Bluetooth Architecture Overview

James Kardach
Principle Engineer
Bluetooth SIG Program Manager
Intel Corporation

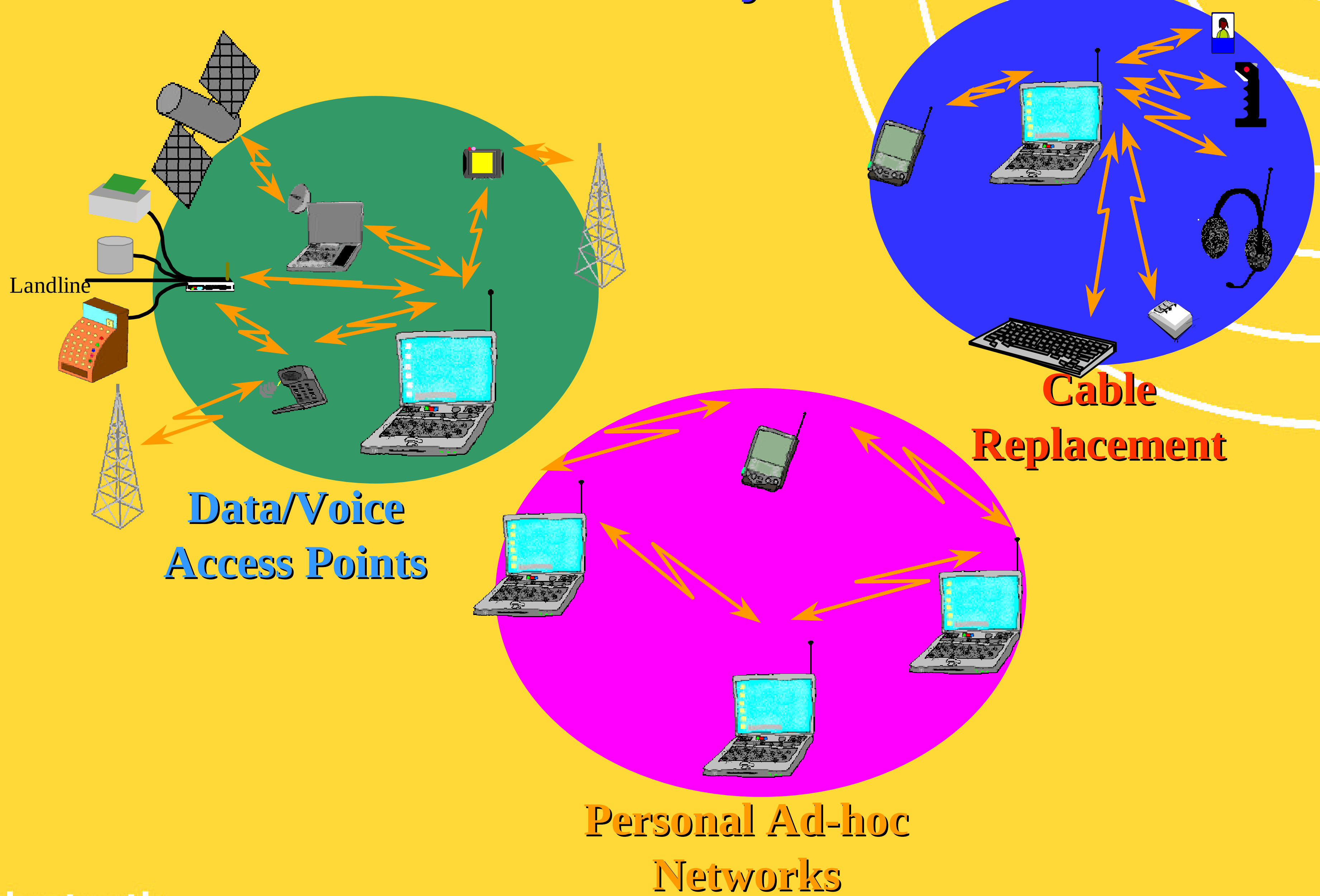
Bluetooth

"The Bluetooth Specification is still preliminary. All information regarding Bluetooth is subject to change without notice."

Agenda

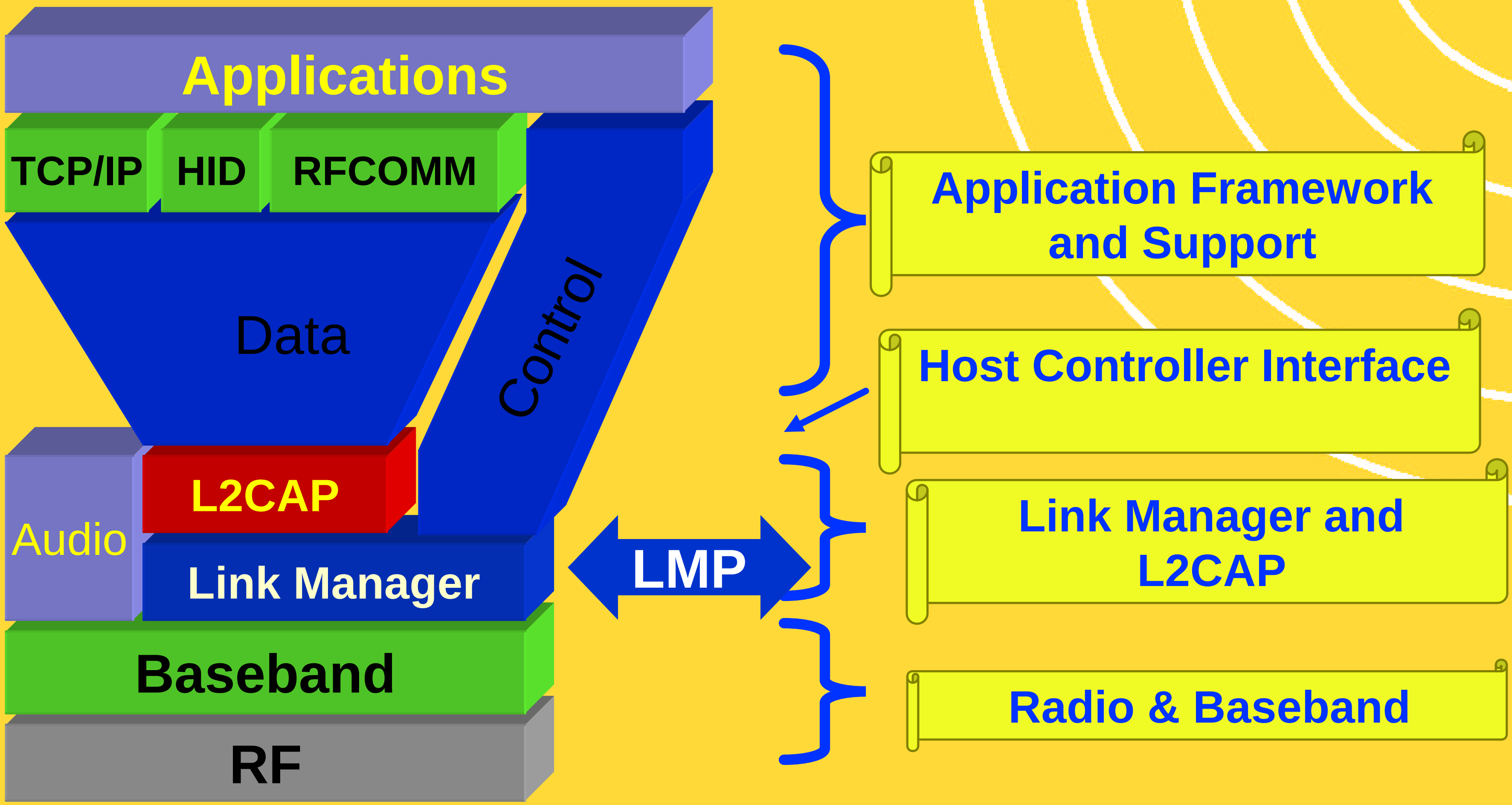
- **What does Bluetooth do for you?**
  - Usage model
- **What is Bluetooth?**
  - Compliance, compatibility
- **What does Bluetooth do?**
  - Technical points
- **Who is Bluetooth?**
  - History
- **Architectural Overview of Bluetooth**

What does Bluetooth do for you?



Bluetooth

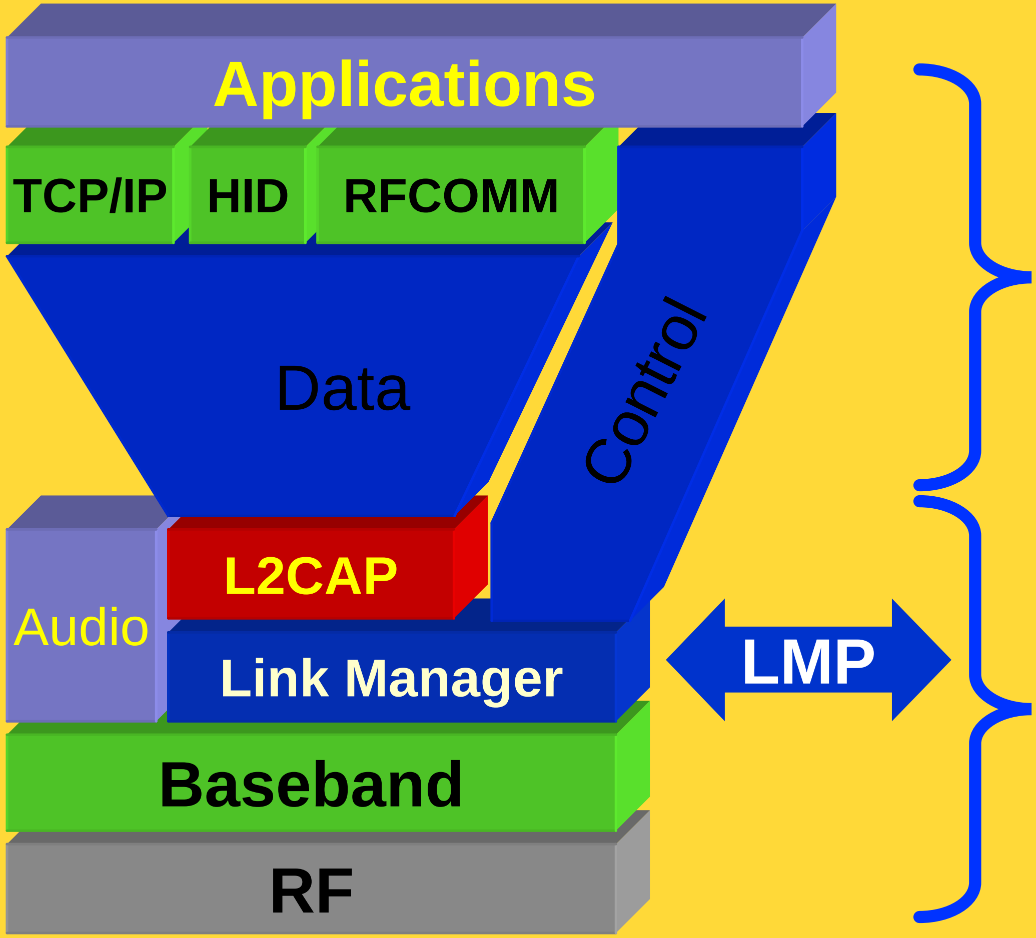
What is Bluetooth?

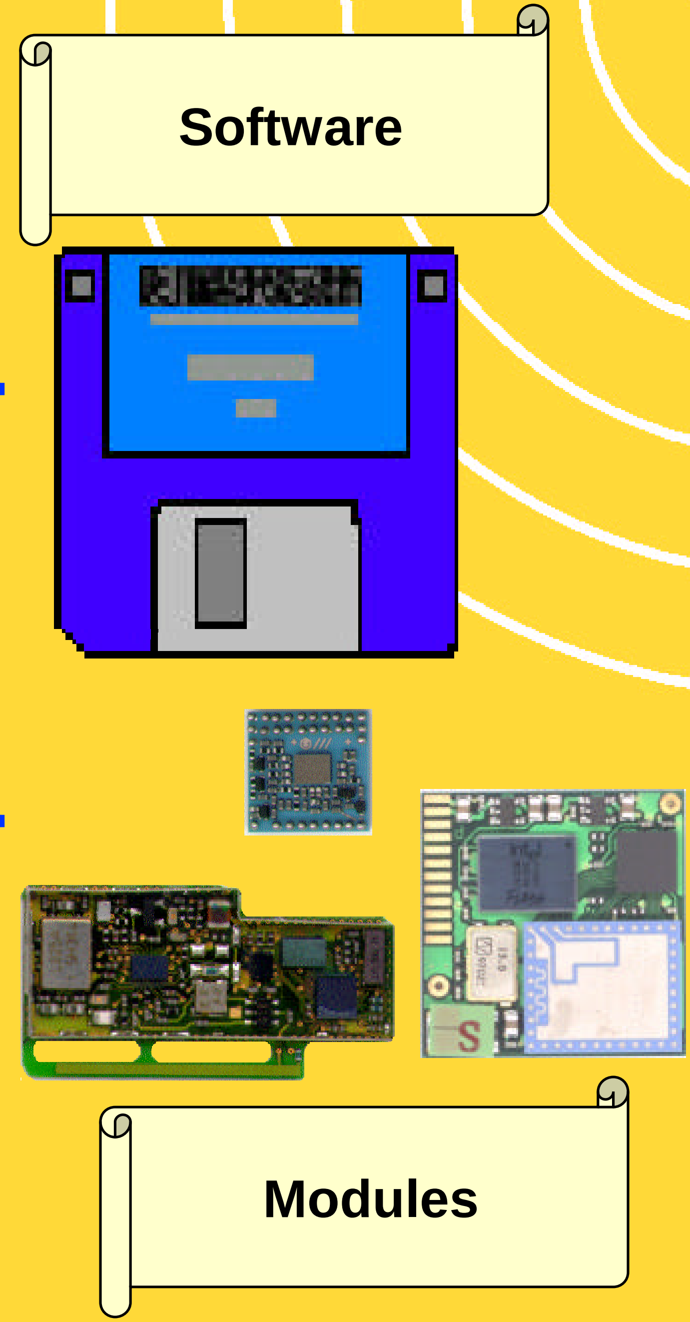


- A hardware description
- An application framework

Latest Version on Bluetooth Website: www.Bluetooth.com

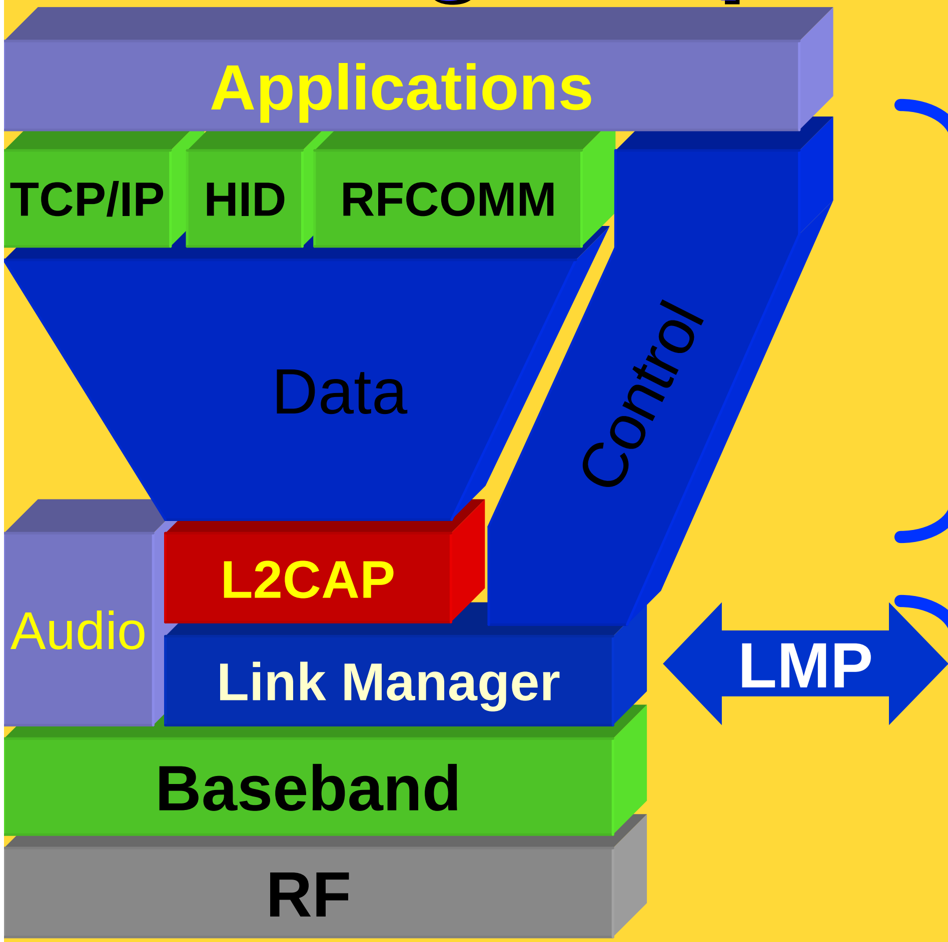
What is Bluetooth?





- A hardware description
- An application framework

Testing to Specification



Application Framework Certification

Service	Lower Interface Type	Lower Interface Class	Certification Class
vCard	IrOBEX	BT.OBEX	BT.vCard
vCal	IrOBEX	BT.OBEX	BT.vCal
UDP	PPP	BT.PPP	BT.UDP
PPP	RFCOMM	BT.TS0710	BT.PPP
IrOBEX	RFCOMM	BT.TS0710	BT.OBEX
WAP	TCP/IP	BT.TCP/IP	BT.WAP
Still Images	HID	BT.HID	BT.SImg
Audio Ctrl	L^{2}CAP	BT.L^{2}CAP-A	BT.AudioCtrl
RFCOMM	L^{2}CAP	BT.L^{2}CAP-D	BT.TS0710
TCP/IP	L^{2}CAP	BT.L^{2}CAP-D	BT.TCP/IP
HID	L^{2}CAP	BT.L^{2}CAP-D	BT.HID

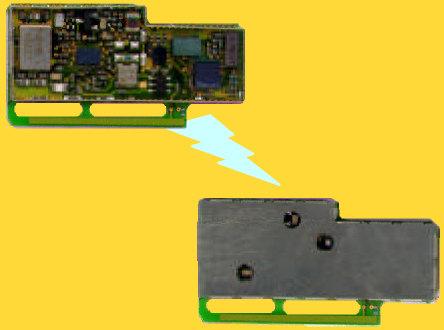
Basic Layer Certification

Service	Lower Interface Type	Lower Interface Class: Audio	Lower Interface Class: Data	Certification Class: Audio	Certification Class: Data
L^{2}CAP	LM	BT.LM-A	BT.LM-D	BT.L^{2}CAP-A	BT.L^{2}CAP-D
LM	BB	BT.BB-A	BT.BB-D	BT.LM-A	BT.LM-D
BB	RF	BT.RF	BT.RF	BT.BB-A	BT.BB-D
RF	Air	-	-	BT.RF	BT.RF

A unit that supports both audio and data gets the certification class A and D.
Example: BT.BB-A,D

- **Bluetooth devices will be tested against the specification**

What does Bluetooth Do?



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

- **Cable Replacement**

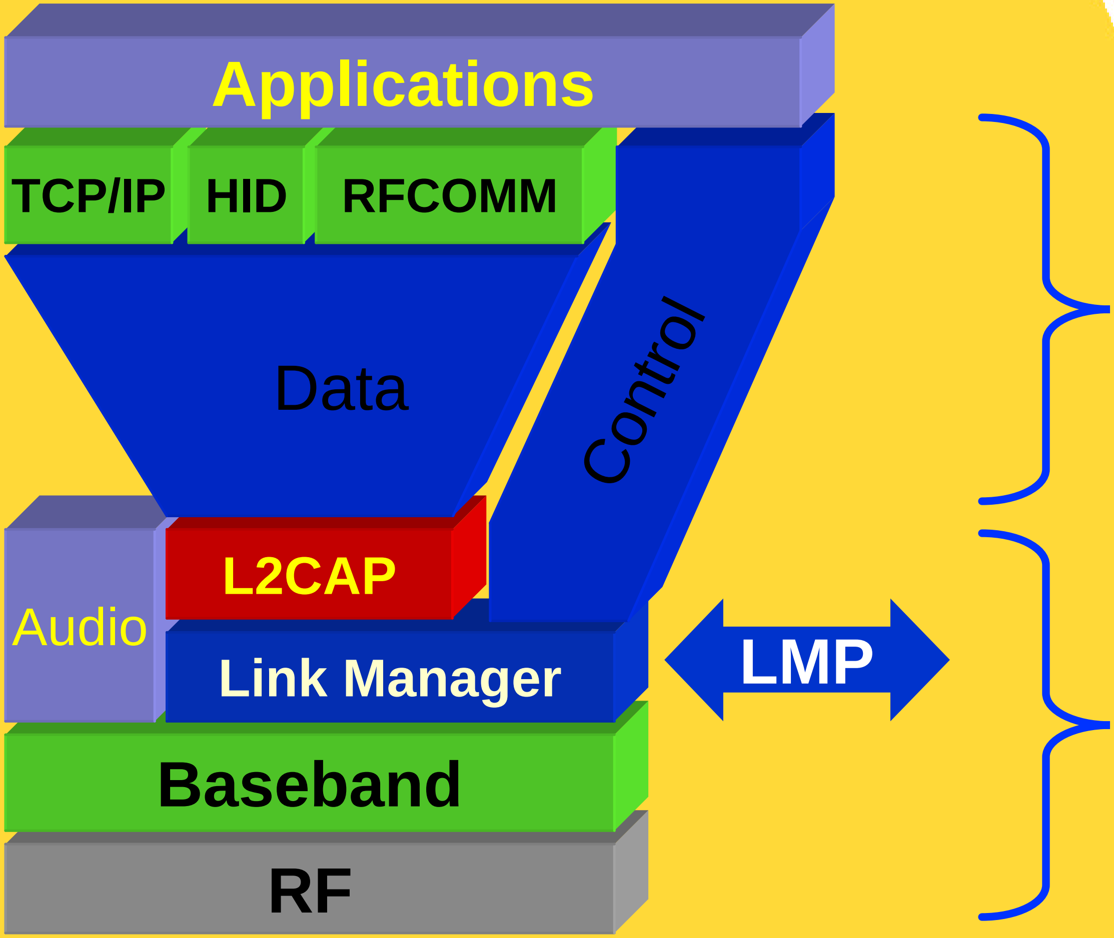
Who is Bluetooth?

- **Harald Blaatand "Bluetooth" II**
- **King of Denmark 940-981**
  - Son of Gorm the Old (King of Denmark) and Thyra Danebod (daughter of King Ethelred of England)

- **This is one of two Runic stones erected in his capitol city of Jelling (central Jutland)**
  - This is the front of the stone depicting the chivalry of Harald.
  - The stone's inscription ("runes") say:
    - Harald christianized the Danes
    - Harald controlled Denmark and Norway
    - Harald thinks notebooks and cellular phones should seamlessly communicate

Bluetooth

Architectural Overview



And a bit of this

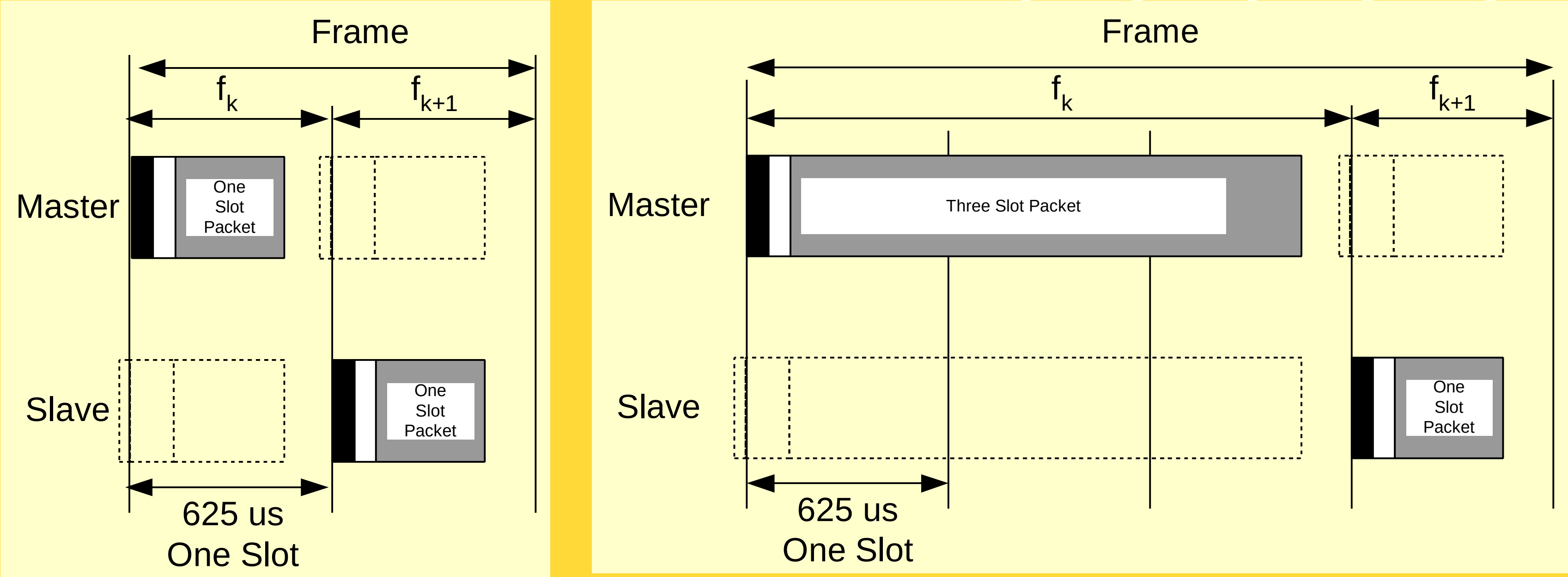
Cover This

Bluetooth RF Specifications

Specified for low cost, single chip implementation

- Noise floor margin for substrate noise and low current LNA
- Linearity set by near-far problem
- In-band image allows low-cost low IF
- VCO phase noise enables integrated VCO
- TX-RX turn around time enables single synthesizer
- 2.4 ISM band chosen for global use and process capabilities

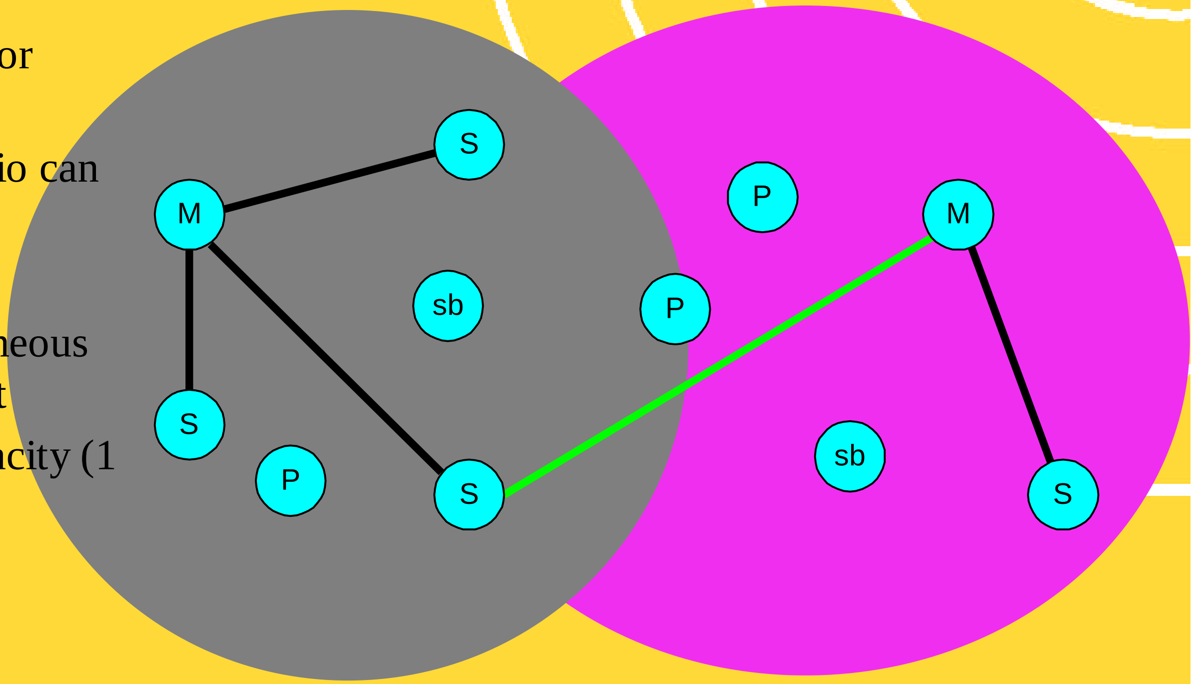
Basic Baseband Protocol



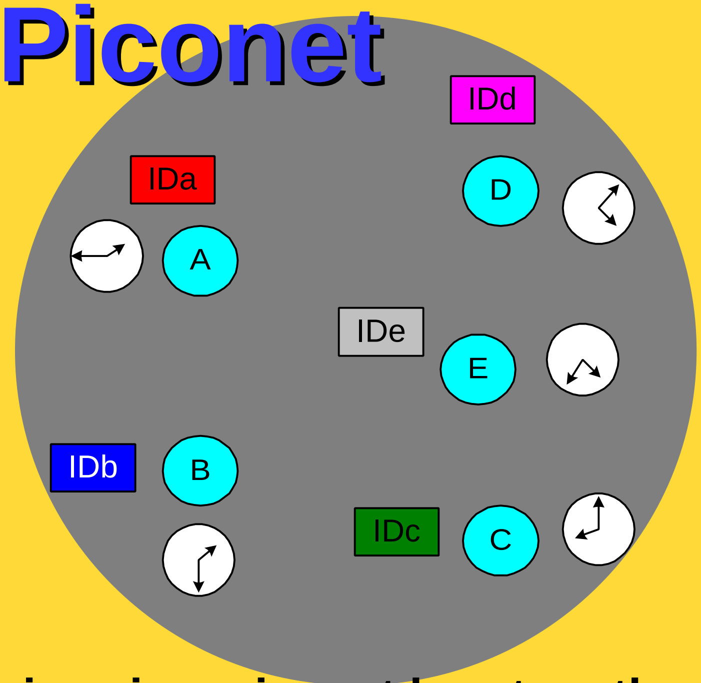
- **Spread spectrum frequency hopping radio**
  - 79/23 one MHz channels
  - Hops every packet
    - Packets are 1, 3 or 5 slots long
  - Frame consists of two packets
    - Transmit followed by receive
  - Nominally hops at 1600 times a second (1 slot packets)

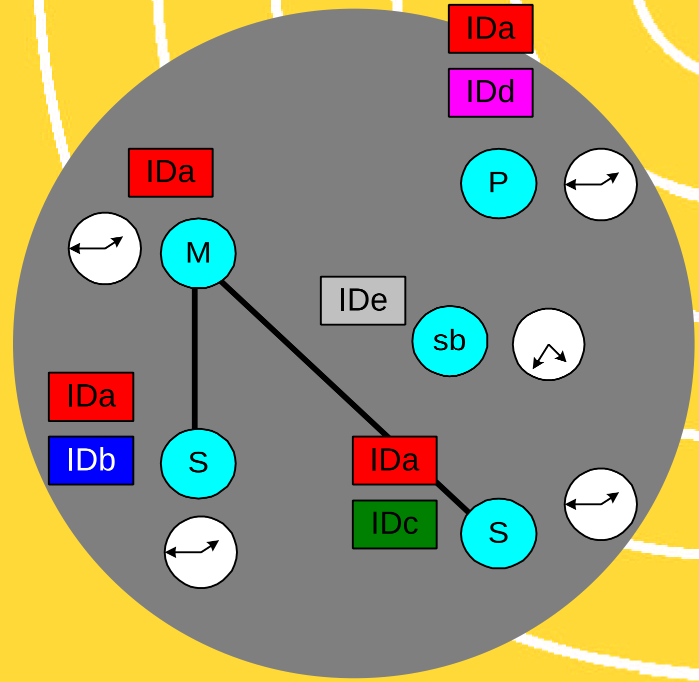
Network Topology

- **Radio Designation**
  - Connected radios can be master or slave
  - Radios are symmetric (same radio can be master or slave)
- **Piconet**
  - Master can connect to 7 simultaneous or 200+ active slaves per piconet
  - Each piconet has maximum capacity (1 MSPS)
    - Unique hopping pattern/ID
- **Scatternet**
  - High capacity system
    - Minimal impact with up to 10 piconets within range
  - Radios can share piconets!



The Piconet

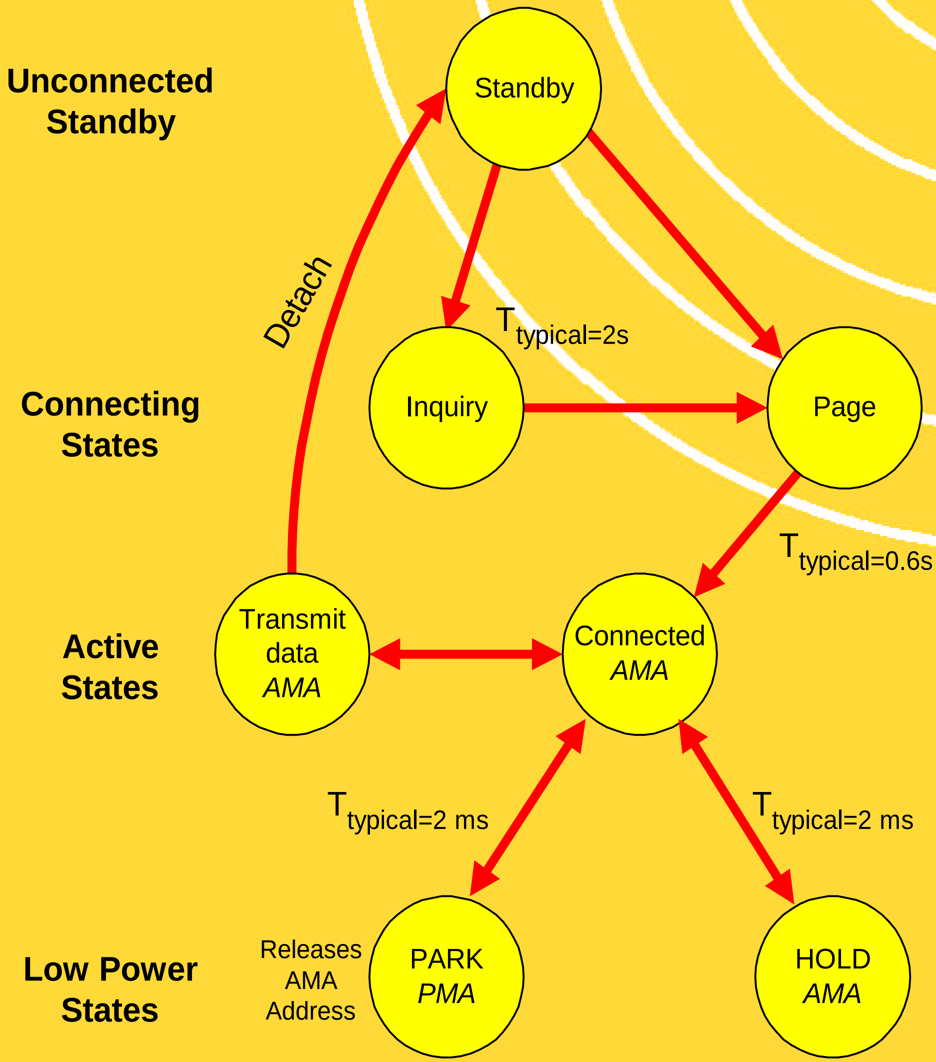




- **All devices in a piconet hop together**
  - In forming a piconet, master gives slaves its ***clock*** and ***device ID***
    - Hopping pattern determined by ***device ID*** (48-bit) IDa
    - Phase in hopping pattern determined by ***Clock***
- **Non-piconet devices are in standby** sb
- **Piconet Addressing**
  - ***Active Member Address*** (AMA, 3-bits) M **or** S
  - ***Parked Member Address*** (PMA, 8-bits) P

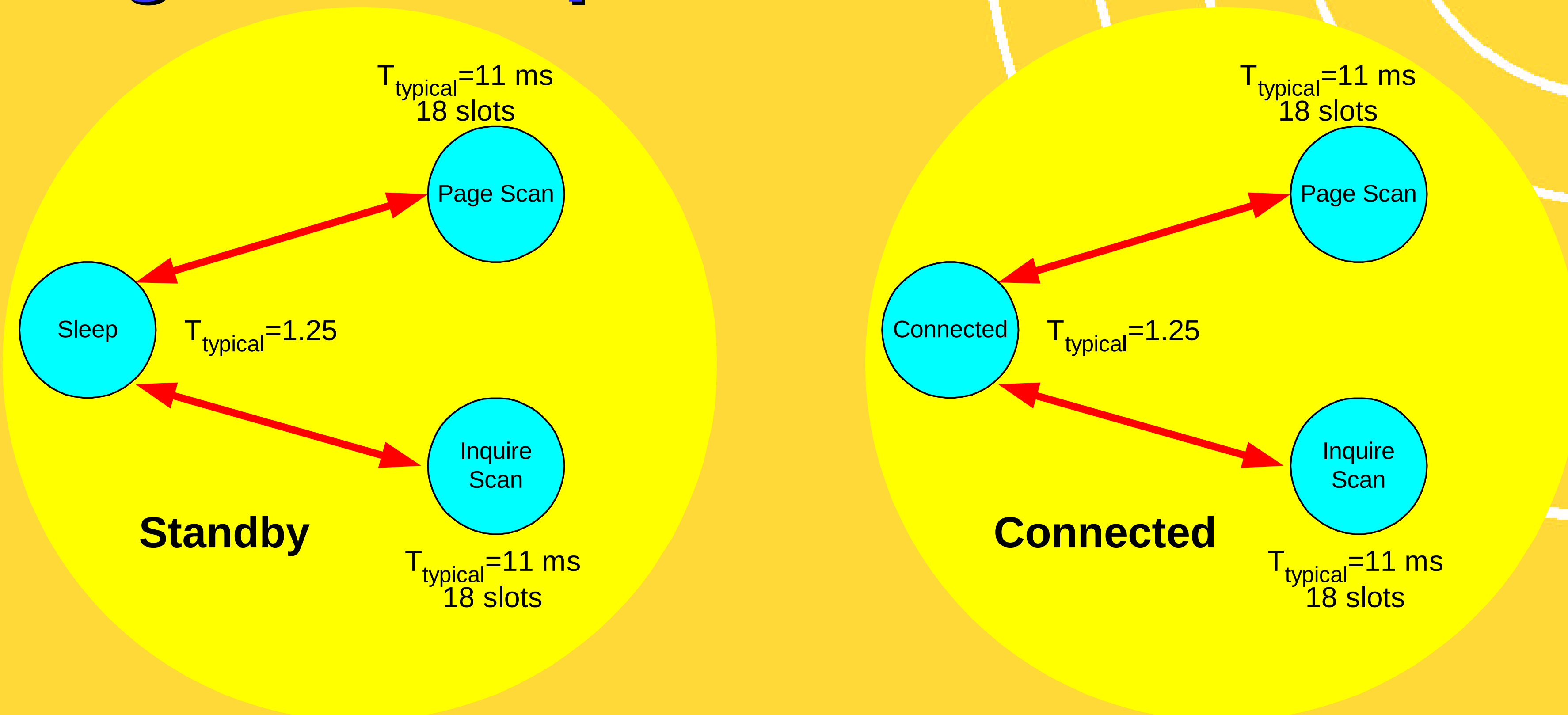
Functional Overview

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



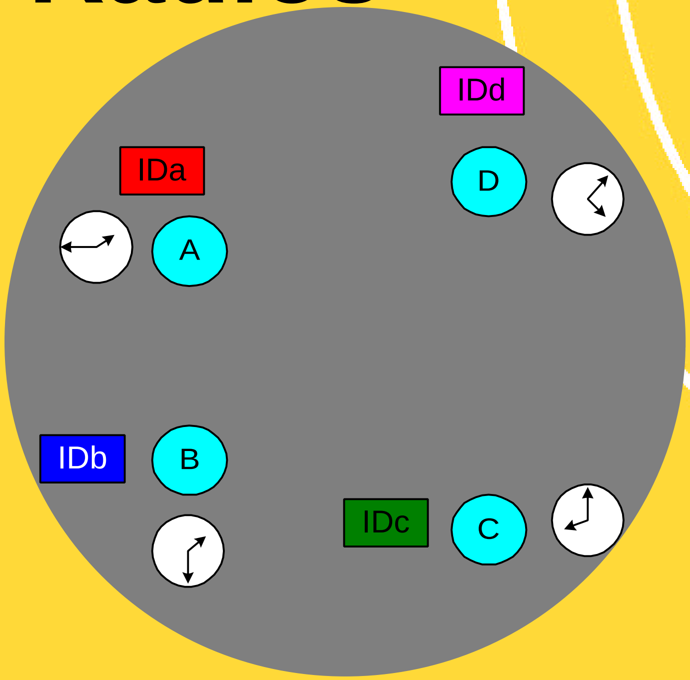
Bluetooth

Page and Inquire Scans



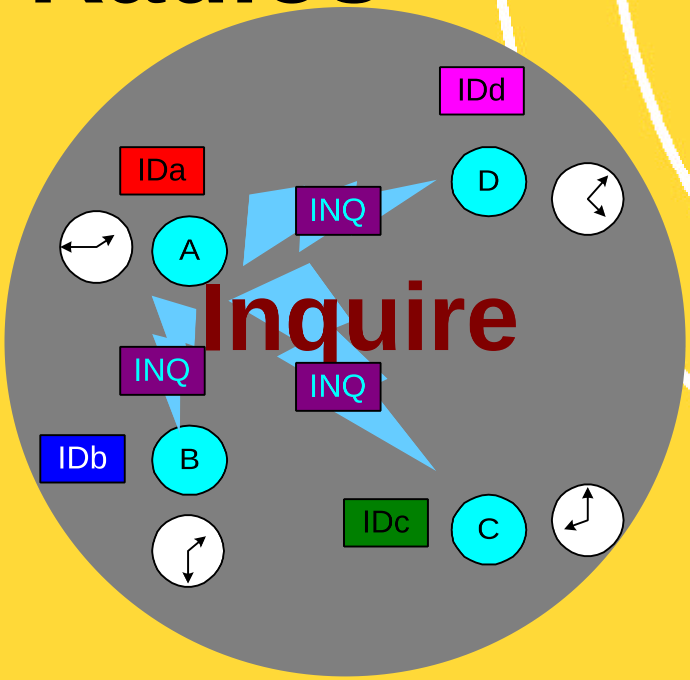
- **A radio must be enabled to accept pages or inquires**
  - Consumes 18 slots every 1.25 s (or so) for each scan
    - slot is 0.625 ms

Inquiring for Radios



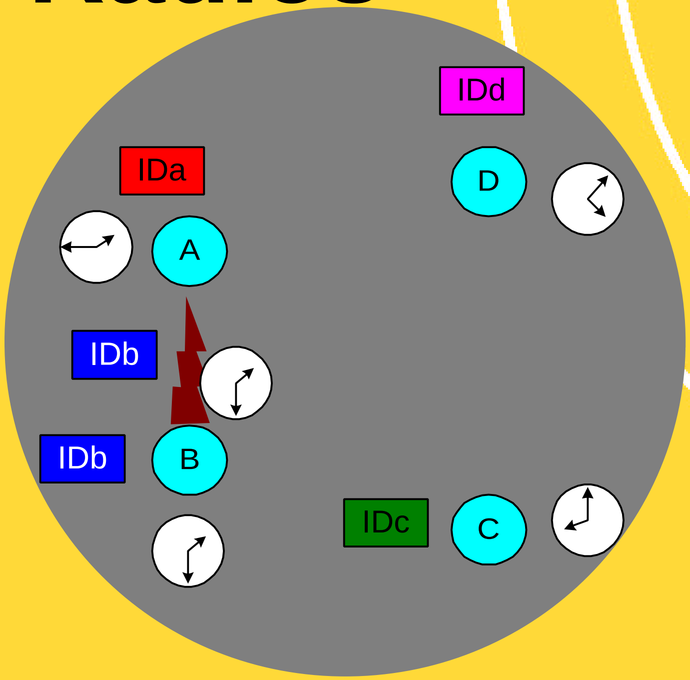
- Radio Wants to find other radios in the area

Inquiring for Radios



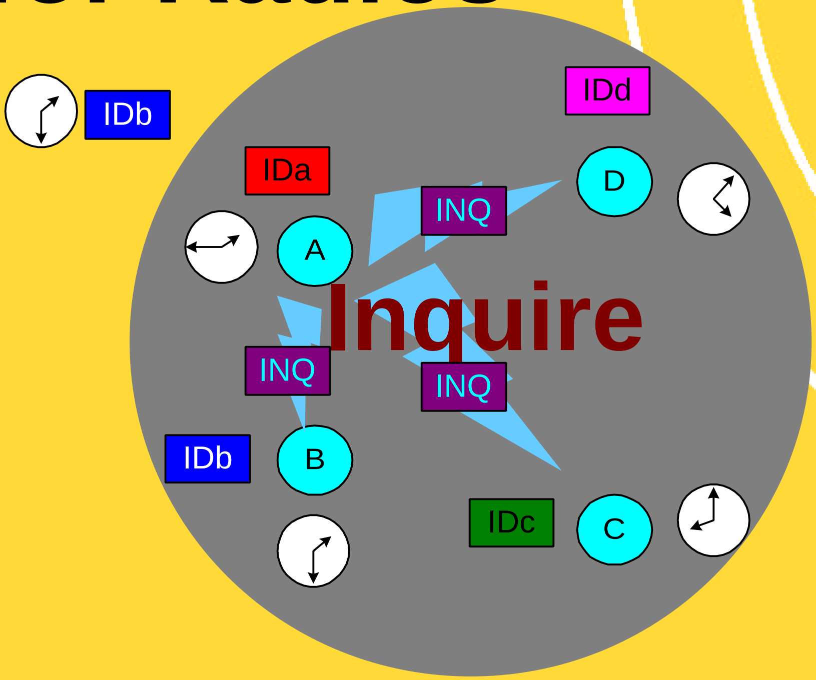
- **Radio Wants to find other radios in the area**
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing an Inquire Scan

Inquiring for Radios



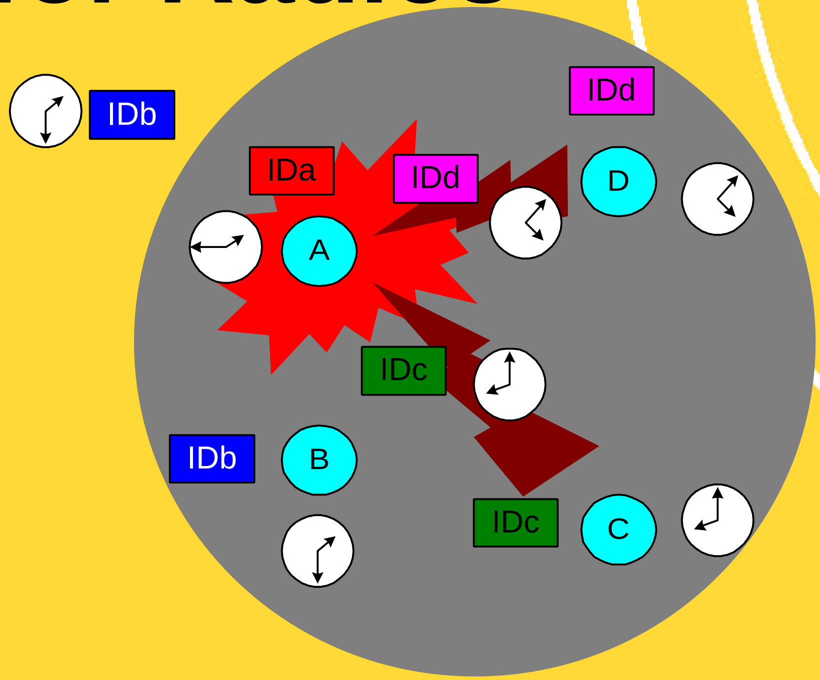
- **Radio Wants to find other radios in the area**
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing a Inquire Scan
  - Radio B recognizes Inquire and responds with an FHS packet
    - Has slave's ***Device ID*** and ***Clock***

Inquiring for Radios



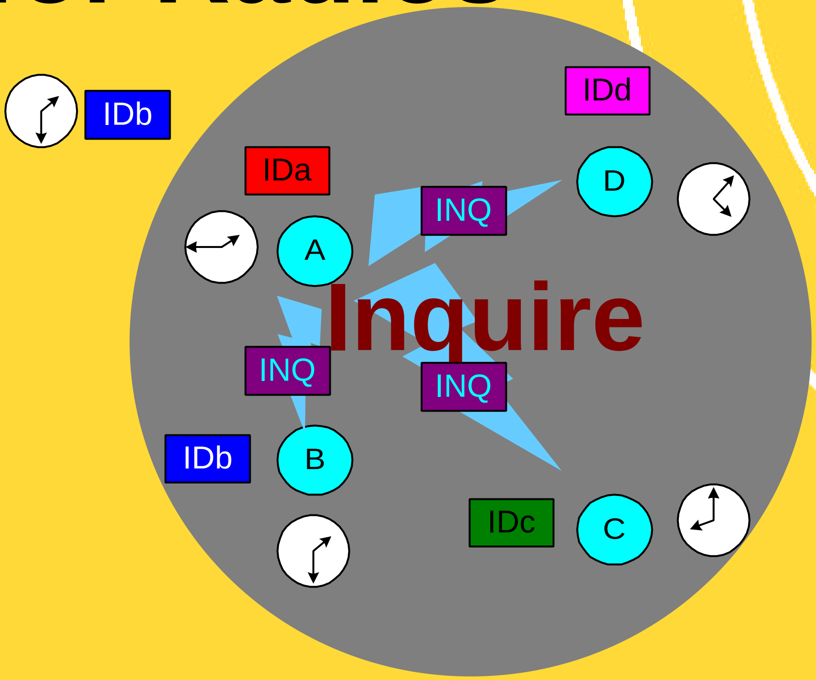
- **Radio Wants to find other radios in the area**
  - Radio A issues an Inquire (pages with the Inquire ID)
    - Radios B, C and D are doing a Inquire Scan
  - Radio B recognizes Inquire and responds with an FHS packet
    - Has slave's ***Device ID*** and ***Clock***

Inquiring for Radios



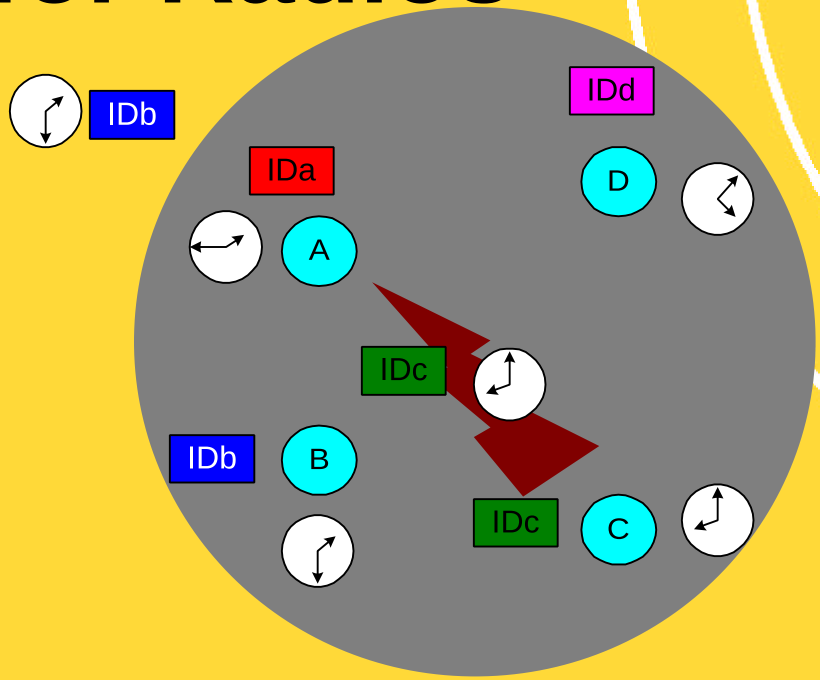
- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)
  - Radios C and D respond with FHS packets
    - As radios C & D respond simultaneously packets are corrupted and Radio A won't respond
    - Each radio waits a random number of slots and listens

Inquiring for Radios



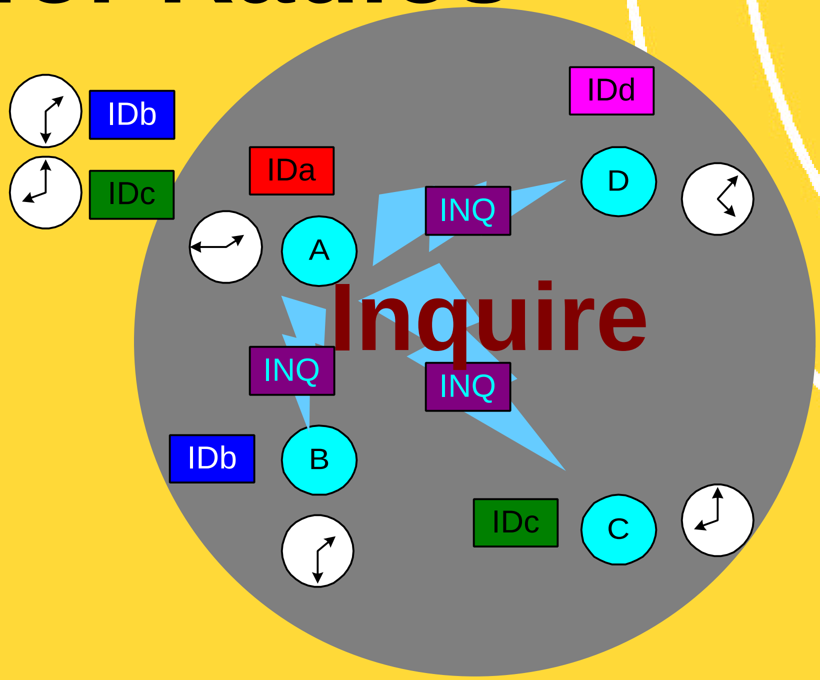
- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)

Inquiring for Radios



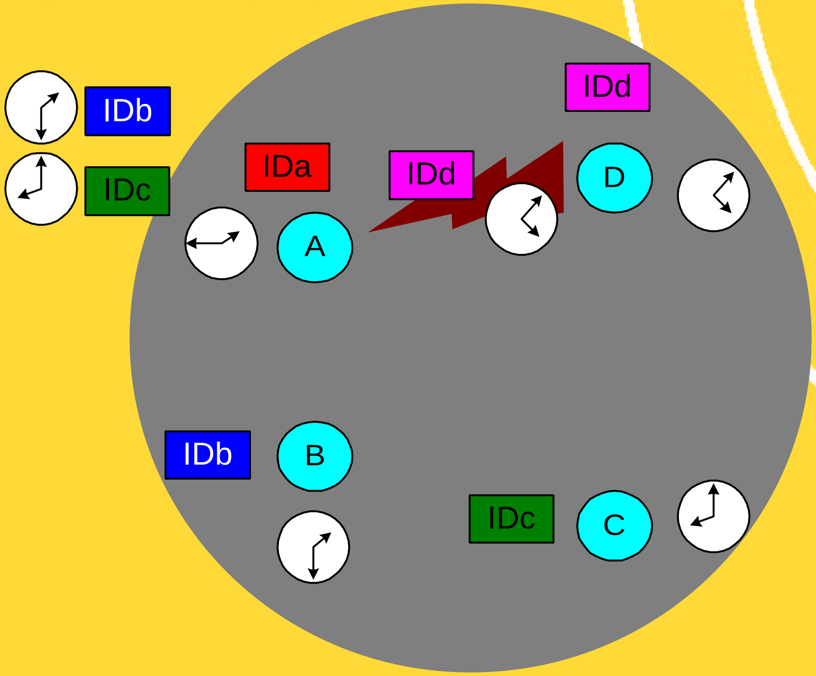
- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)
  - Radios C respond with FHS packets

Inquiring for Radios



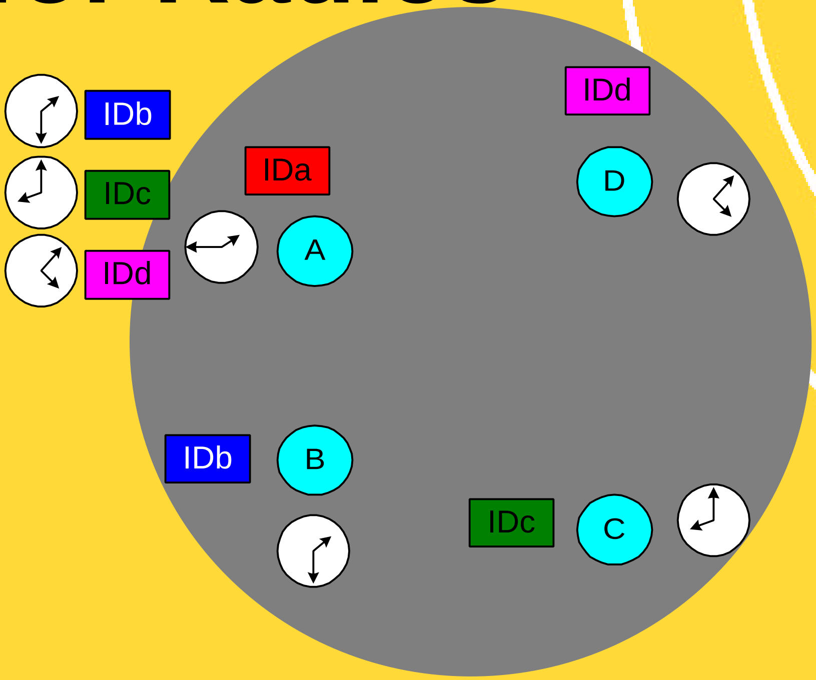
- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)

Inquiring for Radios



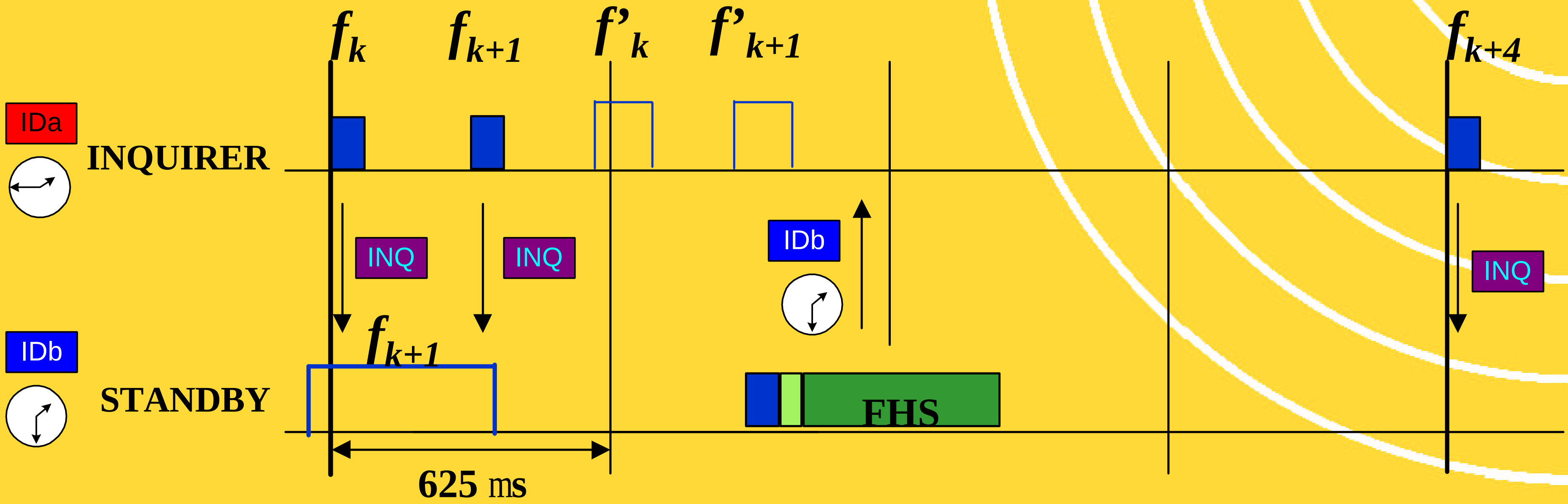
- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)
  - Radios D respond with FHS packets

Inquiring for Radios



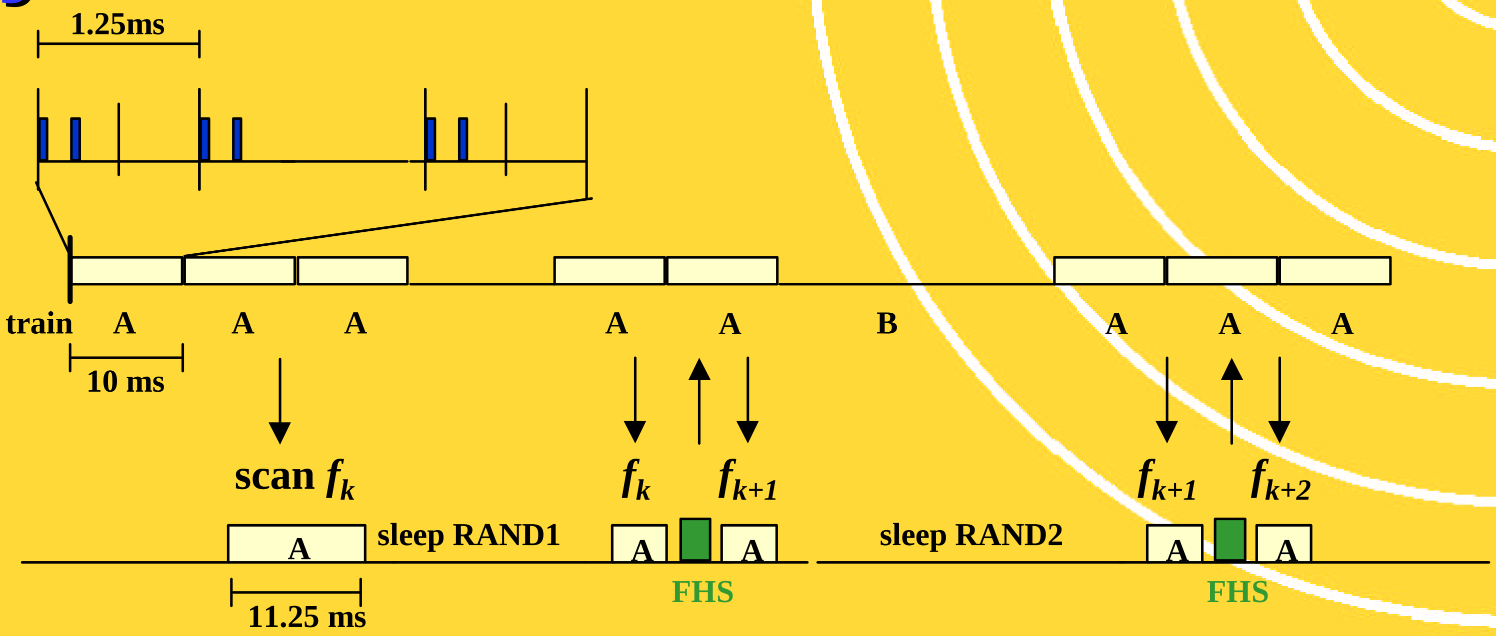
- **Radio Wants to find other radios in the area**
  - Radio A Issues an Inquire (again)
  - Radios D respond with FHS packets
  - Radio A now has information of all radios within range

Inquiry Procedure



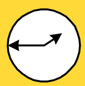
- **Inquiry has unique device address (all BT radio use)**
  - Unique set of “Inquiry” hop frequencies
- **Any device can inquire by paging the Inquiry address**
- **Correlater hit causes slave to respond with FHS packet**
  - ***Device ID***
  - ***Clock***

Inquiry Procedure

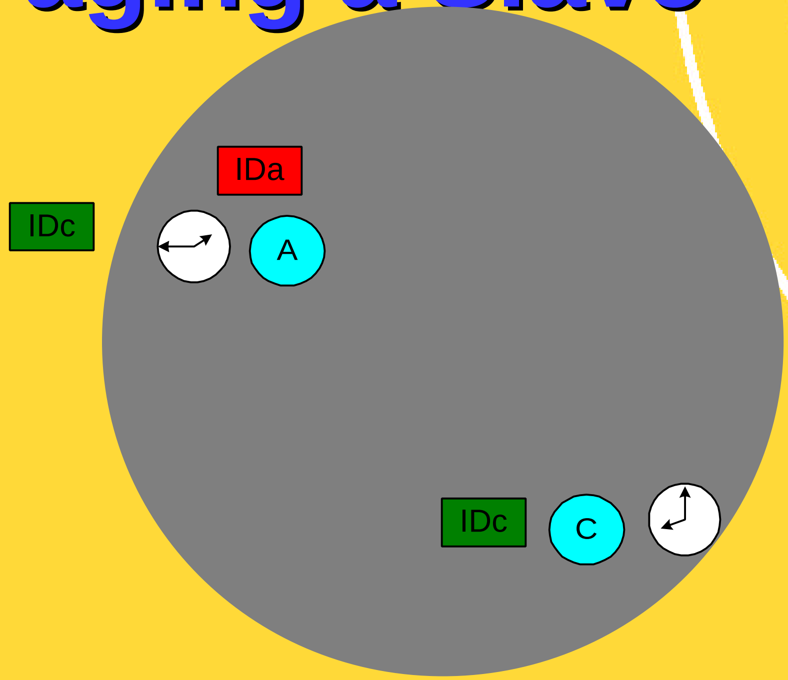


- **Multiple slaves are expected to respond**
  - Correlater hit causes slave to
    - respond with FHS packet
    - Wait a random number of slots
    - Wait for another Inquiry page and repeat
- **Master should end up with a list of slave FHS packets in area**

Inquire Summary

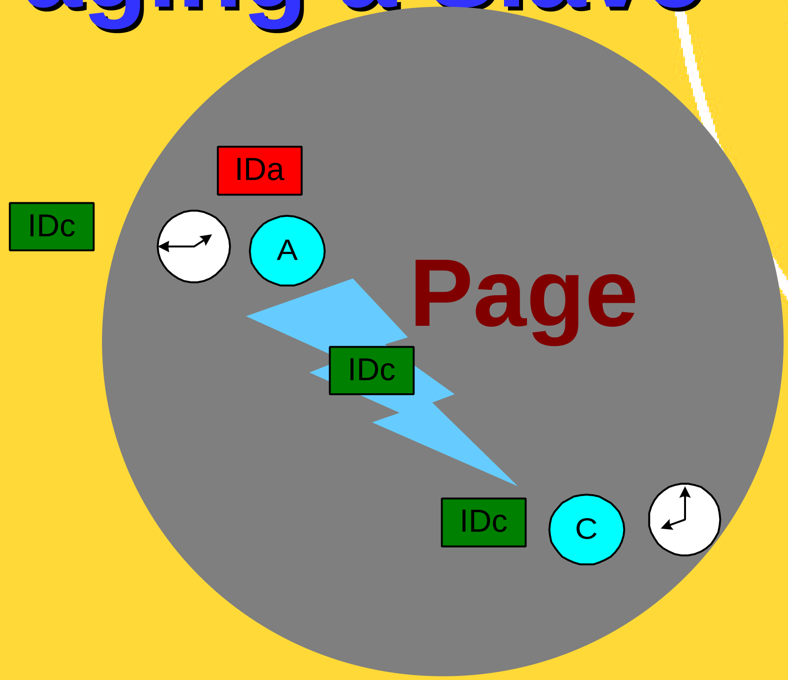
- **Paging radio Issues page packet with Inquire ID**
- **Any radio doing an Inquire scan will respond with an FHS packet**
  - FHS packet gives Inquiring radio information to page
    - ***Device ID*** IDa
    - ***Clock*** 
  - If there is a collision then radios wait a random number of slots before responding to the page inquire
- **After process is done, Inquiring radio has *Device IDs* and *Clocks* of all radios in range**

Master Paging a Slave



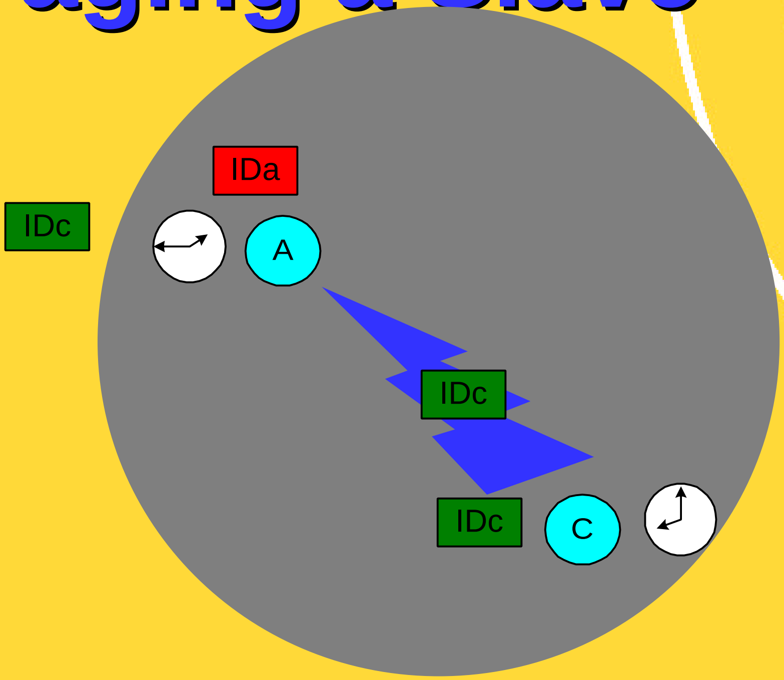
- Paging assumes master has slaves ***Device ID*** **and an idea of its** ***Clock***

Master Paging a Slave



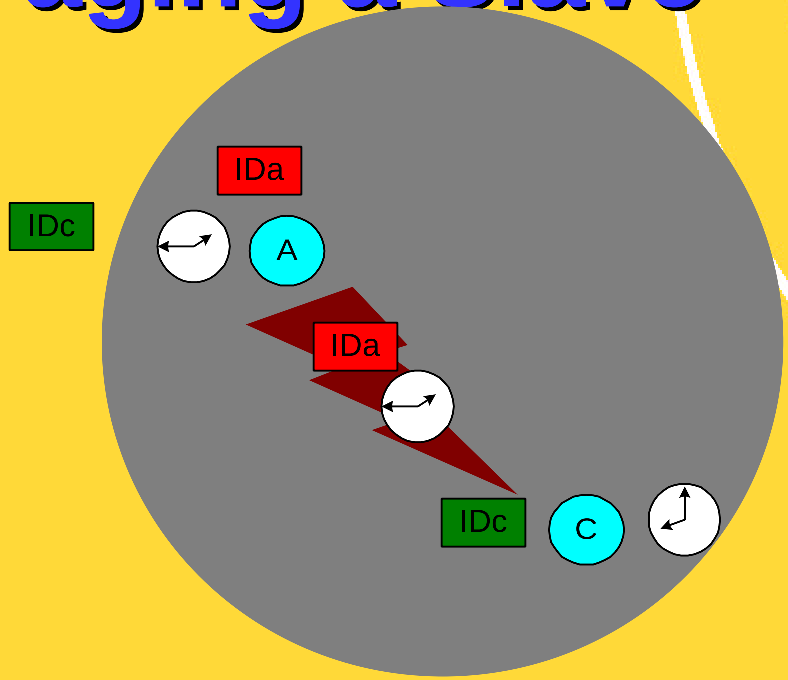
- **Paging assumes master has slaves *Device ID* and an idea of its *Clock***
  - A pages C with C’s ***Device ID***

Master Paging a Slave



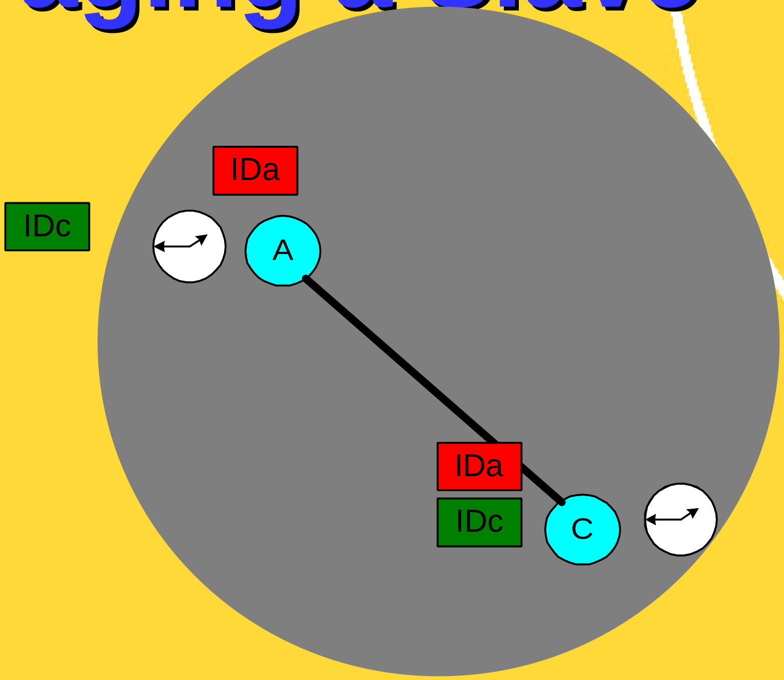
- **Paging assumes master has slaves *Device ID* and an idea of its *Clock***
  - A pages C with C's ***Device ID***
  - C Replies to A with C's ***Device ID***

Master Paging a Slave



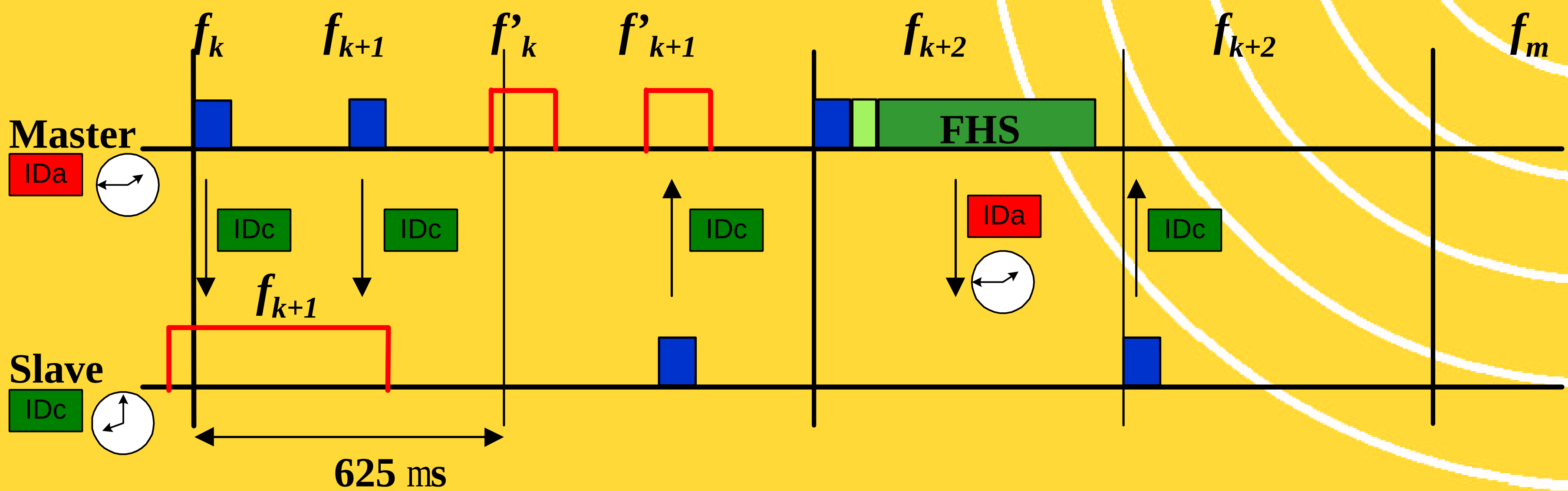
- **Paging assumes master has slaves *Device ID* and an idea of its *Clock***
  - A pages C with C's ***Device ID***
  - C Replies to A with C's ***Device ID***
  - A sends C its ***Device ID*** and ***Clock*** (FHS packet)

Master Paging a Slave



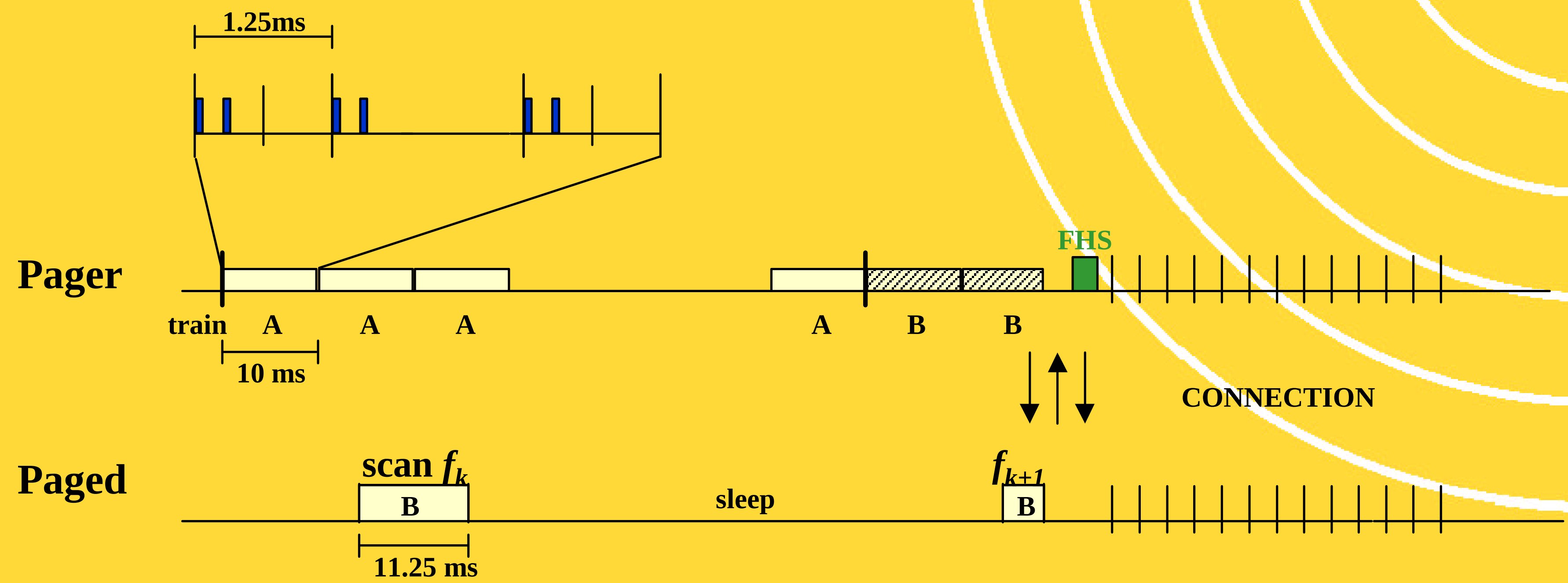
- **Paging assumes master has slaves *Device ID* and an idea of its *Clock***
  - A pages C with C's ***Device ID***
  - C Replies to A with C's ***Device ID***
  - A sends C its ***Device ID*** and ***Clock*** (FHS packet)
  - A connects as a master to C

Master Paging a slave



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

Paging Procedure



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

PHYSICAL LINK DEFINITION (II)

SYNCHRONOUS CONNECTION-ORIENTED (SCO) LINK

- circuit switching
- symmetric, synchronous services
- slot reservation at fixed intervals

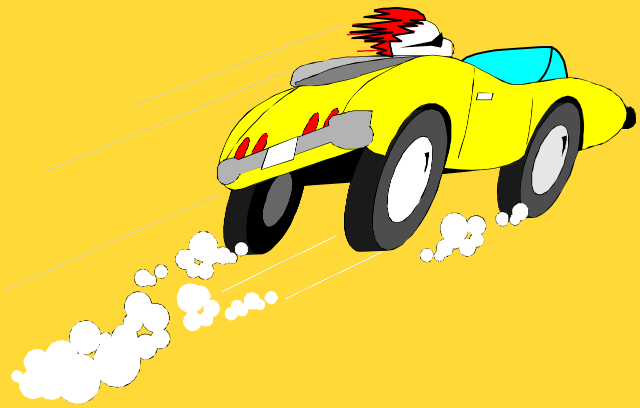
ASYNCHRONOUS CONNECTION-LESS (ACL) LINK

- packet switching
- (a)symmetric, asynchronous services
- polling access scheme

Packet Types/Data Rates

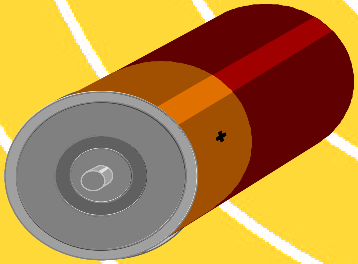
Packet Types			
SEGMENT	TYPE	SCO link	ACL link
1	0000	NULL	NULL
	0001	POLL	POLL
	0010	FHS	FHS
	0011	DM1	DM1
2	0100		DH1
	0101	HV1	
	0110	HV2	
	0111	HV3	
	1000	DV	
	1001		AUX1
3	1010		DM3
	1011		DH3
	1100		
	1101		
4	1110		DM5
	1111		DH5

Data Rates (Kbps)			
TYPE	symmetric	asymmetric	
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



Mobile = Battery life

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

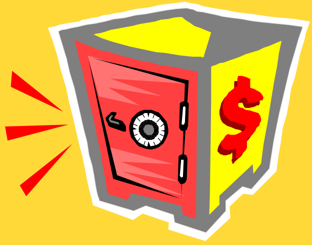


* Estimates calculated with 600 mAh battery and internal amplifier, power will vary with implementation

Bluetooth

Bluetooth Security

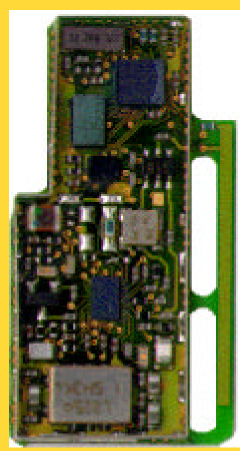
- **Provides link layer security between any two Bluetooth radios**
  - Authentication (E1 algorithm)
    - Challenge/Response system
  - Encryption (privacy)
    - Encrypts data between two devices
    - Stream cipher with E0 algorithm
  - Key management and usage
    - Configurable Encryption key length (0-16 bytes)
      - Government export regulations
      - Radio negotiate key size
    - Key generation with E2-E3 algorithms
      - Authentication and Encryption keys

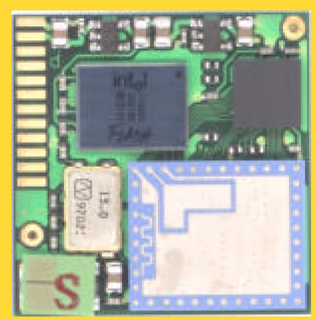


Bluetooth Radio Modules

- **Complete radio on a module**
  - Designed to meet “Limited Module Compliance” requirements
    - Pre-certified to meet global regulatory requirements
    - Allows devices assembled with modules to be “self-certified”
  - USB or Serial Interface
  - Solder-ball connections
  - External Antennae

Production Module





Compact FLASH Card

25 mm dia	17x33mm	19x35mm	25x25mm	36x43mm

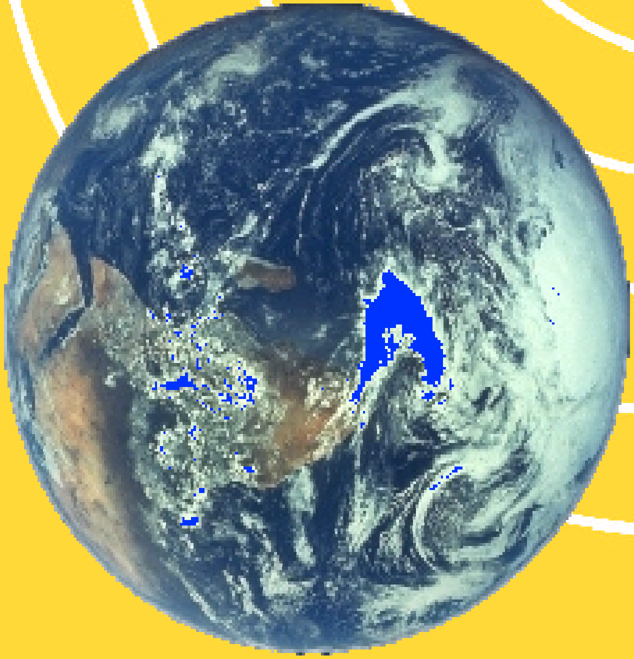
The international 2.4 GHz ISM band

- **Requirements**
  - Channel bandwidth limited to 1 MHz
  - Spectrum spreading must be employed
  - Multiple uncoordinated networks may exist and cause interference
  - Microwave ovens also use this band
  - 2.4 GHz IC electronics must run at high current levels

- **Bluetooth solution**
  - 1 Mb/s symbol rate exploits maximum channel bandwidth
  - Fast frequency hopping and short data packets avoids interference
  - CVSD voice coding enables operation at high bit error rates
  - Air interface tailored to minimize current consumption
  - Relaxed link budget supports low cost single chip integration

Bluetooth is global

- **One version for the world**
  - Architecture compliant with global emission rules (2.4 GHz ISM band)
    - Working through FCC, EC, MPT for spectrum and power harmonization
  - Architecture compliant and safe for use on airlines
    - Working with FAA, JAA, FCC, airplane manufacturers and airlines
  - Reviewing security architecture with affected countries

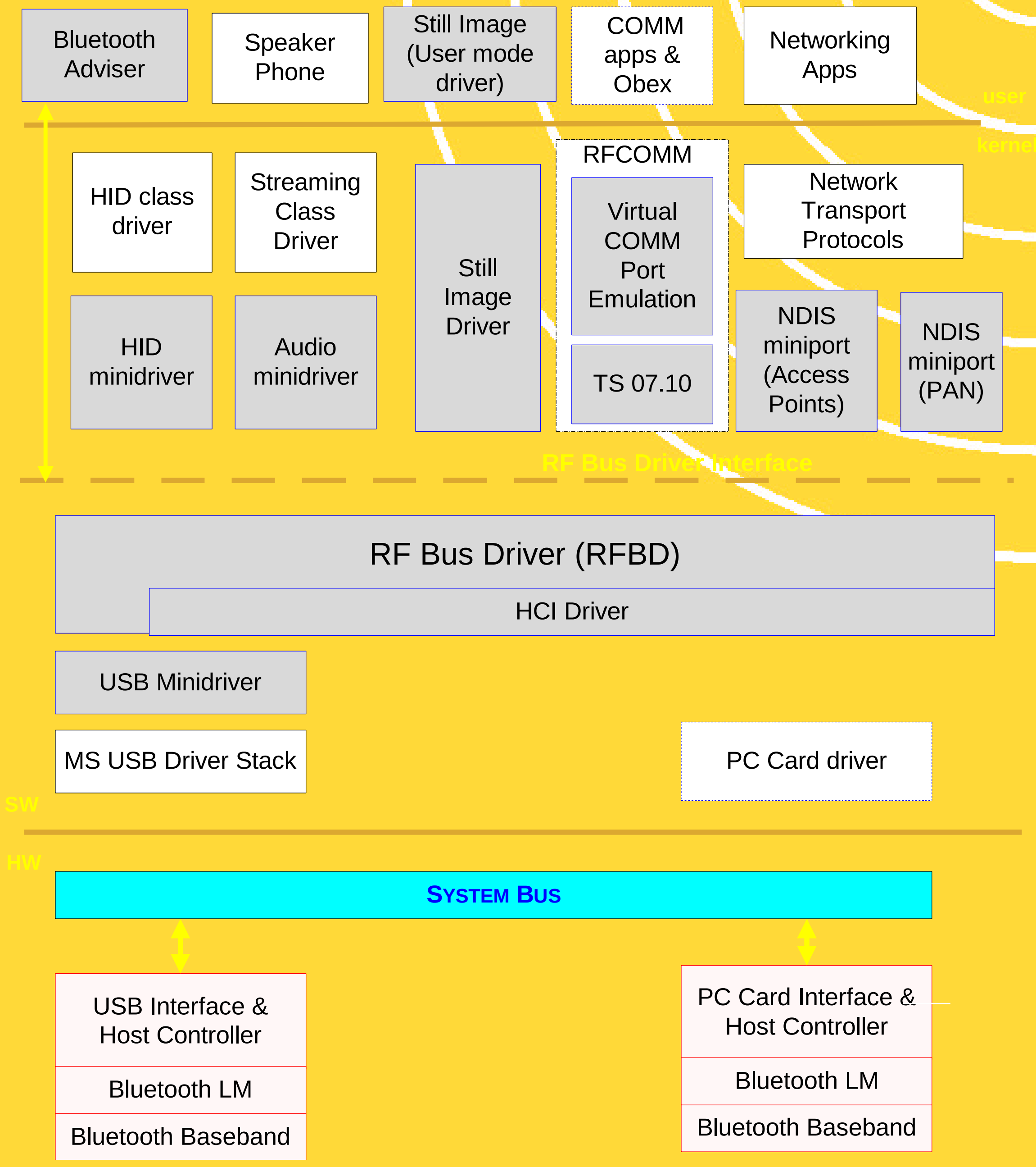


Software Goals

- **Good out of box experience**
  - Should provide value with existing applications
    - Utilize existing APIs and protocols where possible
  - Should be introduced with hardware that provides value
    - Notebooks
    - Cellphones
    - Handhelds
  - Should support the usage model
    - Data access points (POTs Modem, cellphone, …)
    - Cable replacement (Speaking laptop, instant postcard, …)
    - Ad-hoc networking (File exchange, …)

Example Software Implementation

- **PC Windows* example supporting the Bluetooth usage model**
  - WDM Driver
    - Windows* 2000
    - Windows 98*



Bluetooth

Summary

- **Bluetooth is a radio system (not a radio)**
  - Hardware
  - Software framework
  - Interoperability requirements
- **Bluetooth Radio System is optimized for mobility**
  - Primarily cable replacement
    - NOT a WLAN technology
  - Targeted for Global use by mobile users