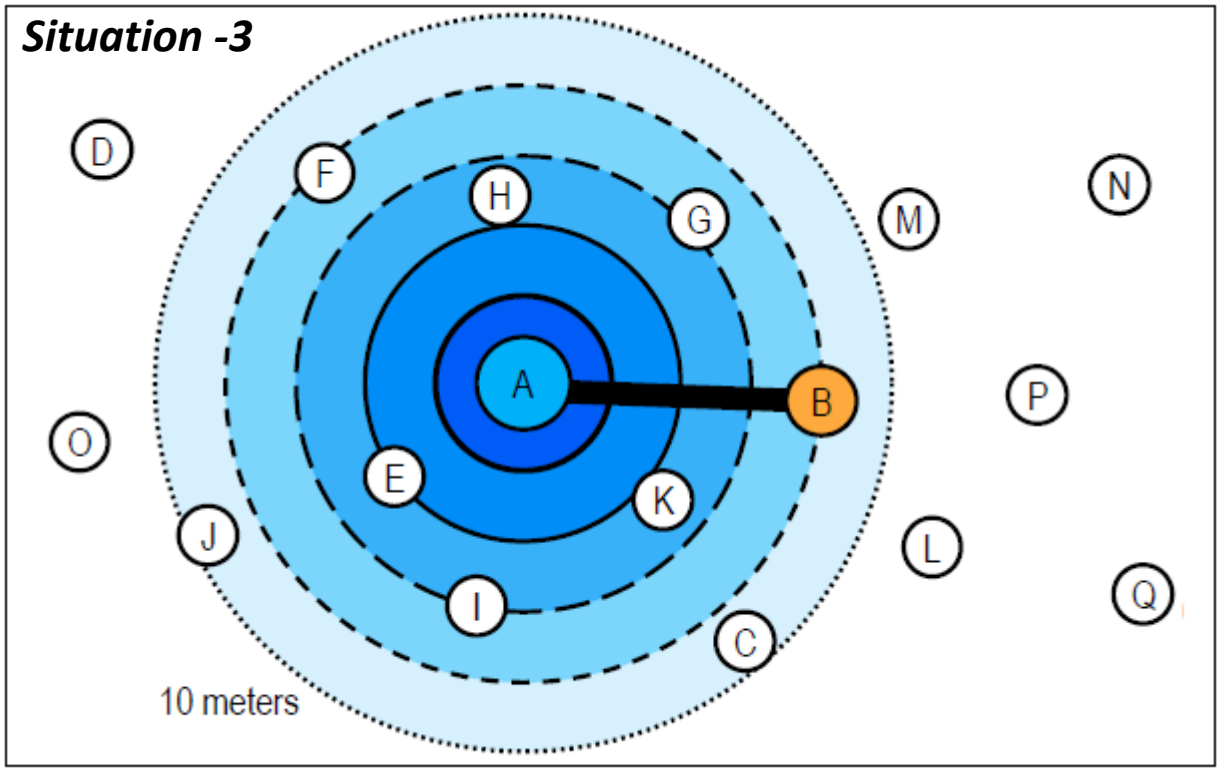
Inquiry

- Discovering other devices within range

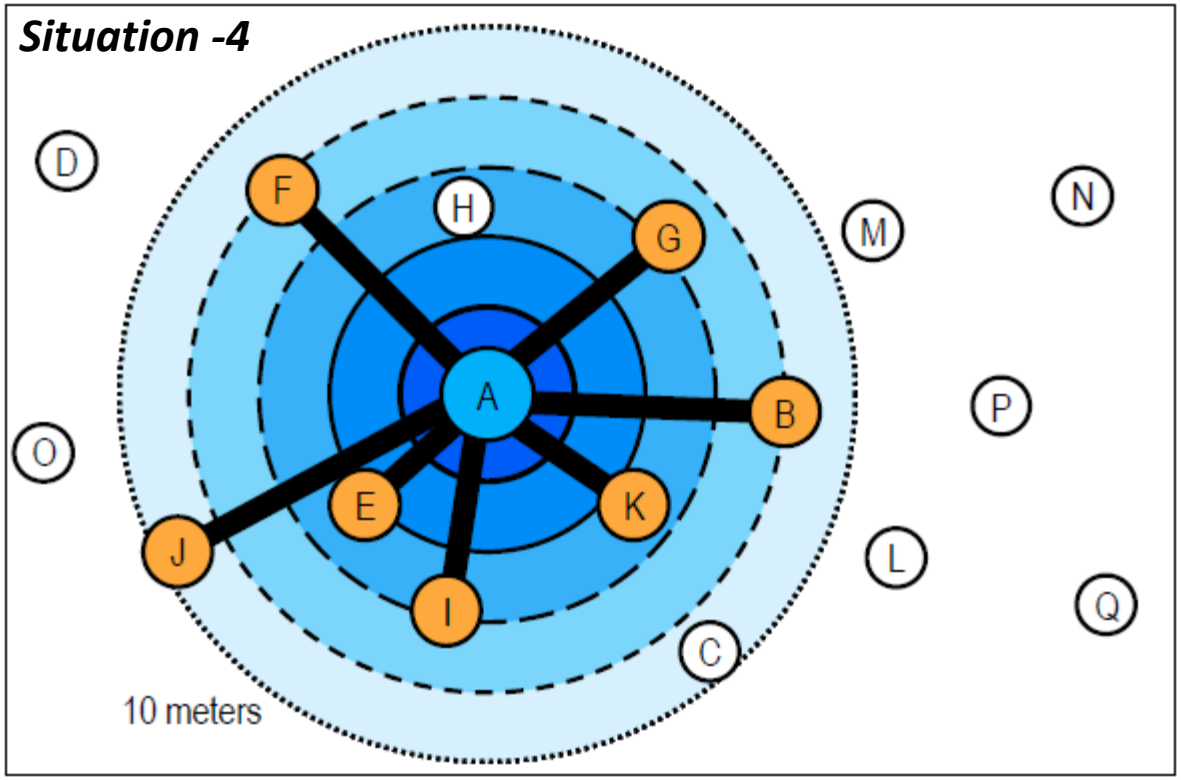


Paging

- Paging creates master and slave link called piconet

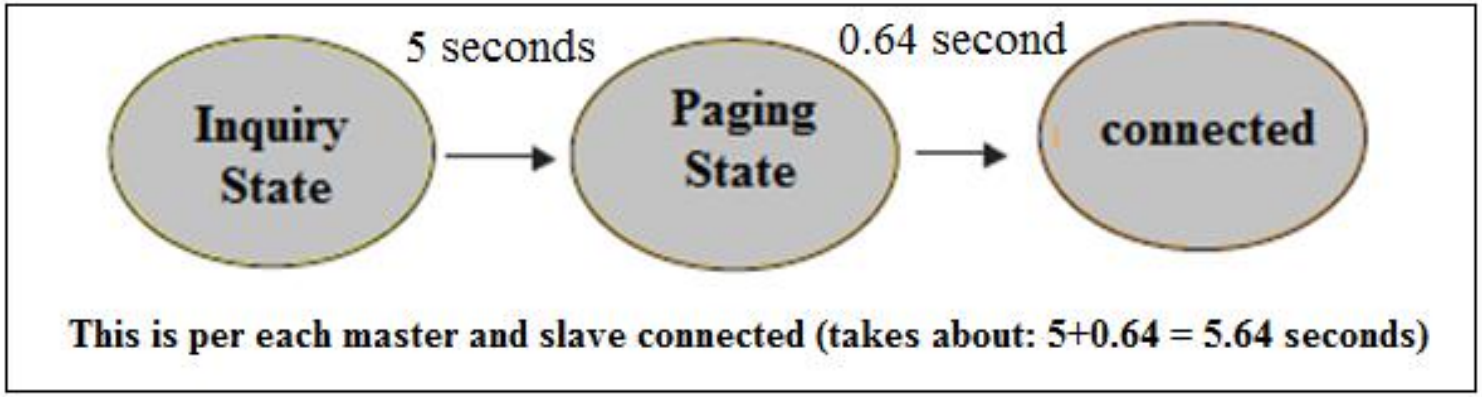


- Other paging will create more slave connections up to 7
- A = Master
- B, E, F, G,
  I, J, K = slaves
- H, C, both hear
  the master but
  they are parked.
- D, O, M, L, P, N,
  Q, are standby



Connection time per master-slave

- Inquiry phase (average time period 5 s)
  - Inquiry sent by master to get slave address.
  - No master slave connect at this phase.
- Paging phase (average time period: 0.64 s)
  - For synchronisation with slave.



Piconet Created time

In order to set up a piconet with the maximum number of active slave devices (seven), an average time of 5 s for the Inquiry phase, and 0.64 s for each Page phase (0.64 × 7 = 4.48 s) are necessary, thes requiring a maximum of 9.48 s [3].

Piconet created time= 5 + (0.64 * number_of_slaves_in_piconet)

Bluetooth Security

- Bluetooth security is divided into three modes:
  - *Mode 1:* non-secure
  - *Mode 2:* Service level enforced security (after channel establishment)
  - *Mode 3:* Link level enforced security (before channel establishment).
- Bluetooth uses a *pairing process* to establish encryption and authentication between two devices. Authentication and encryption at the link level are handled by means of four basic entities:
  - The Bluetooth device address, which is a 48-bit unique identifier assigned to each device.
  - A private authentication key (random number).
  - A private encryption key (random number).
  - A 128-bit frequently changing random number, dynamically generated by each device.
- **HW:** to read the **references** and report the security strength and weakness of the bluetooth?

References

[1] Tanenbaum, Computer Networks, 5ed.

[2] Peter Steenkiste, PAN Lecture.

[3] Ferro, et al., Bluetooth and WiFi wireless protocols: a survey and comparison, 2011.

[4] Hackmann, 802.15 PAN, scientific paper.