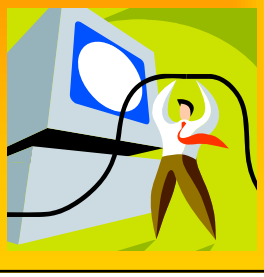
Mobile Networks

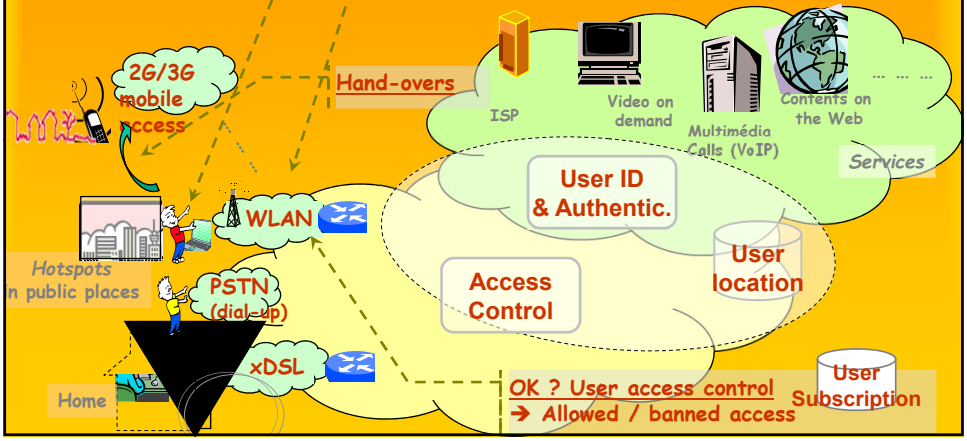
Connections and structures

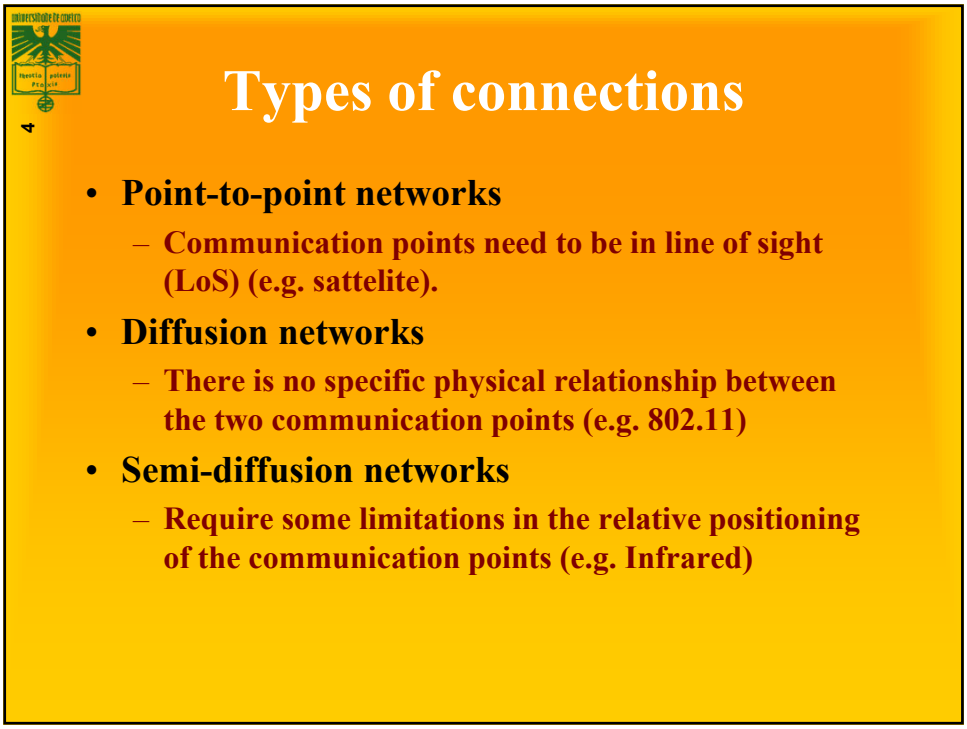


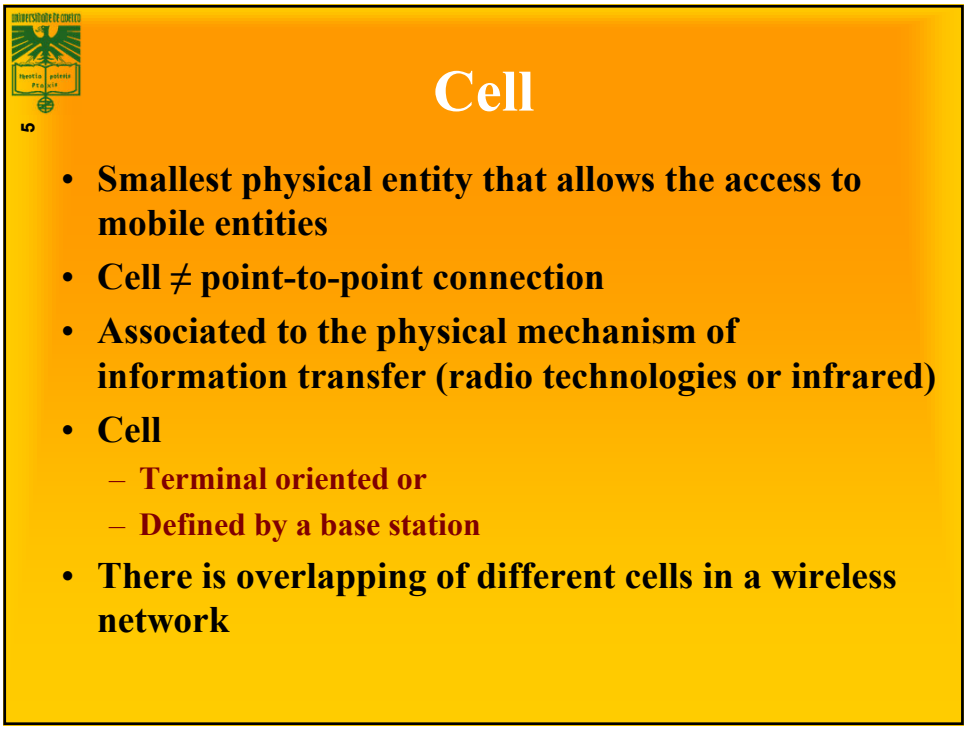
Requirements in a mobile network

Who ? → user identification + authentication
→ Identify the user separatly from the access

Where ? → user location management
→ Retrieve where the user is located, over which access he's connected



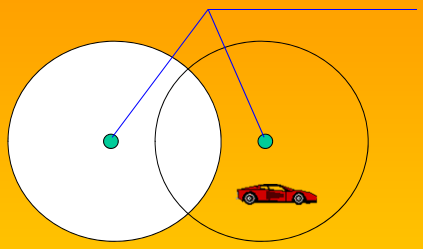

4
Types of connections
• Point-to-point networks
– Communication points need to be in line of sight (LoS) (e.g. sattelite).
• Diffusion networks
– There is no specific physical relationship between the two communication points (e.g. 802.11)
• Semi-diffusion networks
– Require some limitations in the relative positioning of the communication points (e.g. Infrared)


5
Cell
• Smallest physical entity that allows the access to mobile entities
• Cell ≠ point-to-point connection
• Associated to the physical mechanism of information transfer (radio technologies or infrared)
• Cell
– Terminal oriented or
– Defined by a base station
• There is overlapping of different cells in a wireless network

6

Public cellular network

- **Access network with radio link**
  - **Space is divided in cells with a base station**
  - **Mobile Node (MN) can work when changing between cells**

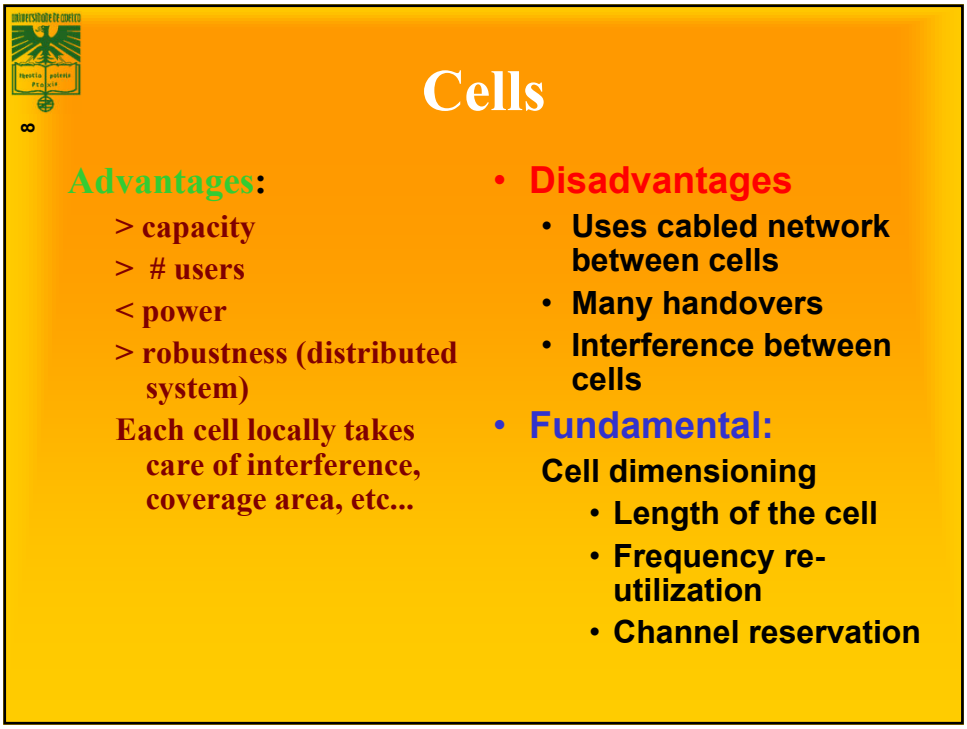


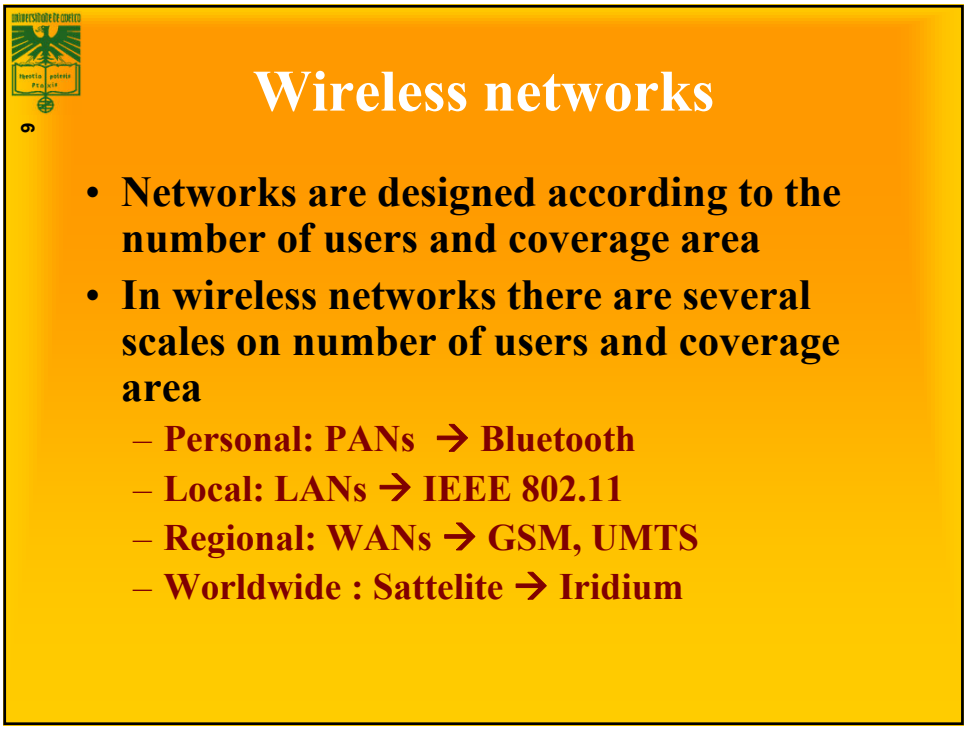
Cell length is
- **Highly variable**
- **Depends on the technology**
- **Depends on the number of users**

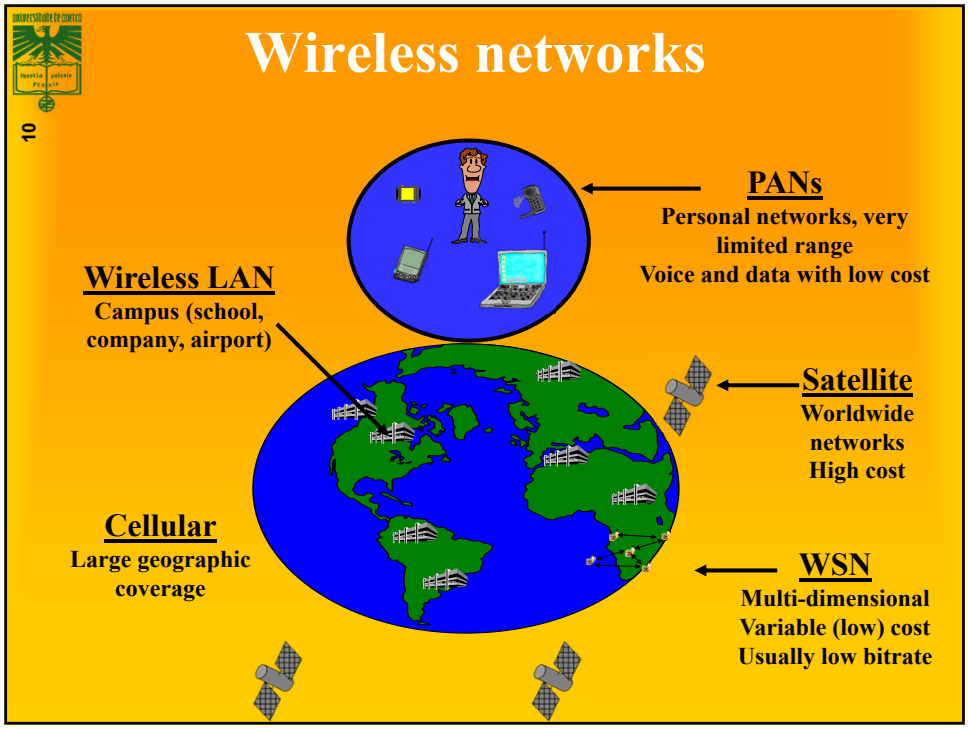
7

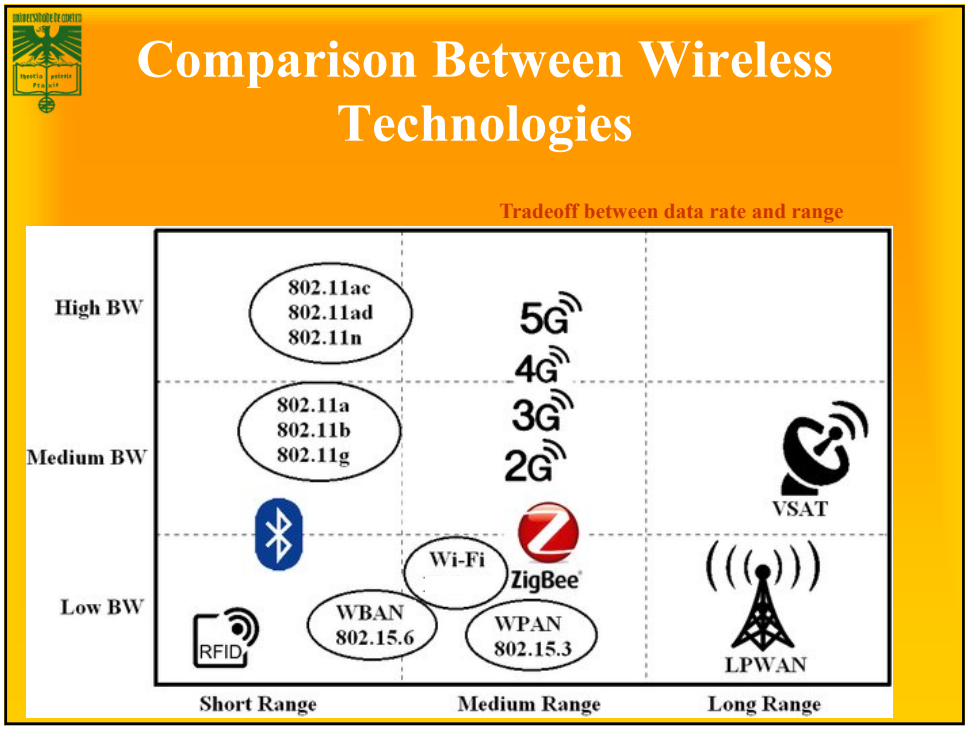
Cells

- **Length:**
  - **100m to 35 km (GSM)**
  - **Microcells: closed spaces**
  - **Hat cell: set of cells**
    - Avoid frequent handoffs in critical places
- **Format:**
  - **Teoretically analyzed as a hexagon**
  - **Reality: it depends on the place**
- **BS positioning:**
  - **Cell centrally excited**
    - BS in the center of the cell, with omni-directional antenna
  - **Cell side excited**
    - BSs in the vertices (in three)
    - Directional antennas


8
Cells
Advantages:
> capacity
> # users
< power
> robustness (distributed system)
Each cell locally takes care of interference, coverage area, etc...
Disadvantages
Uses cabled network between cells
Many handovers
Interference between cells
Fundamental:
Cell dimensioning
Length of the cell
Frequency re-utilization
Channel reservation


9
Wireless networks
Networks are designed according to the number of users and coverage area
In wireless networks there are several scales on number of users and coverage area
– Personal: PANs → Bluetooth
– Local: LANs → IEEE 802.11
– Regional: WANs → GSM, UMTS
– Worldwide : Sattelite → Iridium


Wireless networks
10
PANs
Personal networks, very limited range
Voice and data with low cost
Wireless LAN
Campus (school, company, airport)
Satellite
Worldwide networks
High cost
Cellular
Large geographic coverage
WSN
Multi-dimensional
Variable (low) cost
Usually low bitrate

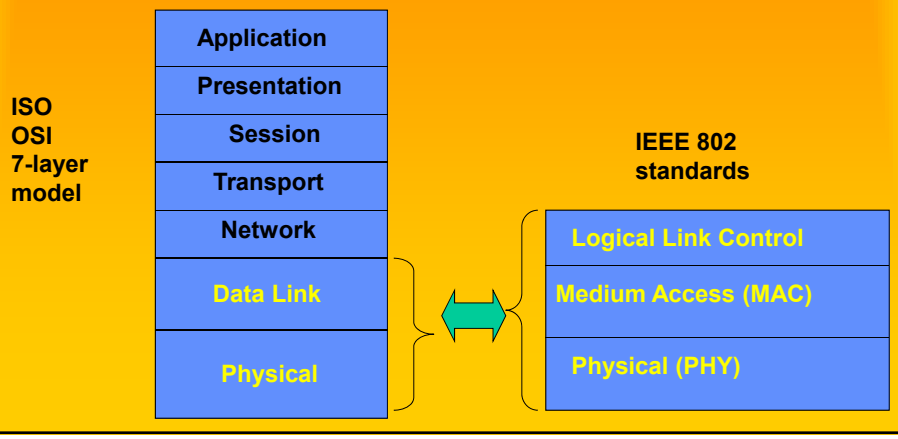

Comparison Between Wireless Technologies
Tradeoff between data rate and range
High BW
Medium BW
Low BW
802.11ac
802.11ad
802.11n
802.11a
802.11b
802.11g
5G
4G
3G
2G
VSAT
Wi-Fi
ZigBee
WBAN
802.15.6
WPAN
802.15.3
RFID
LPWAN
Short Range
Medium Range
Long Range

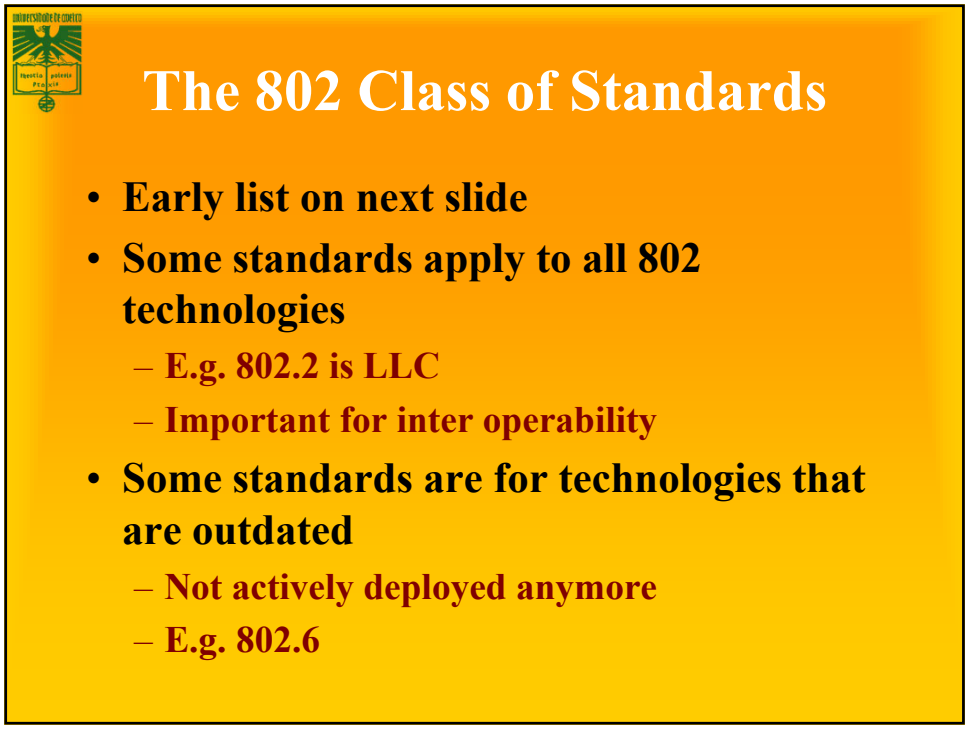
Wireless Technologies (@~2000)

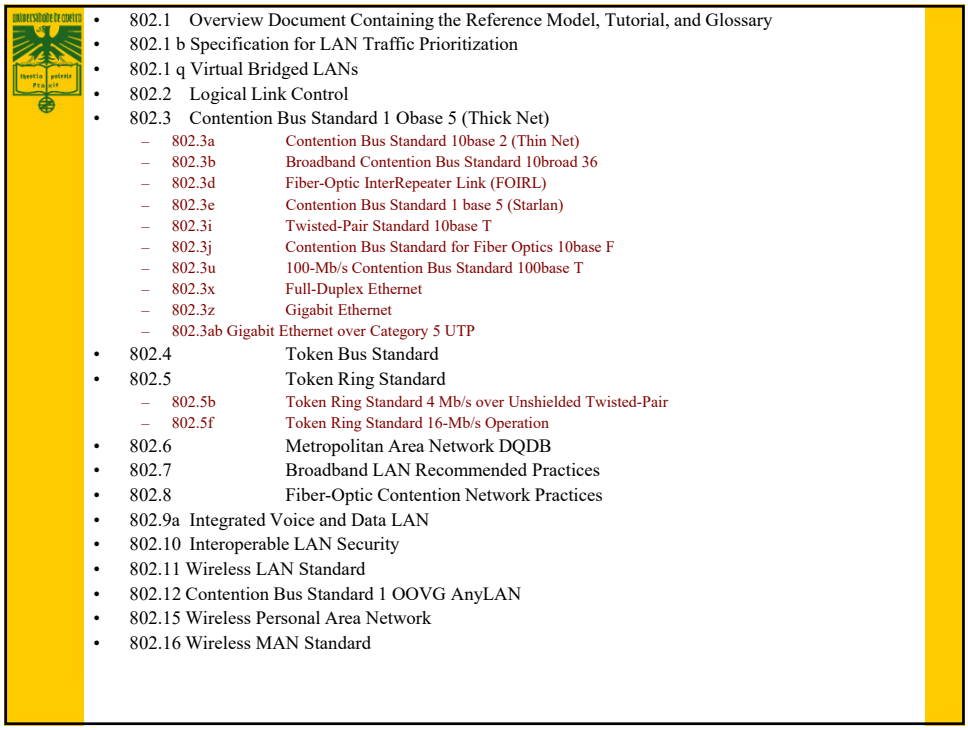
	PAN	LAN	MAN	MAN
Access speed	1-2Mb	11Mb	Mbs	>56kb
Range	10m	100-400m	kms	global
Standard	IEEE 802.15	IEEE 802.11	IEEE 802.16	GPRS 1xRTT
Scalability	Low device specific	Medium ethernet	Infra structure	High regional Infrastructure
Architecture	FHSS	DSSS	cellular	cellular

Standardization of Wireless Networks

- **Wireless networks are standardized by IEEE.**
- **Under 802 LAN MAN standards committee.**

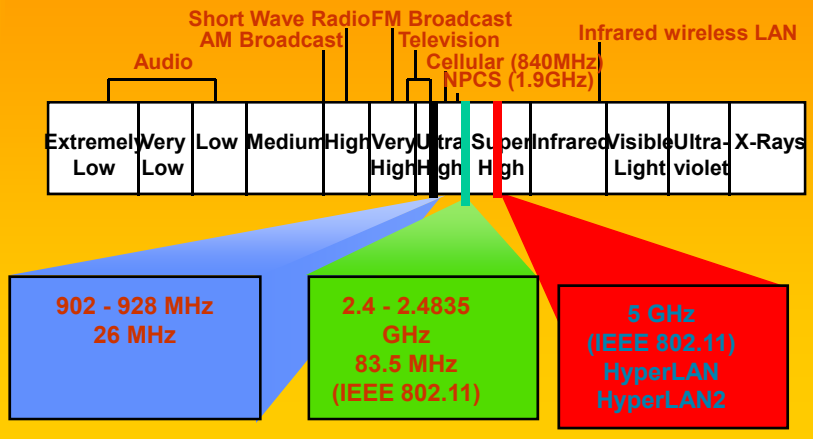



The 802 Class of Standards
• Early list on next slide
• Some standards apply to all 802 technologies
– E.g. 802.2 is LLC
– Important for inter operability
• Some standards are for technologies that are outdated
– Not actively deployed anymore
– E.g. 802.6


• 802.1 Overview Document Containing the Reference Model, Tutorial, and Glossary
• 802.1 b Specification for LAN Traffic Prioritization
• 802.1 q Virtual Bridged LANs
• 802.2 Logical Link Control
• 802.3 Contention Bus Standard 1 Obase 5 (Thick Net)
– 802.3a Contention Bus Standard 10base 2 (Thin Net)
– 802.3b Broadband Contention Bus Standard 10broad 36
– 802.3d Fiber-Optic InterRepeater Link (FOIRL)
– 802.3e Contention Bus Standard 1 base 5 (Starlan)
– 802.3i Twisted-Pair Standard 10base T
– 802.3j Contention Bus Standard for Fiber Optics 10base F
– 802.3u 100-Mb/s Contention Bus Standard 100base T
– 802.3x Full-Duplex Ethernet
– 802.3z Gigabit Ethernet
– 802.3ab Gigabit Ethernet over Category 5 UTP
• 802.4 Token Bus Standard
• 802.5 Token Ring Standard
– 802.5b Token Ring Standard 4 Mb/s over Unshielded Twisted-Pair
– 802.5f Token Ring Standard 16-Mb/s Operation
• 802.6 Metropolitan Area Network DQDB
• 802.7 Broadband LAN Recommended Practices
• 802.8 Fiber-Optic Contention Network Practices
• 802.9a Integrated Voice and Data LAN
• 802.10 Interoperable LAN Security
• 802.11 Wireless LAN Standard
• 802.12 Contention Bus Standard 1 OOVG AnyLAN
• 802.15 Wireless Personal Area Network
• 802.16 Wireless MAN Standard

Frequency Bands

- Industrial, Scientific, and Medical (ISM) bands
- Unlicensed, 22 MHz channel bandwidth



17

Bluetooth

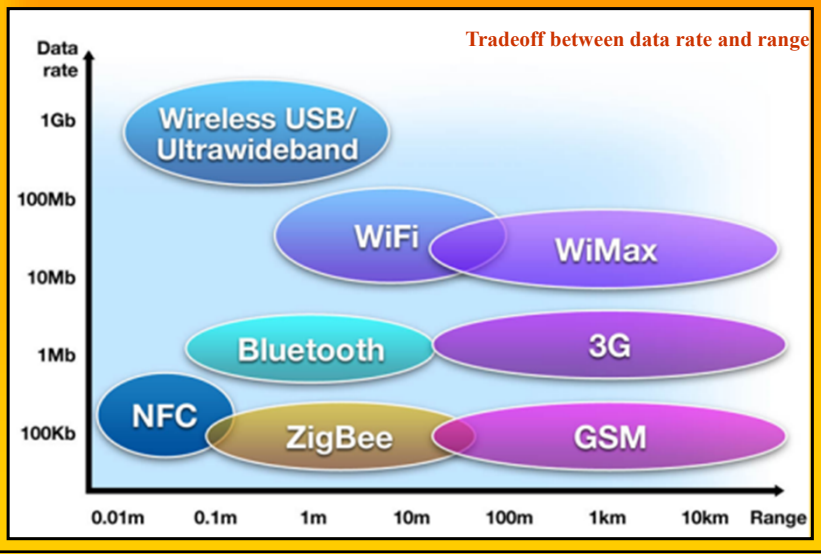
WPAN

18

Outline

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

Comparison Between Wireless Technologies



20

Personal networks: when?

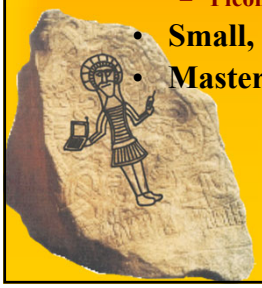
- Access mostly to “transported devices”
- No dominant need for Information Technologies
- No physical access to cabled networks
- No need for large communication rates
- Very low cost system required
- Consumer electronics integration is mandatory

Personal Area Networks

- **Target deployment environment: communication of personal devices working together**
  - **Short-range**
  - **Low Power**
  - **Low Cost**
  - **Small numbers of devices**
  - **Sometimes have more “bus-like” characteristics**
- **PAN Standards**
  - **Bluetooth – Industry consortia**
  - **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**

Bluetooth

- **Originally for "USB", not "Ethernet"**
  - **Cable replacement technology**
  - **Later also used as Internet connection, phone, or headset**
- **Created by Ericsson**
- **PAN - Personal Area Network**
  - **Up to 1 Mbps connections**
  - **1600 hops per second FHSS**
  - **Includes synchronous, asynchronous, voice connections**
  - **Piconet routing**
- **Small, low-power, short-range, cheap, versatile radios**
- **Master/slave configuration and scheduling**



» Harald Blaatand "Bluetooth" II, Danish King 940-981

» Conquer of Norway, brought Christianity to Norway

Rune Stone, Jelling

History

1998 - Bluetooth technology is officially introduced and the BLUETOOTH SIG is formed. 1999 - Bluetooth 1.0 Specification is introduced.

2003 - The BLUETOOTH SIG overhauls the Bluetooth Core Specification with the announcement of Version 2.1.

2004 - Bluetooth Version 2.0 + EDR (Enhanced Data Rate) is introduced.

2005 - Devices using Version 2.0 + EDR begin to hit the market in late 2005.

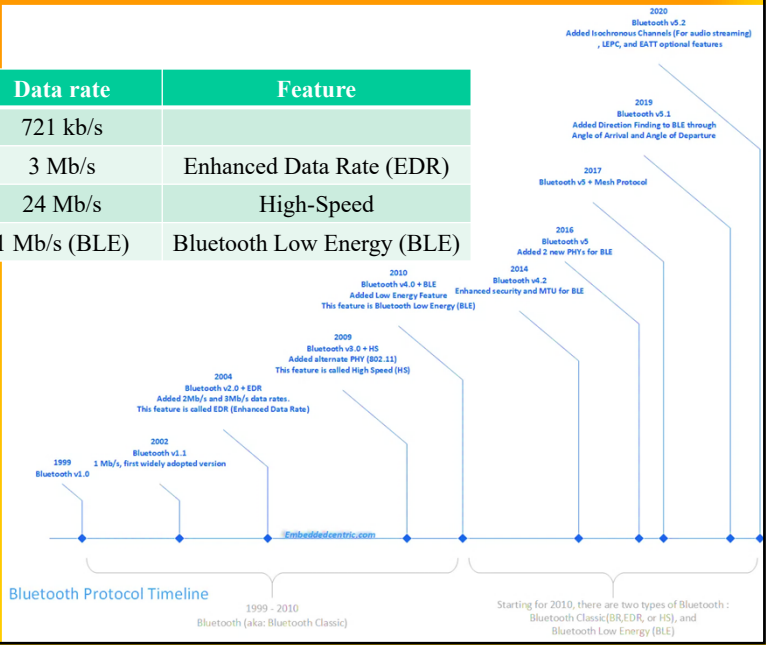
2007 - Bluetooth Core Specification Version 2.1 + EDR is adopted by the BLUETOOTH SIG.

2009 - Bluetooth Core Specification Version 3.0 + HS (High Speed) is adopted by the BLUETOOTH SIG.

2010 - Bluetooth Core Specification Version 4.0 is adopted by the BLUETOOTH SIG.

Bluetooth Versions

Version	Data rate	Feature
1.2	721 kb/s	
2.0 + EDR	3 Mb/s	Enhanced Data Rate (EDR)
3.0 + HS	24 Mb/s	High-Speed
4.0	1 Mb/s (BLE)	Bluetooth Low Energy (BLE)



Bluetooth higher speeds (in BT classic)

- Enhanced Data Rate (EDR)
  - Introduced in Bluetooth v2.0 to support faster data transfer
  - Supports a data rate up to 3 Mbps
  - Using reduced duty cycle control, EDR can provide lower power consumption
- High Speed (HS)
  - BT HS released in April 2009 (in Bluetooth version 3.0+HS)
  - Bluetooth 3.0+HS provides data transfer speeds of up to 24 Mbps, though not over the Bluetooth link itself
  - BT link is used for negotiation and establishment, and the high data rate traffic is carried over a collocated 802.11 link
  - HS part of the specification is not mandatory in BT 3.0
  - Only devices that display the "+HS" logo actually support Bluetooth over 802.11 high-speed data transfer

Bluetooth Spec Evolution (BT classic)

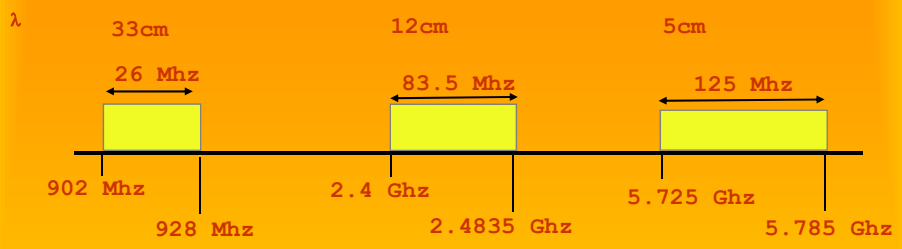
Specifications	1.1	1.2	2.0 + EDR	2.1 + EDR	3.0 +HS	4.0
Adopted	2002	2005	2004	2007	2009	2010
Transmission Rate	723.1 kbps	723.1 kbps	2.1 Mbps	3 Mbps	24 Mbps	25 Mbps
Standard PAN Range	10 m	10 m	10 m	10 m	10 m	50 m
Improved Pairing (without a PIN)				Yes	Yes	Yes
Improved Security		Yes	Yes	Yes	Yes	Yes
NFC Support			Yes	Yes	Yes	Yes
Voice Dialing	Yes	Yes	Yes	Yes	Yes	Yes
Call Mute	Yes	Yes	Yes	Yes	Yes	Yes
Last-Number Redial	Yes	Yes	Yes	Yes	Yes	Yes
Fast Transmission Speeds			Yes	Yes	Yes	Yes
Lower Power Consumption			Yes	Yes	Yes	Yes
Bluetooth Low Energy						Yes

27

Bluetooth features

- **Radio network, on the 2.4 GHz, world-wide!**
- **Airplane friendly!**
- **FH (Frequency Hopping) spread spectrum:**
  79 (23 - .jp .es .fr) channels (de 2.402GHz - 2.480GHz)
- **Defines a master that syncrhonizes everyone to his hop-pattern.**
- **Defines two types of networks:**
  - **piconets**
  - **scaternets**
- **Maximum 8 devices per piconet (1 master + 7 slaves)**
- **Transmission rate: 720 Kb/s (max), assymetrical variable**

Unlicensed Radio Spectrum



cordless phones
baby monitors
Wireless LANs

802.11
Bluetooth
Microwave oven

unused

28

29

Frequency Hopping Spread Spectrum (FHSS)

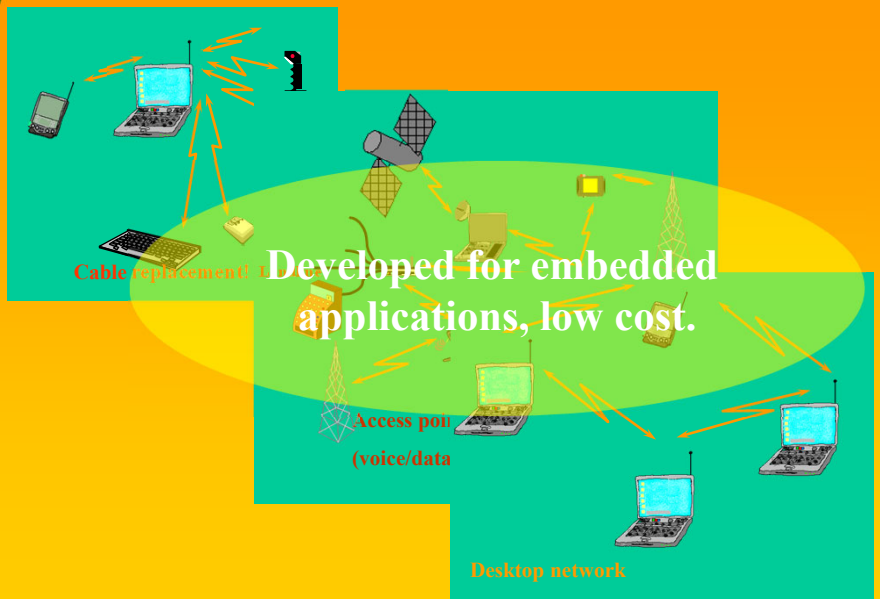
- **Signal broadcast over seemingly random series of frequencies**
- **Receiver hops between frequencies in sync with transmitter**
  - **Each frequency has the bandwidth of the original signal**
  - **Dwell time is the time spent using one frequency**
- **Spreading code determines the hopping sequence**
  - **Must be shared by sender and receiver (e.g. standardized)**
- **Eavesdroppers hear unintelligible blips**
- **Jamming on one frequency affects only a few bits**
  - **Typically large number of frequencies used**
    - Improved resistance to jamming

39

Bluetooth classic vs. cable

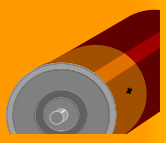
Topology	Max. 7 simultaneous lines	1 line = 1 cable
Flexibility	Crosses walls, bodies, etc.	Line-of-sight, physical path
Transmission rate	1 MSPS, 720 Kbps	115Kbps - 400Mbps
Power	0.1 watts active power	0.05 watts or more
Dimensions	25 mm x 13 mm x 2 mm, several grams	Typical 1-2 metros. Weight varies with size
Cost	ci. 5 €/access	~ €4-€100/meter
Range	~ 10 meters	Typical 1-2 metros. Size = range.
Geographic coverage	~similar everywhere.	Cables and connections vary along the world.
Security	Link layer, SS radio. Very safe.	Ideal.

Bluetooth: more than a PAN!



42

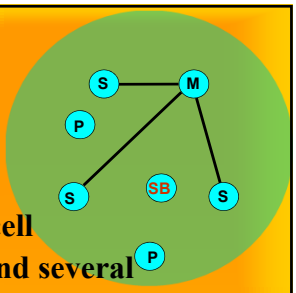
Low power



- **Global architecture for low power**
  - **Hold and Park mode: 60 µA current**
    - Connected device, but not operating
    - Device operates after a 2 ms wait process.
    - In Hold: keeps its AMA; in Park has to free AMA, and later has to claim it back
- **Transmission power ~1mW**
  - **100mW classes also exist**
- **Standby Current < 0.3 mA**
  - ⇒ **3 months**
- **Voice mode: 8-30 mA**
  - ⇒ **75 hours**
- **Data mode (medium): 5 mA (0.3-30mA, 20 kbit/s, 25%)**
  - ⇒ **120 hours**

43

Piconets



- **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**

P=Parked
SB=Standby

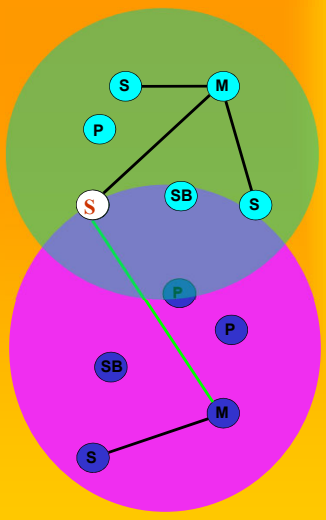
M=Master
S=Slave

- **Master defines radio parameters ("clock" and "deviceID")**
  - **Channel, hopping sequence, timing, …**
- **Each piconet has an unique FH pattern (e and a single ID)**
- **Each piconet has a maximum bandwidth (1MSPS)**
- **A slave in one piconet can also be part of another piconet**
  - **Either as a master or as a slave**
  - **If master, it can create scatternets**

44

Scatternet

- Connection of several piconets
- Through a common device (bridge) (M/S)
- One device can be M/S at the same time
  - Or at least Slave in two piconets
  - Bridge node "stay" in a piconet for some time, then switch to another piconet by changing hop sequence.
- Global system BW unlimited, but piconet BW always <1Mbps
- Impact on piconets is minimal for < 10 piconets.
- Potentially any device can share piconets
  - Reality: limitations on commercial stacks



M=Master P=Parked
S=Slave SB=Standby

45

Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- Profiles and security
- 802.15.x

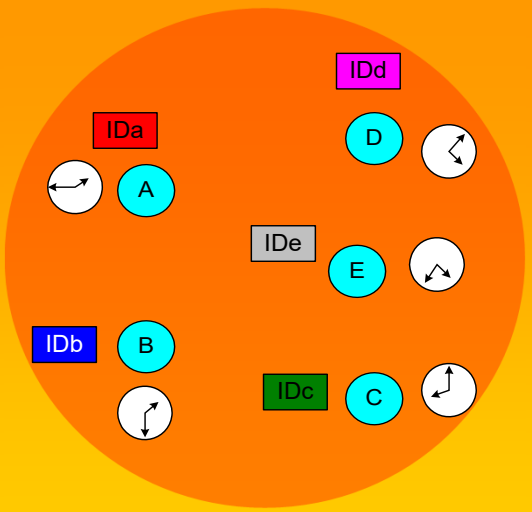
46

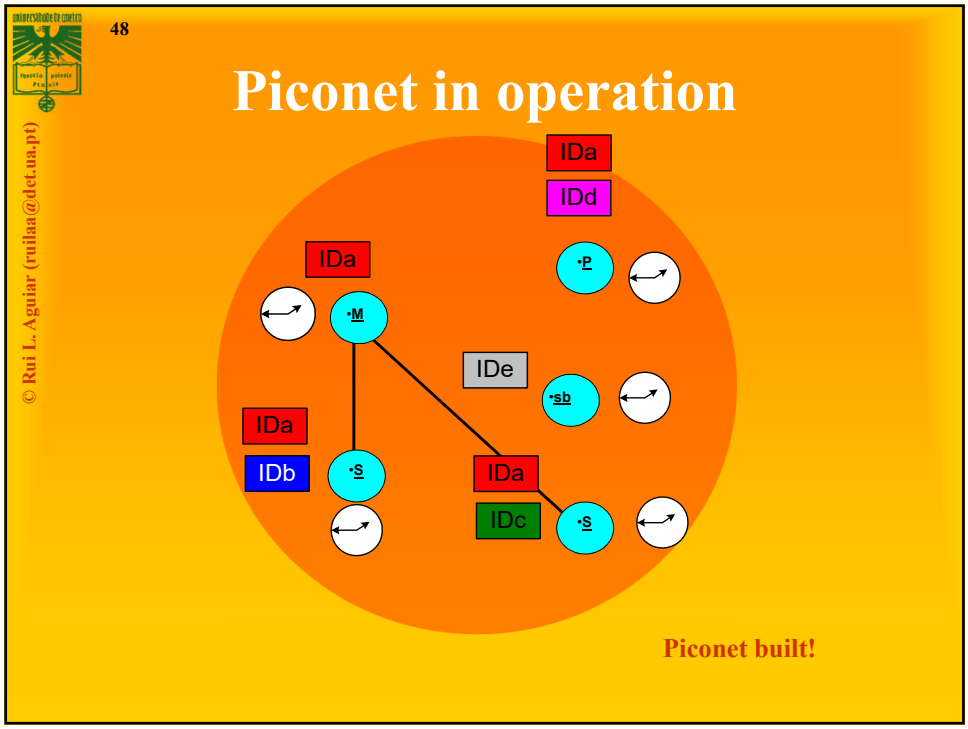
Piconet operation

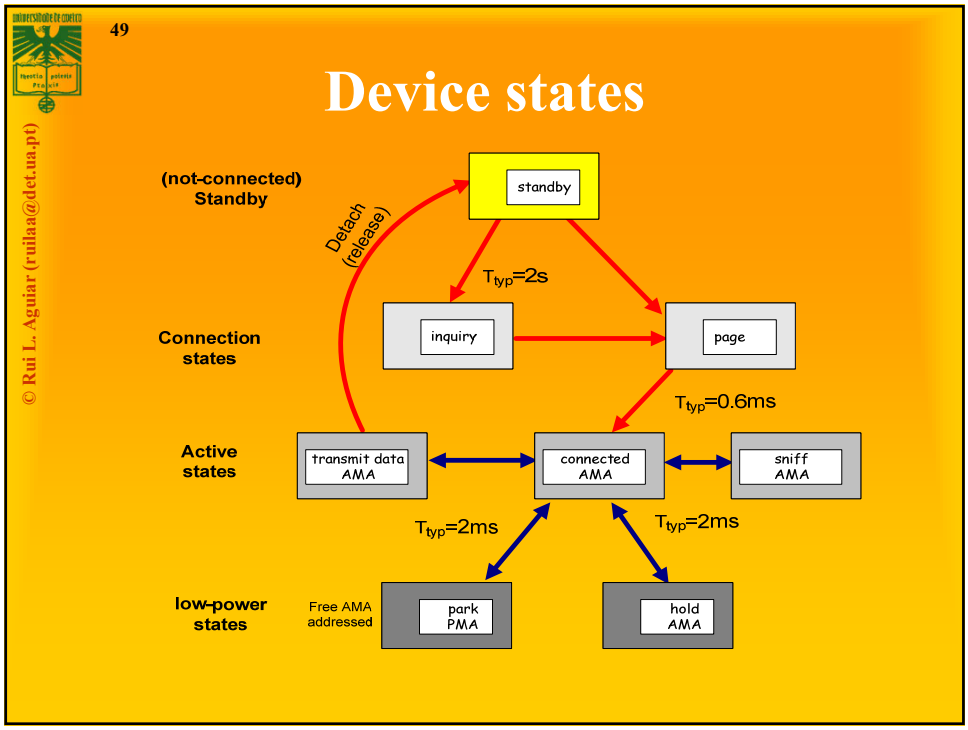
- **FH-SS: all devices must share the same hopping pattern:**
  - ***Master* provides clock and deviceID such that:**
    - deviceID (48-bits) defines hopping pattern
    - Clock defines phase inside the pattern.
- **If a device is inside a piconet, and is not connected, it must be in *standby***
- **There are two types of piconet addresses (7+200...)**
  - *Active Member Address* **(AMA, 3-bits)**
  - *Parked Member Address* **(PMA, 8-bits)**

47

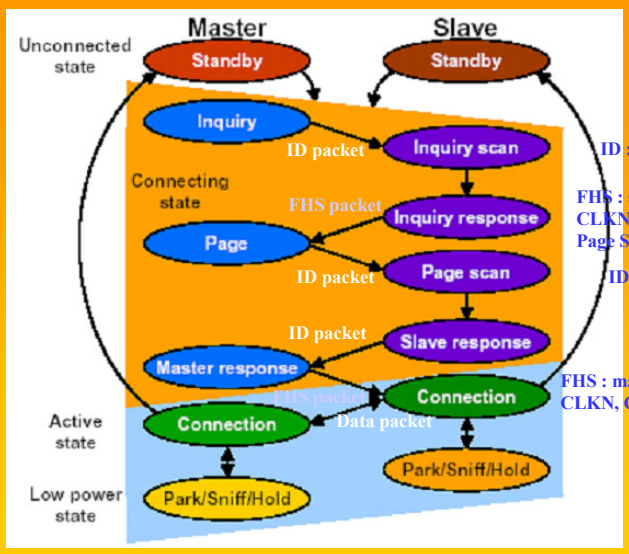
Piconet before setup




48
Piconet in operation
IDa
IDd
IDa
·P
·M
IDe
·sb
IDa
IDb
·S
IDa
IDc
·S
Piconet built!
© Rui L. Aguiar (ruilaa@det.ua.pt)


49
Device states
(not-connected) Standby
standby
Detach (release)
Ttyp=2s
Connection states
inquiry
page
Ttyp=0.6ms
Active states
transmit data AMA
connected AMA
sniff AMA
Ttyp=2ms
Ttyp=2ms
low-power states
Free AMA addressed
park PMA
hold AMA
© Rui L. Aguiar (ruilaa@det.ua.pt)

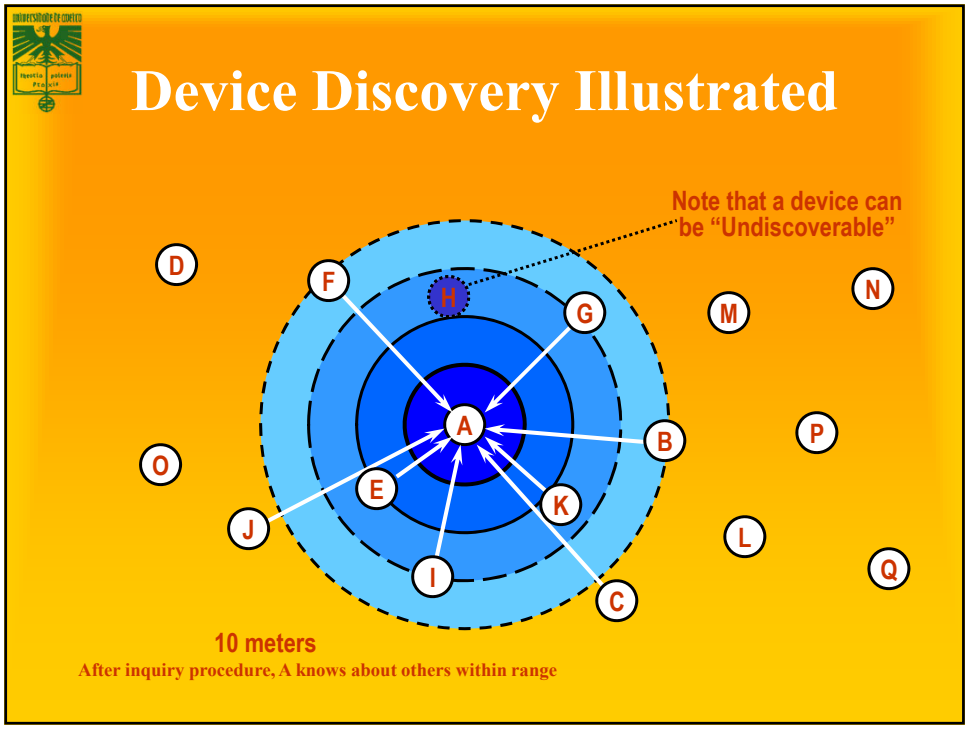
Connection Procedure

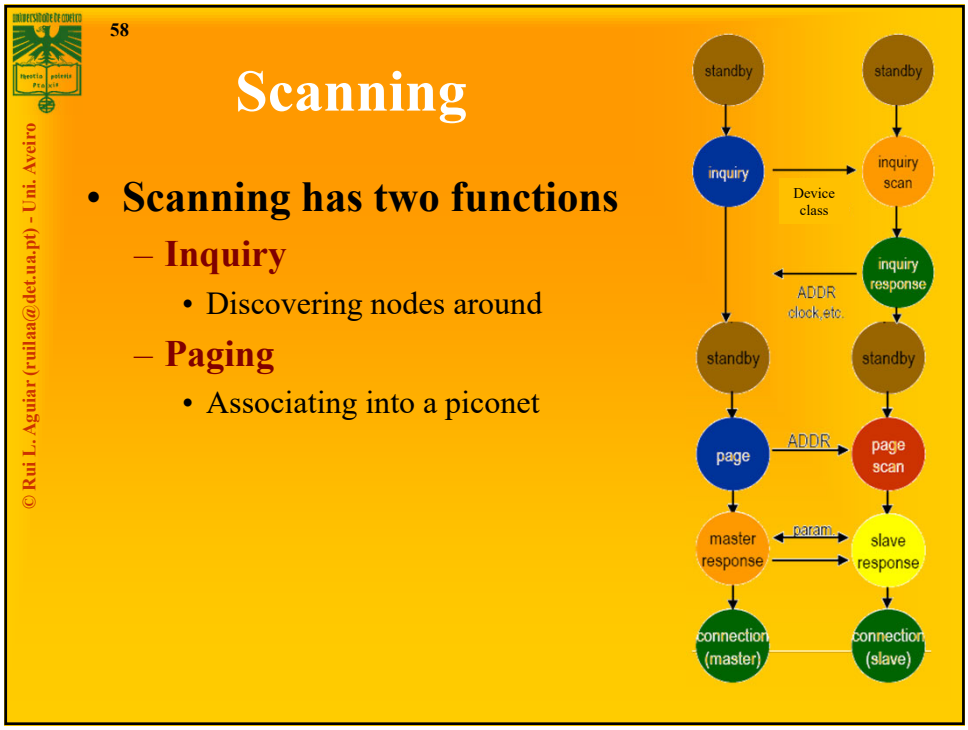


Low-Power Operation in BT classic

- **3 modes:**
  - **Hold: node sleeps for specified interval.**
    - Master can put slaves in hold while searching for new members, attending another piconet, etc.
    - No ACL packets.
  - **Sniff: slave low-duty cycle mode.**
    - Slave wakes up periodically to talk to master.
    - Fixed "sniff" intervals.
  - **Park:**
    - Very low power state.
    - Used to admit more than 7 slaves in piconet.
      - Slave gives up its active member address.
      - Receives "parked" member address.
    - Wakes up periodically listening for broadcasts which can be used to "unpark" node.

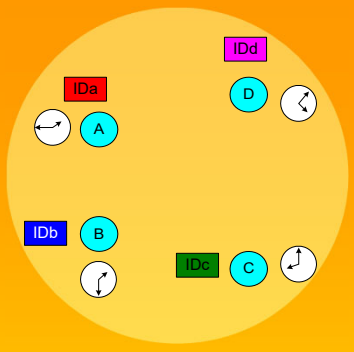
56


Device Discovery Illustrated
Note that a device can be "Undiscoverable"
D
F
H
G
N
M
A
B
P
O
E
K
J
L
I
C
Q
10 meters
After inquiry procedure, A knows about others within range


58
Scanning
• Scanning has two functions
– Inquiry
• Discovering nodes around
– Paging
• Associating into a piconet
© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro
standby
standby
inquiry
inquiry scan
Device class
inquiry response
ADDR
clock,etc.
standby
standby
page
ADDR
page scan
master response
param.
slave response
connection (master)
connection (slave)

59

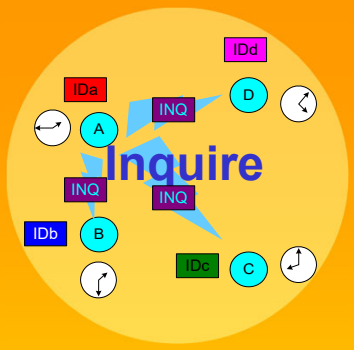
Scanning units



Device A wants to search for stations

60

Scanning units



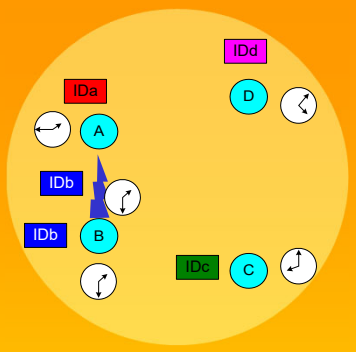
Device A wants to search for stations

A does an inquire (page with ID 000)

Devices B,C,D are doing an inquire scan

61

Scanning units



Device A wants to search for stations

A does an inquire (page with ID 000)

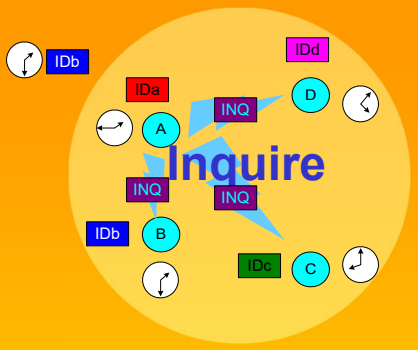
Devices B,C,D are doing na inquire scan

B answers with FHS packet

Contains ***DeviceID*** **and** ***Clock***

62

Scanning units



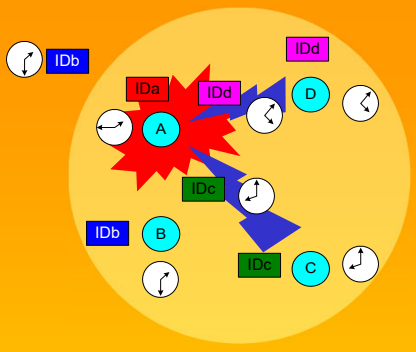
Device A wants to search for stations

- **A does an inquire (page with ID 000)**
  - Devices B,C,D are doing na inquire scann
- **B answers with FHS packet**
  - Contains *DeviceID* and *Clock*

A does an inquire again

63

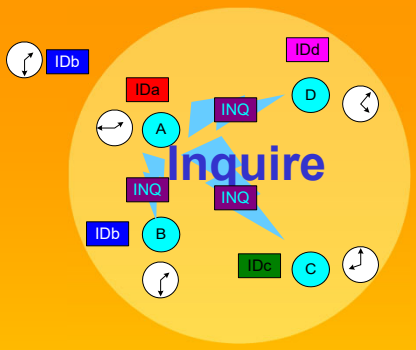
Scanning units



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 an random number of slots

64

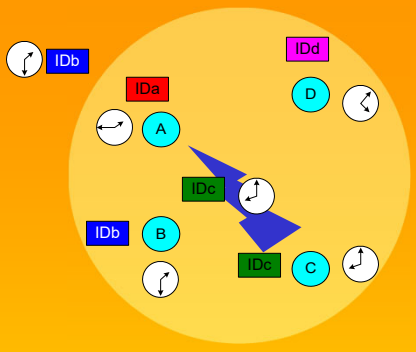
Scanning units



A wants to search for stations
A does an inquire again

65

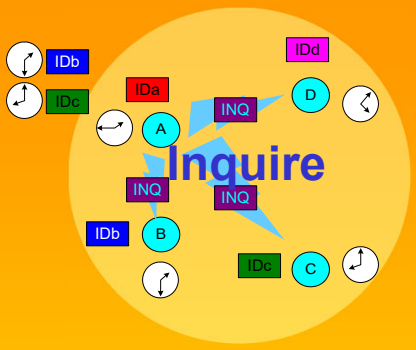
Scanning units



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

66

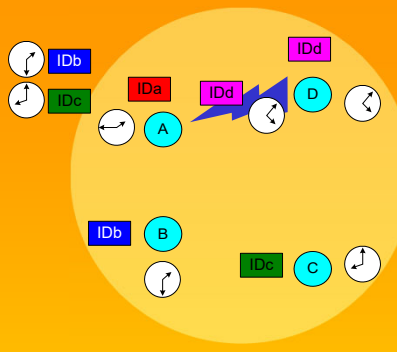
Scanning units



A wants to search for stations
A does an inquire again

67

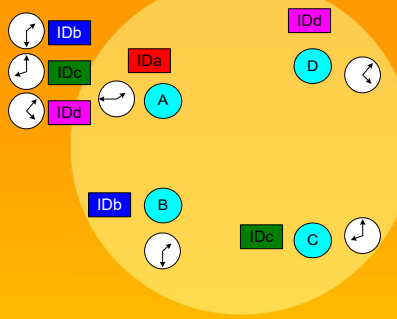
Scanning units



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

68

Scanning units



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

69

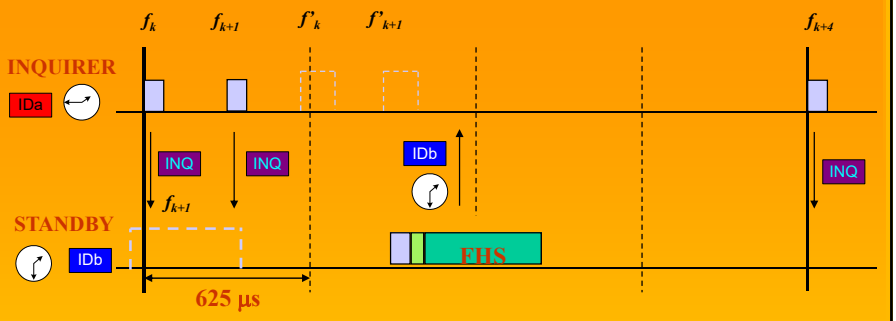
Inquiry scanning: summary

- **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 e 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.**

70

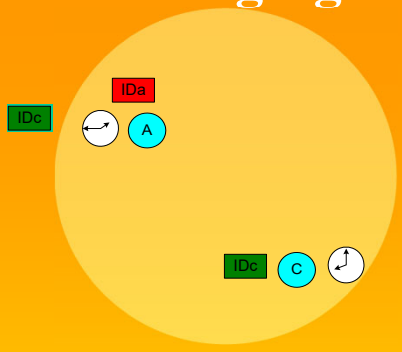
Timing: Inquiry



Inquiry requires two packets before the slave answers.

71

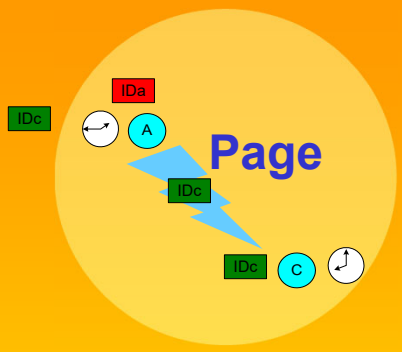
Master Paging Slave



- **Paging:**
  - **Assumes that the master has the *Device ID* and *Clock***

72

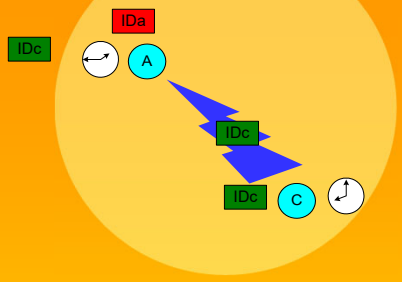
Master Paging Slave



- **Paging:**
  Assumes that the master has the *Device ID* and *Clock*
  - ***A* pages C with the *deviceID* of C**

73

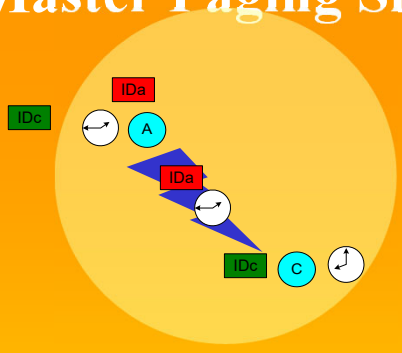
Master Paging Slave



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

74

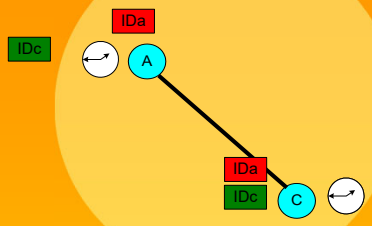
Master Paging Slave



- **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)**

75

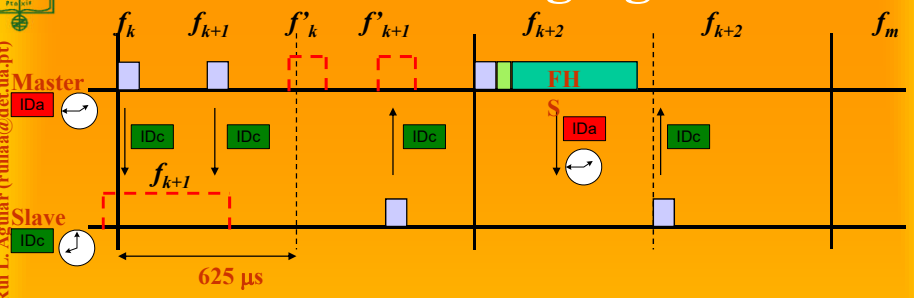
Master Paging Slave



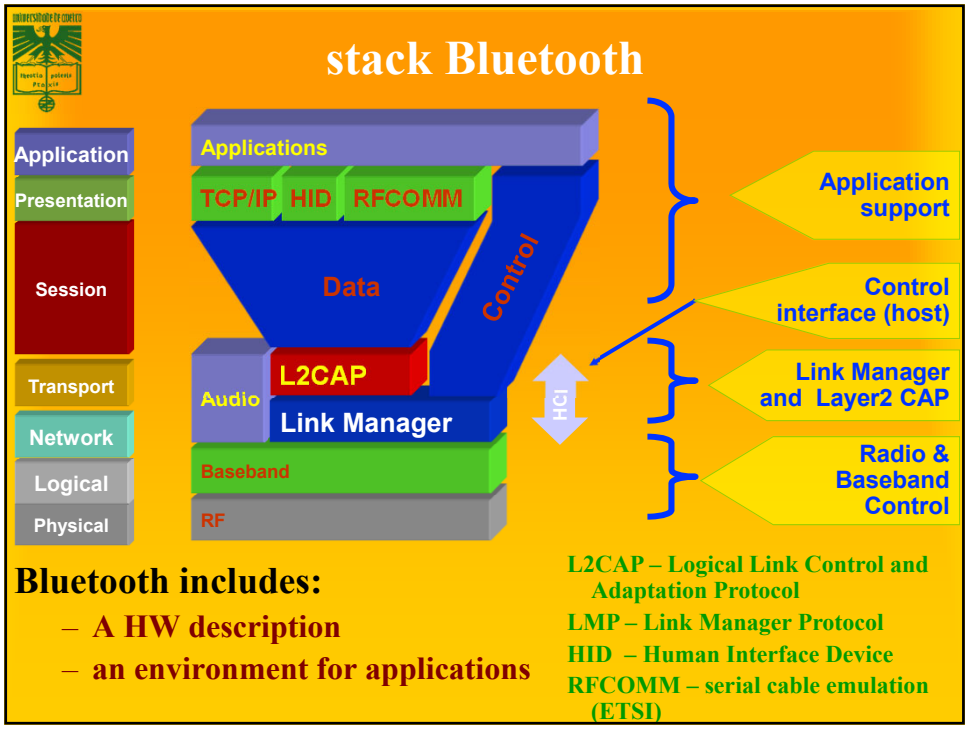
- **Paging: master has the *Device ID* and *Clock***
  - ***A* pages C with the *deviceID* of C**
  - **C answers A with his *deviceID***
  - **A send C his *deviceID* and *Clock* (FHS packet)**
  - **A becomes master of C**

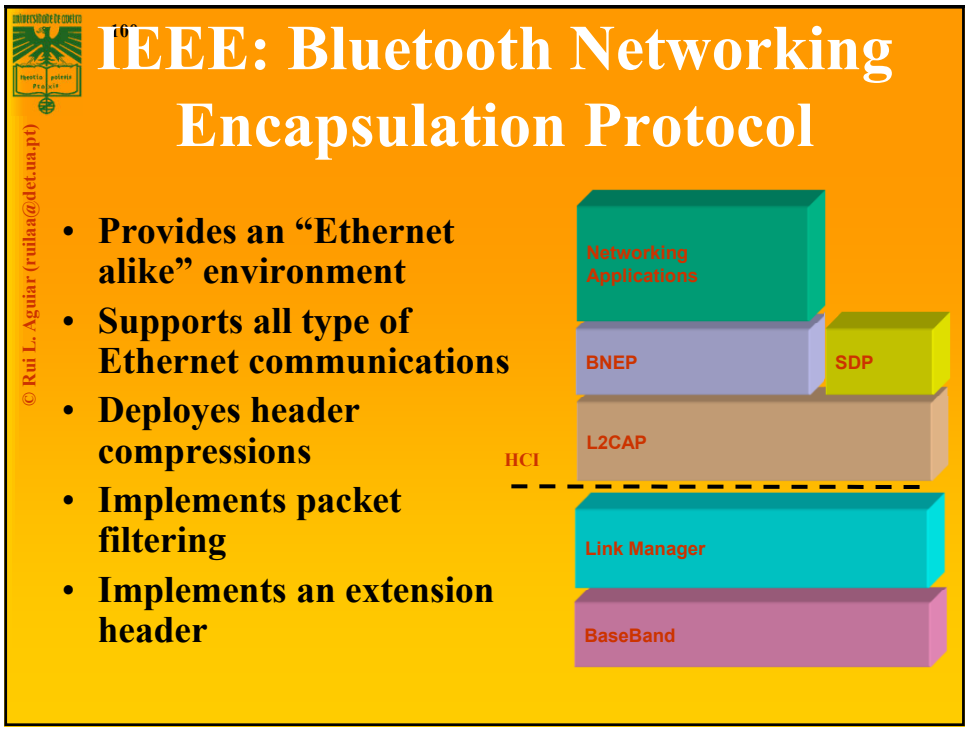
76

Time: Master Paging Slave



- **Master pages slave (packet has slave's ID) at the paging frequency of the slave (1 of 32)**
  - **Master send a train of 16 fqs in the slave hop set.**
    - Slave ID sent twice in the slave frequency
    - Master waits for two answers in the salve frequency
  - **If it does not work, master will send**
- **Slave listens for 11 ms (page scan)**
  - **If it identifies packets, slave wakes up and sends packets in that frequency.**
  - **Master answers with FHS (*Device ID* e *Clock*)**
  - **Slave joins piconet.**


stack Bluetooth
Application
Presentation
Session
Transport
Network
Logical
Physical
Applications
TCP/IP
HID
RFCOMM
Data
Control
Audio
L2CAP
Link Manager
Baseband
RF
HCI
Application support
Control interface (host)
Link Manager and Layer2 CAP
Radio & Baseband Control
Bluetooth includes:
– A HW description
– an environment for applications
L2CAP – Logical Link Control and Adaptation Protocol
LMP – Link Manager Protocol
HID – Human Interface Device
RFCOMM – serial cable emulation (ETSI)

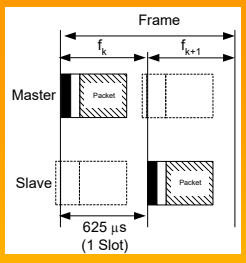

IEEE: Bluetooth Networking Encapsulation Protocol
© Rui L. Aguiar (ruilaa@det.ua.pt)
Provides an "Ethernet alike" environment
Supports all type of Ethernet communications
Deploys header compressions
Implements packet filtering
Implements an extension header
Networking Applications
BNEP
SDP
L2CAP
HCI
Link Manager
BaseBand

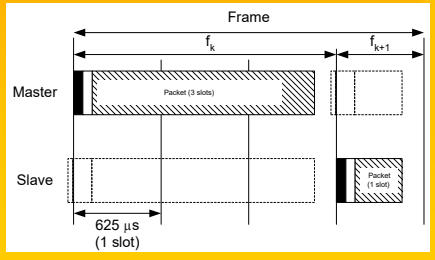
Bluetooth Protocol

- **Radio layer**
  - **Defines requirements for a Bluetooth radio transceiver**
  - **Handles conformity to 2.4GHz band**
  - **Establishes specifications for using Spread-Spectrum Frequency Hopping**
  - **Classifies device into one of three power classes:**
    - long range; (Class 1 - 100mW, 100m)
    - normal/standard range; (Class 2 - 2.5mW, 10m)
    - short range; (Class 3 - 1 mW, 1m)

Radio Layer

- **Rádio: FH SS**
  - **79/23 channels of 1 Mb/s**
  - **Hoping: per slot**
    - Packets have 1, 3, or 5 slots of 625 µs.
    - Hoping (nominal) 1600 times per second
  - **Frame includes two packets**
    - Transmission followed by reception
  - **Radio designed to low cost and universal usage**
    - (noise, synchronous action technology← 2.4GHz, etc…)





104

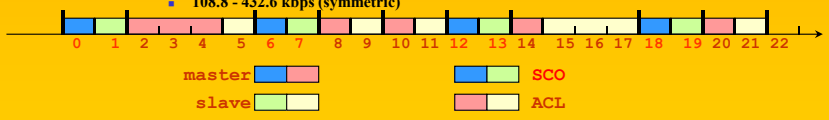
Baseband in Bluetooth

- **Manages physical channels and logical lines**
  - **Controls device addressing, channel control, power-saving operations, and flow control and synchronization among devices**
  - **Implements TDD aspects: master and slave switch in communications**
- **Works closely with Link controller:**
  - **Manages link (a)synchronism**
  - **Controls paging and inquiries**
  - **Controls power save modes**

105

Baseband link types

- **Polling-based (TDD) frame 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 frame assignment**
  - **symmetric 64Kbps full-duplex**
- **Asynchronous connection-less (ACL) link**
  - **Frame switching**
  - **asymmetric bandwidth**
    - **variable frame size (1-5 slots)**
      - **max. 721 kbps (57.6 kbps return channel)**
      - **108.8 - 432.6 kbps (symmetric)**



106

Baseband no Bluetooth

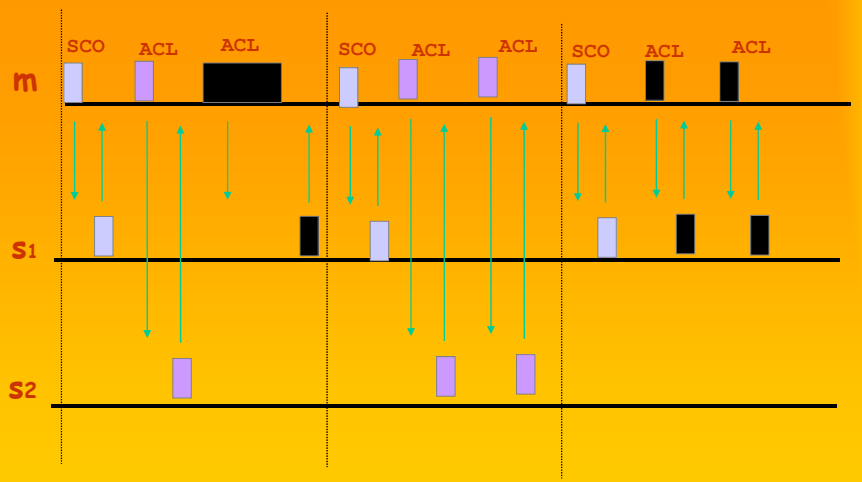
SYNCHRONOUS CONNECTION-ORIENTED (SCO) LINK

- Circuit switching
- Point to point, symmetric and synchronous services
- Slot reservation at fixed time intervals.
- Master can control 3 SCO channels
- Slave can receive 3 SCO to same master, 2 SCO to different masters
- Packets are never retransmitted
- Usually for 64Kb/s connections (voice)

ASYNCHRONOUS CONNECTION-LESS (ACL) LINK

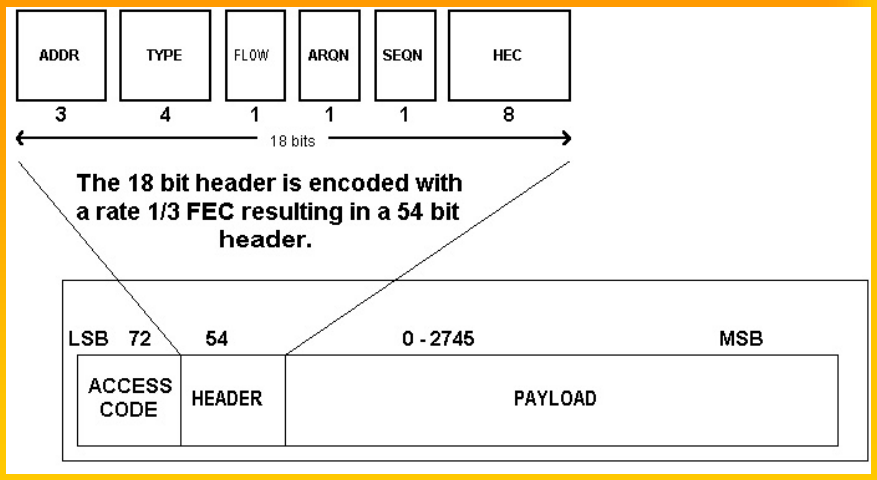
- Packet switching
- Asymmetric and asynchronous services
- Polling
- Only one link allower

Mixed Link Example



108

Baseband Packet

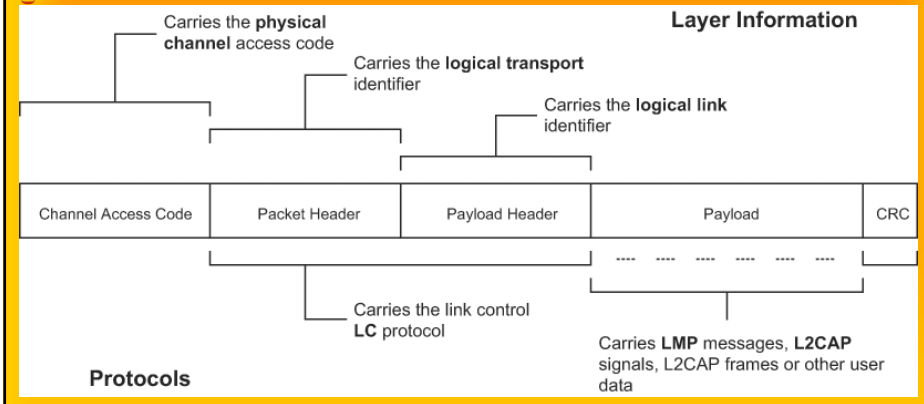


109

Baseband Frame

- **Access Code: time synchronization, offset, paging, inquiry.**
  - **Channel Access Code (CAC), piconet identification, synchronization, DC offset.**
  - **Device Access Code (DAC), paging and replies.**
  - **Inquiry Access Code (IAC), inquiries (GIAC, general; DIAC, dedicated)**
- **Header: packet acknowledgement and numbering, flow control, slave address, error checking**
- **Payload: voice, data or both (DV packets).**
  - **When data, the payload has additional internal header**

Bluetooth Frame Structure



ACCESS CODE - based on identity and system clock of Master

Provides means for synchronization; Unique for channel;

Used by all frames on the channel

111

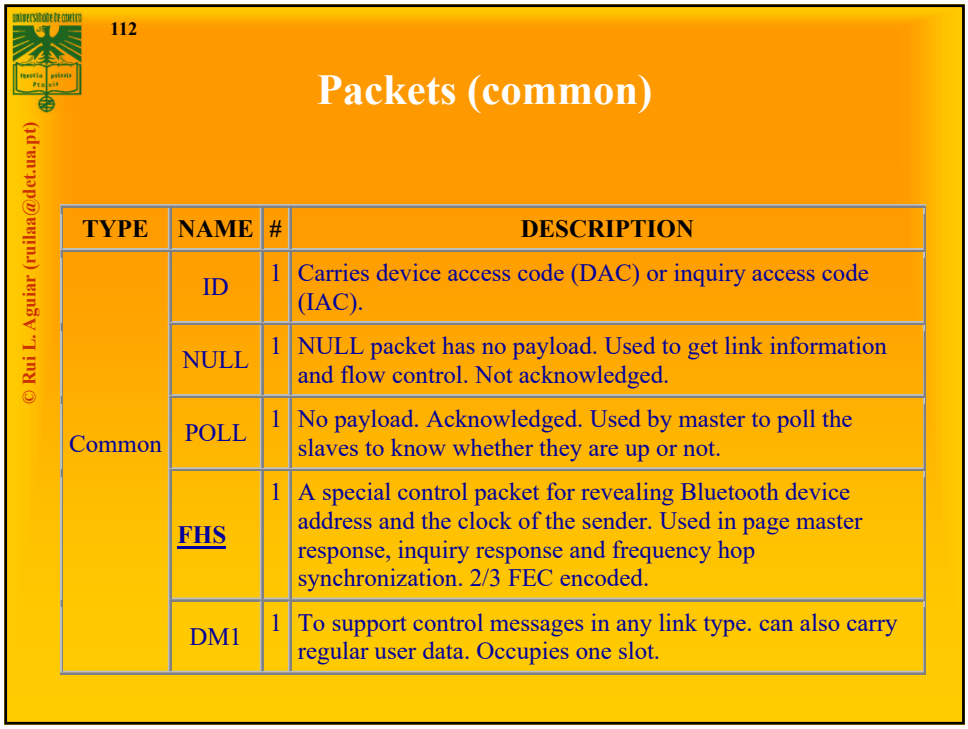
Packet types and transmission rates

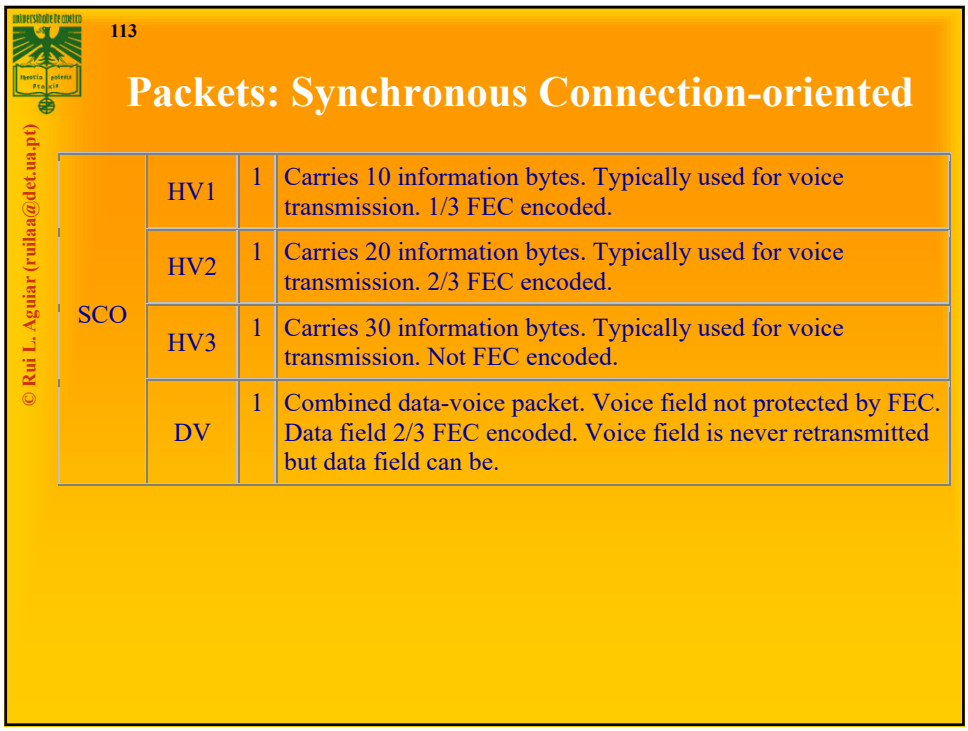
Packet types

Segments	Type	SCO line	ACL line
1	0000	NULL	NULL
	0001	POLL	POLL
	0010	FHS	FHS
	0011	DM1	DM1
2	0100		DH1
	0101	HV1	
	0110	HV2	
	0111	HV3	
	1000	*DV*	
	1001		AUX1
3	1010		DM3
	1011		DH3
	1100		
	1101		
4	1110		DM5
	1111		DH5

Transmission rate (Kbps)

Type	symetric	assymetric	
DM1	108.8	108.8	108.8
DH1	172.8	172.8	172.8
DM3	256.0	384.0	54.4
DH3	384.0	576.0	86.4
DM5	286.7	477.8	36.3
DH5	432.6	721.0	57.6


112
Packets (common)
TYPE
NAME
#
DESCRIPTION
Common
ID
1
Carries device access code (DAC) or inquiry access code (IAC).
NULL
1
NULL packet has no payload. Used to get link information and flow control. Not acknowledged.
POLL
1
No payload. Acknowledged. Used by master to poll the slaves to know whether they are up or not.
FHS
1
A special control packet for revealing Bluetooth device address and the clock of the sender. Used in page master response, inquiry response and frequency hop synchronization. 2/3 FEC encoded.
DM1
1
To support control messages in any link type. can also carry regular user data. Occupies one slot.
© Rui L. Aguiar (ruilaa@det.ua.pt)


113
Packets: Synchronous Connection-oriented
SCO
HV1
1
Carries 10 information bytes. Typically used for voice transmission. 1/3 FEC encoded.
HV2
1
Carries 20 information bytes. Typically used for voice transmission. 2/3 FEC encoded.
HV3
1
Carries 30 information bytes. Typically used for voice transmission. Not FEC encoded.
DV
1
Combined data-voice packet. Voice field not protected by FEC. Data field 2/3 FEC encoded. Voice field is never retransmitted but data field can be.
© Rui L. Aguiar (ruilaa@det.ua.pt)

114

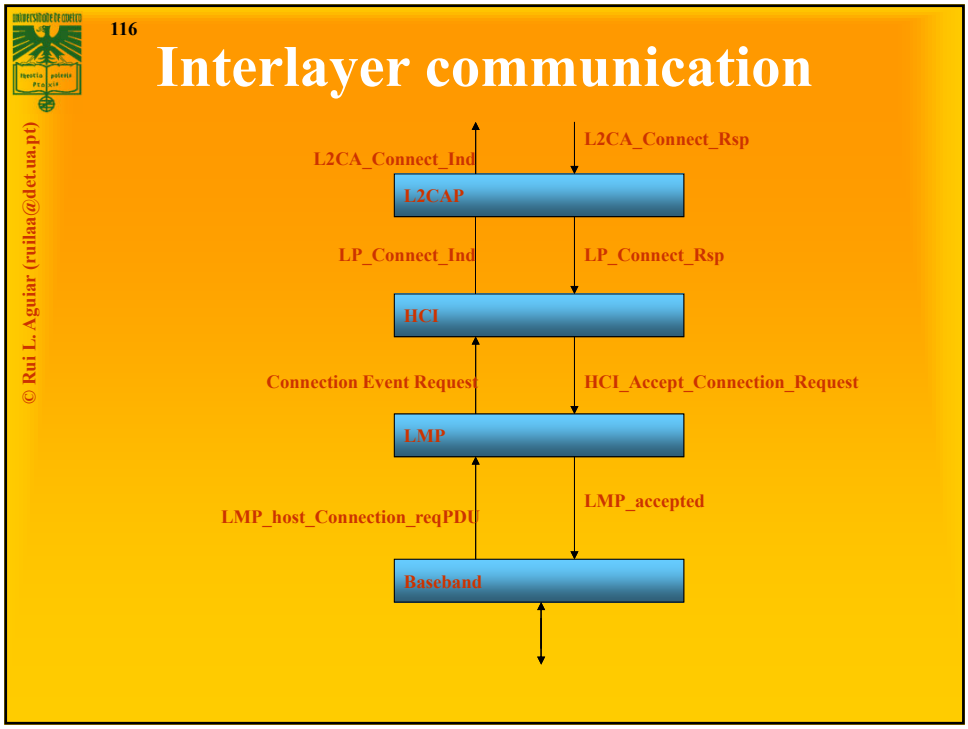
Packets : Assynchronous Connection-Less

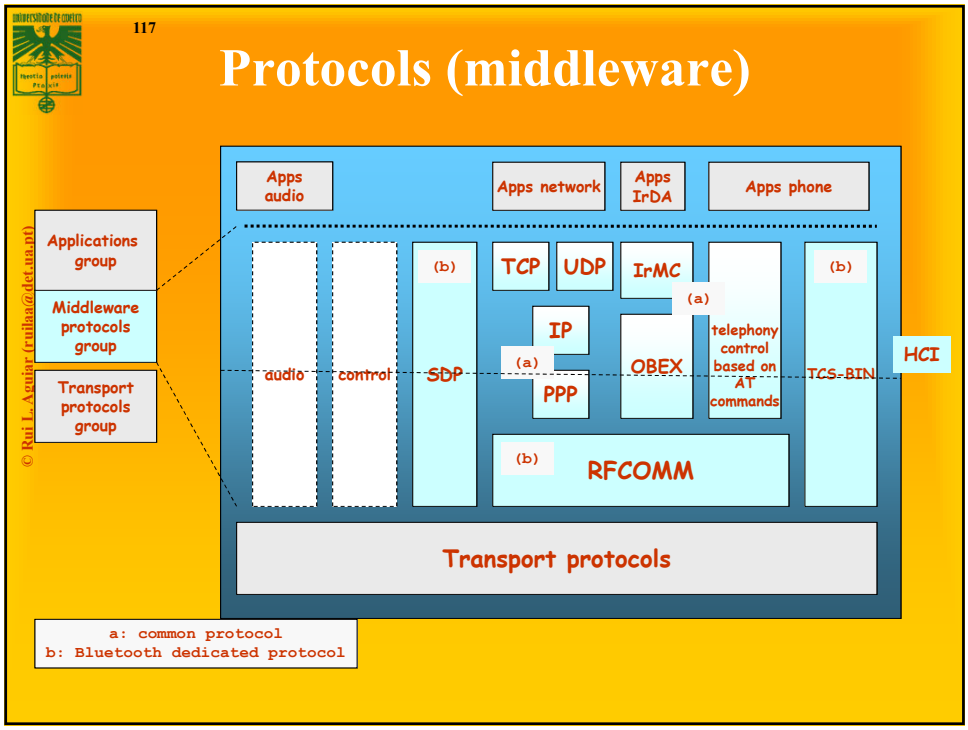
ACL	DM1	1	Carries 18 information bytes. 2/3 FEC encoded.
	DH1	1	Carries 28 information bytes. Not FEC encoded.
	DM3	3	Carries 123 information bytes. 2/3 FEC encoded.
	DH3	3	Carries 185 information bytes. Not FEC encoded.
	DM5	5	Carries 226 information bytes. 2/3 FEC encoded.
	DH5	5	Carries 341 information bytes. Not FEC encoded.
	AUX1	1	Carries 30 information bytes. Resembles DH1 but no CRC code.

115

Adaptation protocols

- **Link Manager**
  - **carries out link setup, above baseband, with authentication, link configuration and other protocols**
    - Support protocol multiplexing
      - BT may support other protocols besides IP
    - Segmenting and reassembly
- **Link Layer Control & Adaptation (L2CAP)**
  - **Link control protocol, provides connection-oriented and connectionless data services to upper layer protocols**
    - Handles ACL and SCO connections
    - Handle QoS specifications per connection (logical channel)
    - Manages concepts as “group of connections”
- **Host Controller Interface (HCI)**
  - **Allows command line access to the baseband layer and LM for control and status information**
    - Current interfaces: USB; UART; RS-232
  - **Made up of three parts:**
    - HCI firmware, HCI driver, Host Controller Transport Layer


116
Interlayer communication
© Rui L. Aguiar (ruilaa@det.ua.pt)
L2CA_Connect_Ind
L2CA_Connect_Rsp
L2CAP
LP_Connect_Ind
LP_Connect_Rsp
HCI
Connection Event Request
HCI_Accept_Connection_Request
LMP
LMP_host_Connection_reqPDU
LMP_accepted
Baseband


117
Protocols (middleware)
© Rui L. Aguiar (ruilaa@det.ua.pt)
Applications group
Middleware protocols group
Transport protocols group
Apps audio
Apps network
Apps IrDA
Apps phone
audio
control
(b)
SDP
TCP
UDP
IrMC
(a)
IP
(a)
PPP
OBEX
telephony control based on AT commands
(b)
TCS-BIN
HCI
(b)
RFCOMM
Transport protocols
a: common protocol
b: Bluetooth dedicated protocol

118

Middleware

- **Service Discovery Protocol (SDP)**
  - **Provides a way for application to detect which services are available and their characteristics**
  - **Protocol question ⇔ answer**
    - (search and browsing of services)
  - **Defines a format for service registry**
    - Information provided by the service *atributes,* a name (ID) + value
    - IDs can be universal (UUID)
- **Protocol reusage**
  - **BT aims to reuse older protocols (e.g. WAP, OBEX–IrDA)**
    - Interaction with applications and phones, as commonly done before

119

Middleware

- **RFCOMM**
  - **Based on GSM TS07.10**
  - **Emulates a serial port, supporting all traditional applications that were able to use a serial port.**
  - **Supports multiple ports over a single physical channel between two devices.**
- **Telephony Control Protocol Spec (TCS)**
  - **Handles call control (setup, release)**
  - **Group management for gateways, serving multiple devices**
    - Audioconference, e.g.

120

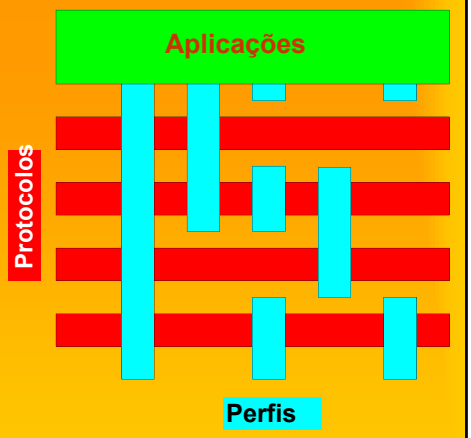
Outline

- Bluetooth networks
- Piconet operation
  - Inquiry
  - Paging
- Bluetooth stack
- **Profiles and security**
- 802.15.x

121

Interoperability: Profiles

- **Profile: base for BT interoperability (BT too much flexible!)**
- **"vertical cut" in Bluetooth stack**
- **A given usage model ↔ typical solution**
- **Each BT device supports one or more profiles**



122

Profiles (v.1)

- **Generic Access**
  - **Profile SDA**
    (service discovery application)
  - **Profiles for serial port, including:**
    - Profile Dial-up
    - Profile Fax
    - Profile headset
    - LAN Access (uses PPP)
    - Profile for generic object exchange (OBEX)
      - File transfer
      - Data synchronization
      - Push-pull
- **Profile of coordless phone(TCS_BIN)**
  - **Profile interphone**
  - **Profile Cordless Telephony**

123

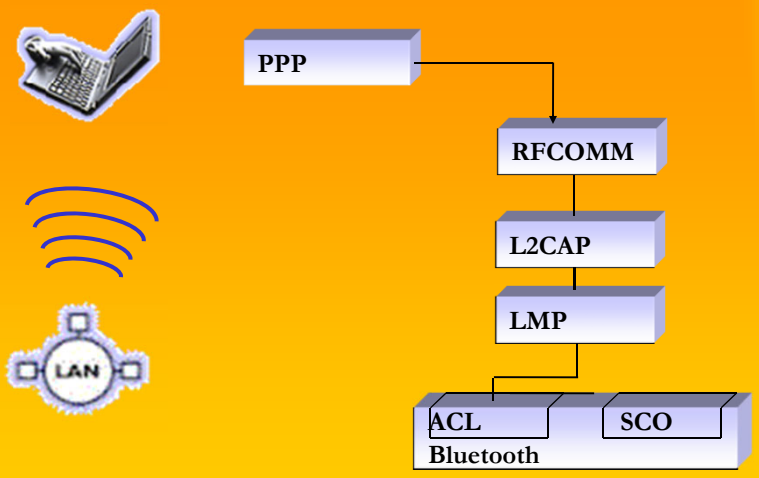
Profiles (v.2)

- **Radio 2 (next generation radio)**
  Compatible with existing systems
- **Car Profile**
- **PAN Profile**
- **GPS Profile**
- **Printing Profile**
- **Still image Profile**

(globally better facilitie in audio/voice/video)
(better service discovery)
(improved human interfaces)
(improved interoperation with other devices at the 2.4GHz ISM)

126

Example: LAN Access Point



127

Illustration of BT evolution (headset profile)

Specifications	Bluetooth 1.1	Bluetooth 1.2	Bluetooth 2.0	Bluetooth 2.1 plus EDR (Enhanced Data Rate)
Voice dialing	Yes	Yes	Yes	Yes
Call mute	Yes	Yes	Yes	Yes
Last-number redial	Yes	Yes	Yes	Yes
Improved resistance to radio frequency interference	-	Yes	Yes	Yes
10-meter range	Yes	Yes	Yes	Yes
100-meter range	-	-	Yes	Yes
Fast transmission speeds	-	-	Yes	Yes
Lower power consumption	-	-	Yes	Yes
Improved pairing (without a PIN)	-	-	-	Yes
Greater security	-	Yes	Yes	Yes

Bluetooth Spec Evolution (BT classic)

Specifications	1.1	1.2	2.0 + EDR	2.1 + EDR	3.0 +HS	4.0
Adopted	**2002**	**2005**	**2004**	**2007**	**2009**	**2010**
Transmission Rate	723.1 kbps	723.1 kbps	2.1 Mbps	3 Mbps	24 Mbps	25 Mbps
Standard PAN Range	10 m	10 m	10 m	10 m	10 m	50 m
Improved Pairing (without a PIN)				Yes	Yes	Yes
Improved Security		Yes	Yes	Yes	Yes	Yes
NFC Support			Yes	Yes	Yes	Yes
Voice Dialing	Yes	Yes	Yes	Yes	Yes	Yes
Call Mute	Yes	Yes	Yes	Yes	Yes	Yes
Last-Number Redial	Yes	Yes	Yes	Yes	Yes	Yes
Fast Transmission Speeds			Yes	Yes	Yes	Yes
Lower Power Consumption			Yes	Yes	Yes	Yes
Bluetooth Low Energy						Yes

149

Bluetooth 4.0: Low Energy

150

What are the USE CASES for BT 4.0?

- Proximity
- Time
- Emergency
- Network availability
- Personal User Interface
- Simple remote control
- Browse over Bluetooth
- Temperature Sensor
- Humidity Sensor
- HVAC
- Generic I/O (automation)
- Battery status
- Heart rate monitor
- Physical activity monitor
- Blood glucose monitor
- Cycling sensors
- Pulse Oximeter
- Body thermometer

151

Short range wireless application areas

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS	x	Y	Y	x	x
Bluetooth SCO/eSCO	Y	x	x	x	x
Bluetooth low energy (BLE)	x	x	x	x	Y
Wi-Fi	(VoIP)	Y	Y	Y	x
Wi-Fi Direct	Y	Y	Y	x	x
ZigBee	x	x	x	x	Y

State =
low bandwidth, average/low latency data
Low Power

152

How much energy does traditional Bluetooth use?

- **Traditional Bluetooth is *connection oriented*. When a device is connected, a link is maintained, even if there is no data flowing.**
- **Sniff modes allow devices to sleep, reducing power consumption to give months of battery life**
- **Peak transmit current is typically around 25mA**
- **Even though it has been independently shown to be lower power than other radio standards, it is still not low enough power for coin cells and energy harvesting applications**

153

What is Bluetooth Low Energy?

- **Bluetooth low energy is a open, short range radio technology**
  - **Blank sheet of paper design**
  - **Different to Bluetooth classic (BR/EDR)**
  - **Optimized for ultra low power**
  - **Enable coin cell battery use cases**
    - < 20mA peak current
    - < 5 uA average current

154

Basic Concepts of Bluetooth 4.0

- **Everything is optimized for lowest power consumption**
  - **Short packets reduce TX peak current**
  - **Short packets reduce RX time**
  - **Less RF channels to improve discovery and connection time**
  - **Simple state machine**
  - **Single protocol**
  - **Etc.**

155

Bluetooth low energy factsheet

Range:	**~ 150 meters open field**
Output Power:	~ 10 mW (10dBm)
Max Current:	**~ 15 mA**
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current:	**~ 1µA**
Modes:	Broadcast, Connection, Event Data Models, Reads, Writes

157

Designed for exposing state

PLAY >>

23.2˚C

12:23 pm

3.2 kWh

Gate 10 BOARDING

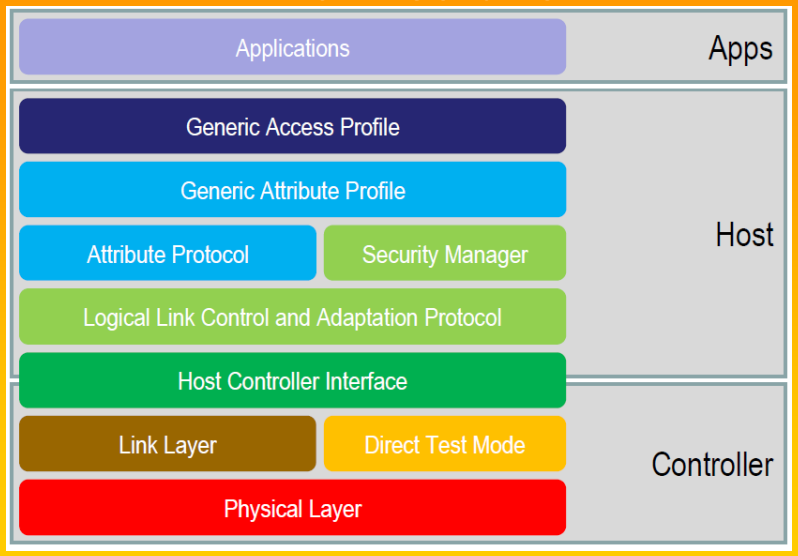
- **Data Throughput**
  - **Data throughput is not a meaningful parameter. It does not support streaming.**
  - **Data rate (typical) = 1Mbps, but is not optimized for file transfer.**
  - **Designed for sending small chunks of data (expos**
    - It's good at small, discrete data transfers.
    - Data can triggered by local events.
    - Data can be read at any time by a client.
    - Interface model is very simple (GATT)

Network Available

60.5 km/h

158

Bluetooth Low Energy Architecture



159

Device Modes

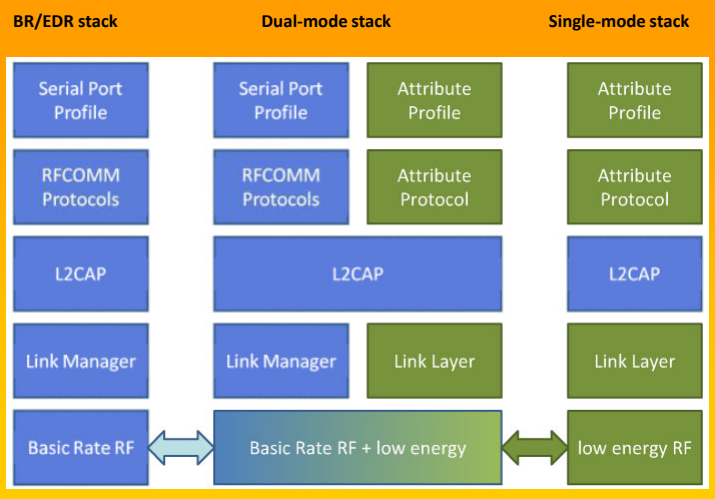
- **Dual Mode**
  - **Bluetooth BR/EDR and LE**
  - **Used anywhere that BR/EDR is used today**

- **Single Mode**
  - **Implements only Bluetooth low energy**
  - **Will be used in new devices / applications**

160

Device Modes

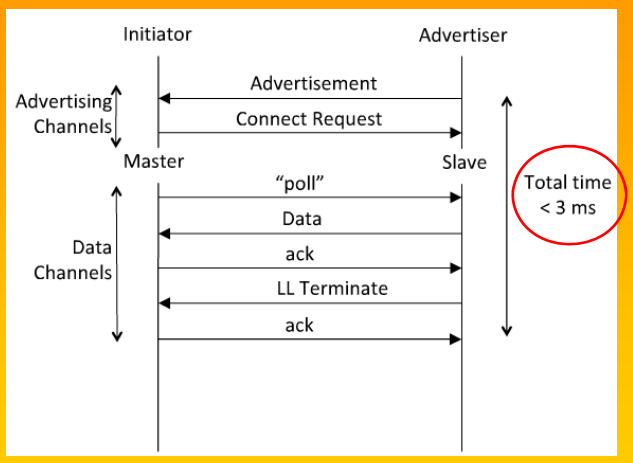
- **Dual mode + single modes**



164

Link Layer Connection

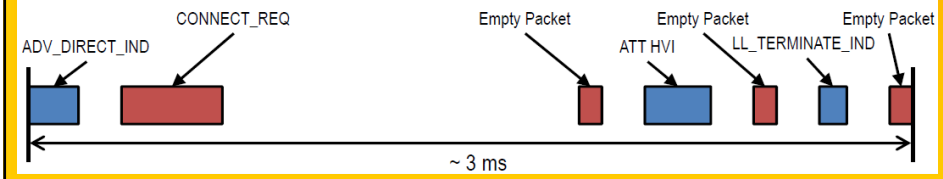
- **Very low latency connection**



165

Time From Disconnected to Data ~ 3ms

Time (us)	Master Tx	Radio Active (us)	Slave Tx
0		176	ADV_DIRECT_IND
326	CONNECT_REQ	352	
1928	Empty Packet	80	
2158		144	Attribute Protocol Handle Value Indication
2452	Empty Packet (Acknowledgement)	80	
2682		96	LL_TERMINATE_IND
2928	Empty Packet (Acknowledgement)	80	



166

How low can the energy get?

- From the previous slide, calculate energy per transaction
  - Assume an upper bound of 3ms per minimal transaction
  - Estimated TX power is 15mW (mostly TX power amp for 65nm chips)
  - For 1.5v battery, this is 10mA. 0.015W * 0.003 sec = 45 micro Joule
- How long could a sensor last on a battery?
  - An example battery: Lenmar WC357, 1.55v, 180mAh, $2-5
  - 180mAh/10mA = 18Hr = 64,800 seconds = 21.6M transactions
  - Suppose this sensor sends a report every minute = 1440/day
  - For just the BT LE transactions, this is 15,000 days, or > 40 years
  - This far exceeds the life of the battery and/or the product
- This means that battery will cost more than the electronics
  - This sensor could run on scavenged power, e.g. ambient light

BLE and GAP

- **Generic Access Profile (GAP)**
  - **GAP defines a base profile which all Bluetooth devices implement, which ties all the various layers together to form the basic requirements for a Bluetooth device**
  - **GAP also defines generic procedures for connection-related services:**
    - Device Discovery
    - Link Establishment
    - Link Management
    - Link Termination
    - Initiation of security features

BLE and GAP

- **The GAP layer works in one of four profile roles:**
  - **Broadcaster: an advertiser that is non-connectable**
  - **Observer: scans for advertisements, but cannot initiate connections**
  - **Peripheral: an advertiser that is connectable and can operate as a slave in a single link layer connection**
  - **Central: scans for advertisements and initiates connections; operates as a master in a single or multiple link layer connections**

BLE and GAP

Temperature Sensor (Broadcaster) → Temperature Display (Observer)

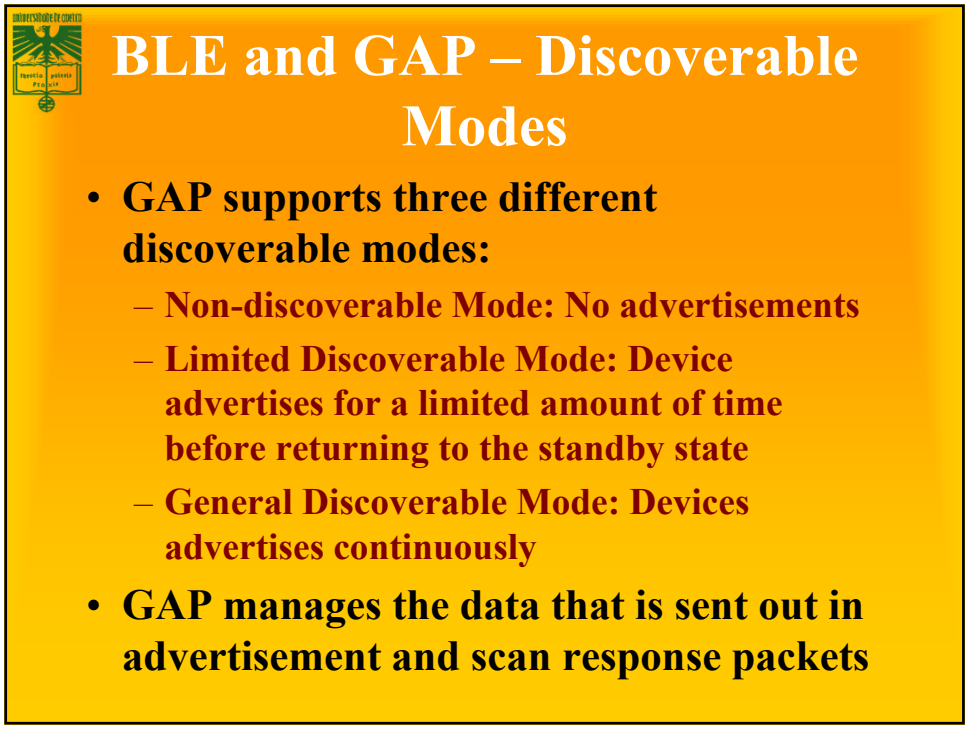
Figure 1 – Temperature Sensor (Broadcaster)

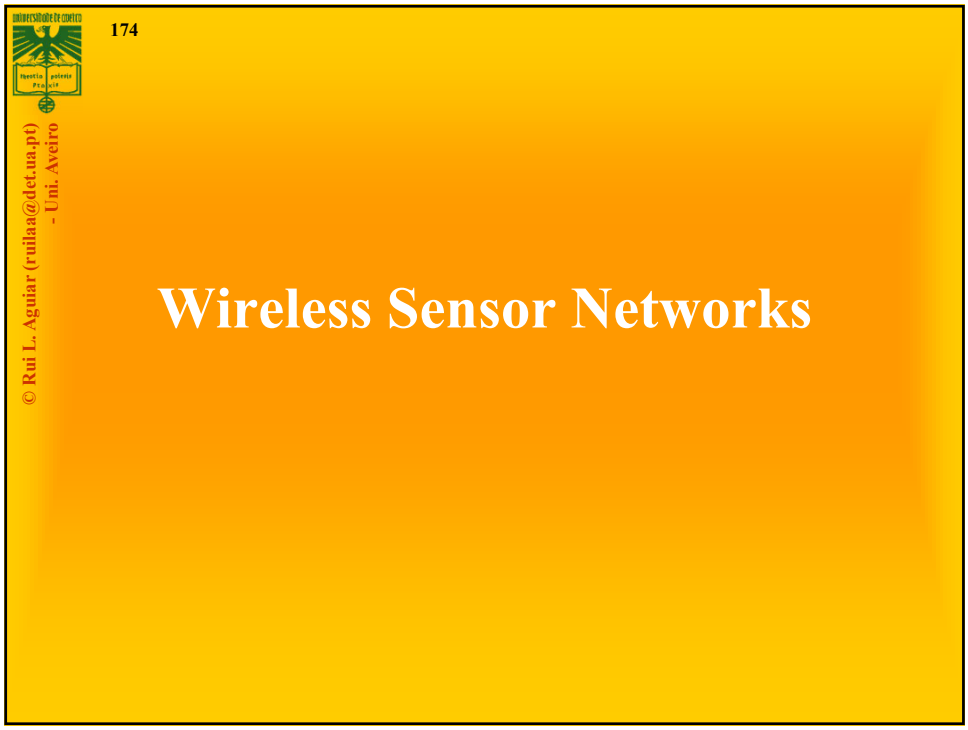
Figure 2 – Temperature Display (Observer)

Watch (Peripheral) ← → Mobile Phone (Central)

Figure 3 - Watch (Peripheral)

Figure 4 – Mobile Phone (Central)


BLE and GAP – Discoverable Modes
• GAP supports three different discoverable modes:
– Non-discoverable Mode: No advertisements
– Limited Discoverable Mode: Device advertises for a limited amount of time before returning to the standby state
– General Discoverable Mode: Devices advertises continuously
• GAP manages the data that is sent out in advertisement and scan response packets


174
© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro
Wireless Sensor Networks

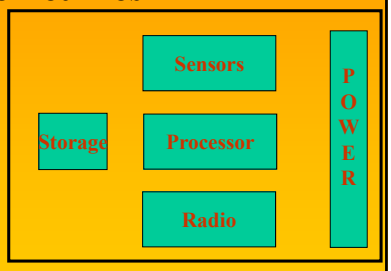
What are wireless sensor networks (WSNs)?

- A wireless sensor network (WSN) is a wireless network using sensors to cooperatively monitor physical or environmental conditions
- Networks of typically small, battery-powered, wireless devices (often MANY, sometimes heterogeneous)
  - On-board processing,
  - Communication, and
  - Sensing capabilities.

Or…

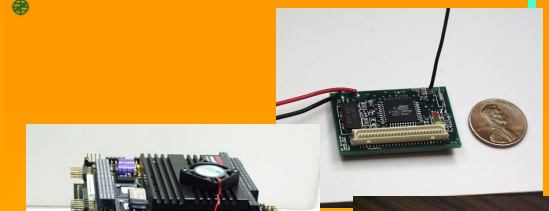
➢ Wireless sensing + Data Networking!

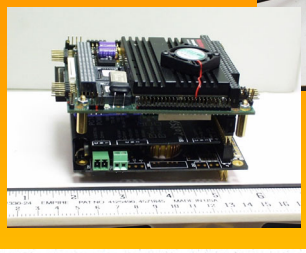
  ➢ Group of sensors linked by wireless media to perform distributed sensing tasks

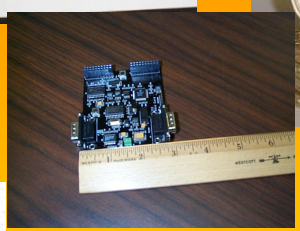


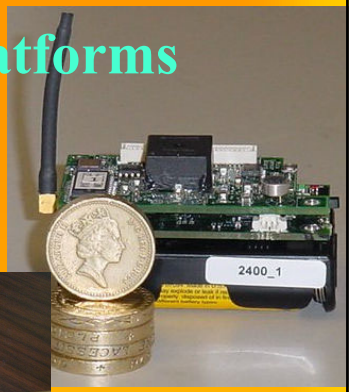
WSN device schematics

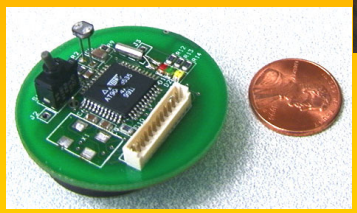
Sensor Nodes and platforms







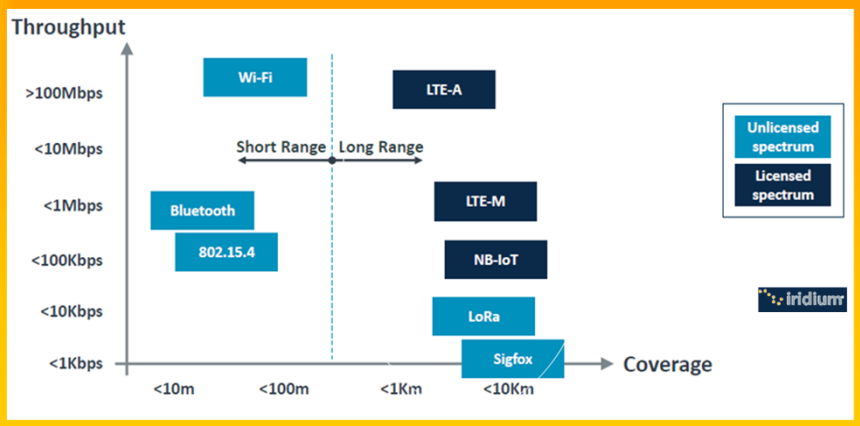




178

IoT Wireless Connectivity

As with wireless in general, multiple standards with different properties



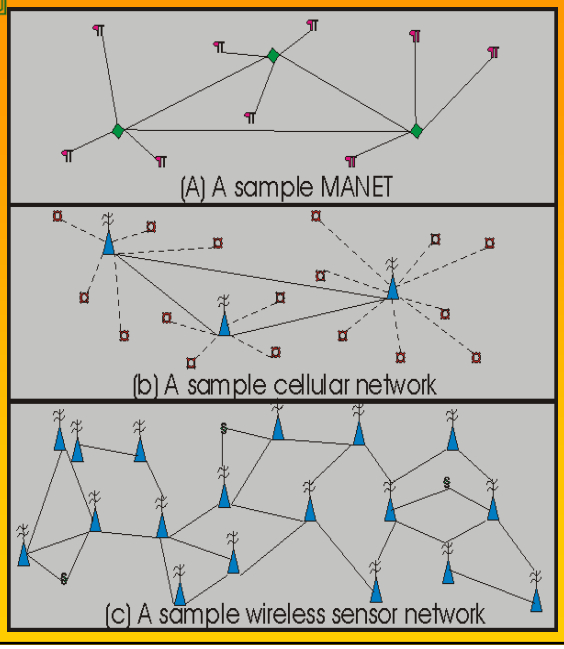
179

MIoT and HIoT are different

- **IoT has multiple scenarios, from human-oriented to machine-oriented, and from industrial to forest environments**
- **WSN need to adapt to these environments.**

	Manufacturing IoT	Consumer IoT
Goal	Manufacturing-industry Centric	Consumer Centric
Devices	Machines, Sensors, Controllers, Actuators, Smart meters	Consumer devices and Smart appliances
Working Environment	Harsh (vibration, noisy, extremely high/low temperature)	Moderate
Data rate	High (usually)	Low or average
Delay	Delay sensitive	Delay tolerant
Mission	Mission-critical	Non-mission-critical

Types of wireless Networks

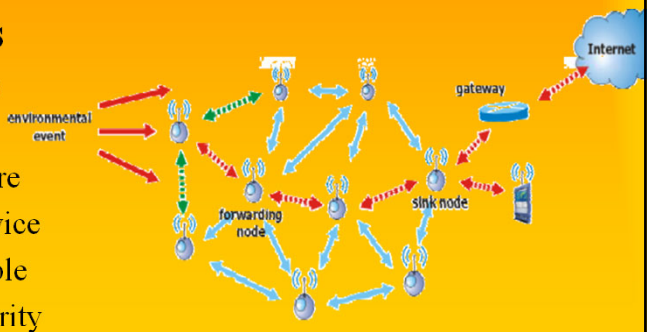


WSN can explore the architecture and protocol concepts both of MANETs (mobile ad-hoc networks) and of celular networks.

181

Wireless Sensor Network

- **Focus on:**
  - Ubiquitous Computing
  - Ubiquitous Network Society
  - (often) Human-centric
- **Ubiquitous**
  - Anytime
  - Anyone
  - Anywhere
  - Any Device
  - Affordable
  - All Security
  - Any Information/Service



MAC: challenges for wireless networking

- MAC is a critical layer for networking
- Traditional problems
  - Fairness
  - Latency
  - Throughput
- For Sensor Networks, added
  - Power efficiency
  - Scalability

MAC challenges for WSN

- Sensor networks are deployed in an ad hoc fashion, with individual nodes remaining largely inactive for long periods of time, but then becoming suddenly active when something is detected.
- These characteristics of sensor networks and applications motivate a MAC that is different from traditional wireless MACs :
  - Energy conservation and self-configuration are primary goals.
  - Per-node fairness and latency are less important.

Challenges in WSN's

- Energy and Power Consumption
- Self-organization
- Communication Heterogeneity
- Adaptability
- Security
- Scalability

Design Challenges

Why are WSNs challenging/unique?

- **Typically, severely energy constrained.**
  - **Limited energy sources (e.g., batteries).**
  - **Trade-off between performance and lifetime.**
- **Self-organizing and self-healing.**
  - **Remote deployments.**
- **Scalable.**
  - **Arbitrarily large number of nodes.**

Design Challenges

- **Heterogeneity.**
  - **Devices with varied capabilities.**
  - **Different sensors.**
  - **Hierarchical deployments.**
- **Adaptability.**
  - **Adjust to operating conditions and changes in application requirements.**
- **Security and privacy.**
  - **Potentially sensitive information.**
  - **Hostile environments.**

Sensor Network MAC Protocols

- **The major sources of energy wastage are:**
  - **Collisions** – *interfering packets*
  - **Overhearing** – *hearing more than required from a packet*
  - **Control packet overhead** – *control versus data*
  - **Idle listening** – *hearing for nothing*

Typical solutions in wireless MACs (compare LATER with WiFi)

- **Carrier Sensing**
  - **Only during low traffic load.**
- **Contention**
  - **RTS-CTS only during high traffic load.**
- **Backoff**
  - **Backoff in application layer is desired other than in MAC layer.**

Achieving good scalability and collision avoidance capability is necessary.

Challenges

1. Energy Efficiency:

- Sensor nodes are not connected to any energy source.
- Energy efficiency is a dominant consideration no matter what the problem is.
- Many solutions, both hardware and software related, have been proposed to optimize energy usage.

2. Ad hoc deployment (adaptability):

- Most sensor nodes are deployed in regions which have no infrastructure.
- We must cope with the changes of connectivity and distribution.

Challenges

3. Unattended operation:

- Generally, once sensors are deployed, there is no human intervention for a long time.
- Sensor network must reconfigure by itself when certain errors occur.

4. Dynamic changes (self-healing and scalability)

- As changes of connectivity due to addition of more nodes or failure of nodes, Sensor network must be able to adapt itself to changing connectivity, to arbitrary large numbers of nodes

5. Security

- Both Sensors and Actuators carry sensitive information in an hostile environment

Sensor-MAC (S-MAC)

- **S-MAC is a medium-access control (MAC) protocol designed for wireless sensor networks.**
  - **Explores typical solutions also found in many other sensor MACs.**
  - **Nodes periodically sleep, and sleep during other nodes transmissions**
    - Nearby nodes form virtual clusters to synchronize their wake-up and sleep periods
  - **Trades energy efficiency for lower throughput and higher latency**
    - Message passing is used to reduce the contention latency and control overhead