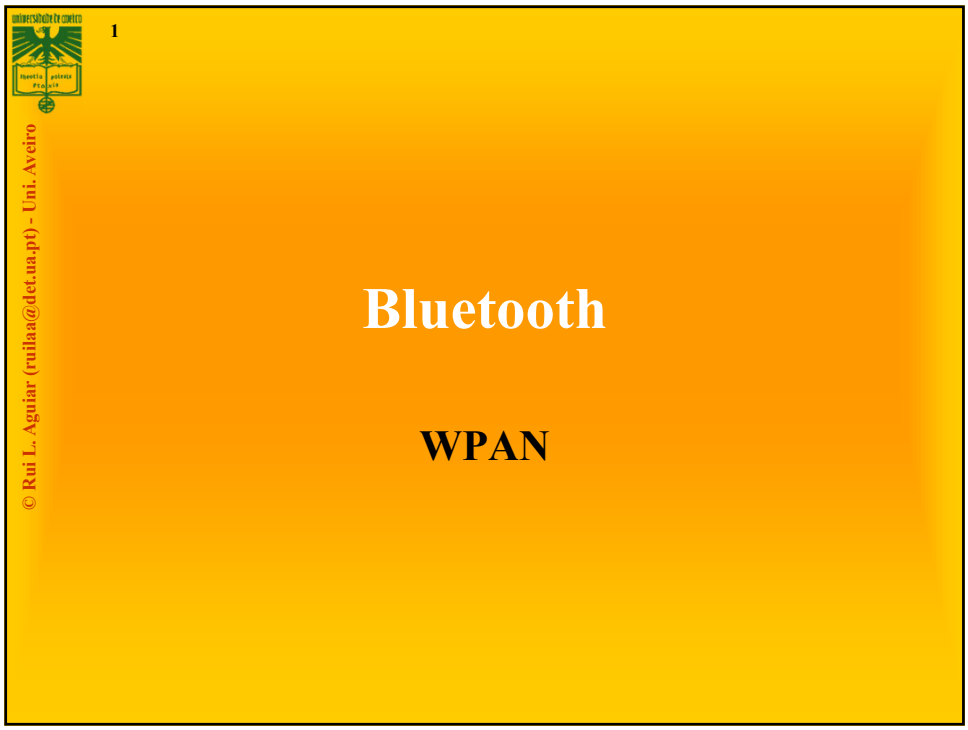
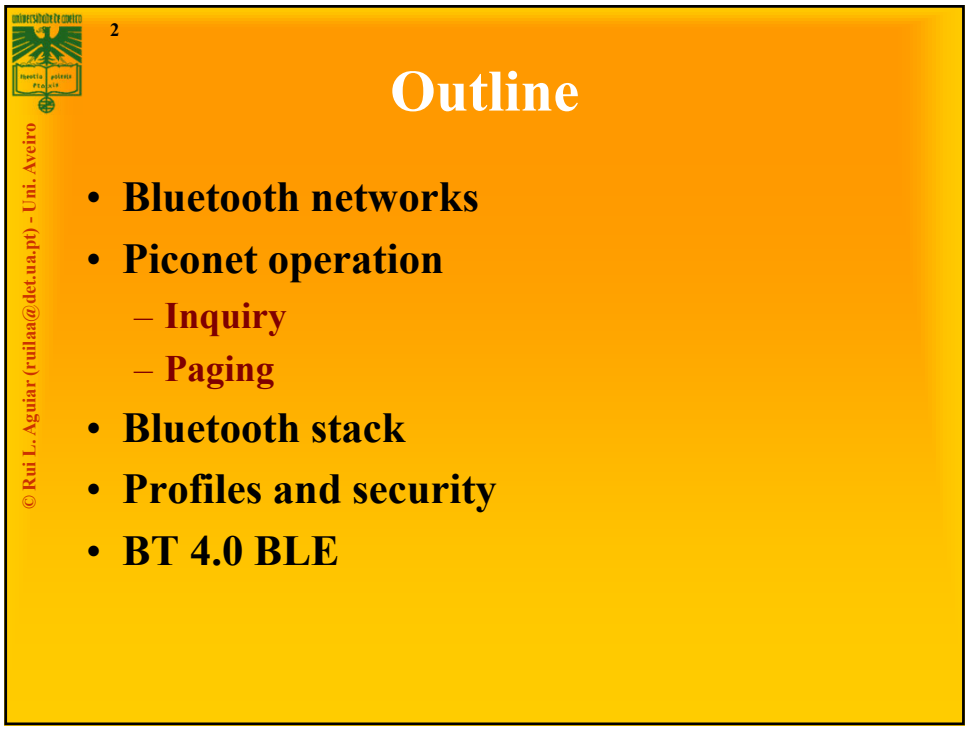
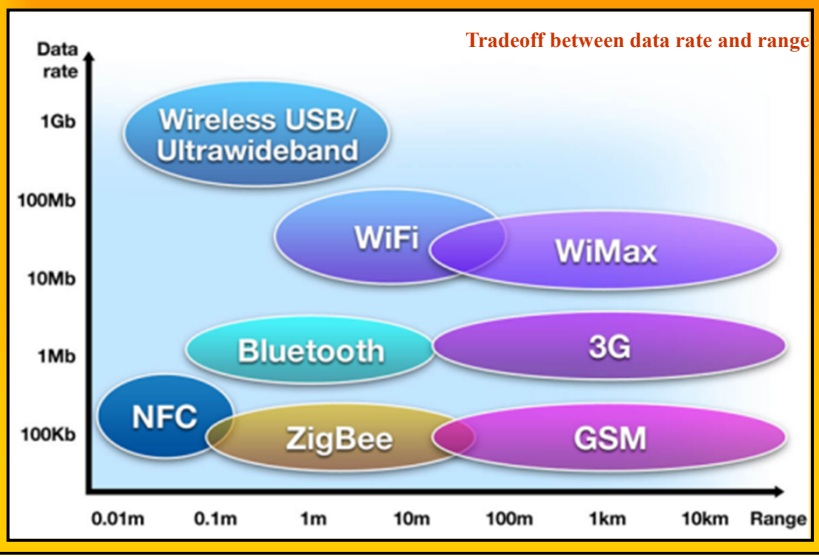

1
Bluetooth
WPAN
© Rui L. Aguiar (ruilaa@det.ua.pt) – Uni. Aveiro

1


2
Outline
• Bluetooth networks
• Piconet operation
– Inquiry
– Paging
• Bluetooth stack
• Profiles and security
• BT 4.0 BLE
© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro

2

Comparison Between Wireless Technologies



3

4

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

© Rui L. Aguiar (ruilaa@det.ua.pt)

4

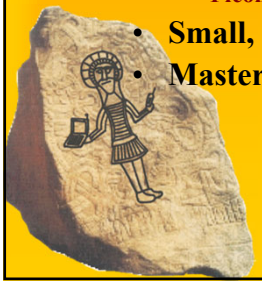
Personal Area Networks

- **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**

5

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

6

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.

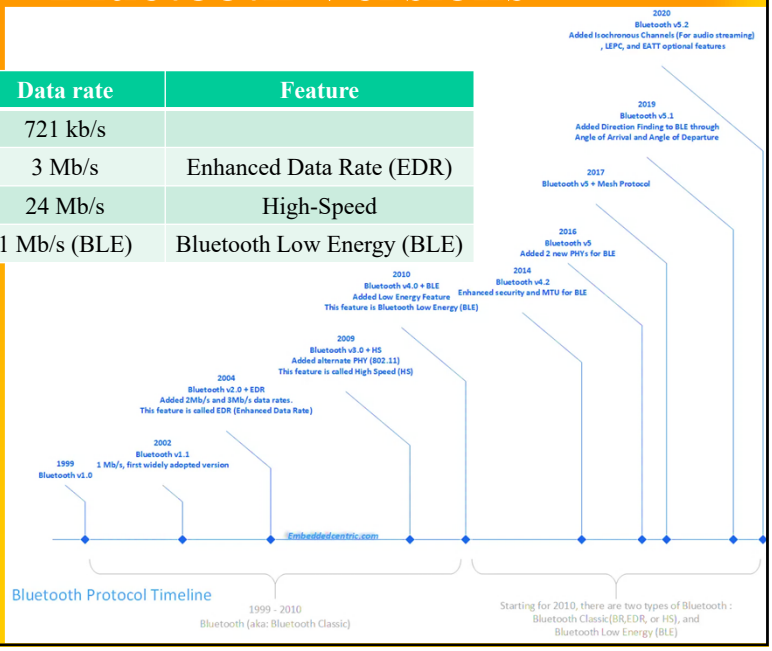
2009 - Bluetooth Core Specification Version 3.0 + HS (High Speed) is adopted by the BLUETOOTH SIG.

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

7

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)



8

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

9

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

10

11

Bluetooth features

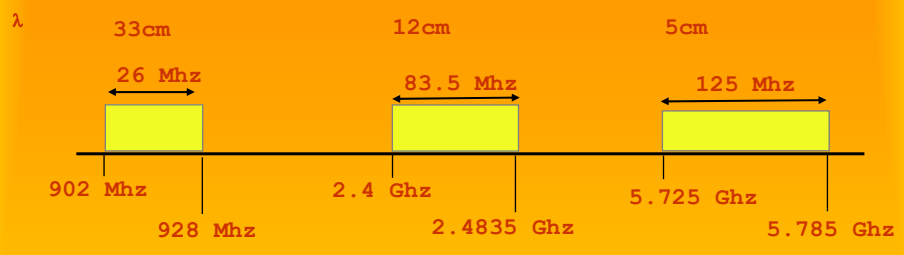
- Radio network, on the 2.4 GHz, world-wide!
- Airplane friendly!
- FH (Frequency Hopping) spread spectrum:
  79 (23 - .jp .es .fr) channels (de 2.402GHz - 2.480GHz)
- Defines a master that syncrhonizes everyone to his hop-pattern.
- Defines two types of networks:
  - piconets
  - scaternets
- Maximum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

© Rui L. Aguiar (ruilaa@det.ua.pt)

11

12

Unlicensed Radio Spectrum



cordless phones
baby monitors
Wireless LANs

802.11
Bluetooth
Microwave oven

unused

12

12

15

Bluetooth classic vs. cable

© Rui L. Aguiar (ruilaa@det.ua.pt)

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.

15

Bluetooth: more than a PAN!

17

18

Low power

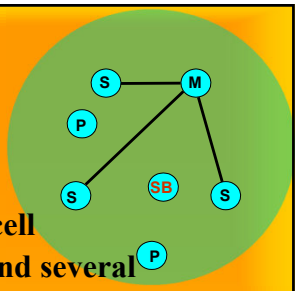
- **Global architecture for low power**
  - **Hold and Park mode: 60 µA current**
    - Connected device, but not operating
    - Device operates after a 2 ms wait process.
    - In Hold: keeps its AMA; in Park has to free AMA, and later has to claim it back
- **Transmission power ~1mW**
  - **100mW 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**

© Rui L. Aguiar (ruilaa@det.ua.pt)

18

19

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**
- **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**

P=Parked
SB=Standby

M=Master
S=Slave

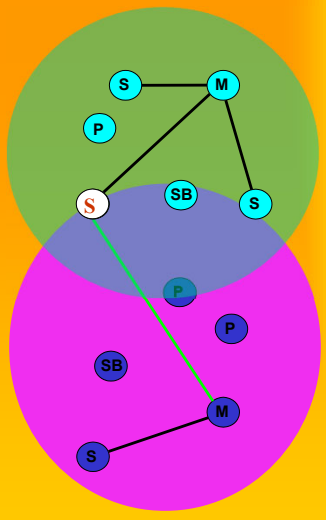
© Rui L. Aguiar (ruilaa@det.ua.pt)

19

20

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

© Rui L. Aguiar (ruilaa@det.ua.pt)

20

21

Outline

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

© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro

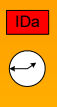
21

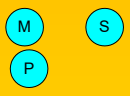
© Rui L. Aguiar (ruilaa@det.ua.pt)

22

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)**



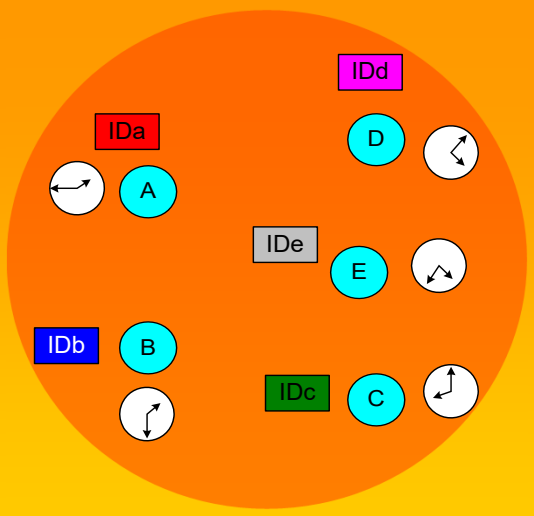


22

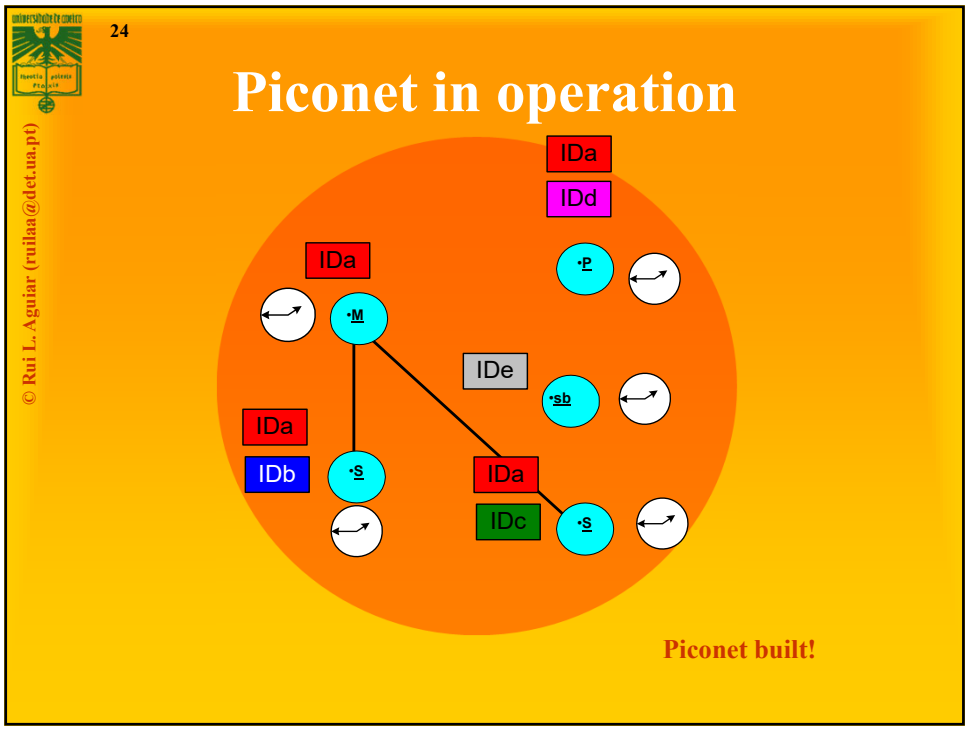
© Rui L. Aguiar (ruilaa@det.ua.pt)

23

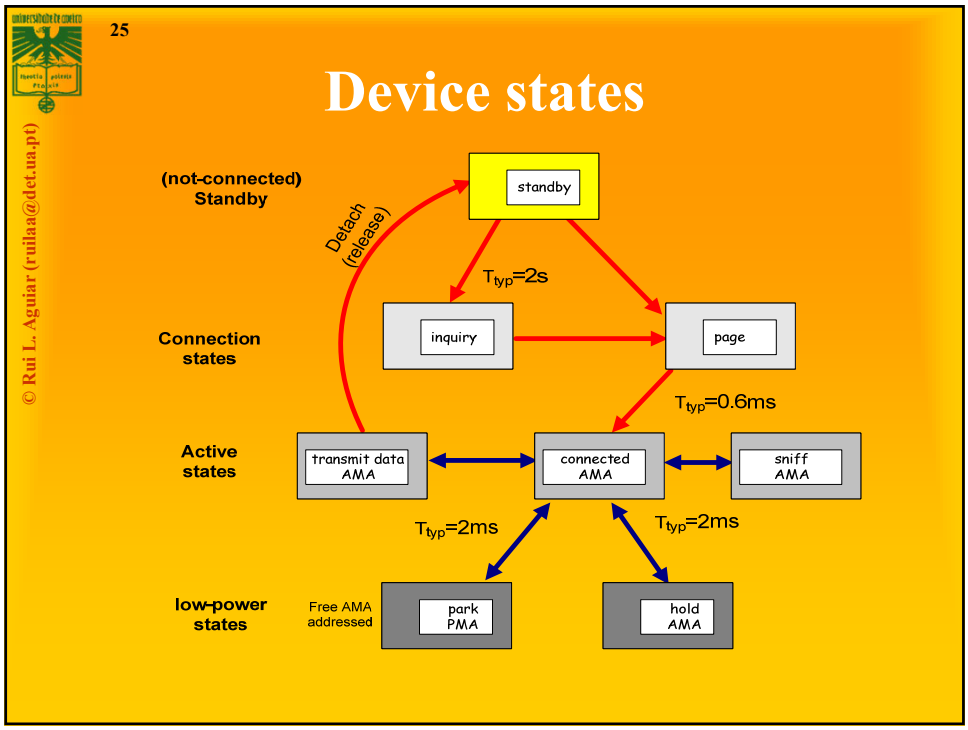
Piconet before setup



23

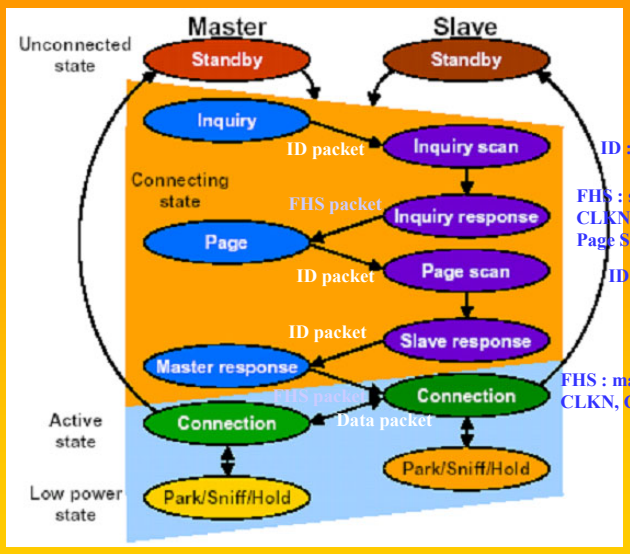

24
Piconet in operation
IDa
IDd
IDa
•P
•M
IDe
•sb
IDa
IDb
•S
IDa
IDc
•S
Piconet built!
© Rui L. Aguiar (ruilaa@det.ua.pt)

24


25
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)

25

Connection Procedure



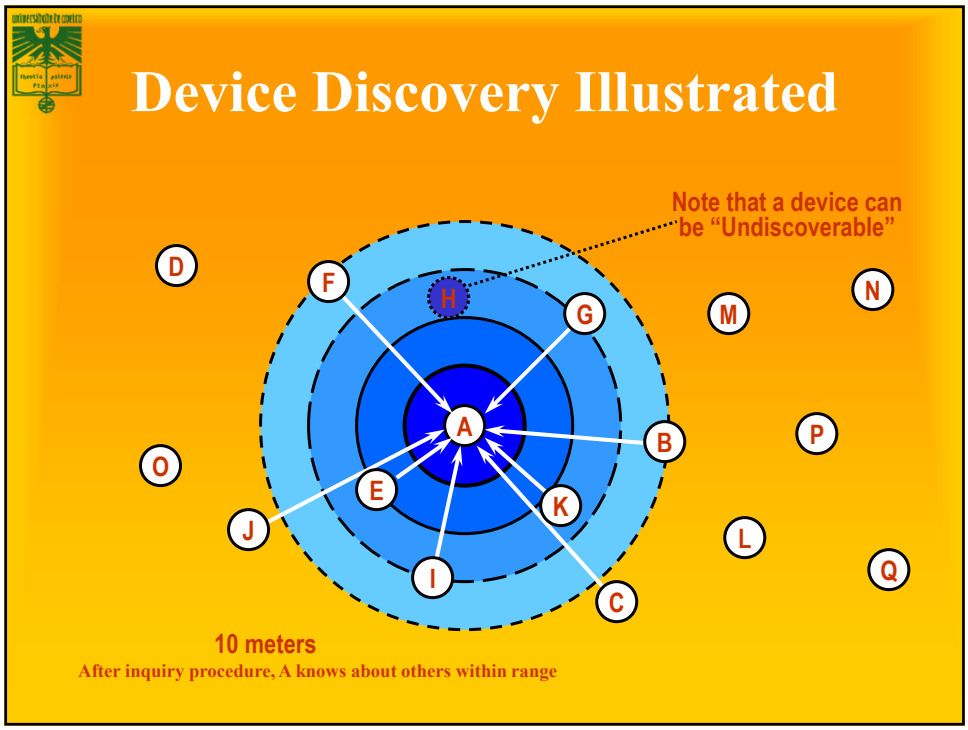
26

Low-Power Operation in BT classic

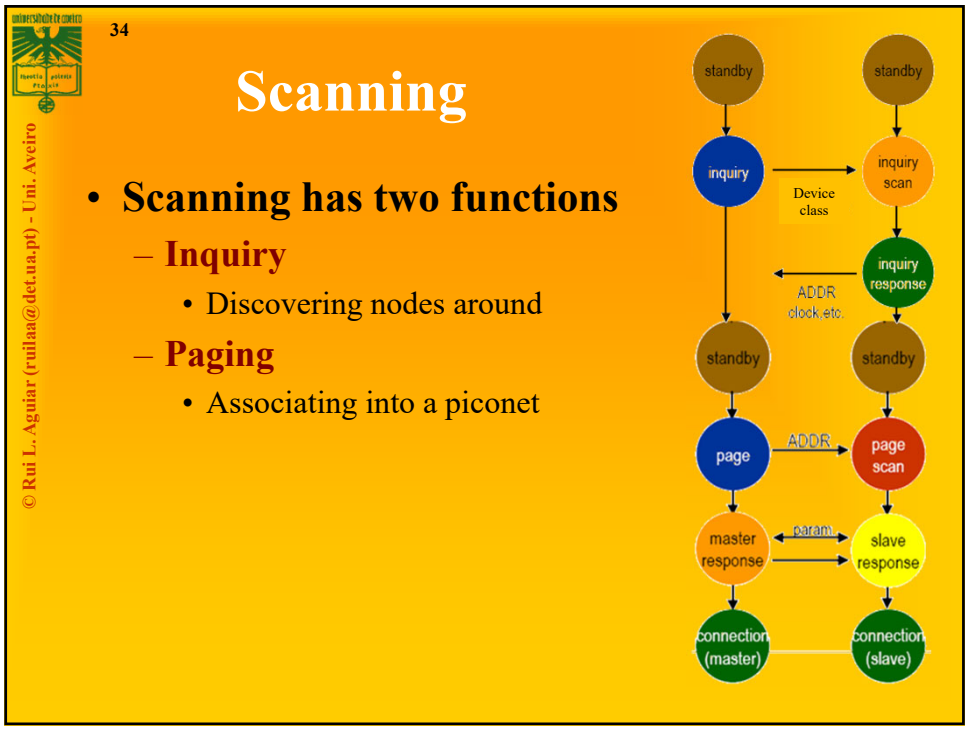
- **3 modes:**
  - **Hold: node sleeps for specified interval.**
    - Master can put slaves in hold while searching for new members, attending another piconet, etc.
    - No ACL packets.
  - **Sniff: slave low-duty cycle mode.**
    - Slave wakes up periodically to talk to master.
    - Fixed "sniff" 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.

32

32


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

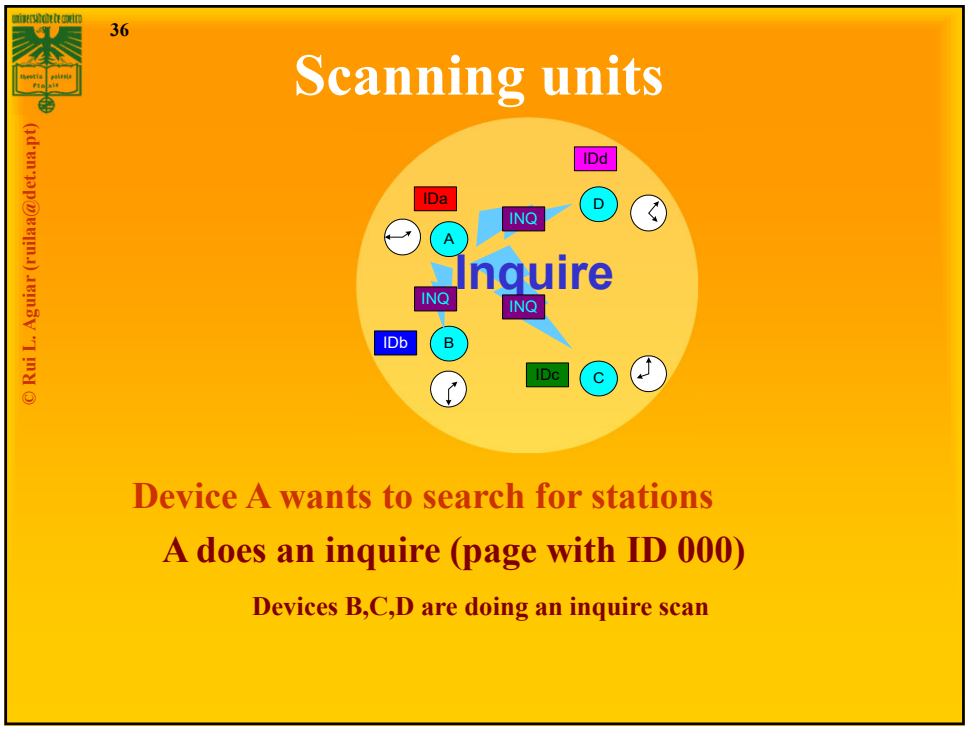
33


34
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)

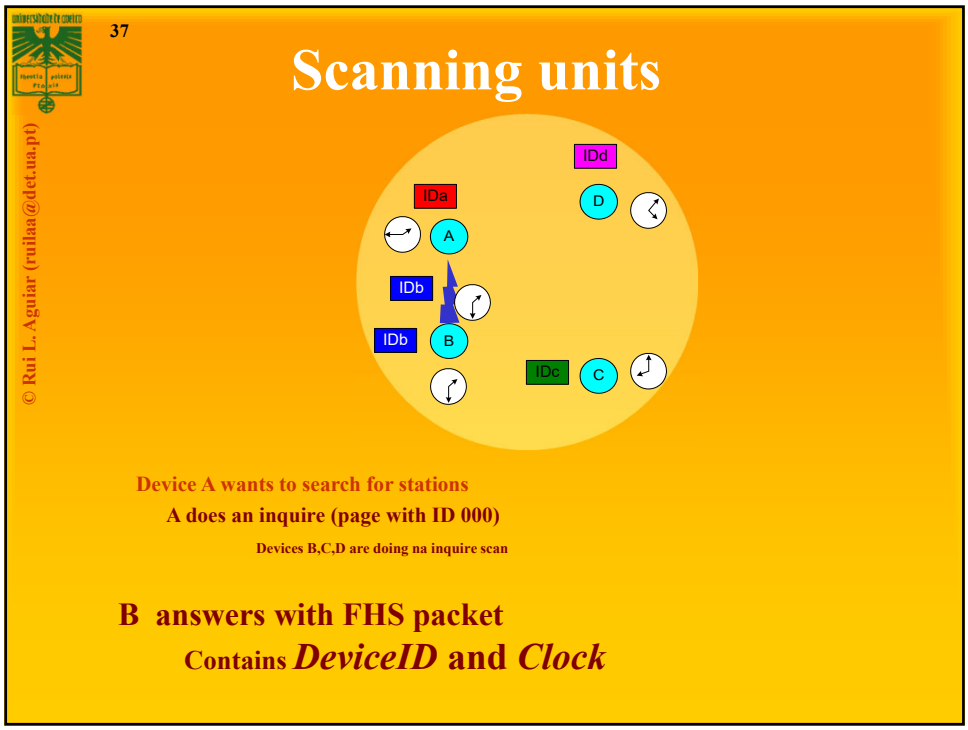
34


35
Scanning units
IDd
D
IDa
A
IDb
B
IDc
C
Device A wants to search for stations
© Rui L. Aguiar (ruilaa@det.ua.pt)

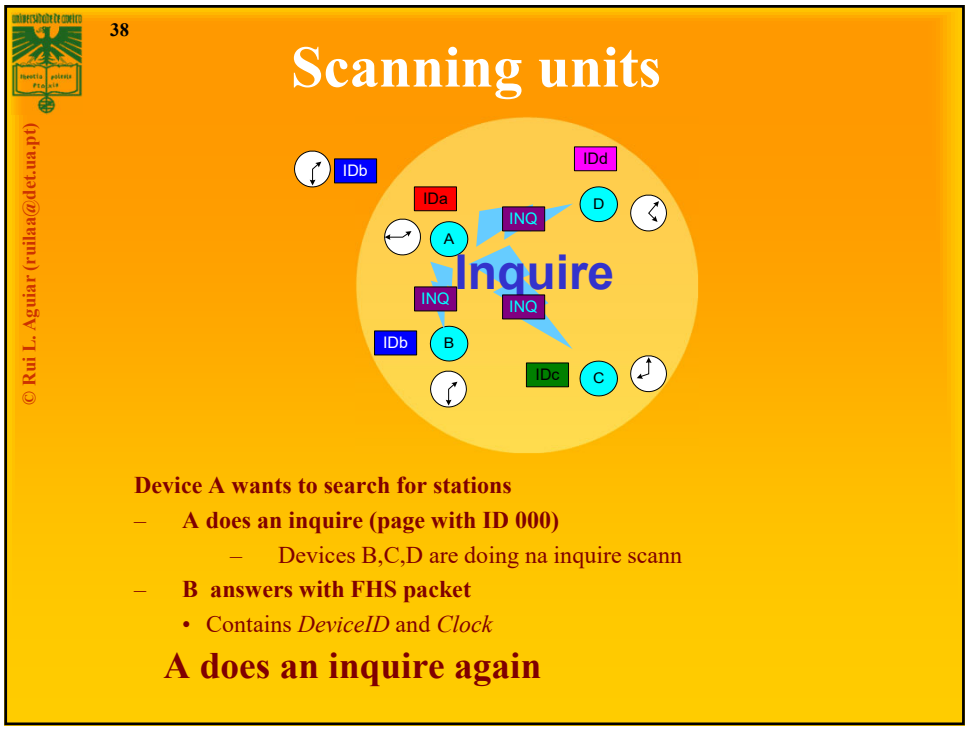
35


36
Scanning units
IDd
D
IDa
A
INQ
Inquire
INQ
INQ
IDb
B
IDc
C
Device A wants to search for stations
A does an inquire (page with ID 000)
Devices B,C,D are doing an inquire scan
© Rui L. Aguiar (ruilaa@det.ua.pt)

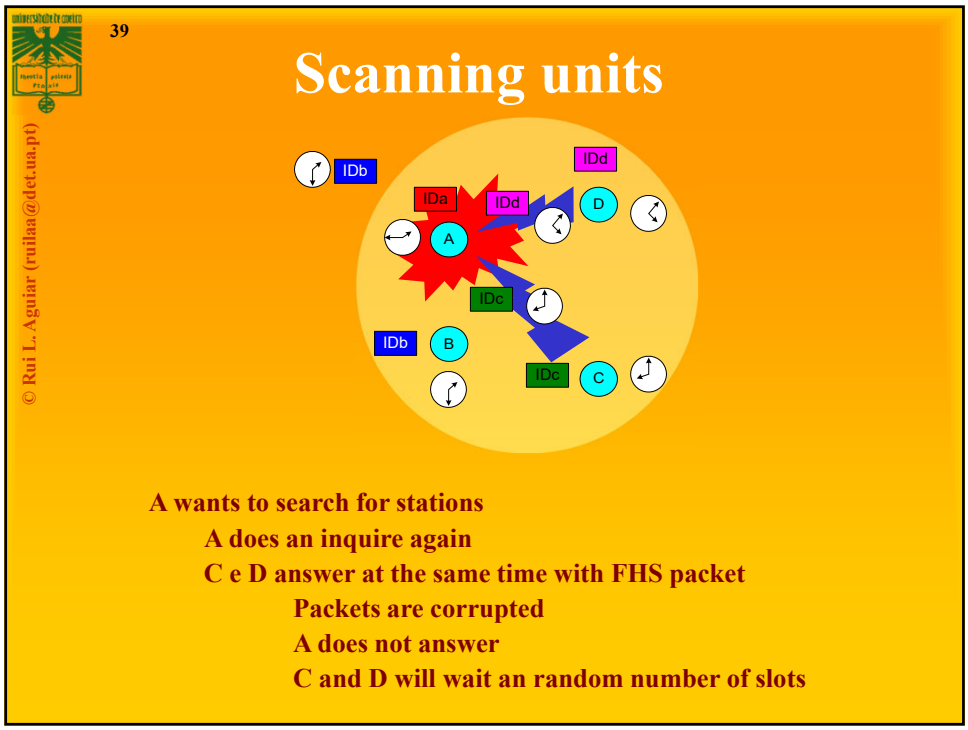
36


37
Scanning units
IDd
IDa
D
A
IDb
IDb
B
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
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

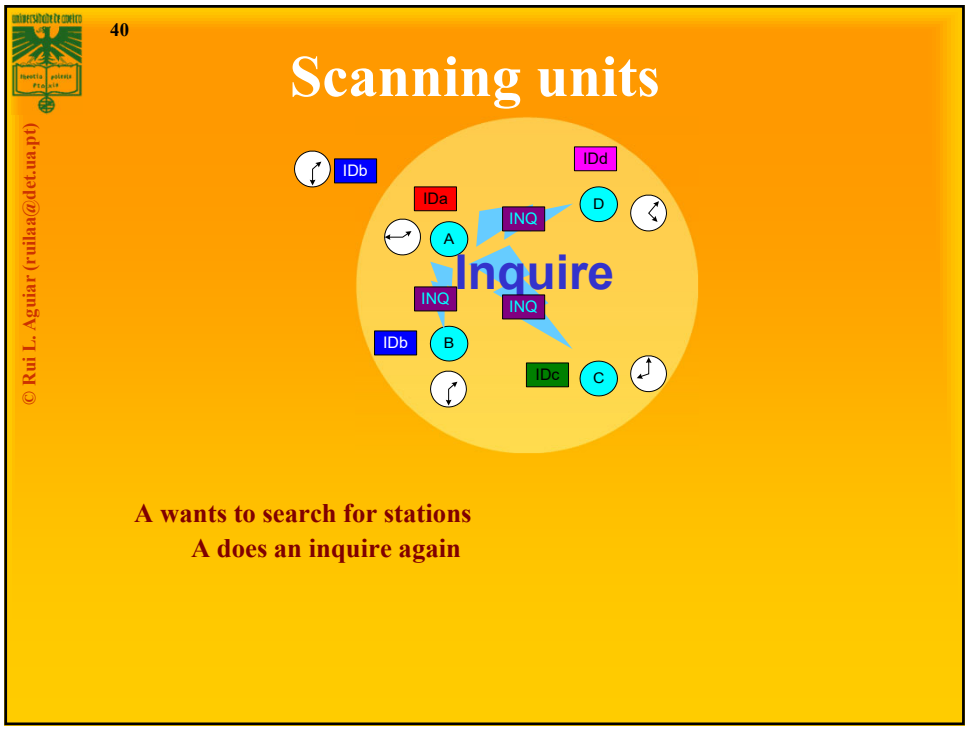
37


38
Scanning units
IDb
IDd
IDa
D
INQ
A
Inquire
INQ
INQ
IDb
B
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
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

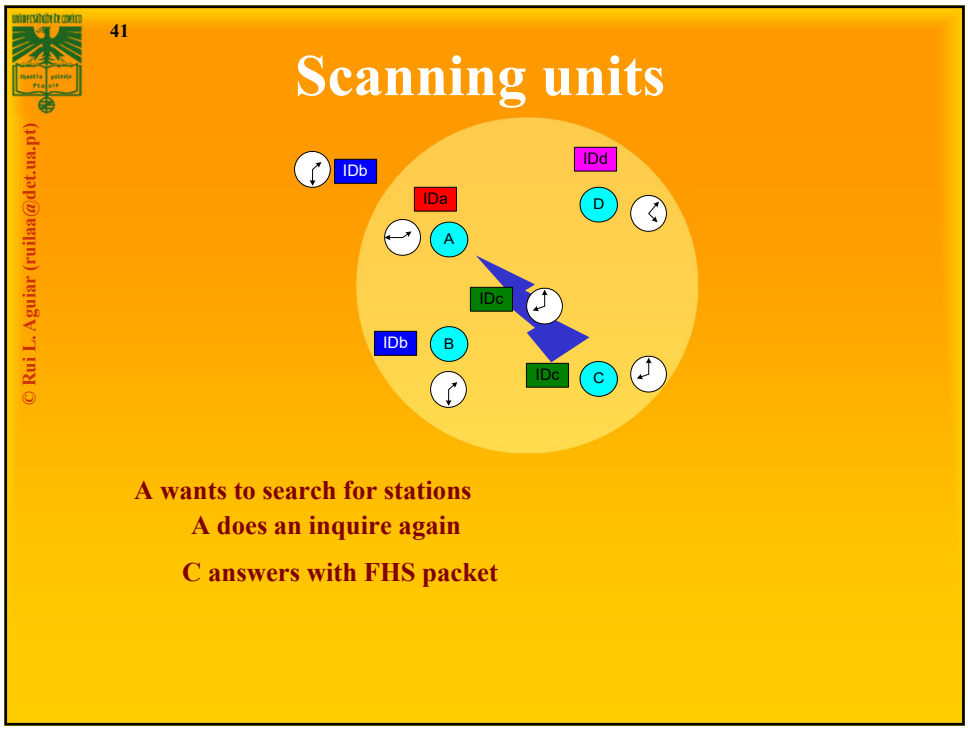
38


39
Scanning units
IDb
IDd
IDa
IDd
D
A
IDc
IDb
B
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
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

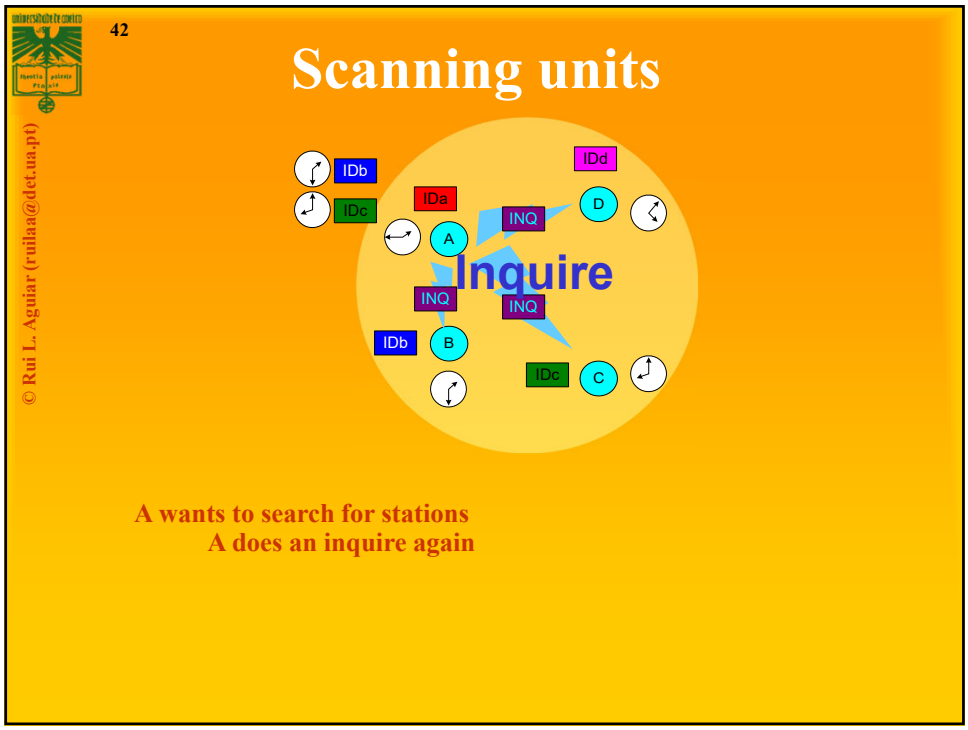
39


40
Scanning units
IDb
IDd
IDa
D
INQ
A
Inquire
INQ
INQ
IDb
B
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
A wants to search for stations
A does an inquire again

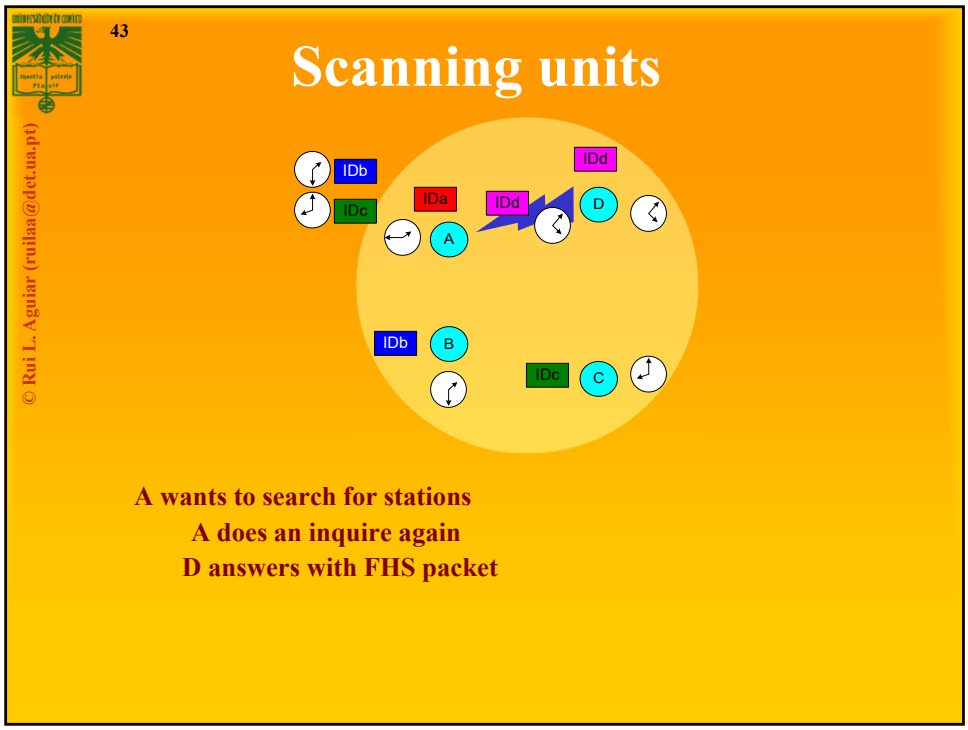
40


41
Scanning units
IDb
IDa
IDd
D
A
IDc
IDb
B
IDc
C
A wants to search for stations
A does an inquire again
C answers with FHS packet
© Rui L. Aguiar (ruilaa@det.ua.pt)

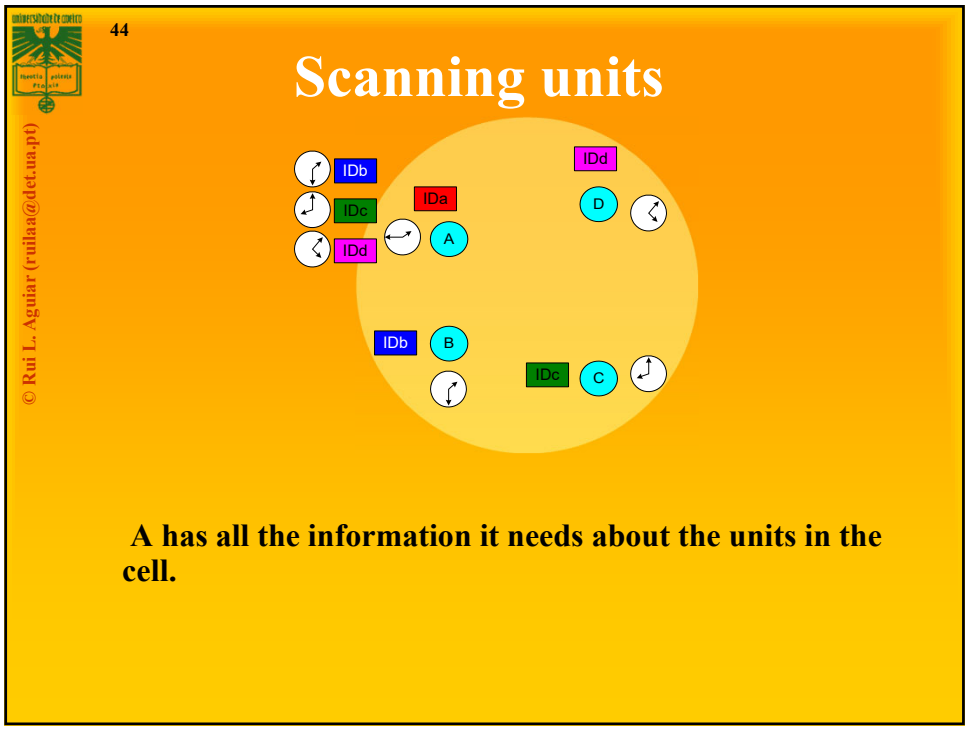
41


42
Scanning units
IDb
IDc
IDa
IDd
D
INQ
A
Inquire
INQ
INQ
IDb
B
IDc
C
A wants to search for stations
A does an inquire again
© Rui L. Aguiar (ruilaa@det.ua.pt)

42


43
Scanning units
IDb
IDc
IDa
IDd
A
IDd
D
IDb
B
IDc
C
A wants to search for stations
A does an inquire again
D answers with FHS packet
© Rui L. Aguiar (ruilaa@det.ua.pt)

43


44
Scanning units
IDb
IDc
IDd
IDa
A
IDd
D
IDb
B
IDc
C
A has all the information it needs about the units in the cell.
© Rui L. Aguiar (ruilaa@det.ua.pt)

44

45

Inquiry scanning: summary

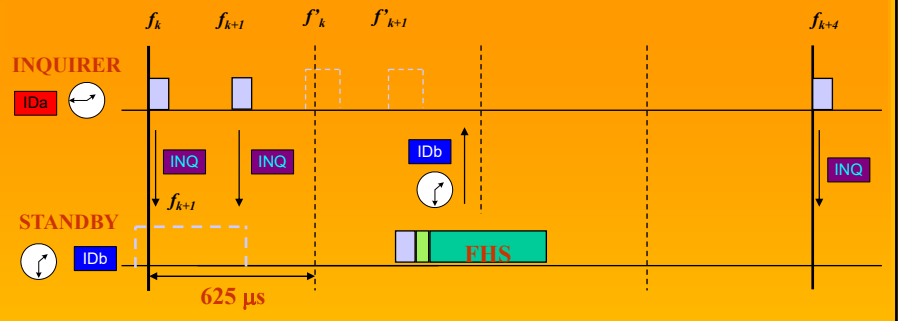
- Inquiry scanning has a common address
  - and a common frequency pattern (from 32 frequencies)
- All devices can page this address (and become masters)
- All machines hearing an inquiry will answer the inquiry request
- There is a detector (*correlator hit*) in the slaves, that detects inquiries, before 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.

© Rui L. Aguiar (ruilaa@det.ua.pt)

45

46

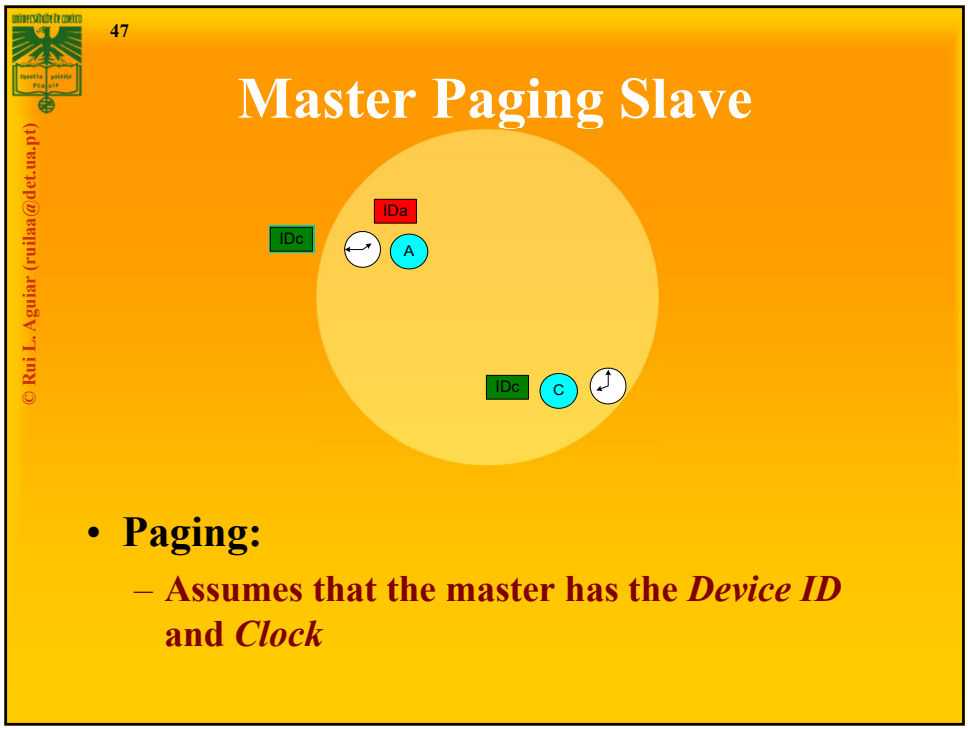
Timing: Inquiry



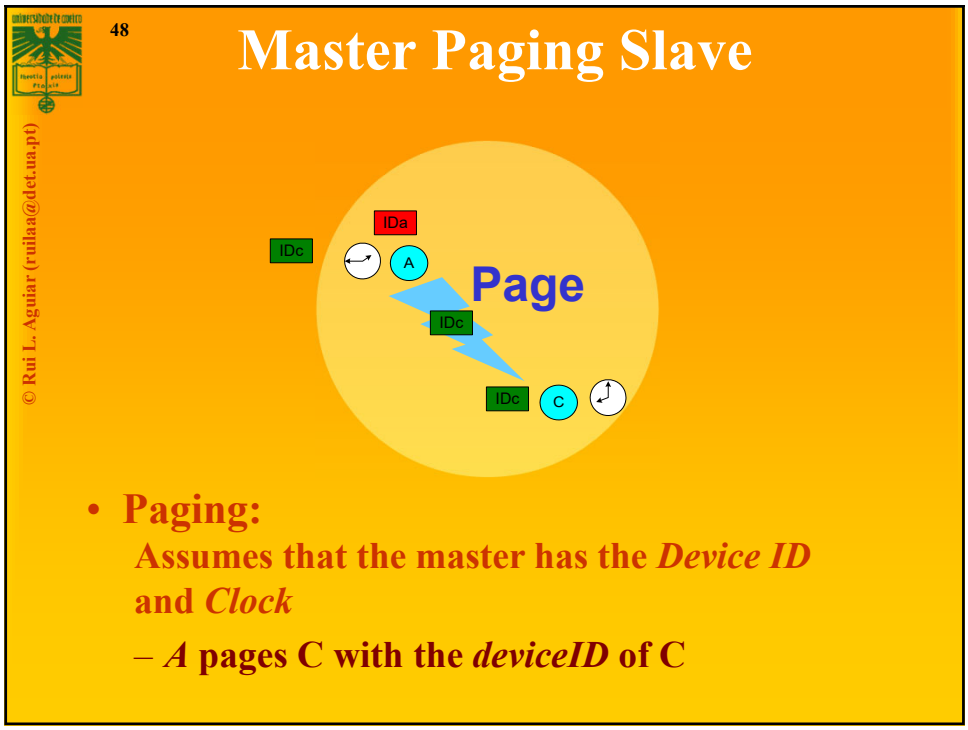
Inquiry requires two packets before the slave answers.

© Rui L. Aguiar (ruilaa@det.ua.pt)

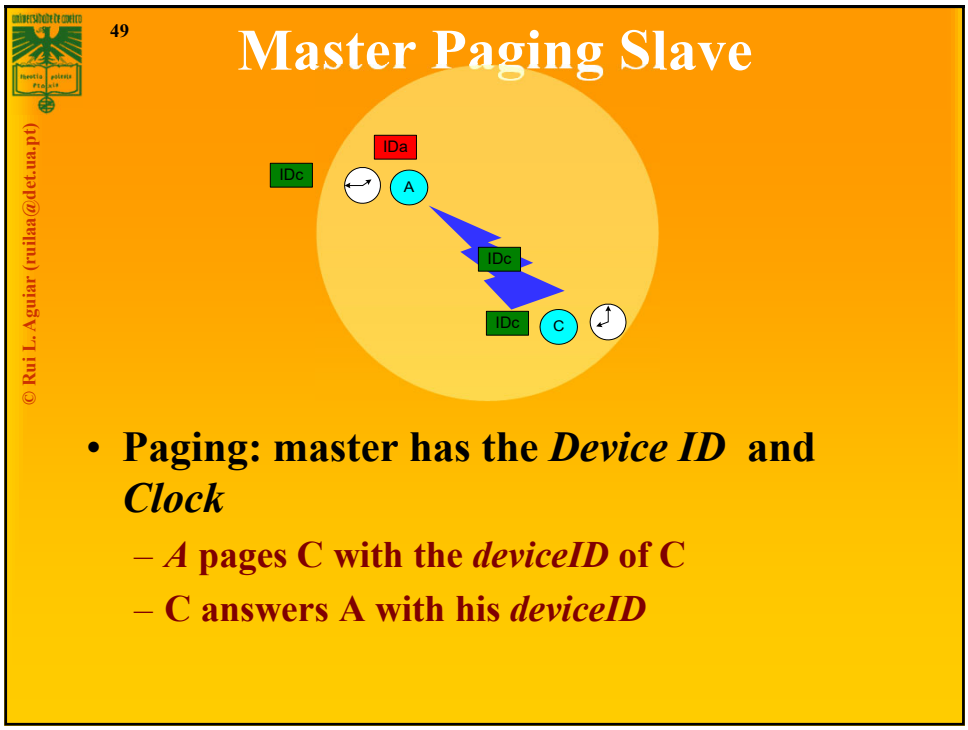
46


47
Master Paging Slave
IDa
IDc
A
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
• Paging:
– Assumes that the master has the Device ID and Clock

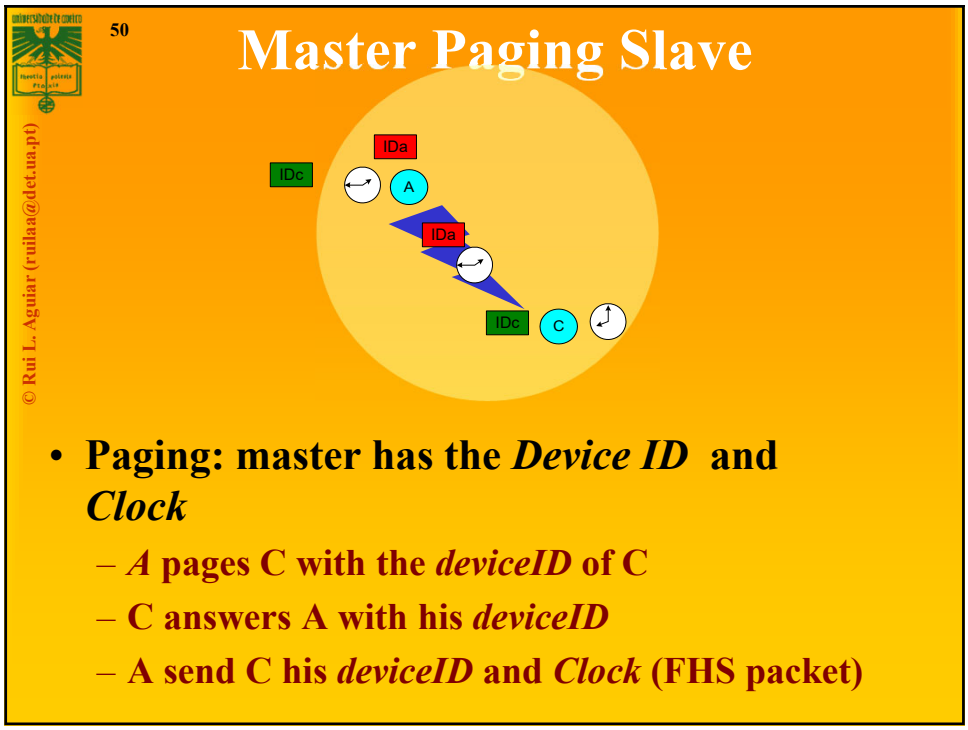
47


48
Master Paging Slave
IDa
IDc
A
Page
IDc
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
• Paging:
Assumes that the master has the Device ID and Clock
– A pages C with the deviceID of C

48


49
Master Paging Slave
IDa
IDc
A
IDc
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
• Paging: master has the Device ID and Clock
– A pages C with the deviceID of C
– C answers A with his deviceID

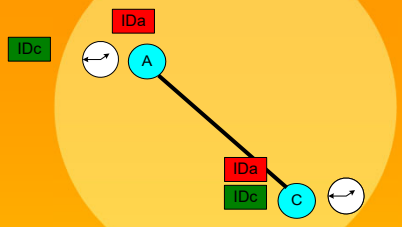
49


50
Master Paging Slave
IDa
IDc
A
IDa
IDc
C
© Rui L. Aguiar (ruilaa@det.ua.pt)
• 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)

50

51

Master Paging Slave



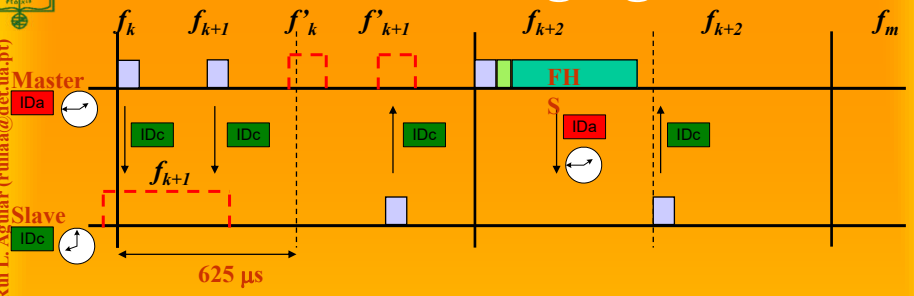
- **Paging: master has the *Device ID* and *Clock***
  - ***A* pages C with the *deviceID* of C**
  - **C answers A with his *deviceID***
  - **A send C his *deviceID* and *Clock* (FHS packet)**
  - **A becomes master of C**

© Rui L. Aguiar (ruilaa@det.ua.pt)

51

52

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.**

© Rui L. Aguiar (ruilaa@det.ua.pt)

52

© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro

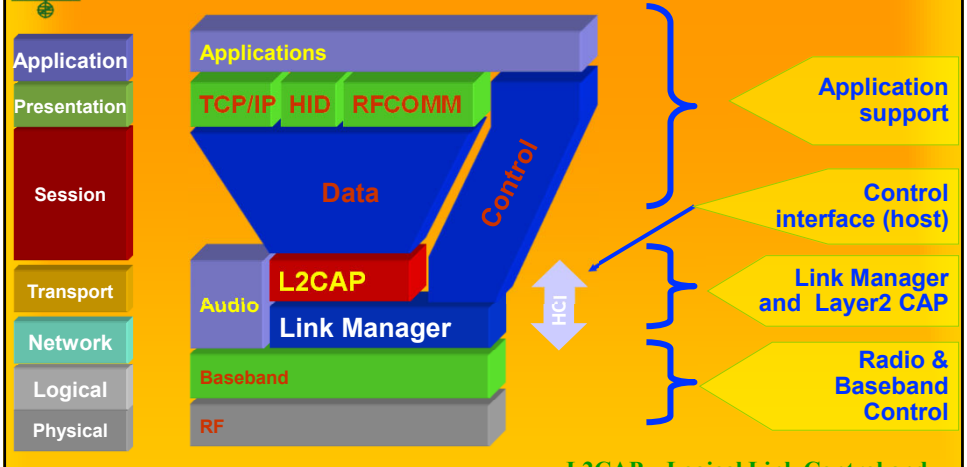
53

Outline

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

53

stack Bluetooth



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)

54

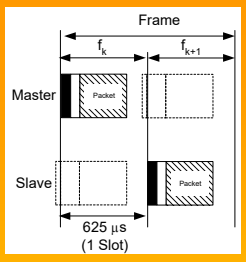
Bluetooth Protocol

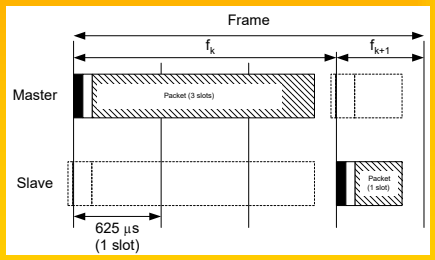
- **Radio layer**
  - **Defines requirements for a Bluetooth radio transceiver**
  - **Handles conformity to 2.4GHz band**
  - **Establishes specifications for using Spread-Spectrum Frequency Hopping**
  - **Classifies device into one of three power classes:**
    - long range; (Class 1 - 100mW, 100m)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

56

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 technologyS 2.4GHz, etc…)





58

59

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

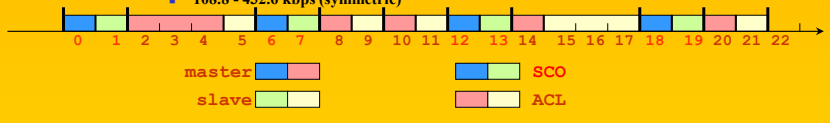
© Rui L. Aguiar (ruilaa@det.ua.pt)

59

60

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)



60

61

Baseband no Bluetooth

© Rui L. Aguiar (ruilaa@det.ua.pt)

SYNCHRONOUS CONNECTION-ORIENTED (SCO) LINK

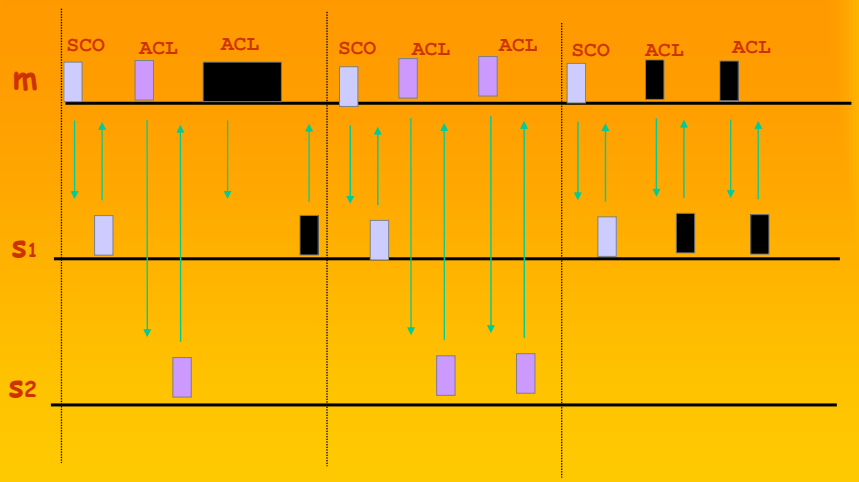
- Circuit switching
- Point to point, symmetric and synchronous services
- Slot reservation at fixed time intervals.
- Master can control 3 SCO channels
- Slave can receive 3 SCO to same master, 2 SCO to different masters
- Packets are never retransmitted
- Usually for 64Kb/s connections (voice)

ASYNCHRONOUS CONNECTION-LESS (ACL) LINK

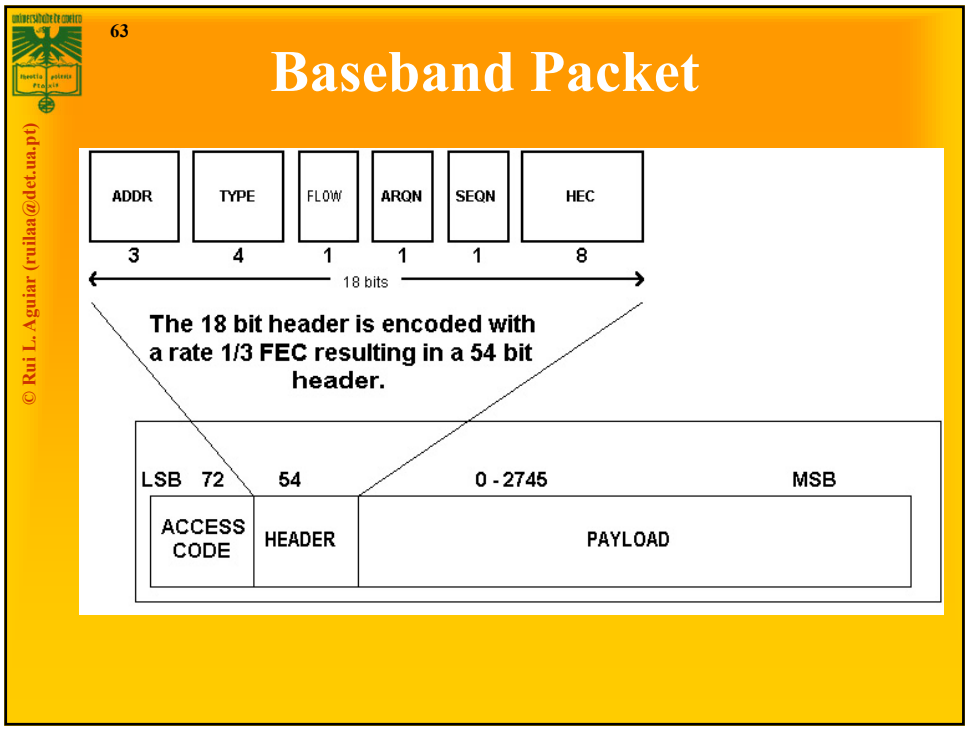
- Packet switching
- Asymmetric and asynchronous services
- Polling
- Only one link allower

61

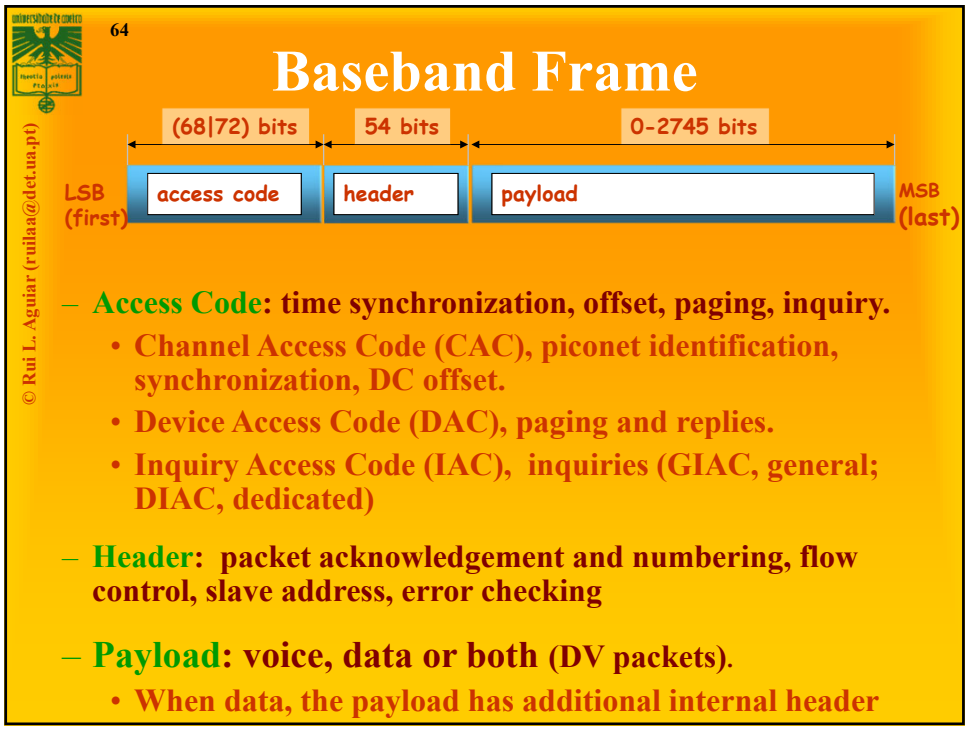
Mixed Link Example



62

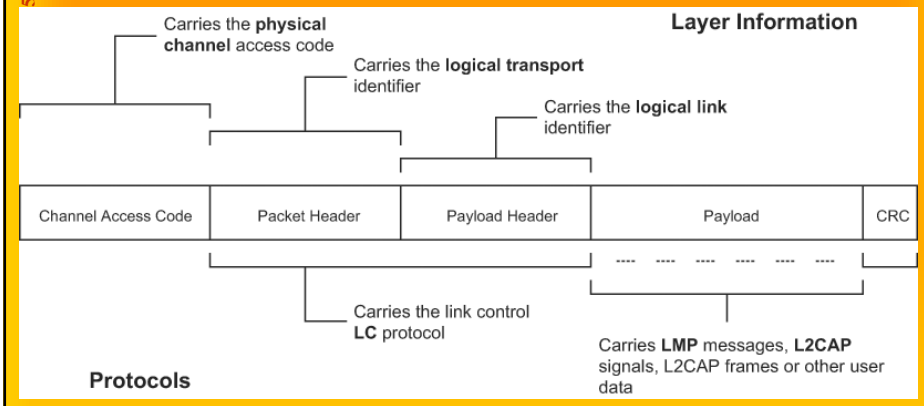

63
Baseband Packet
ADDR
TYPE
FLOW
ARQN
SEQN
HEC
3
4
1
1
1
8
18 bits
The 18 bit header is encoded with a rate 1/3 FEC resulting in a 54 bit header.
LSB
72
54
0 - 2745
MSB
ACCESS CODE
HEADER
PAYLOAD
© Rui L. Aguiar (ruilaa@det.ua.pt)

63


64
Baseband Frame
(68|72) bits
54 bits
0-2745 bits
LSB (first)
access code
header
payload
MSB (last)
– 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
© Rui L. Aguiar (ruilaa@det.ua.pt)

64

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

65

66

Packet types and transmission rates

© Rui L. Aguiar (ruilaa@det.ua.pt)

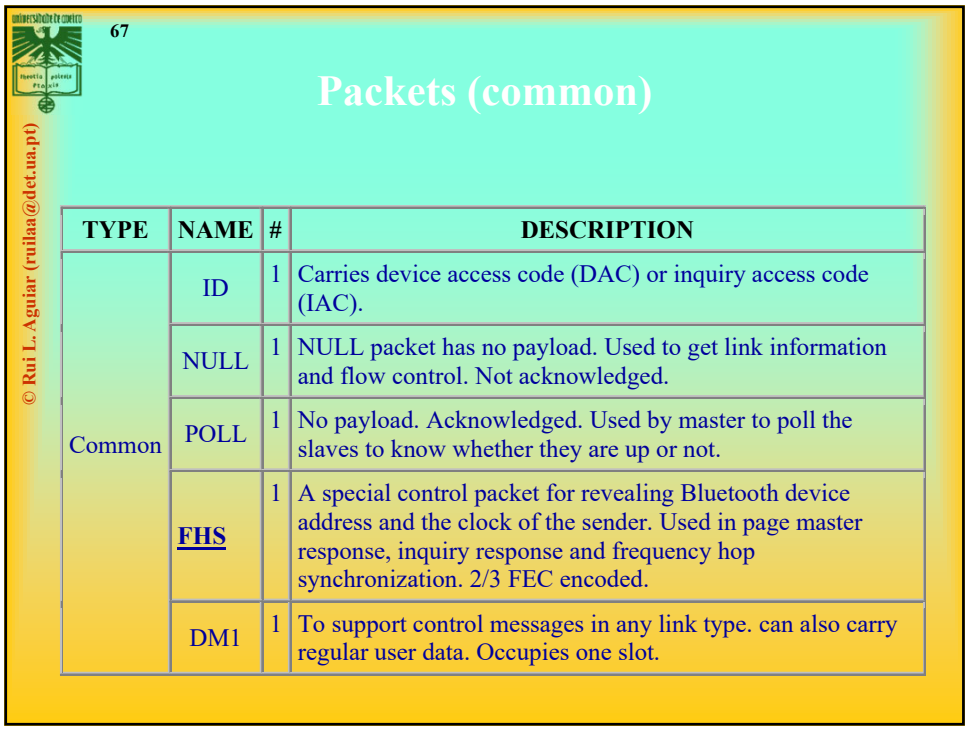
Packet types

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

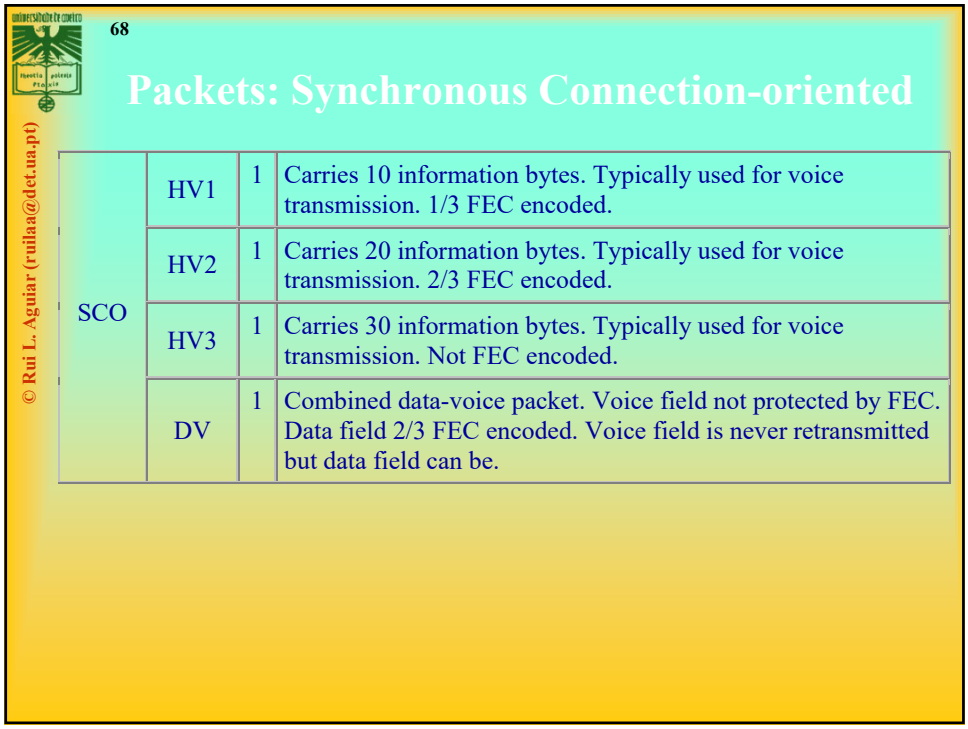
Transmission rate (Kbps)

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

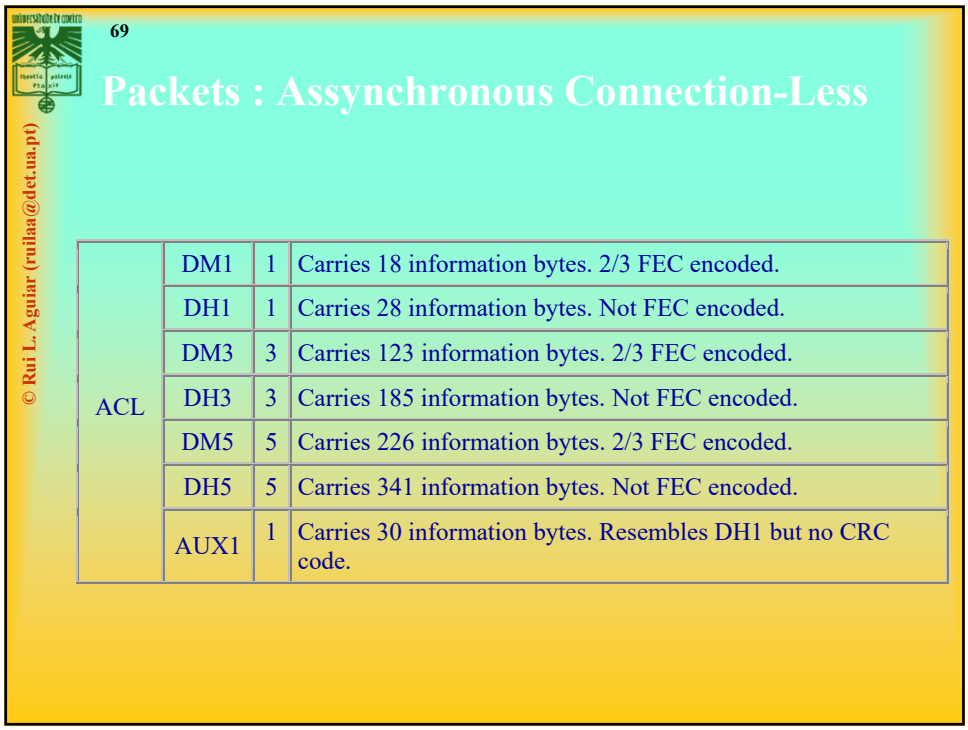
66


67
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)

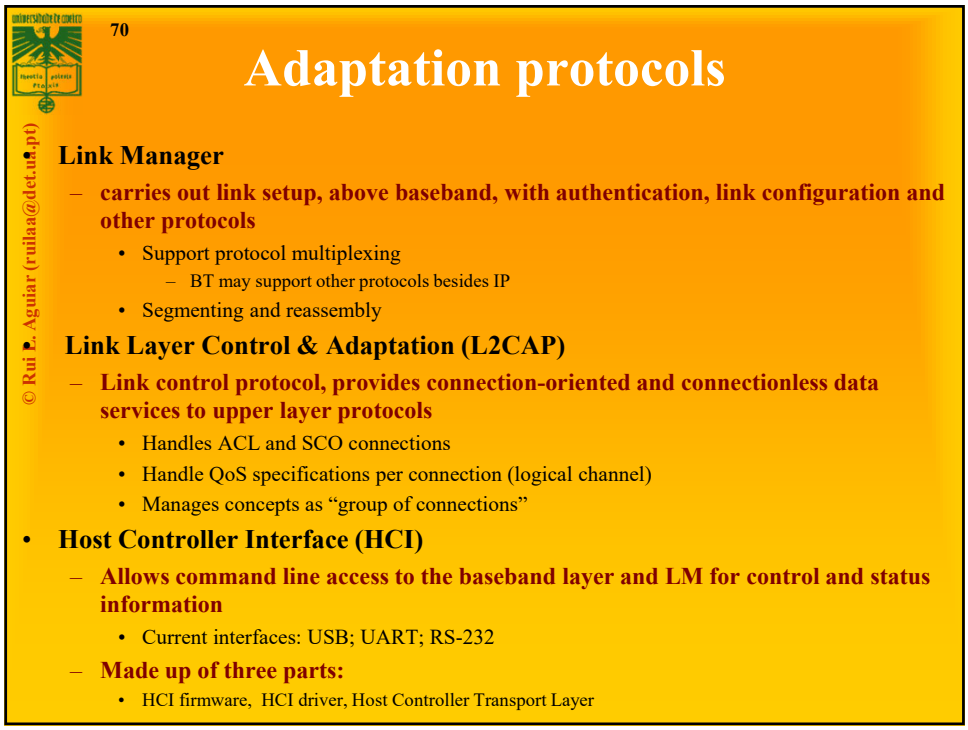
67


68
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)

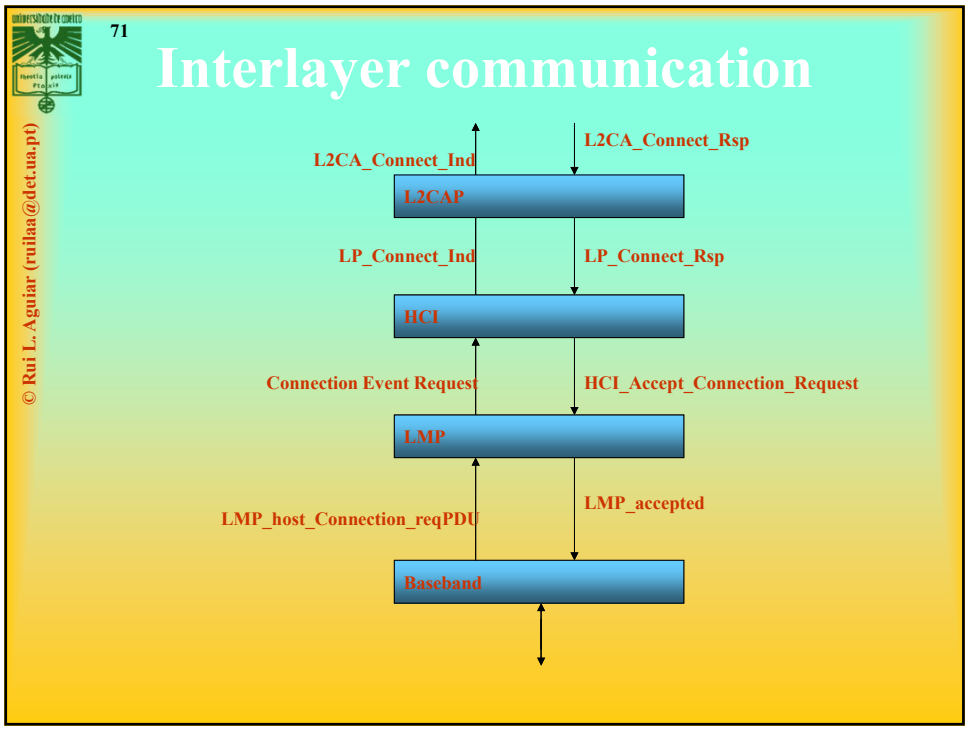
68


69
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.
© Rui L. Aguiar (ruilaa@det.ua.pt)

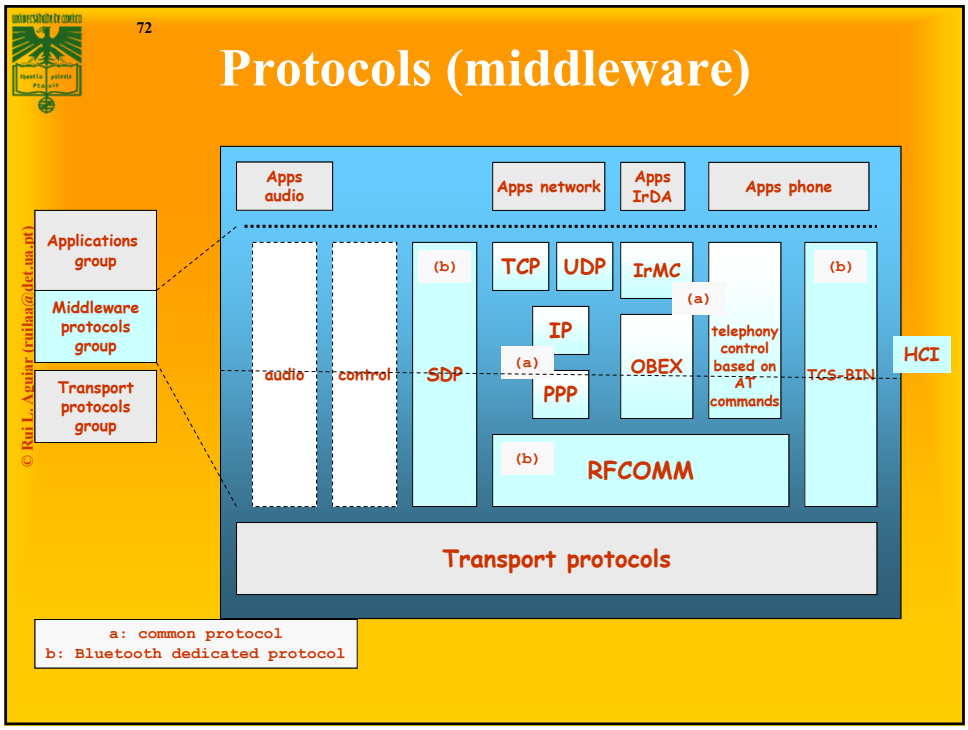
69


70
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
© Rui L. Aguiar (ruilaa@det.ua.pt)

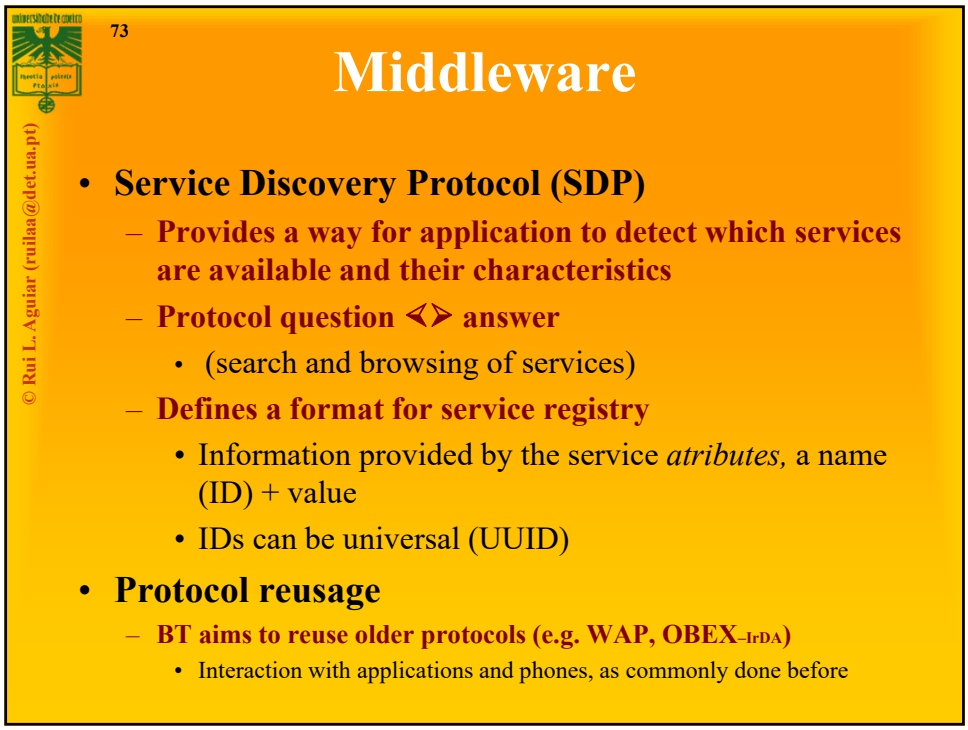
70


71
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

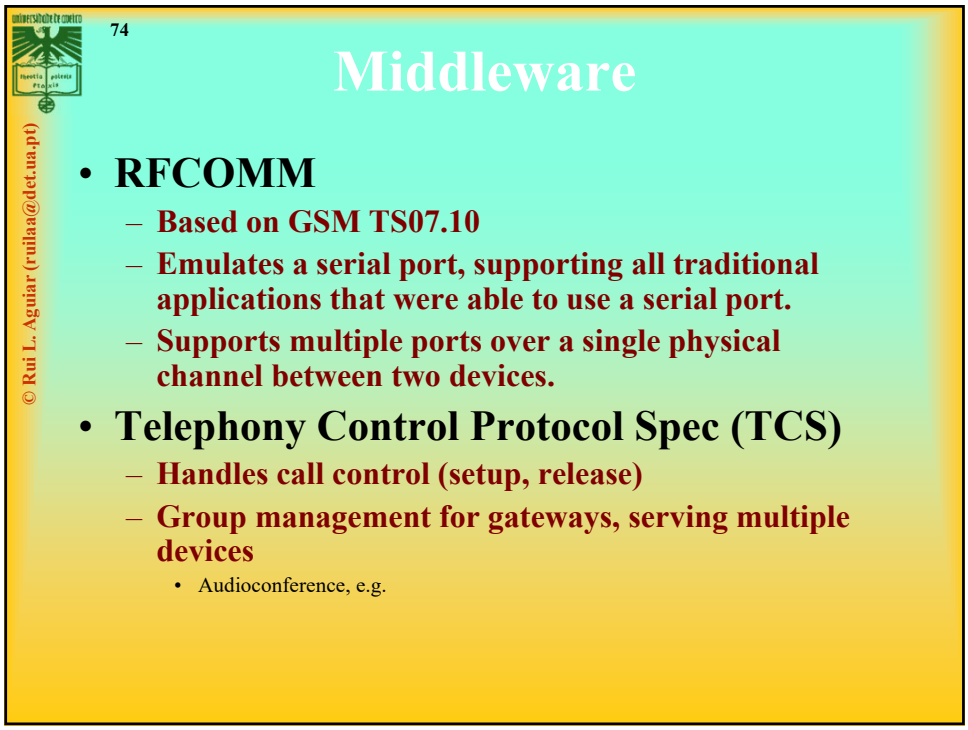
71


72
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

72


73
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
© Rui L. Aguiar (ruilaa@det.ua.pt)

73


74
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.
© Rui L. Aguiar (ruilaa@det.ua.pt)

74

© Rui L. Aguiar (ruilaa@det.ua.pt) – Uni. Aveiro

75

Outline

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

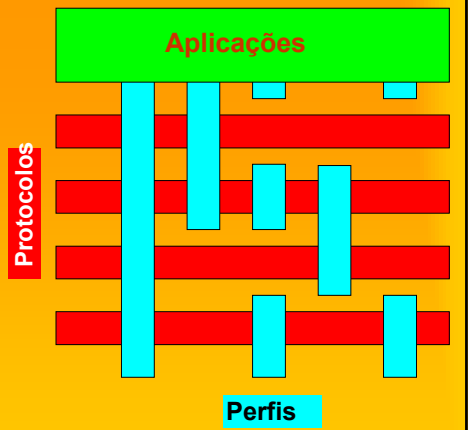
75

© Rui L. Aguiar (ruilaa@det.ua.pt)

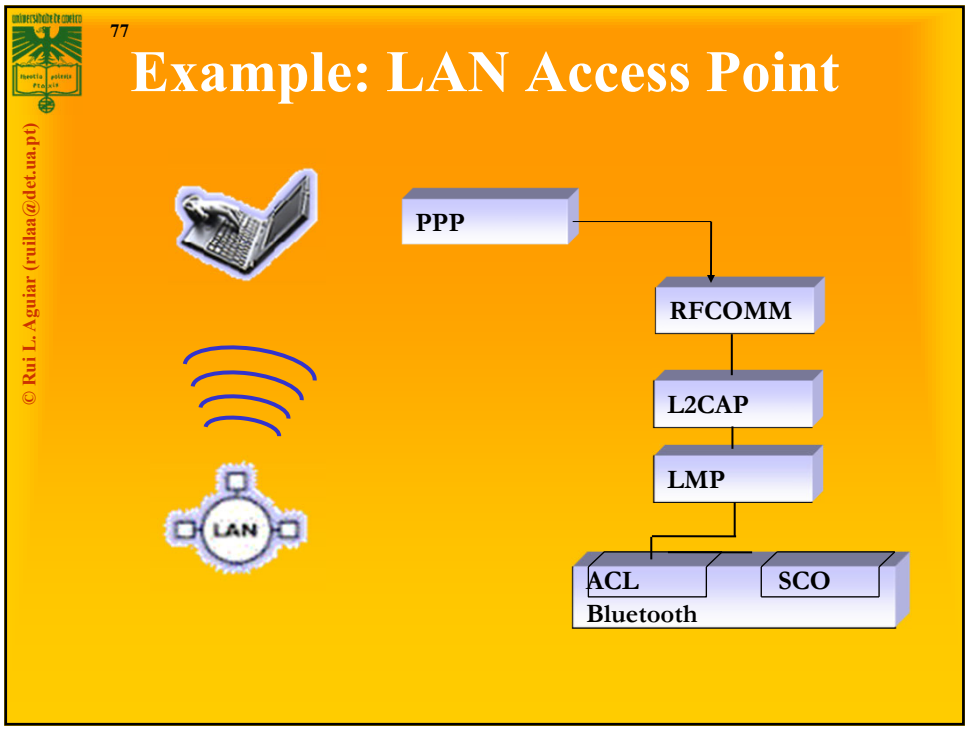
76

Interoperability: Profiles

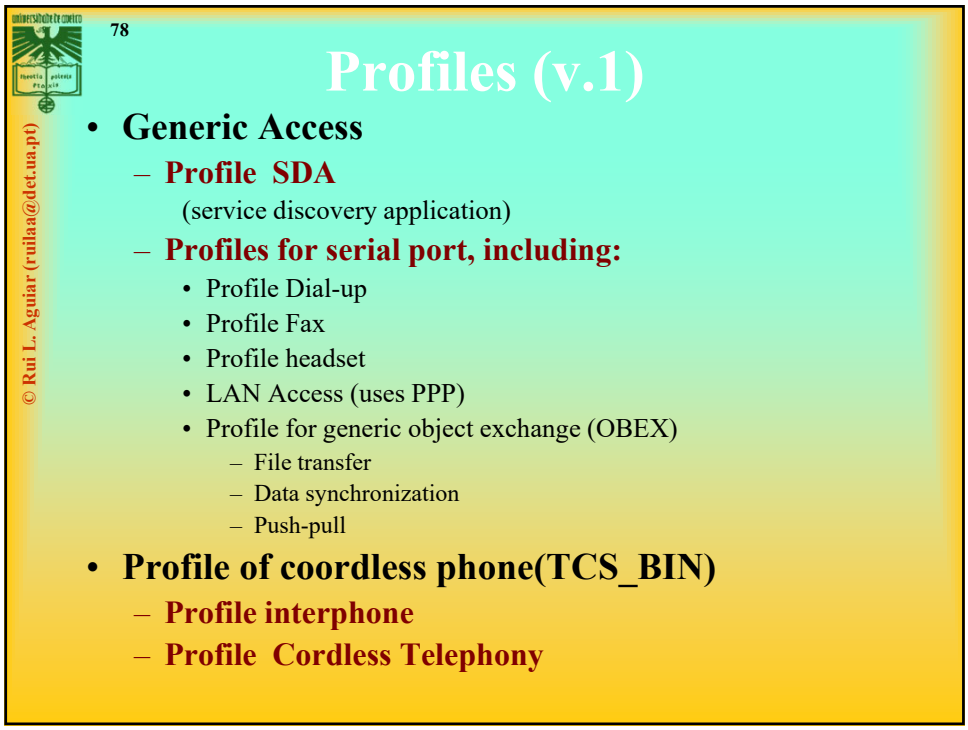
- **Profile: base for BT interoperability (BT too much flexible!)**
- **“vertical cut” in Bluetooth stack**
- **A given usage model ° typical solution**
- **Each BT device supports one or more profiles**



76


77
Example: LAN Access Point
© Rui L. Aguiar (ruilaa@det.ua.pt)
PPP
RFCOMM
L2CAP
LMP
ACL
SCO
Bluetooth
LAN

77


78
Profiles (v.1)
© Rui L. Aguiar (ruilaa@det.ua.pt)
• 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

78

79

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)

© Rui L. Aguiar (ruilaa@det.ua.pt)

79

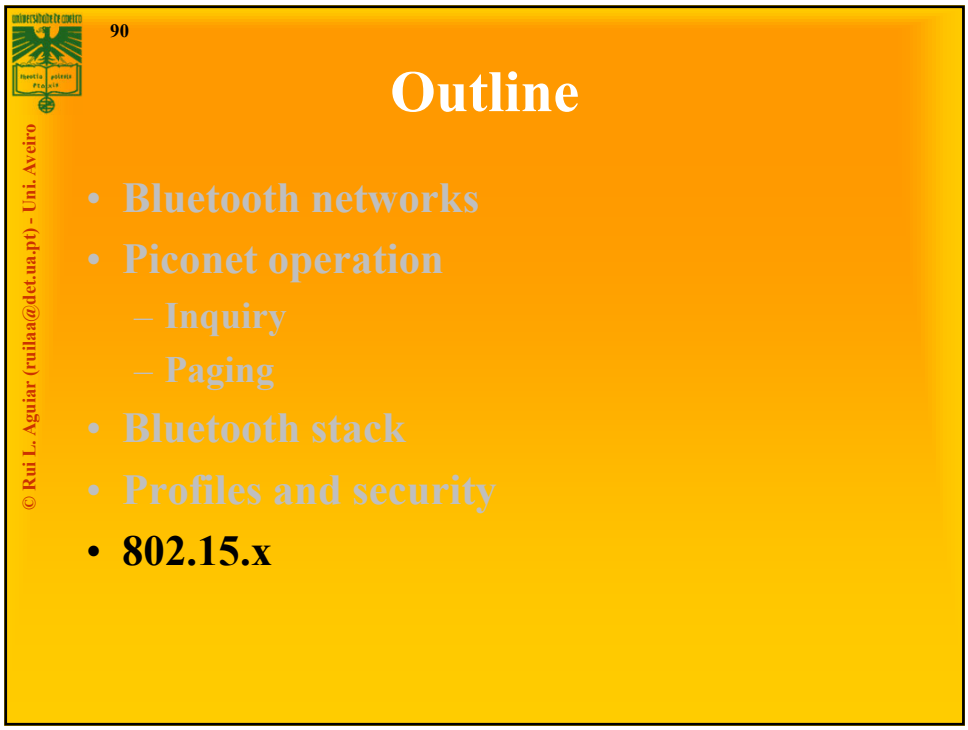
82

Illustration of BT evolution (headset profile)

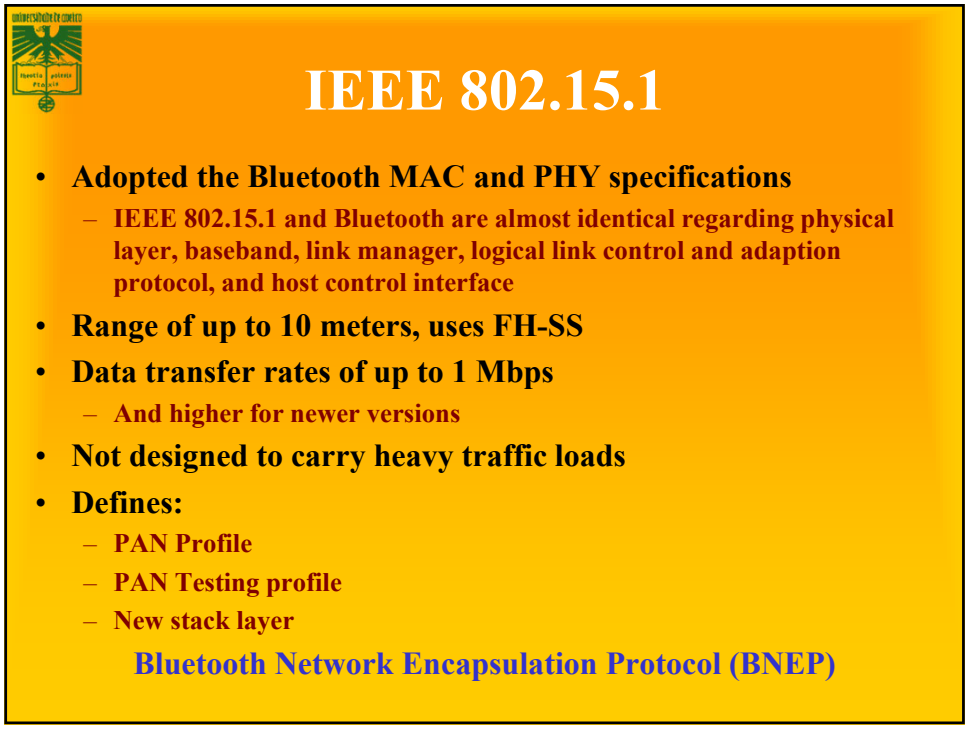
Specifications	Bluetooth 1.1	Bluetooth 1.2	Bluetooth 2.0	Bluetooth 2.1 plus EDR (Enhanced Data Rate)
Voice dialing	Yes	Yes	Yes	Yes
Call mute	Yes	Yes	Yes	Yes
Last-number redial	Yes	Yes	Yes	Yes
Improved resistance to radio frequency interference	-	Yes	Yes	Yes
10-meter range	Yes	Yes	Yes	Yes
100-meter range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

© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro

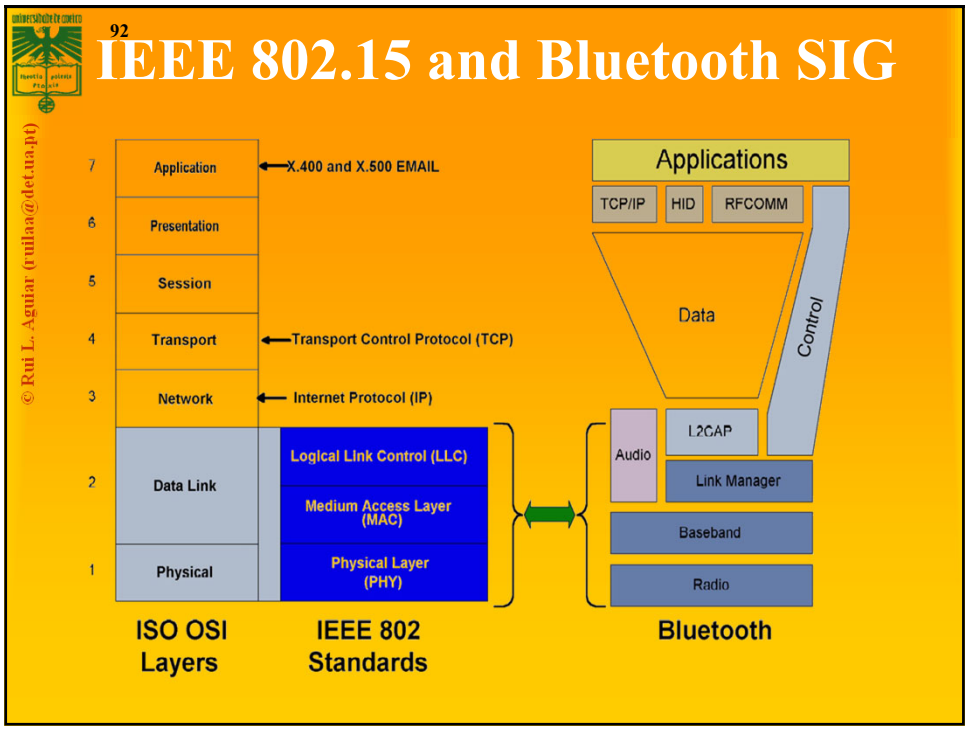
82


90
Outline
• Bluetooth networks
• Piconet operation
– Inquiry
– Paging
• Bluetooth stack
• Profiles and security
• 802.15.x
© Rui L. Aguiar (ruilaa@det.ua.pt) - Uni. Aveiro

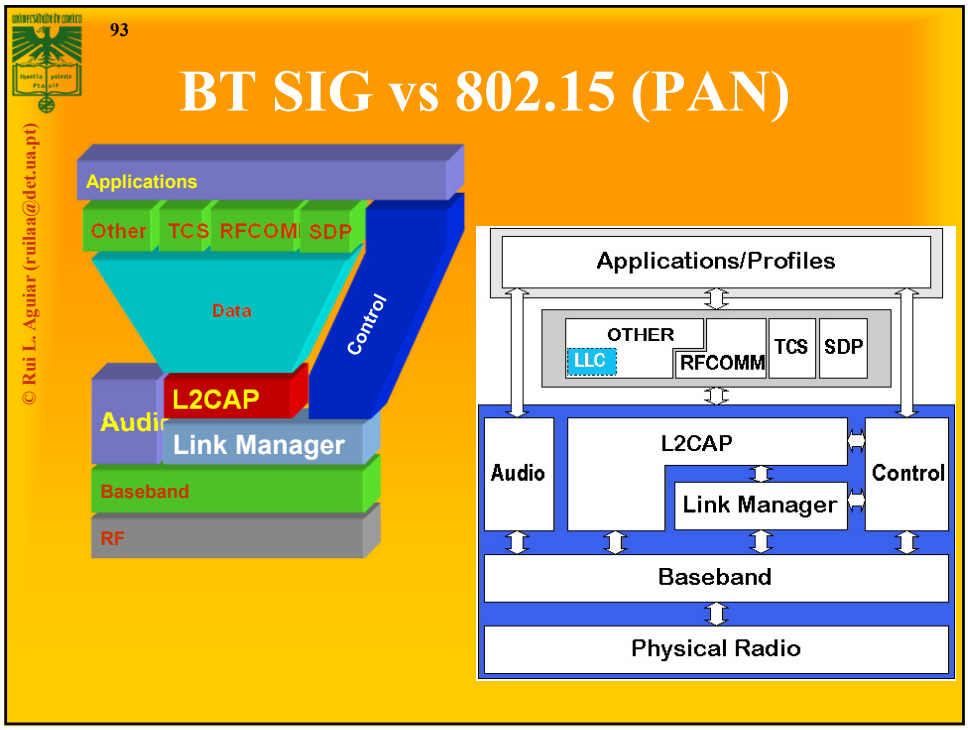
90


IEEE 802.15.1
• Adopted the Bluetooth MAC and PHY specifications
– IEEE 802.15.1 and Bluetooth are almost identical regarding physical layer, baseband, link manager, logical link control and adaption protocol, and host control interface
• Range of up to 10 meters, uses FH-SS
• Data transfer rates of up to 1 Mbps
– And higher for newer versions
• Not designed to carry heavy traffic loads
• Defines:
– PAN Profile
– PAN Testing profile
– New stack layer
Bluetooth Network Encapsulation Protocol (BNEP)

91


92
IEEE 802.15 and Bluetooth SIG
© Rui L. Aguiar (ruilaa@det.ua.pt)
7 Application
6 Presentation
5 Session
4 Transport
3 Network
2 Data Link
1 Physical
X.400 and X.500 EMAIL
Transport Control Protocol (TCP)
Internet Protocol (IP)
Logical Link Control (LLC)
Medium Access Layer (MAC)
Physical Layer (PHY)
Applications
TCP/IP
HID
RFCOMM
Data
Control
Audio
L2CAP
Link Manager
Baseband
Radio
ISO OSI Layers
IEEE 802 Standards
Bluetooth

92

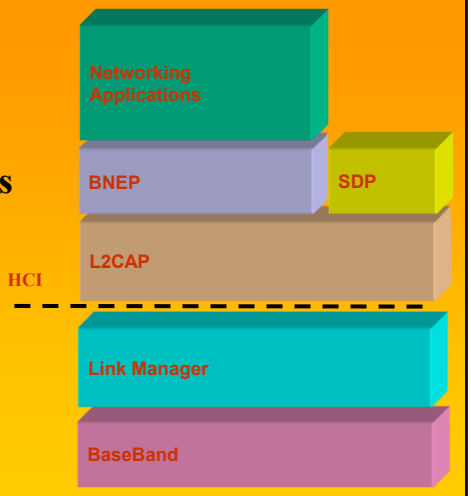

93
BT SIG vs 802.15 (PAN)
© Rui L. Aguiar (ruilaa@det.ua.pt)
Applications
Other
TCS
RFCOMM
SDP
Data
Control
L2CAP
Audio
Link Manager
Baseband
RF
Applications/Profiles
OTHER
LLC
RFCOMM
TCS
SDP
Audio
L2CAP
Control
Link Manager
Baseband
Physical Radio

93

94

Bluetooth Networking Encapsulation Protocol

- Provides an "Ethernet alike" environment
- Supports all type of Ethernet communications
- Deployes header compressions
- Implements packet filtering
- Implements an extension header



© Rui L. Aguiar (ruilaa@det.ua.pt)

94

95

BNEP – Why?

- Supports all network protocols (IPV4, v6, e.g.)
  - LAN access from SIG (PPP) does not scale...
- Allows establishment of peer-to-peer, hiding the notion Master-Slave of Bluetooth
- All IETF protocols should work with 802.15.1 with BNEP (including manet!)
- Resuse all existing network applications
- Solution similar to those in other networks (802.11)
- Keep uniform bridge support inside IEEE
- Cost:
  - Small overhead, balanced by header compression

© Rui L. Aguiar (ruilaa@det.ua.pt)

95

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

102

104

Bluetooth 4.0: Low Energy

104

105

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

105

106

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

106

107

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**

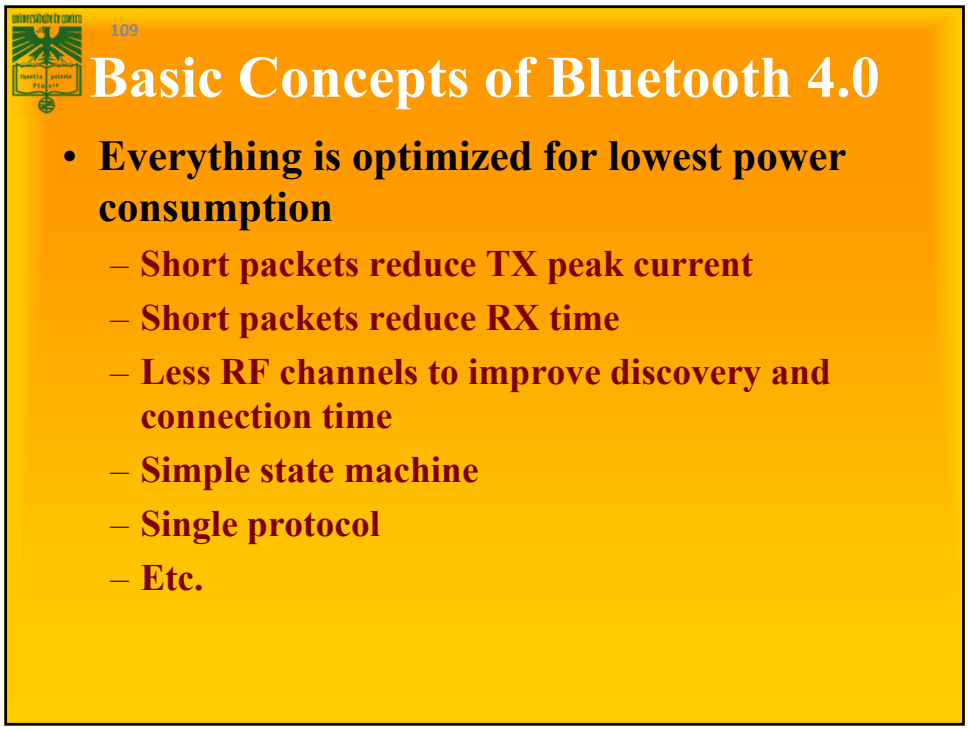
107

108

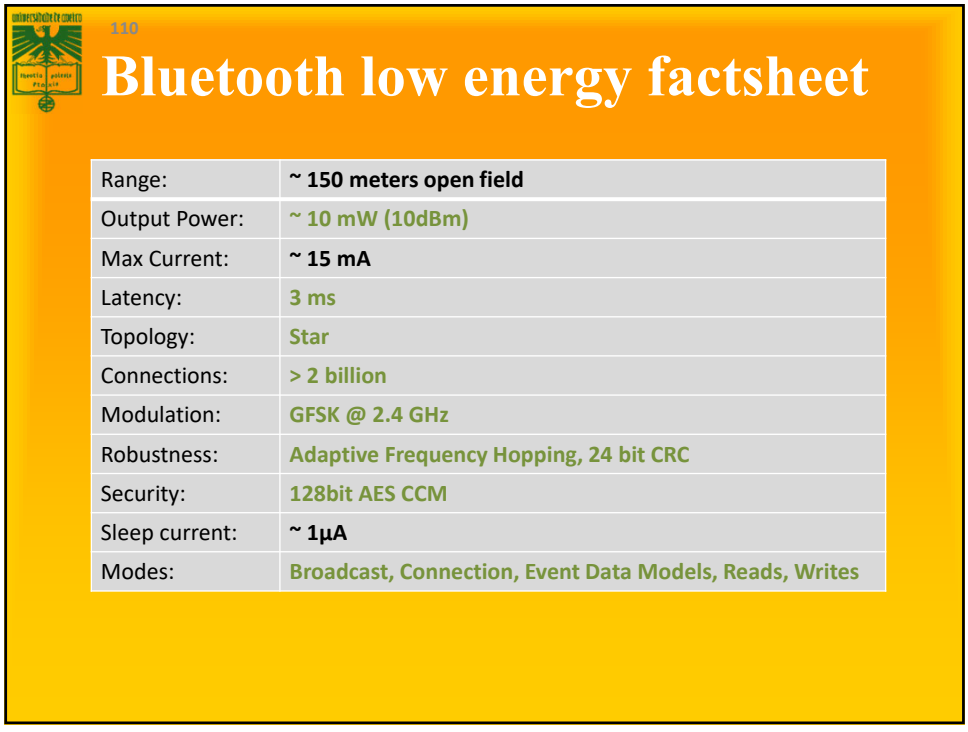
What is Bluetooth Low Energy?

- **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

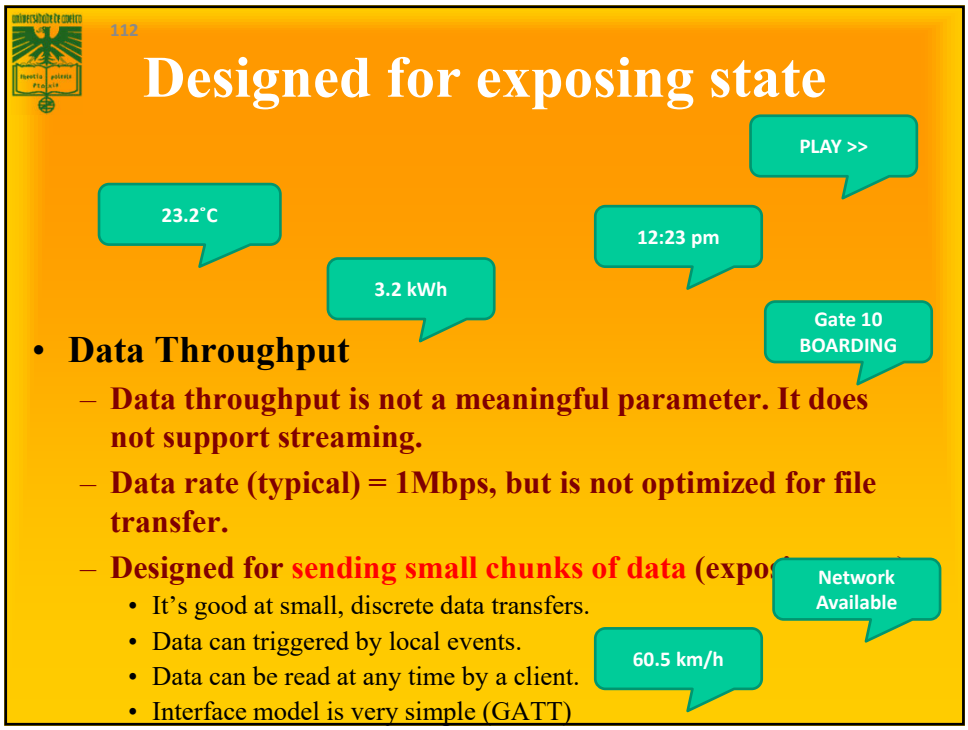
108


109
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.

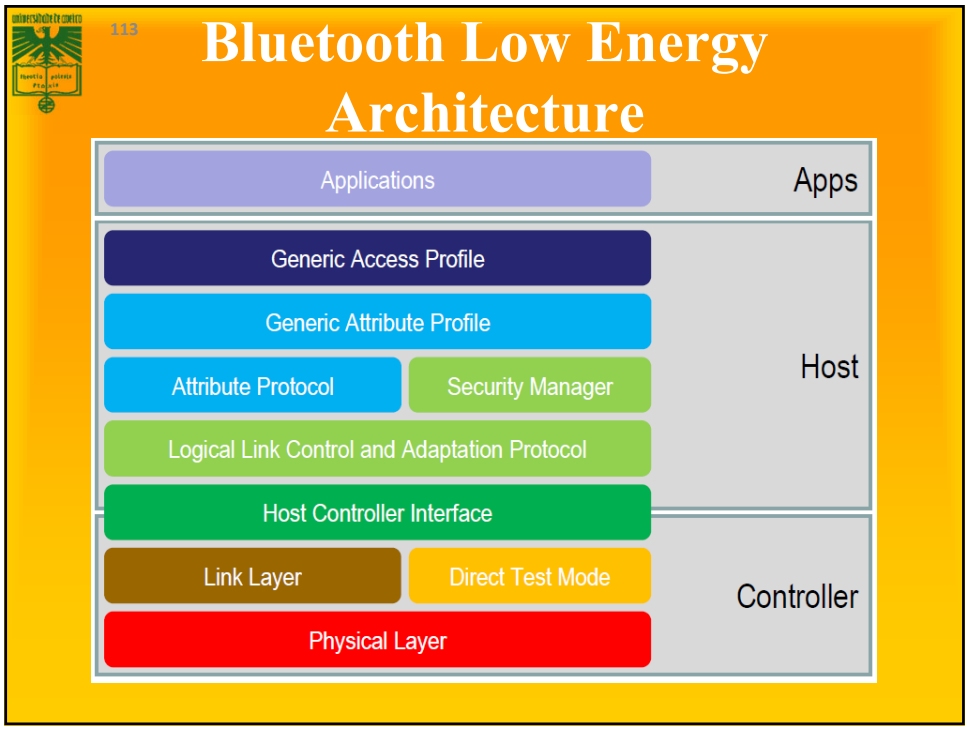
109


110
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

110


112
Designed for exposing state
PLAY >>
23.2˚C
12:23 pm
3.2 kWh
Gate 10
BOARDING
Network
Available
60.5 km/h
• 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 (expo
• 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)

112


113
Bluetooth Low Energy Architecture
Applications
Apps
Generic Access Profile
Generic Attribute Profile
Attribute Protocol
Security Manager
Logical Link Control and Adaptation Protocol
Host
Host Controller Interface
Link Layer
Direct Test Mode
Physical Layer
Controller

113

114

Device Modes

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

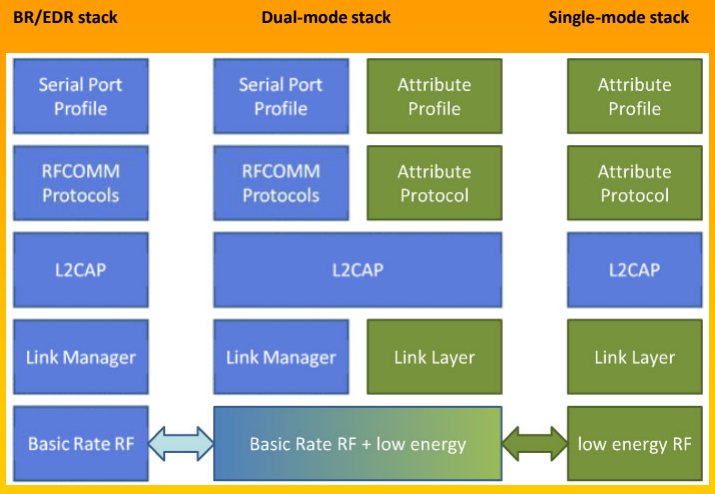
- **Single Mode**
  - Implements only Bluetooth low energy
  - Will be used in new devices / applications

114

115

Device Modes

- **Dual mode + single modes**

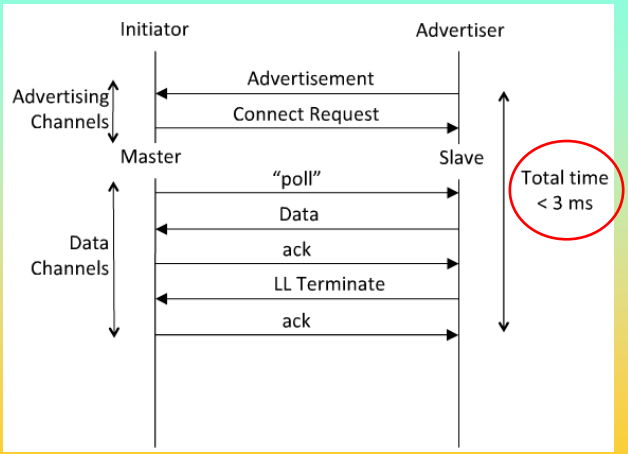


115

119

Link Layer Connection

- **Very low latency connection**

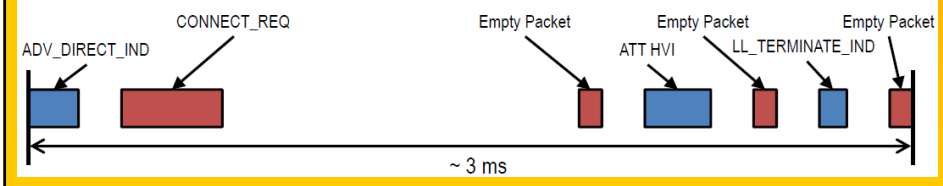


119

120

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	



120

121

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

121

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

122

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**

123

BLE and GAP

Temperature Sensor (Broadcaster) → Temperature Display (Observer)

Figure 1 – Temperature Sensor (Broadcaster)

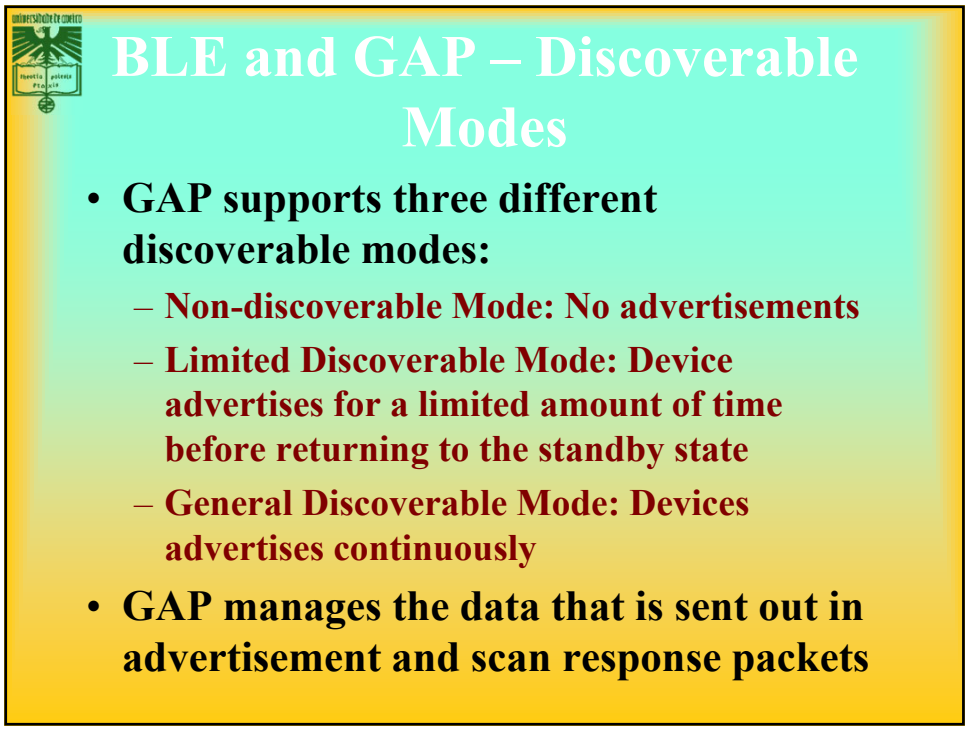
Figure 2 – Temperature Display (Observer)

Watch (Peripheral) ← → Mobile Phone (Central)

Figure 3 - Watch (Peripheral)

Figure 4 – Mobile Phone (Central)

124


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
125