Mobile communications

Bluetooth

(WPAN)

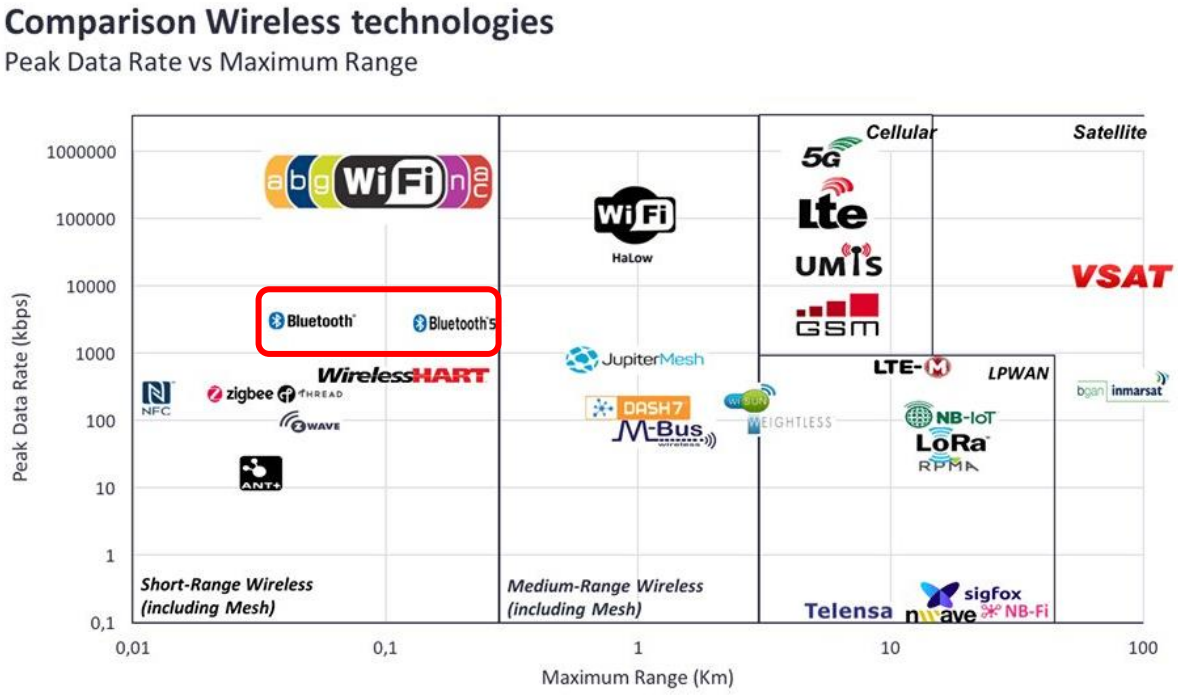
Outline

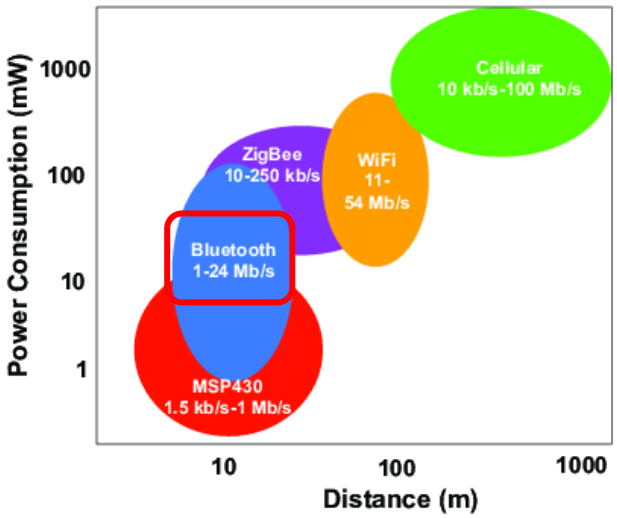
- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE

Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE

Comparison Between Wireless Technologies





Ahmed, Mobyen & Björkman, Mats & Causevic, Aida & Fotouhi, Hossein & Lindén, Maria. (2015). An Overview on the Internet of Things for Health Monitoring Systems.

Tradeoff between data rate, range and energy

Personal Area Networks

- Target deployment environment: communication of personal devices working together
  - Short-range
  - Low Power
  - Low Cost
  - Small numbers of devices

- PAN Standards
  - Bluetooth – Industry consortia (**Bluetooth SIG**)
  - IEEE 802.15.1 – ”Bluetooth” based
  - IEEE 802.15.2 – Interoperability and coexistence
  - IEEE 802.15.3 – High data rate WPAN (UWB)
  - IEEE 802.15.4 – Low data rate WPAN (Zigbee,…)
  - IEEE 802.15.5 – Mesh Networks
  - IEEE 802.15.6 – Body Area Network
  - IEEE 802.15.7 – Visible Light Communication

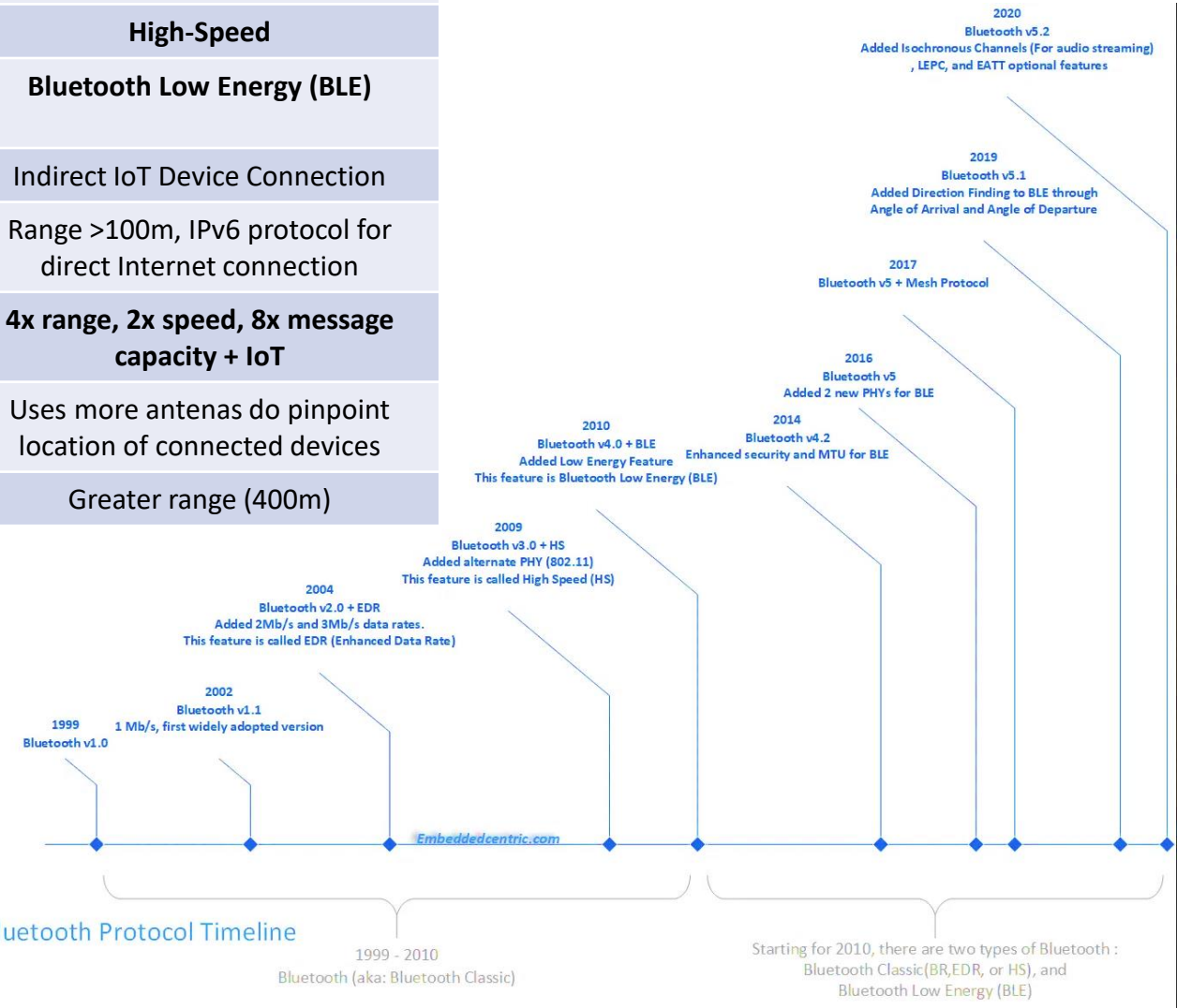
Bluetooth

- Created by Ericsson (1994)
- Maintained by the Bluetooth SIG (https://www.bluetooth.com/)
- Originally for replacing “USB”, not “Ethernet”
  - Cable replacement technology
  - Later also used as Internet connection, phone or headset
- PAN - *Personal Area Network*
  - Started with 1 Mbps connections
  - Includes synchronous, asynchronous, voice connections
  - Piconet routing
- Small, low-power, short-range, cheap, versatile radios (3 classes)
- Master/slave configuration and scheduling

Bluetooth Versions

Version	Data rate	Feature
1.1	1 Mbps	First widely adopted version
2.0 + EDR	**3 Mbps**	**Enhanced Data Rate (EDR)**
3.0 + HS	**24 Mbps**	**High-Speed**
4.0	24 Mbps/ **1 Mbps** (BLE)	**Bluetooth Low Energy (BLE)**
4.1	25 Mbps	Indirect IoT Device Connection
4.2	25 Mbps	Range >100m, IPv6 protocol for direct Internet connection
5.0	**50 Mbps**	**4x range, 2x speed, 8x message capacity + IoT**
5.1	50 Mbps	Uses more antenas do pinpoint location of connected devices
5.2	50 Mbps	Greater range (400m)

Now in 5.4, with some additional improvements



WLAN vs. Bluetooth

	Bluetooth	WLAN / WiFi
Specifications authority	Bluetooth SIG	IEEE, WiFi Alliance
Year of development	1994	1991
Bandwidth	Low (50 Mbps)	Very High (2 Gbps 802.11ax)
Hardware requirement	Bluetooth adaptor on all the devices connecting with each other	Wireless adaptors on all the devices of the network, a wireless router and/or wireless access points
Cost	Low	High
Power Consumption	Low	High
Frequency	2.4 GHz	2.4/5 GHz
Security	It is less secure	It is more secure
Range	10 meters	100 meters
Primary Devices	Mobile phones, mouse, keyboards, office and industrial automation devices	Notebook computers, desktop computers, servers
Ease of Use	Fairly simple to use. Can be used to connect up to 7 devices at a time. It is easy to switch between devices or find and connect to any device.	It is more complex and requires configuration of hardware and software

Bluetooth features (I)

- Radio network, on the **2.4 GHz**, world-wide
  - **ISM (**Industrial, Scientific and Medical**)**; Unlicensed but regulated
- FH (**Frequency Hopping**) **Spread Spectrum**:
  - **79** channels of 1 Mhz in the 2.402 GHz to 2.480 GHz range
- Defines a **Master**
  - Synchronizes everyone to his hop-pattern
- **TDD** (Time Division Duplex)
  - Data is transmitted in one direction at a time with transmission alternating between two directions (**Master transmits in even** timeslots and **receives in odd ones**)

Bluetooth features (II)

- Defines two types of networks:
  - **Piconets** (has 1 Master)
  - **Scatternets** (joining multiple piconets via common Master or Slaves)

- Maximum **8 active devices** per piconet
  - 1 Master + 7 Slaves

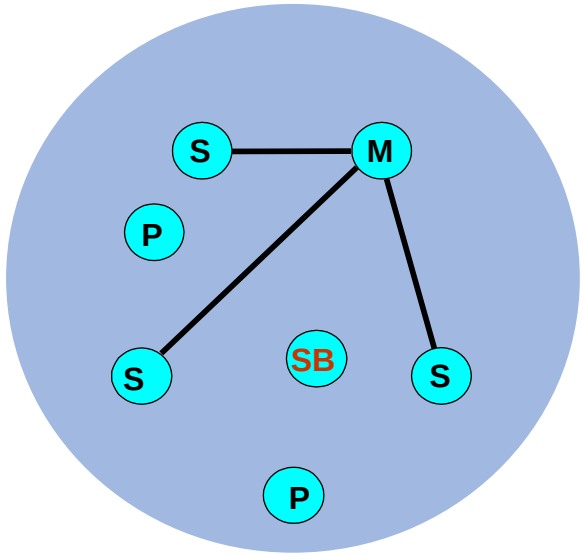
- Two main types of connections
  - **SCO** (Synchronous Connection Oriented), voice link
    - FEC (forward error correction), no retransmission
    - Connection explicitly set up prior to transmitting
  - **ACL** (Asynchronous Connection Less), data link
    - Asynchronous, packets must be acknowledged

Frequency Hopping Spread Spectrum (FHSS)

- Signal broadcast over pseudo random series of frequencies
- Receiver hops between frequencies in sync with transmitter (1600 hops per second, every 625uS)
- Spreading code determines the hopping sequence
  - Must be shared by sender and receiver (e.g. standardized)
- Eavesdroppers hear unintelligible blips
- Jamming on one frequency affects only a few bits

Piconets (I)

- Bluetooth devices connected in an “ad-hoc” cell
- There is a Master with up to 7 active Slaves and several hundreds parked
  - Slaves only communicate with master
  - Slaves must wait for permission from master
  - Communication can be 1-to-1 to 1-to-many
  - No direct communication between slaves
- Each station (Master or Slave), has a 48-bit fixed device address

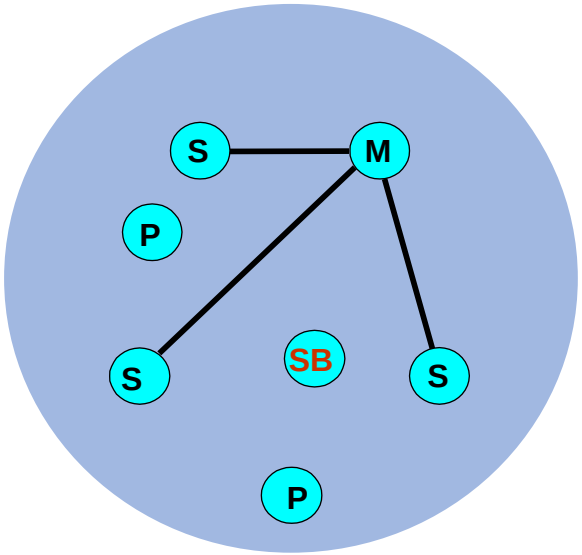


M = Master
S = Slave

P = Parked
SB = Standby

Piconets (II)

- Master defines radio parameters (”clock” and “deviceID”)
  - Channel, hopping sequence, timing, …
- Each Piconet has a unique FH pattern (and a single ID)
- Each piconet has a maximum bandwidth
- A node in one **Piconet** can also be part of another Piconet, either as a Master or as a Slave, creating a **Scatternet**



M = Master
S = Slave

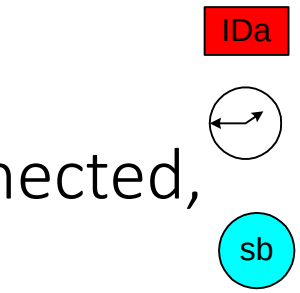
P = Parked
SB = Standby

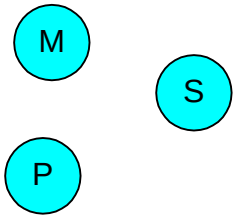
Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE

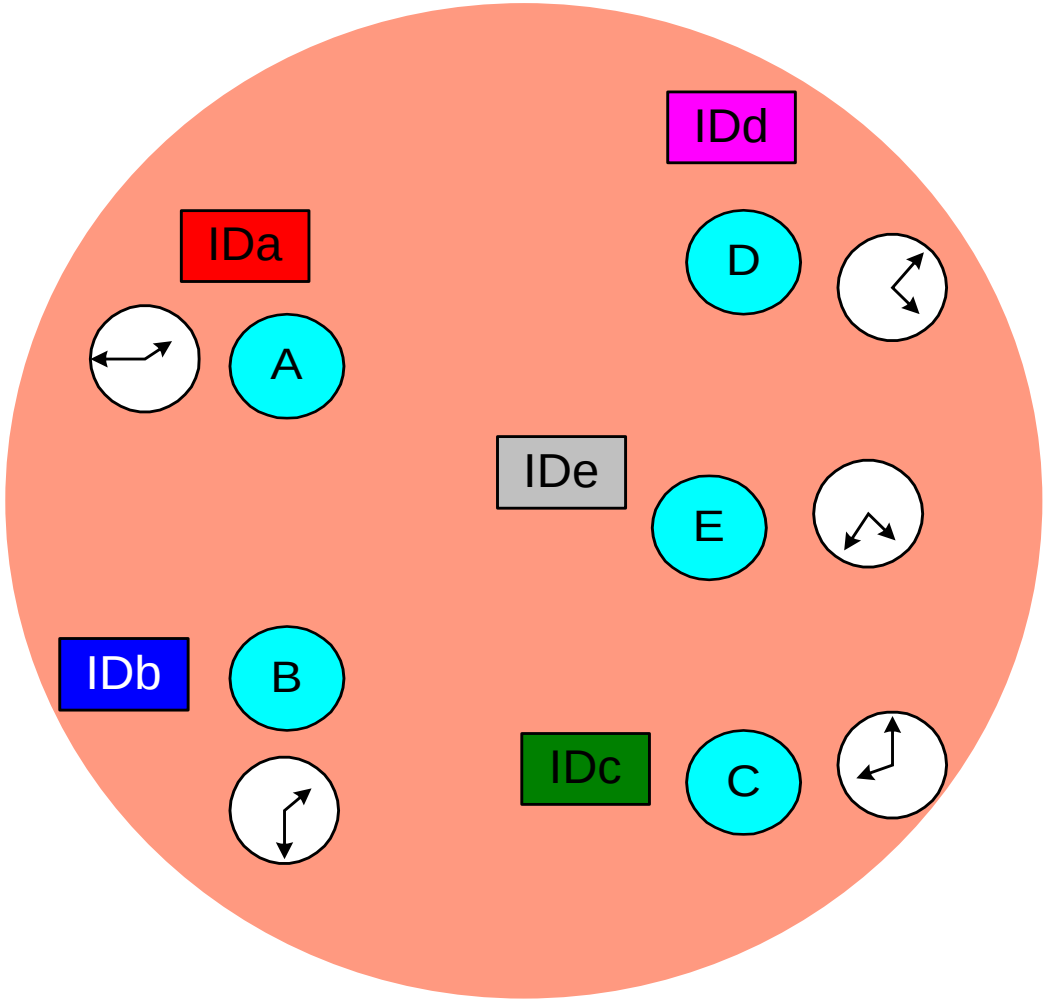
Piconet operation

- FHSS: all devices must share the same hopping pattern:
  - M*aster* provides clock and deviceID such that:
    - The unique deviceID (48-bits) defines hopping pattern
    - Clock defines phase inside the pattern
- If a device is inside a piconet, and is not connected, it must be in *standby*
- There are two types of piconet addresses
  - *Active Member Address* (AMA, 3-bits, 7 addresses)
  - *Parked Member Address* (PMA, 8-bits, 255 addresses)

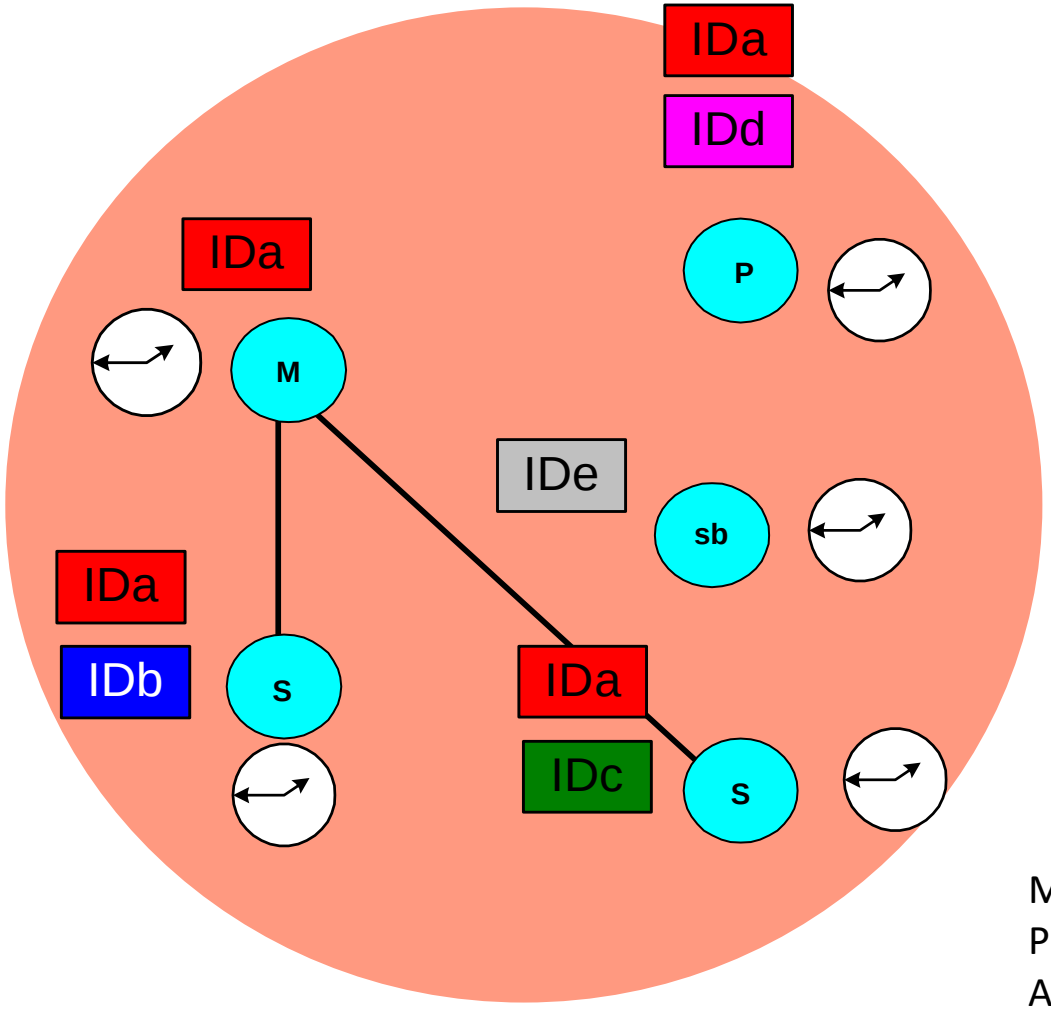




Piconet before setup



Piconet in operation

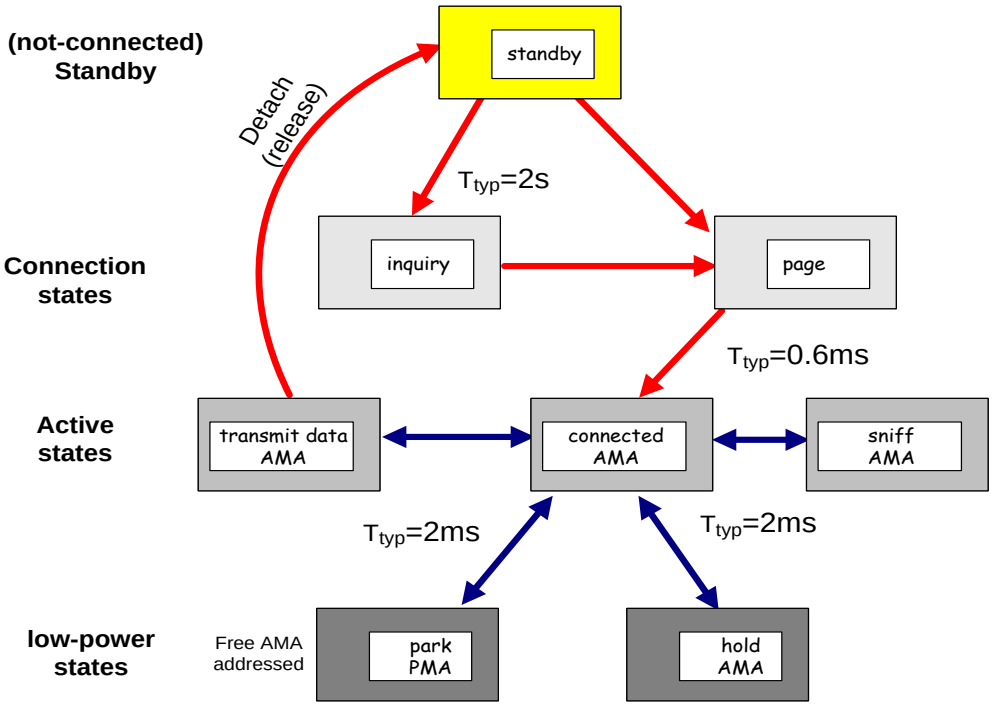


Piconet built!

Master know all slaves
Piconet ID shared
All in sync

Device states

- Standby
  - Do nothing; waiting to join a piconet
- Inquire
  - Search for other devices (discover nodes)
- Page
  - Connect to a specific device
- Connected
  - Active on a piconet (Master or Slave)
- Park/Sniff/Hold
  - Low Power connected states



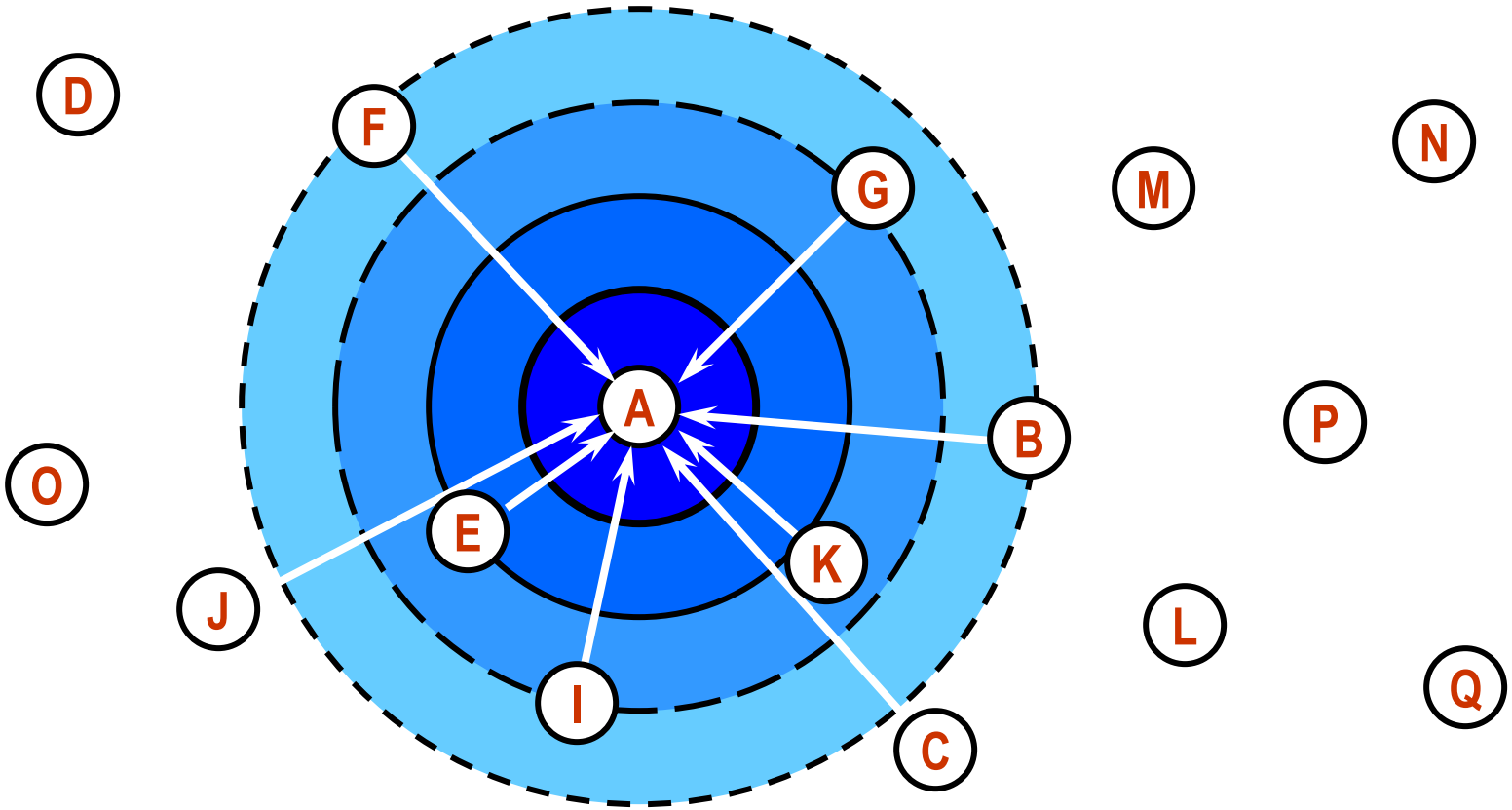
Park: release AMA, get PMA
Sniff: listen periodically, not each slot
Hold: stop ACL, SCO still possible, possibly participate in another piconet

AMA: Active Member Address
PMA: Park Member Address

Low-Power Operation in BT classic

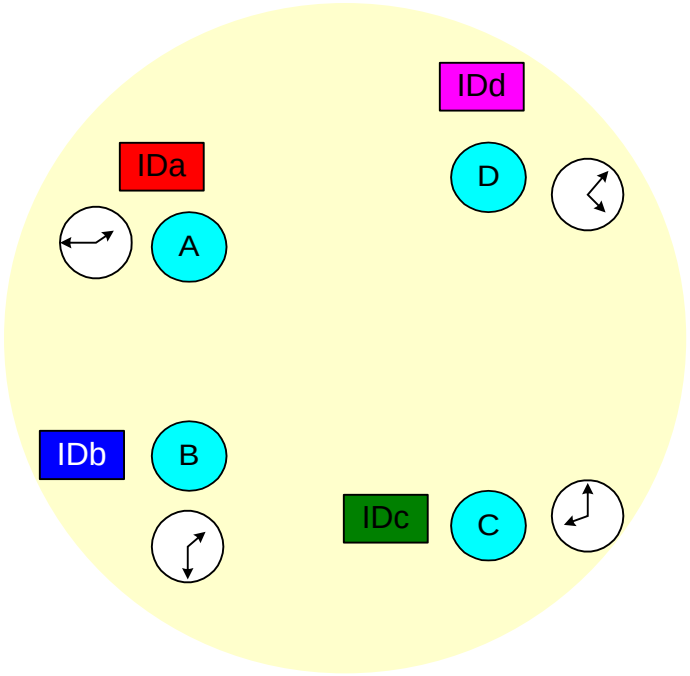
- 3 modes (Slaves):
  1. Sniff
     - Low-duty cycle mode
     - Wakes up periodically to talk to master
     - Fixed “sniff” intervals
  2. Park:
     - Very low power state
     - Used to admit more than 7 slaves in piconet
       - Slave gives up its Active Member Address (AMA)
       - Receives “Parked” Member Address (PMA)
     - Wakes up periodically listening for broadcasts which can be used to “unpark” node
  3. Hold
     - Node sleeps for specified interval
     - Master can put slaves in hold while searching for new members, attending another piconet, etc.
     - No ACL packets (*Asynchronous Connection-Less*) → general data packets
       - But SCO (*Synchronous Connection Oriented*) possible → Audio

Device Discovery Illustrated



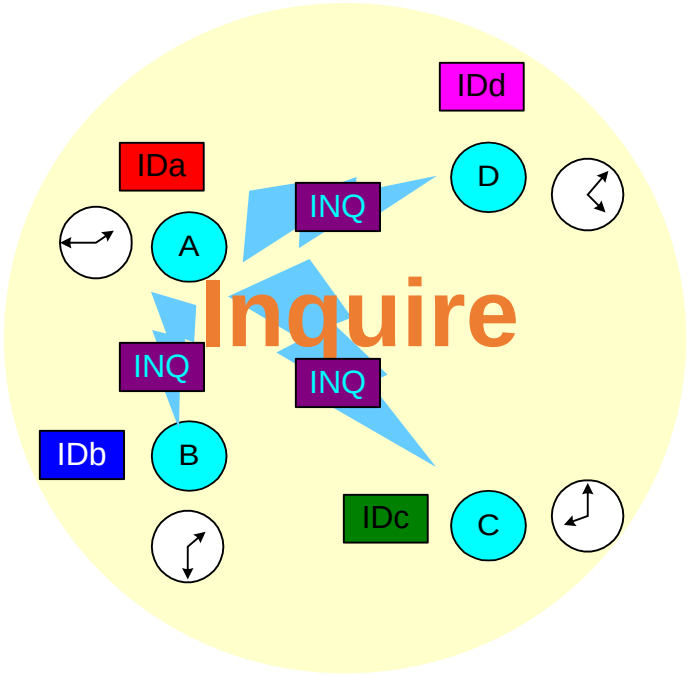
After inquiry procedure, A knows about others within range

Scanning units



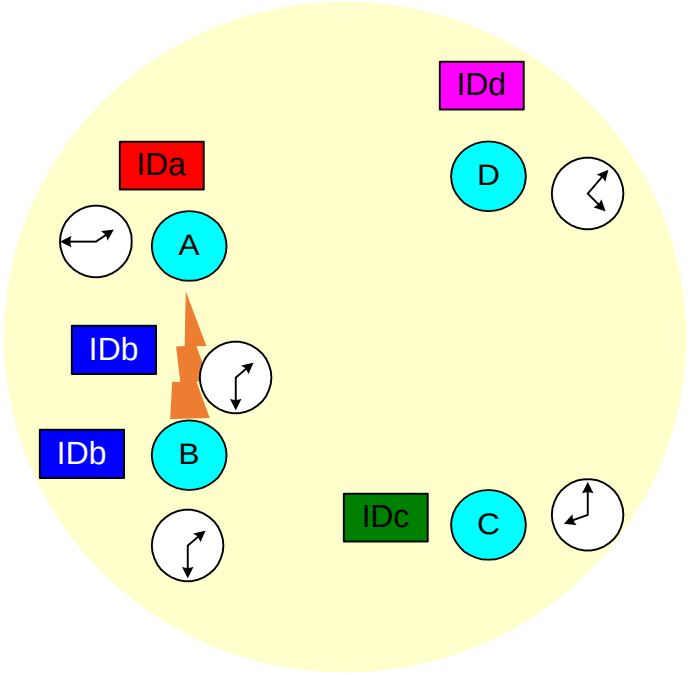
- Device A wants to search for stations

Scanning units



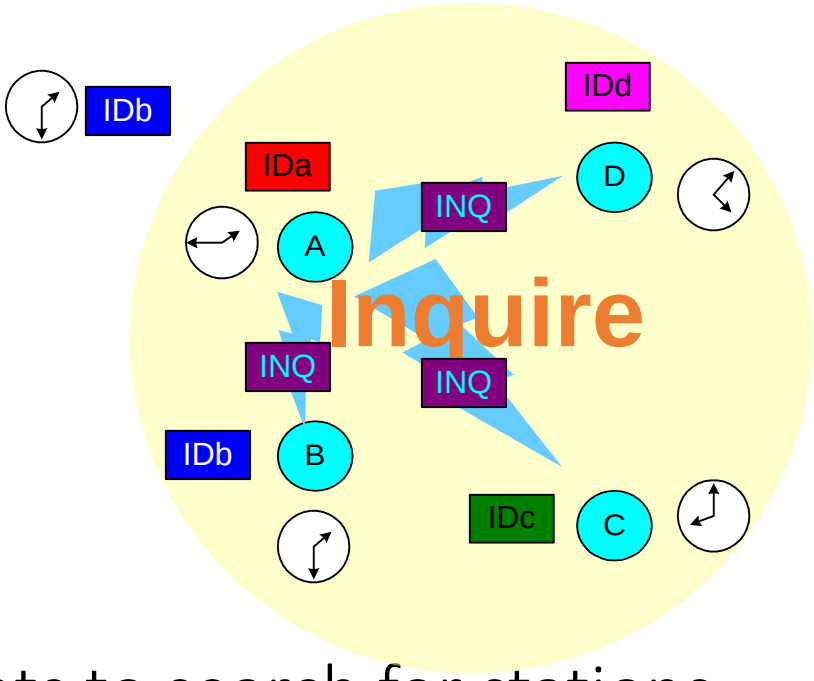
- Device A wants to search for stations
- A does an inquire (page with ID 000)
  - Devices B,C,D are doing an inquire scan

Scanning units



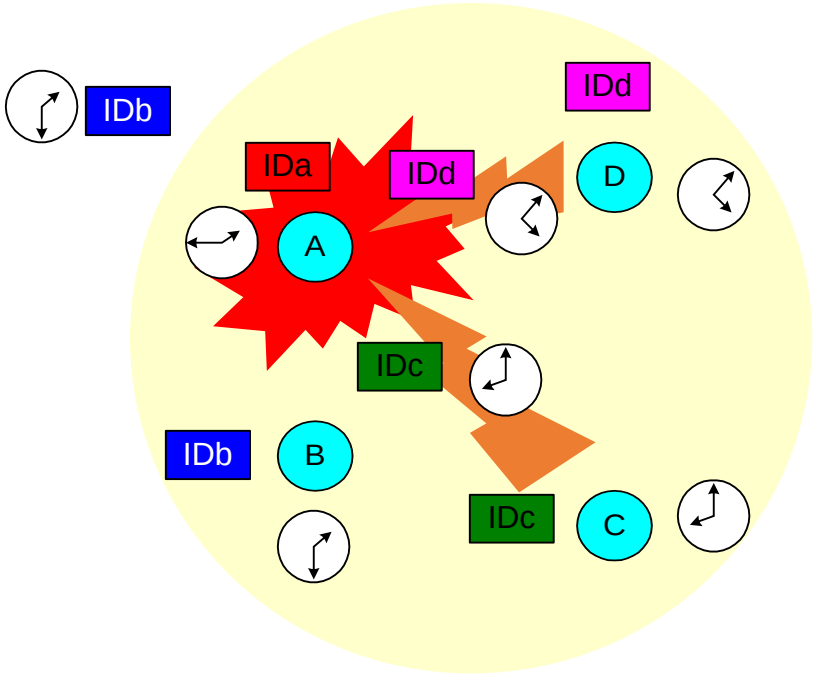
- Device A wants to search for stations
- A does an inquire (page with ID 000)
- B answers with FHS packet
  - Contains *DeviceID* and *Clock*

Scanning units



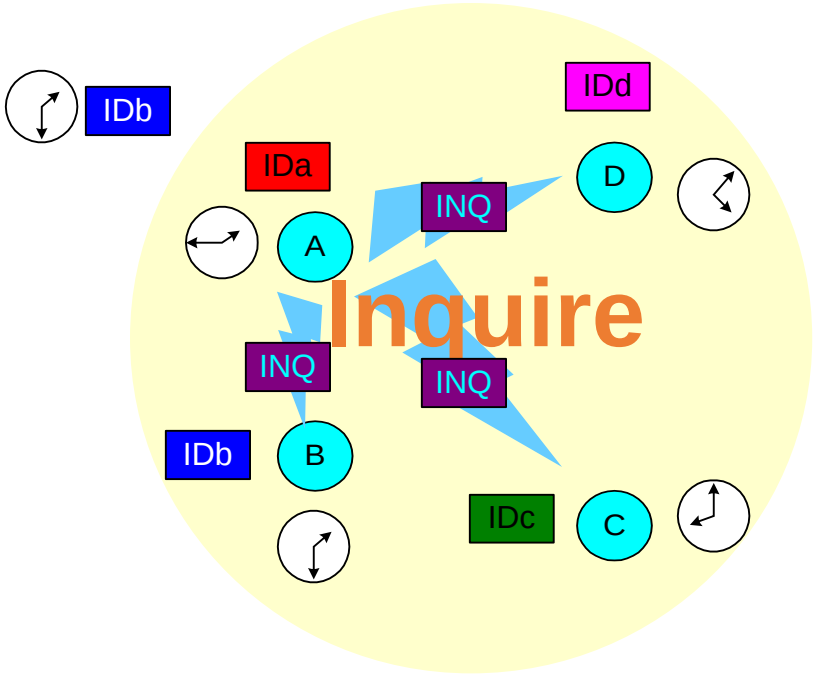
- Device A wants to search for stations
- A does an inquire (page with ID 000)
- B answers with FHS packet
  - Contains DeviceID and Clock
- A does an inquire again

Scanning units



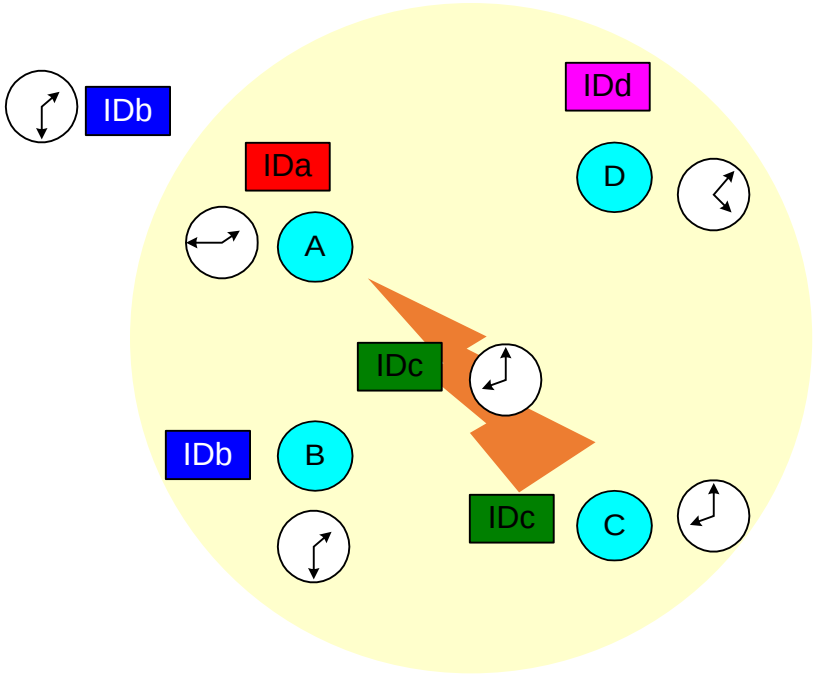
- A wants to search for stations
- …
- A does an inquire again
- C e D answer at the same time with FHS packet
  - Packets are corrupted
  - A does not answer
  - C and D will wait a random number of slots

Scanning units



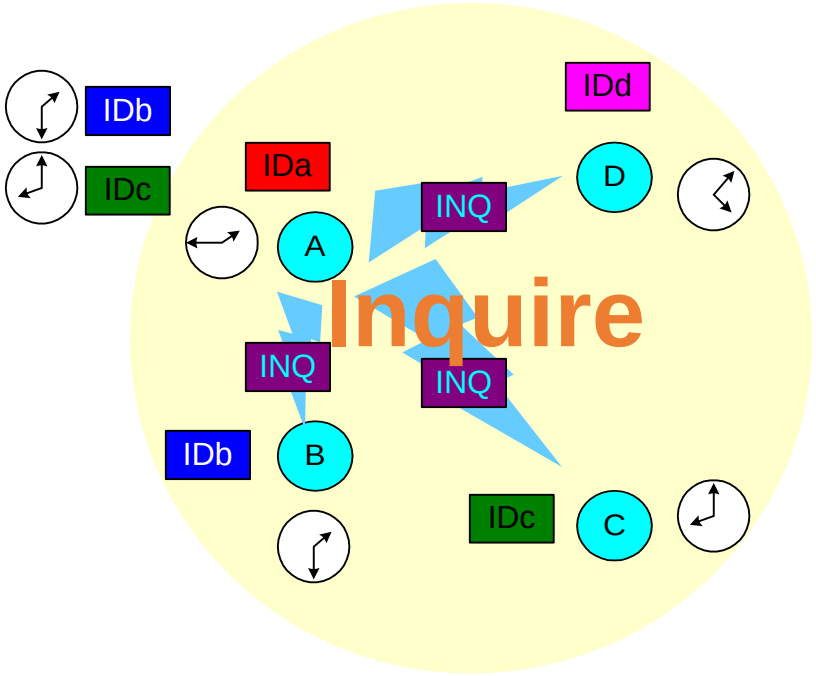
- A wants to search for stations
- …
- A does an inquire again

Scanning units



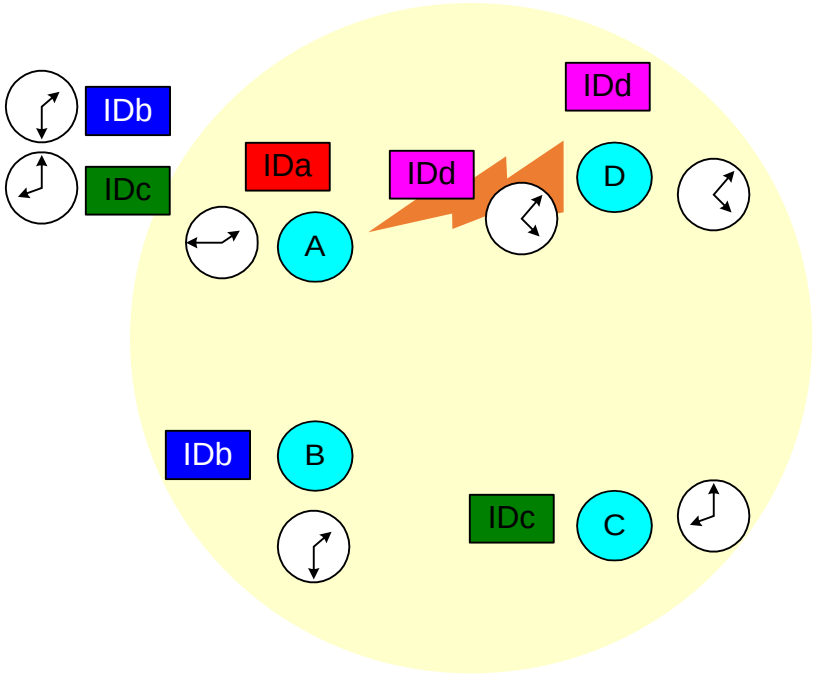
- A wants to search for stations
- …
- A does an inquire again
- C answers with FHS packet

Scanning units



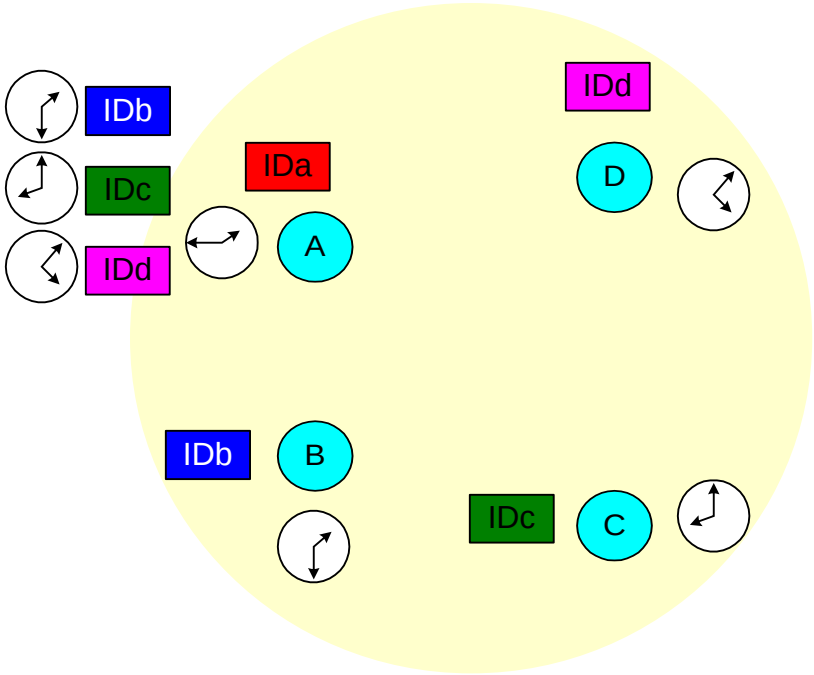
- A wants to search for stations
- A does an inquire again

Scanning units



- A wants to search for stations
- …
- A does an inquire again
- D answers with FHS packet

Scanning units



- A has all the information it needs about the units in the cell

Inquiry scanning: summary

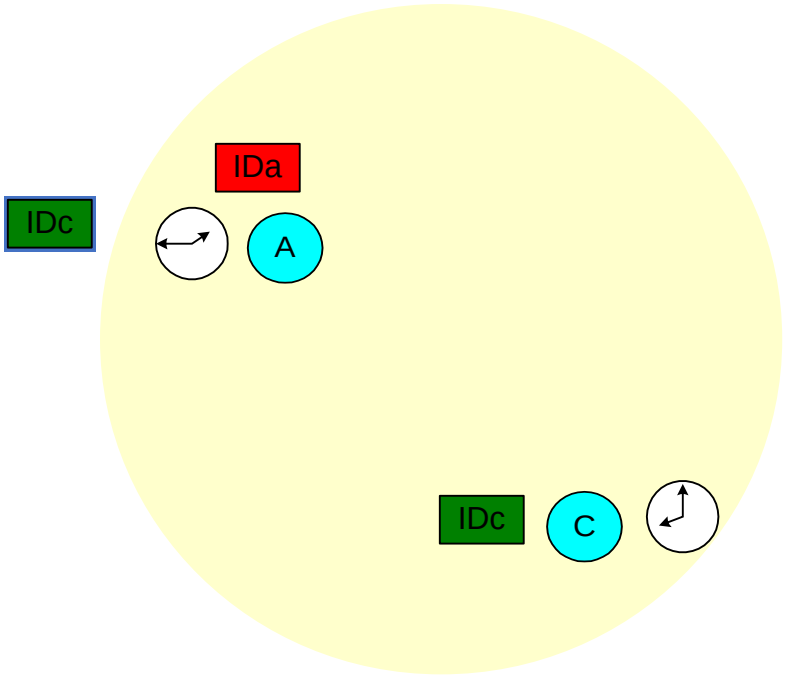
- Inquiry scanning has a common address
  - And a common frequency pattern (from 32 frequencies)
- All devices can page this address (and become masters)
- All machines hearing an inquiry will answer the inquiry request
- There is a detector (correlator hit) in the slaves, that detects inquiries, before answering with a FHS providing:
  - Device ID and Clock
- A machine in low power waits a random time before answering again to a scan
- If there is a collision on answering to a scan, they also wait a random period before answering again

Paging: Will you connect to me?

- Very similar to inquire
- Still have not synchronized clocks or frequencies
- Establishes actual Piconet connection with a device that it knows about
- Connection process involves a 6 steps of communication between the master and the slave

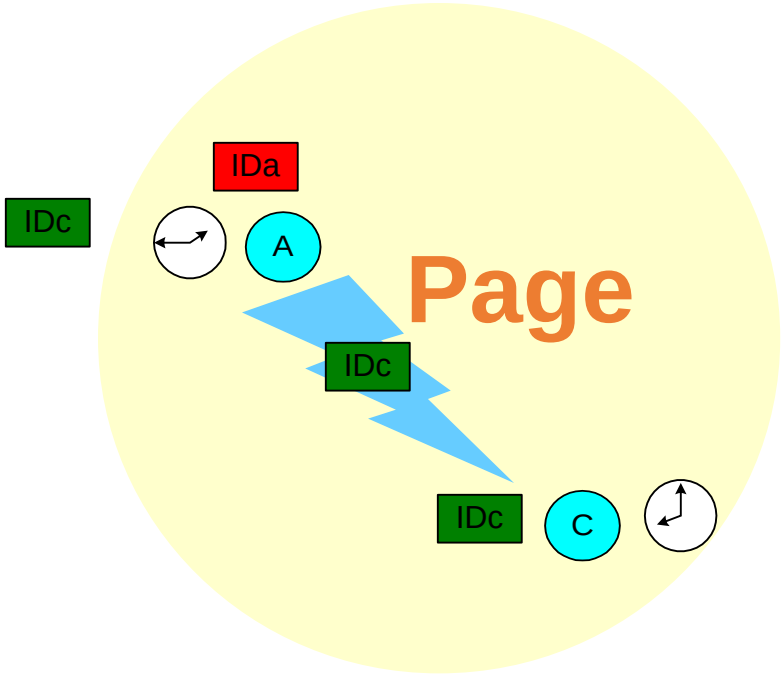
Step	Message	Direction	Hopping Pattern	Pattern Source and Clock
1	Slave ID	Master to Slave	Page	Slave
2	Slave ID	Slave to Master	Page Response	Slave
3	FHS	Master to Slave	Page	Slave
4	Slave ID	Slave to Master	Page Response	Slave
5	1st Master Packet	Master to Slave	Channel	Master
6	1st Slave Packet	Slave to Master	Channel	Master

Master Paging Slave



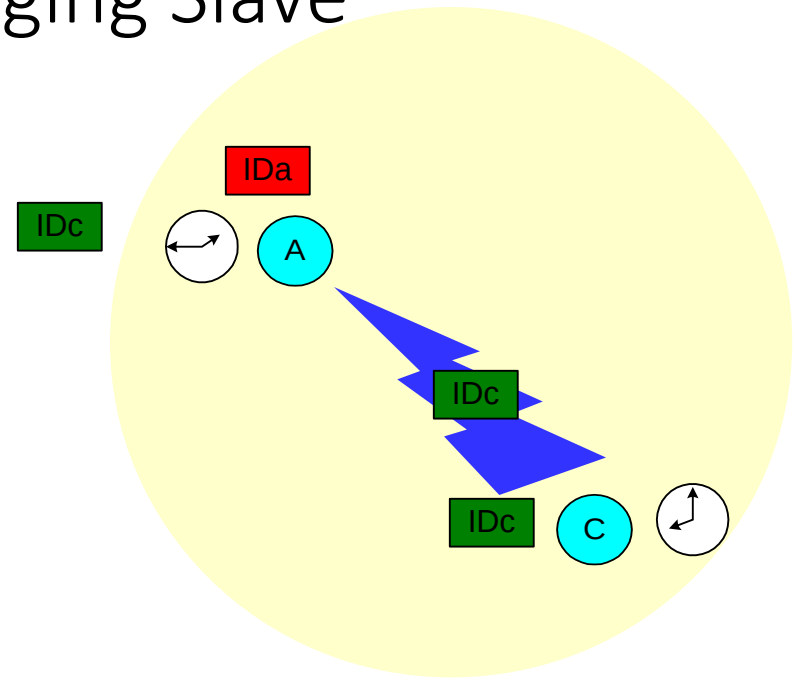
- Paging:
  - Assumes the master has C *deviceID* and *Clock*

Master Paging Slave



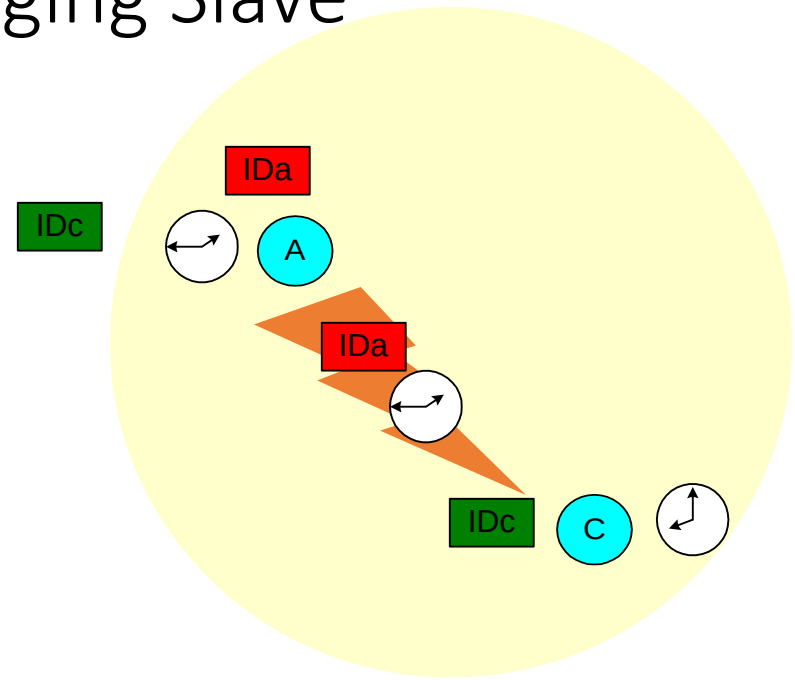
- Paging:
  - Assumes the master has C deviceID and Clock
    - A pages C with the deviceID of C

Master Paging Slave



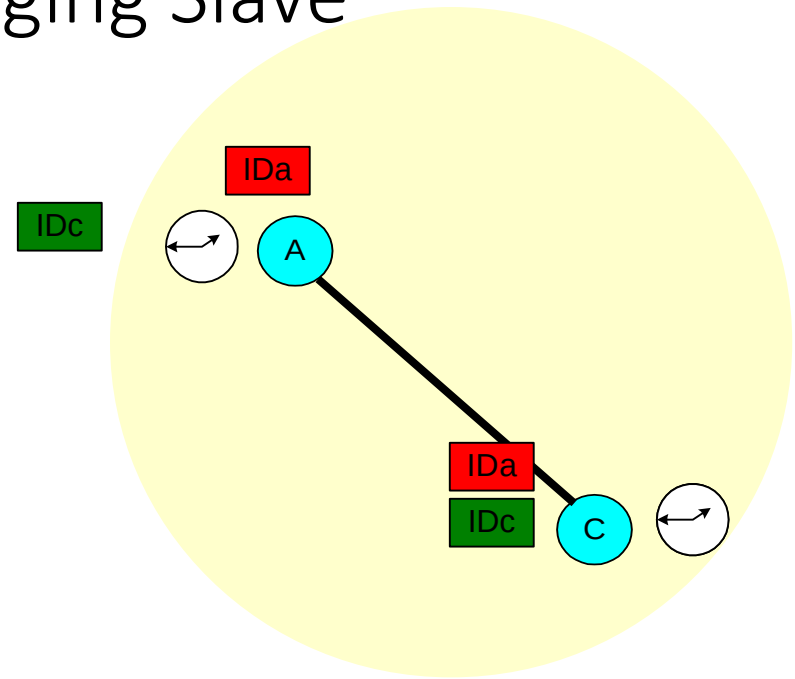
- Paging: master has the Device ID and Clock
  - A pages C with the deviceID of C
  - C answers A with his deviceID

Master Paging Slave



- Paging: master has the Device ID and Clock
  - A pages C with the deviceID of C
  - C answers A with his deviceID
  - A sends C his deviceID and Clock (FHS packet)

Master Paging Slave



- Paging: master has the Device ID and Clock
  - A pages C with the deviceID of C
  - C answers A with his deviceID
  - A send C his deviceID and Clock (FHS packet)
  - A becomes master of C

Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- BT 4.0 BLE