COEN-4720 Embedded Systems

Lecture 8
BlueTooth

Cris Ababei
Dept. of Electrical and Computer Engineering

MARQUETTE UNIVERSITY

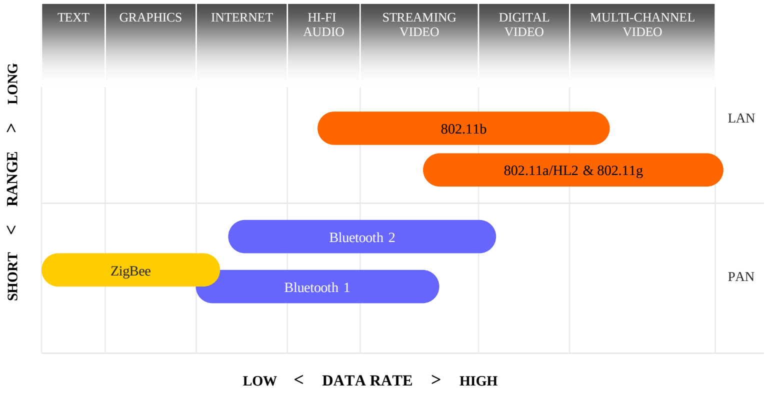
BE THE DIFFERENCE.

Outline

- BlueTooth
  - Motivation, releases
  - Introduction and Specs
  - Basic Idea
  - Protocol stack
  - Network topology
  - Security
  - Antennas
  - Bluetooth vs. Wi-Fi
- BlueTooth Modules
- Example Application + Demo

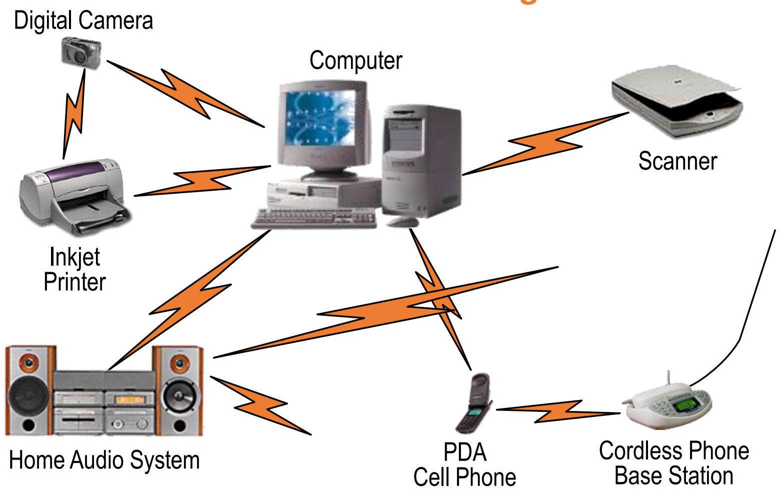
Wireless Technologies: BlueTooth

- Bluetooth
- WiFi
- Cellular
- 3G (3rd Generation)
- UWB (Ultra Wide Band)
- FSO (Free Space Optics)
- WiMAX
- ZigBee
- …



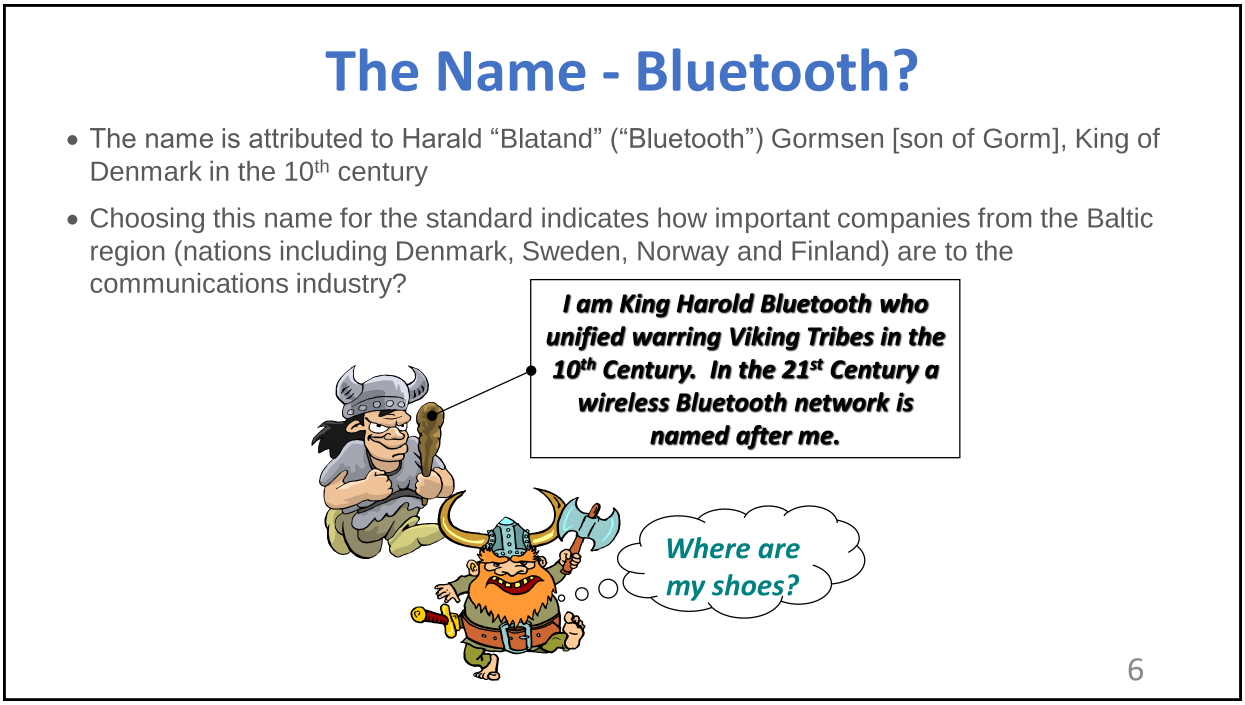
BlueTooth - Motivation

- Cable replacement
- Ad-hoc networking



Requirements

- Low cost as cables – chip $5
- Must be low power, compact and global
- Secure as cables – must support authentication and encryption
- Must support both data and voice
- Must connect to a variety of devices.
- Must support many simultaneous and private “piconets”.
- Must be able to function in a noisy environment.
- Use 2.45GHz radio frequency band – ISM (Industrial, Scientific and Medical)



The Name - Bluetooth?

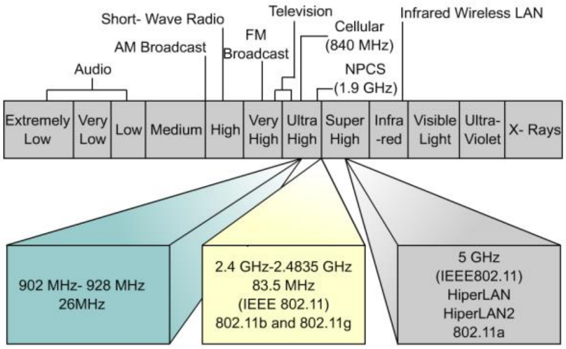
- The name is attributed to Harald “Blatand” (“Bluetooth”) Gormsen [son of Gorm], King of Denmark in the 10th century
- Choosing this name for the standard indicates how important companies from the Baltic region (nations including Denmark, Sweden, Norway and Finland) are to the communications industry?

I am King Harold Bluetooth who unified warring Viking Tribes in the 10th Century. In the 21st Century a wireless Bluetooth network is named after me.

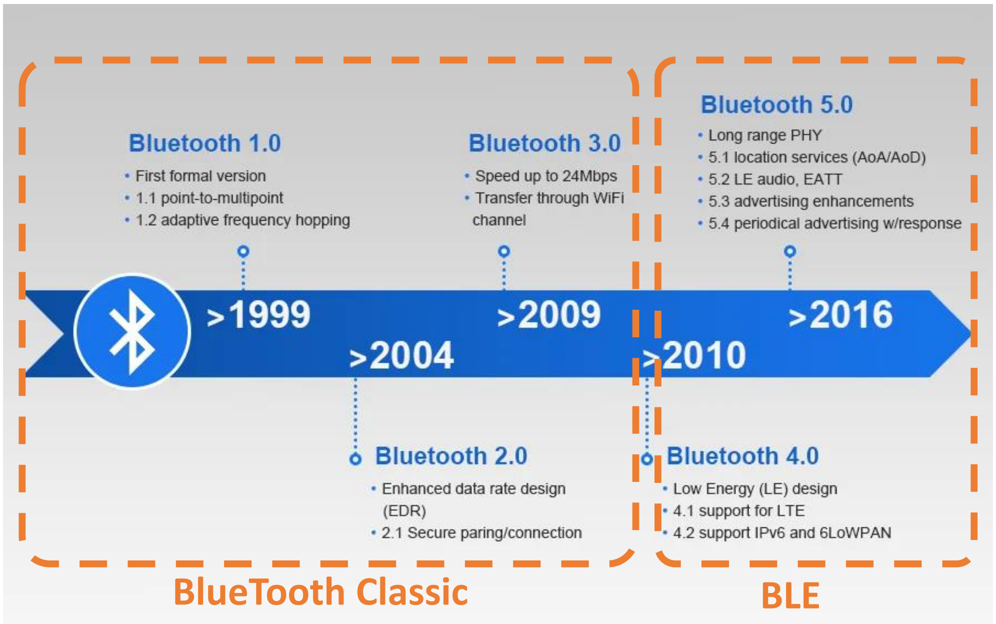
BlueTooth - Introduction

- BlueTooth (BT) is a wireless technology standard
- Invented by Dutch electrical engineer Jaap Haartsen working for Ericsson in 1994
- Initially intended as wireless alternative to RS-232 cables
- IEEE 802.15 committee standardized the physical and link layers
- Managed by Bluetooth Special Interest Group (SIG); >40,000 member companies
- Short distances
- Short-wavelength UHF radio waves in unlicensed ISM (**Industrial, Scientific and Medical**) band, 2.400 to 2.485 GHz
- Fixed and mobile devices
- Building personal area networks (PANs)

US Frequency Bands



Band	**Frequency range**
UHF ISM	902-928 MHz
S-Band	2-4 GHz
S-Band ISM	**2.4-2.5 GHz**
C-Band	4-8 GHz
C-Band satellite downlink	3.7-4.2 GHz
C-Band Radar (weather)	5.25-5.925 GHz
C-Band ISM	5.725-5.875 GHz
C-Band satellite uplink	5.925-6.425 GHz
X-Band	8-12 GHz
X-Band Radar (police/weather)	8.5-10.55 GHz



Bluetooth 1.0
- First formal version
- 1.1 point-to-multipoint
- 1.2 adaptive frequency hopping

Bluetooth 2.0
- Enhanced data rate design (EDR)
- 2.1 Secure paring/connection

Bluetooth 3.0
- Speed up to 24Mbps
- Transfer through WiFi channel

Bluetooth 4.0
- Low Energy (LE) design
- 4.1 support for LTE
- 4.2 support IPv6 and 6LoWPAN

Bluetooth 5.0
- Long range PHY
- 5.1 location services (AoA/AoD)
- 5.2 LE audio, EATT
- 5.3 advertising enhancements
- 5.4 periodical advertising w/response

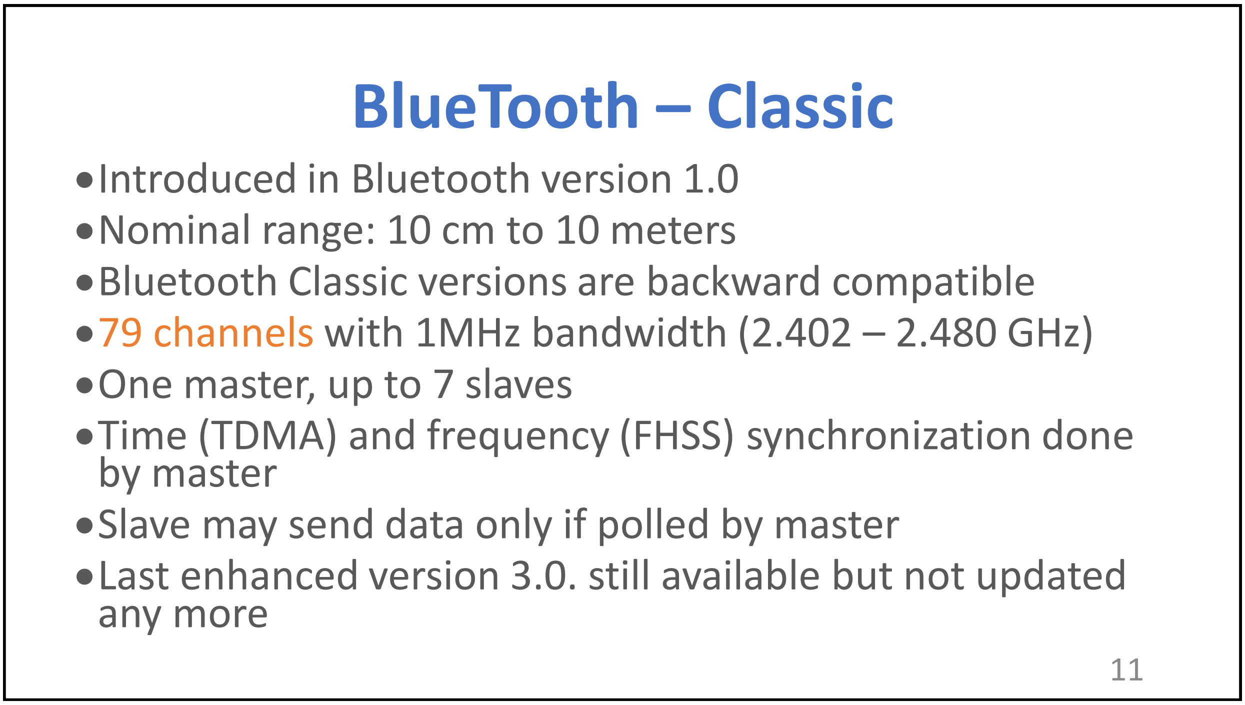
BlueTooth Classic

BLE

https://www.mokosmart.com/guide-on-different-bluetooth-versions/

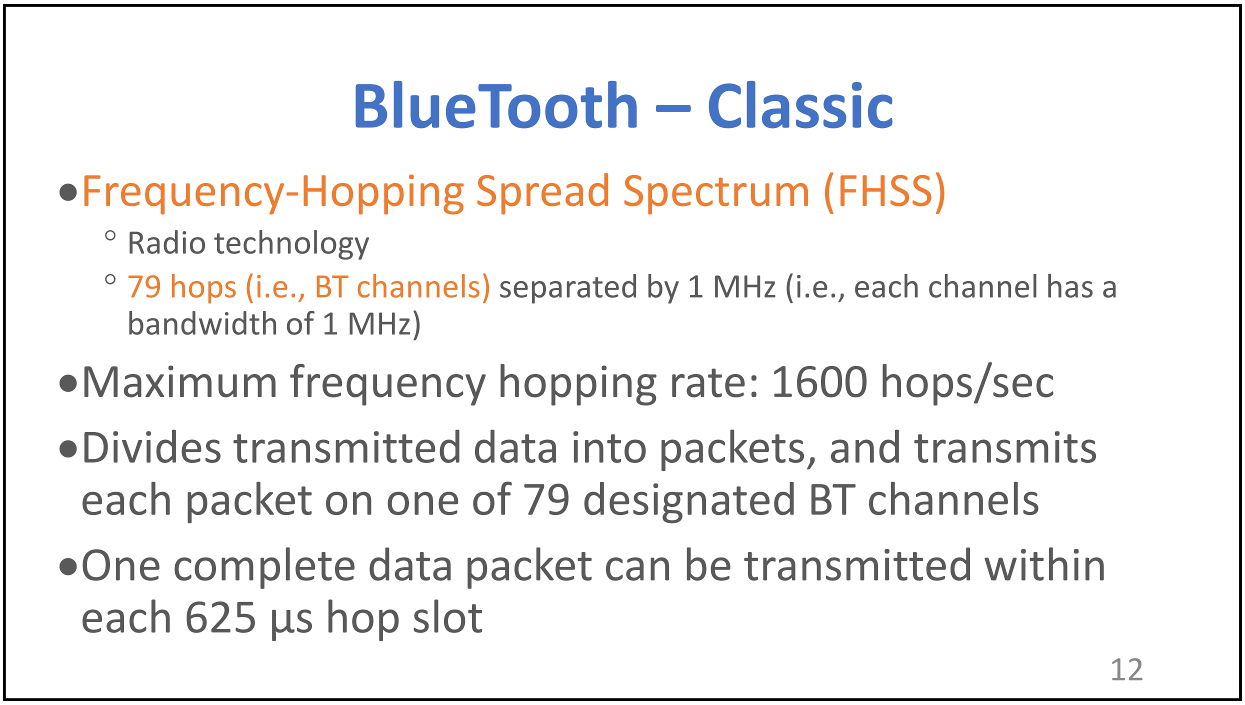
BlueTooth

- Bluetooth is a packet-based protocol with a master/slave architecture
- One master may communicate with up to 7 slaves in a piconet (ad-hoc computer network using BT technology)
- All devices share the master's clock
- Packet exchange is based on the basic clock (which ticks at 312.5 µs intervals), defined by the master
- Two clock ticks make up a slot of 625 µs
- Two slots make up a slot pair of 1250 µs
- In the case of single-slot packets, the master transmits in even slots and receives in odd slots. The slave, conversely, receives in even slots and transmits in odd slots
- Packets may be 1, 3 or 5 slots long, but in all cases the master's transmission begins in even slots and the slave's in odd slots



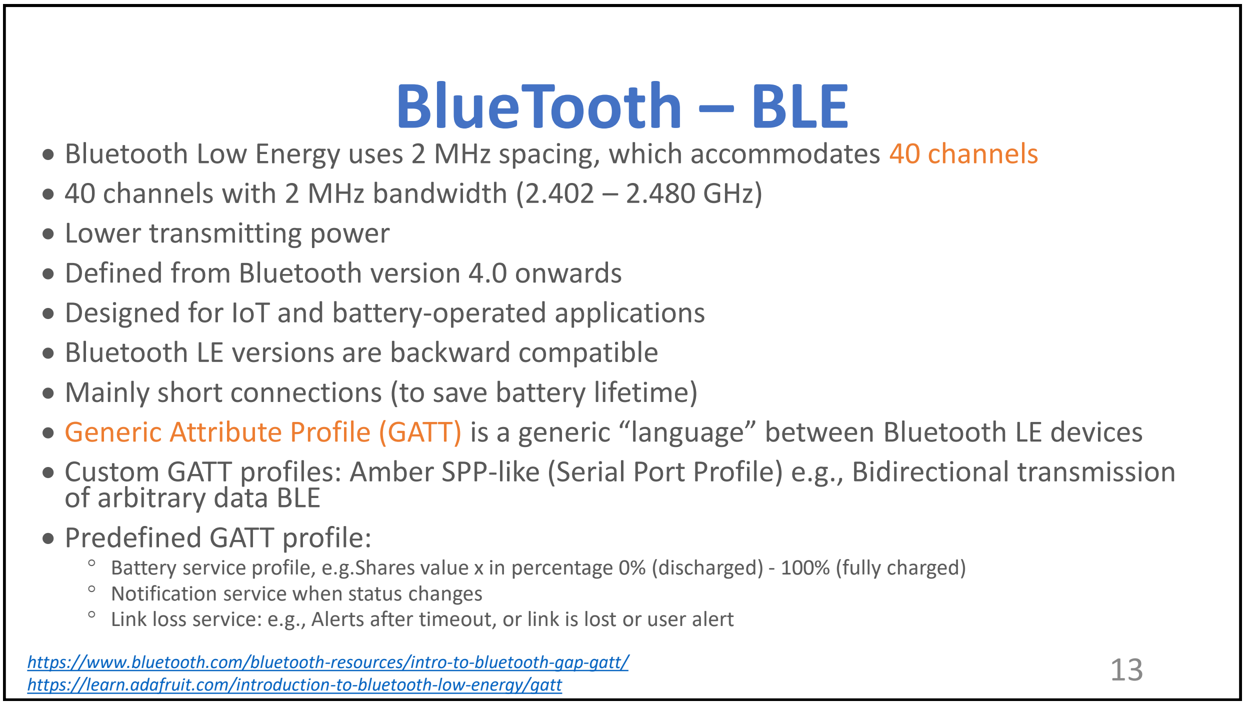
BlueTooth – Classic

- Introduced in Bluetooth version 1.0
- Nominal range: 10 cm to 10 meters
- Bluetooth Classic versions are backward compatible
- 79 channels with 1MHz bandwidth (2.402 – 2.480 GHz)
- One master, up to 7 slaves
- Time (TDMA) and frequency (FHSS) synchronization done by master
- Slave may send data only if polled by master
- Last enhanced version 3.0. still available but not updated any more



BlueTooth – Classic

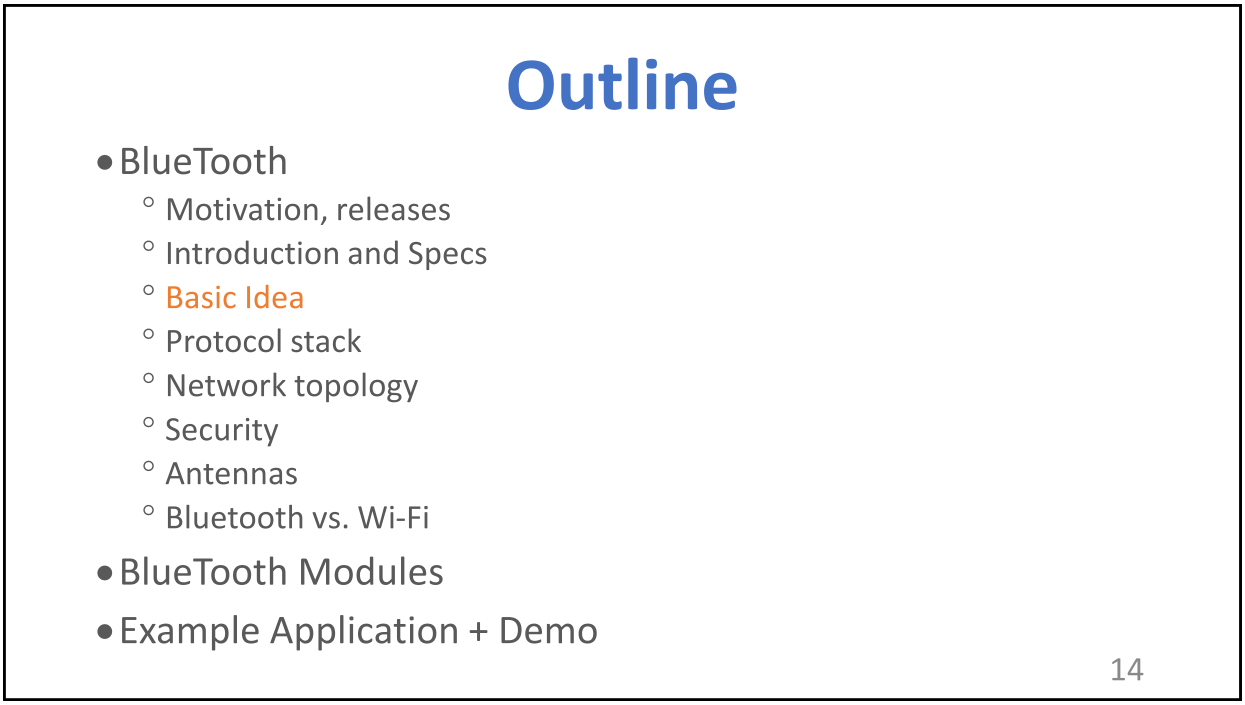
- Frequency-Hopping Spread Spectrum (FHSS)
  - Radio technology
  - 79 hops (i.e., BT channels) separated by 1 MHz (i.e., each channel has a bandwidth of 1 MHz)
- Maximum frequency hopping rate: 1600 hops/sec
- Divides transmitted data into packets, and transmits each packet on one of 79 designated BT channels
- One complete data packet can be transmitted within each 625 µs hop slot



BlueTooth – BLE

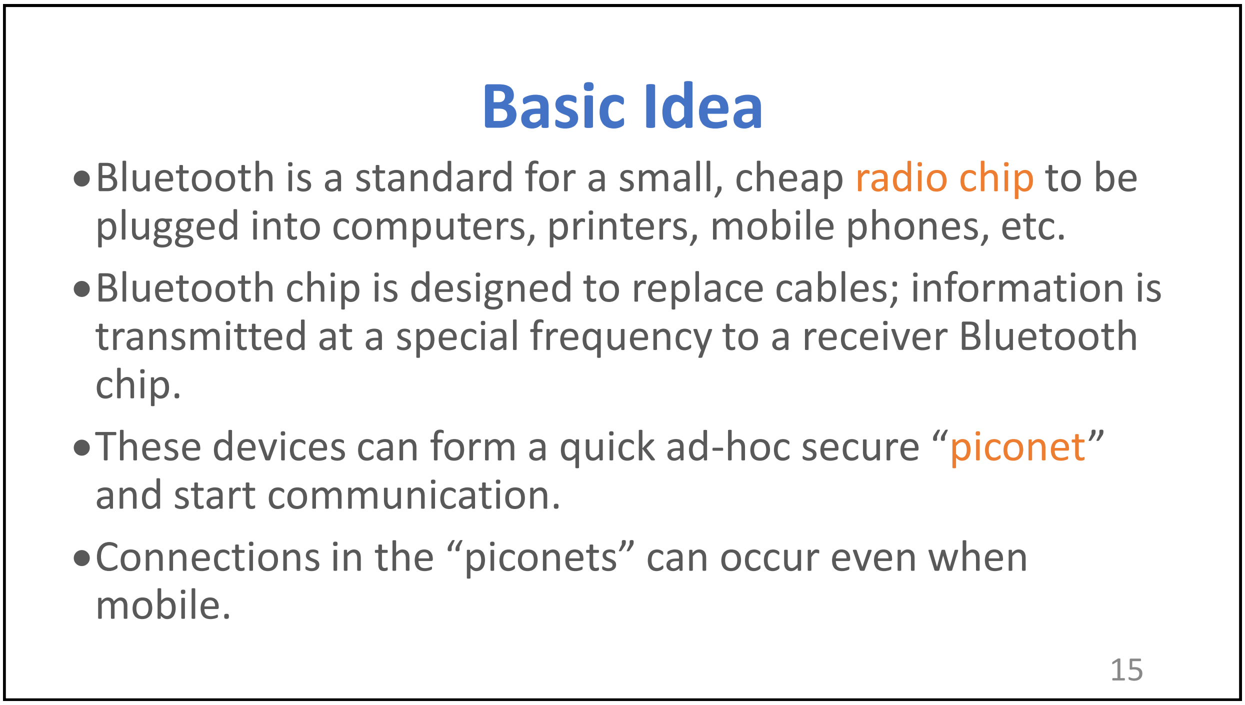
- Bluetooth Low Energy uses 2 MHz spacing, which accommodates 40 channels
- 40 channels with 2 MHz bandwidth (2.402 – 2.480 GHz)
- Lower transmitting power
- Defined from Bluetooth version 4.0 onwards
- Designed for IoT and battery-operated applications
- Bluetooth LE versions are backward compatible
- Mainly short connections (to save battery lifetime)
- Generic Attribute Profile (GATT) is a generic "language" between Bluetooth LE devices
- Custom GATT profiles: Amber SPP-like (Serial Port Profile) e.g., Bidirectional transmission of arbitrary data BLE
- Predefined GATT profile:
  - Battery service profile, e.g.Shares value x in percentage 0% (discharged) - 100% (fully charged)
  - Notification service when status changes
  - Link loss service: e.g., Alerts after timeout, or link is lost or user alert

https://www.bluetooth.com/bluetooth-resources/intro-to-bluetooth-gap-gatt/
https://learn.adafruit.com/introduction-to-bluetooth-low-energy/gatt



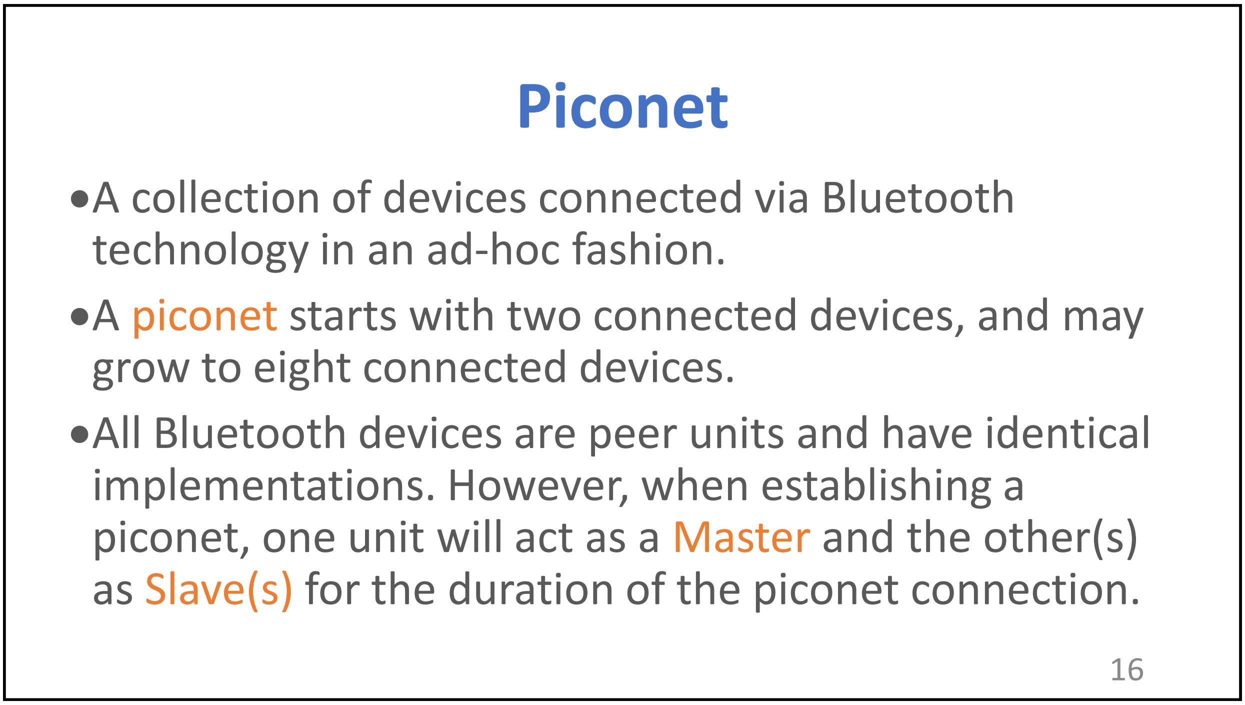
Outline

- BlueTooth
  - Motivation, releases
  - Introduction and Specs
  - Basic Idea
  - Protocol stack
  - Network topology
  - Security
  - Antennas
  - Bluetooth vs. Wi-Fi
- BlueTooth Modules
- Example Application + Demo



Basic Idea

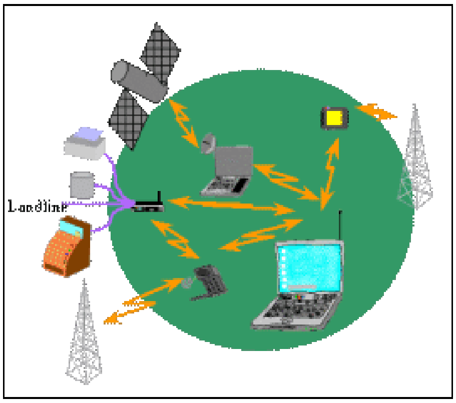
- Bluetooth is a standard for a small, cheap radio chip to be plugged into computers, printers, mobile phones, etc.
- Bluetooth chip is designed to replace cables; information is transmitted at a special frequency to a receiver Bluetooth chip.
- These devices can form a quick ad-hoc secure “piconet” and start communication.
- Connections in the “piconets” can occur even when mobile.



Piconet

- A collection of devices connected via Bluetooth technology in an ad-hoc fashion.
- A piconet starts with two connected devices, and may grow to eight connected devices.
- All Bluetooth devices are peer units and have identical implementations. However, when establishing a piconet, one unit will act as a Master and the other(s) as Slave(s) for the duration of the piconet connection.

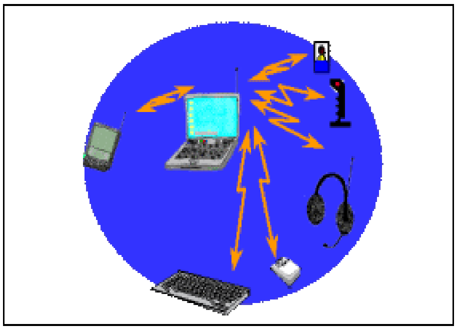
Usage models - Voice/Data Access Points



- Connecting a computing device to a communicating device.
- Allows any device with a bluetooth chip to connect to the internet while located within the range of the access point.
- Example - a notebook could link to the internet using a mobile phone as an access point.

17

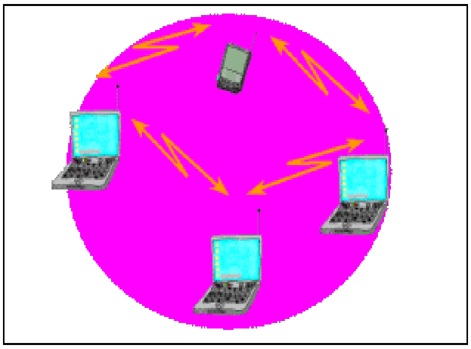
Usage models - Peripheral Interconnects



- Standard peripheral devices like keyboards, mice, headsets, etc. working over a wireless link.
- The same device can be used in multiple functions, e.g., a headset can access phones while in the office and can interface with a cellular phone when mobile.

18

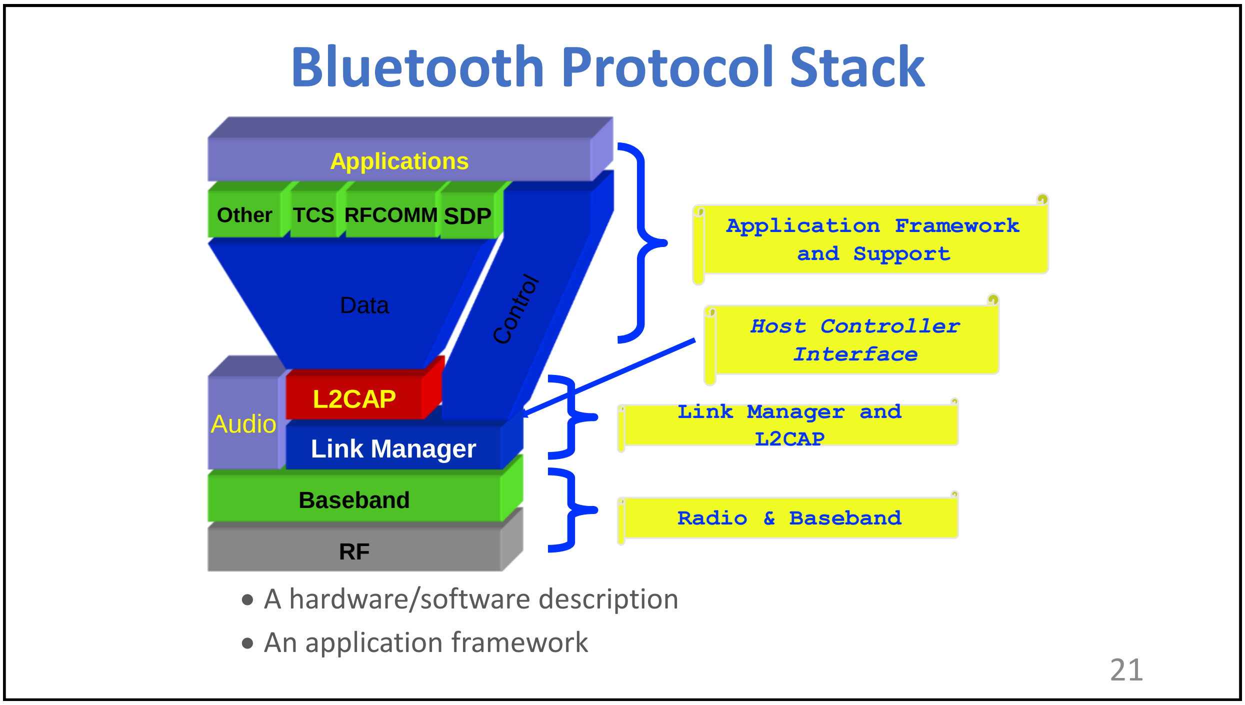
Usage models - Personal Area Networking (PAN)



- Allows dynamic formation and breakdown of “PICONETS”: ad-hoc personal networks.

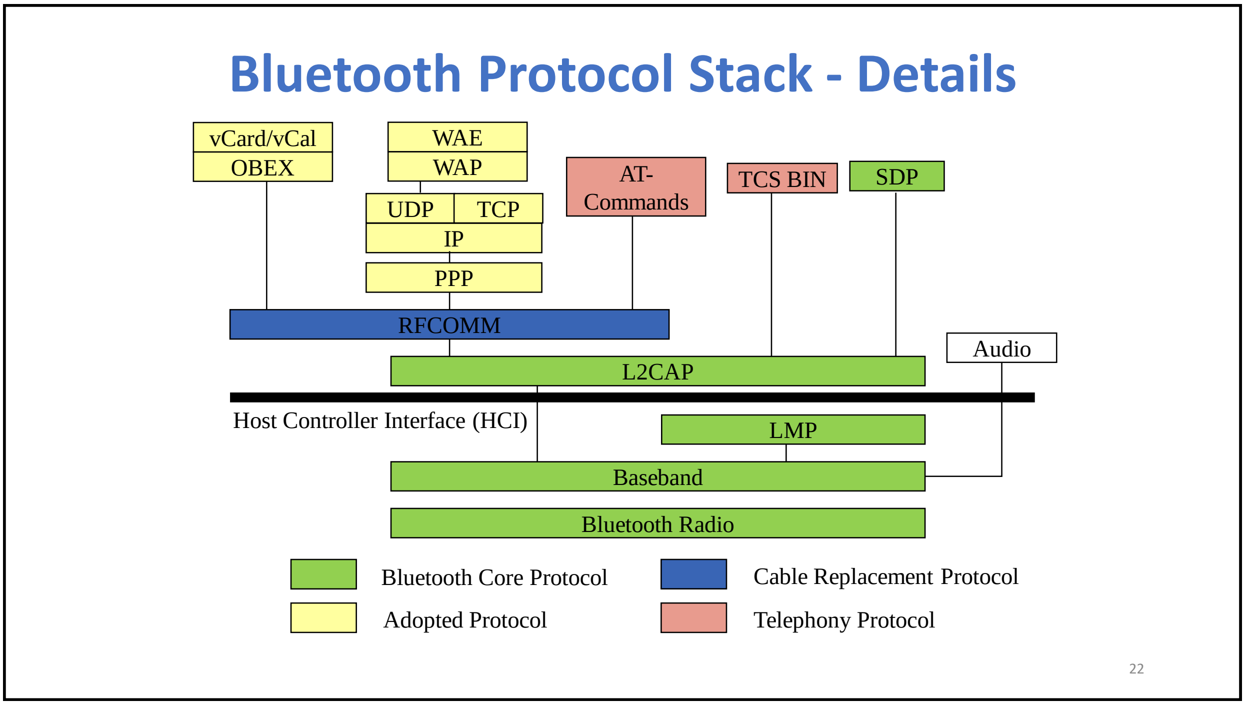
Outline

- BlueTooth
  - Motivation, releases
  - Introduction and Specs
  - Basic Idea
  - Protocol stack
  - Network topology
  - Security
  - Antennas
  - Bluetooth vs. Wi-Fi
- BlueTooth Modules
- Example Application + Demo



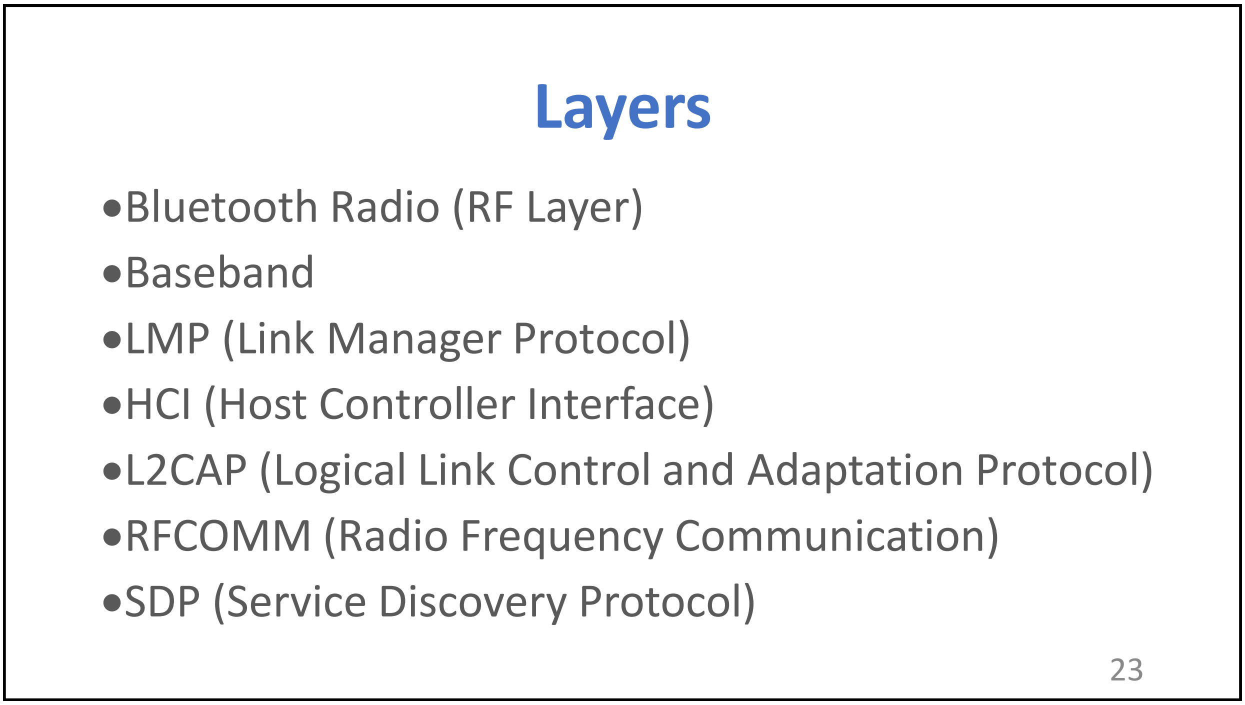
Bluetooth Protocol Stack

- A hardware/software description
- An application framework



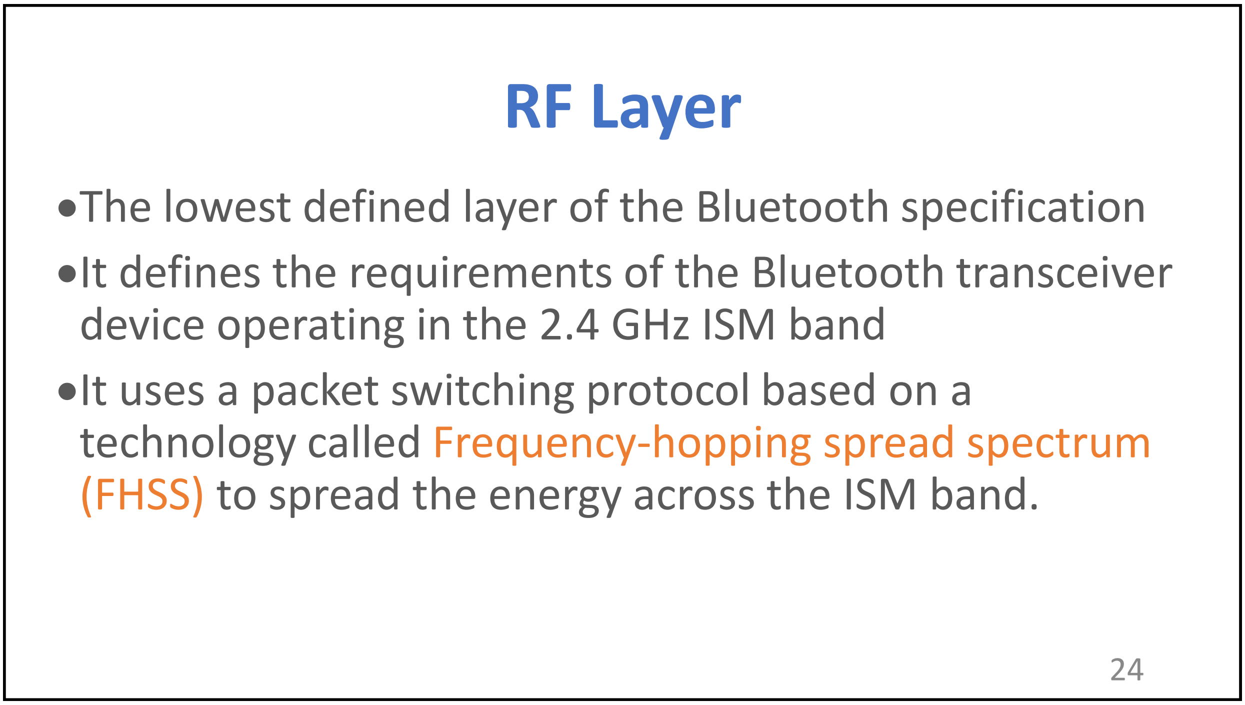
Bluetooth Protocol Stack - Details

🟩 Bluetooth Core Protocol
🟦 Cable Replacement Protocol
🟨 Adopted Protocol
🟥 Telephony Protocol



Layers

- Bluetooth Radio (RF Layer)
- Baseband
- LMP (Link Manager Protocol)
- HCI (Host Controller Interface)
- L2CAP (Logical Link Control and Adaptation Protocol)
- RFCOMM (Radio Frequency Communication)
- SDP (Service Discovery Protocol)



RF Layer

- The lowest defined layer of the Bluetooth specification
- It defines the requirements of the Bluetooth transceiver device operating in the 2.4 GHz ISM band
- It uses a packet switching protocol based on a technology called Frequency-hopping spread spectrum (FHSS) to spread the energy across the ISM band.

- In order to minimize interference, the nominal antenna power is 1 mW which can be extended to 100 mW.
- The low power limits the range to about 10 centimeters to 10 meters.
- With higher power of 100 mW range of 100 meters can be achieved.
- 3 different power classes
  - Power Class1: long range (100m,100mW)
  - Power Class2: mid range (10m,1-2,5mW)
  - Power Class3: short range (0.1-10m,1mW)

Frequency-hopping spread spectrum (FHSS)

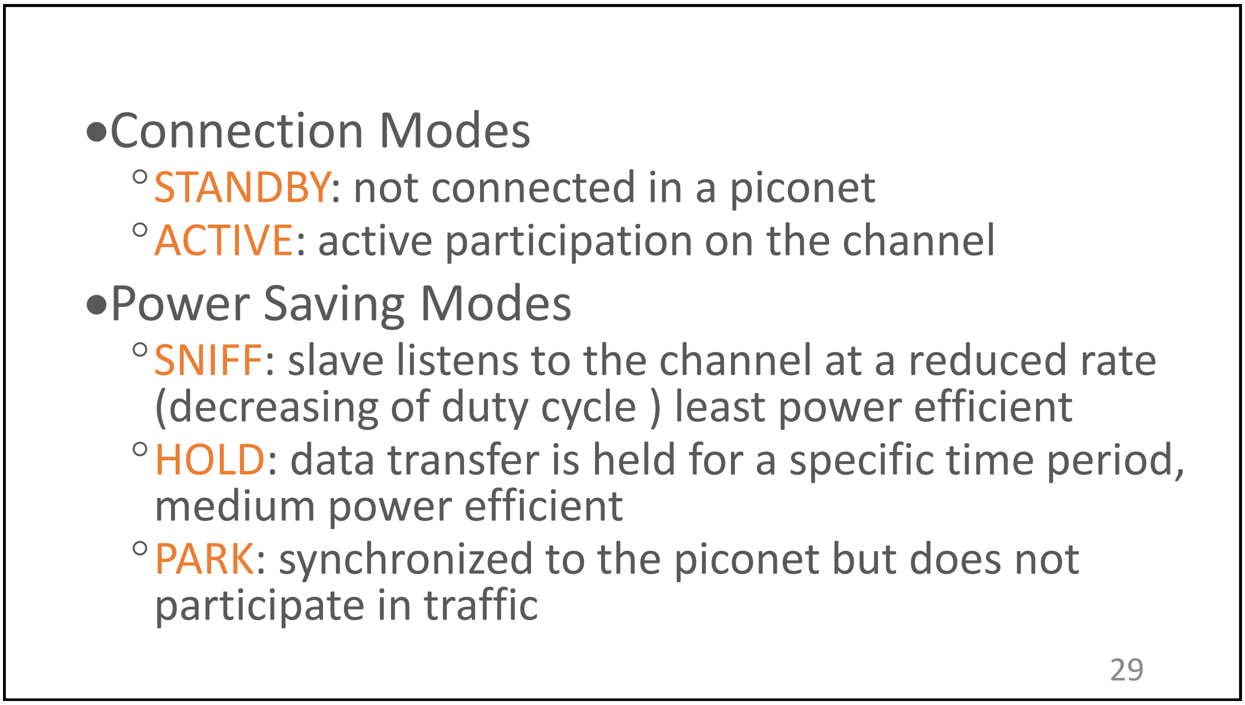
- FHSS is a method of transmitting radio signals by shifting carriers across numerous channels with a pseudorandom sequence which is already known to the sender and receiver.
- Divides the designated range of the ISM-band (2.402GHz to 2.480GHz) into 79 of 1 MHz channels.
- Every frequency is GFSK (Gaussian frequency-shift keying) modulated with channel width of 1MHz.

Frequency-hopping spread spectrum (FHSS)

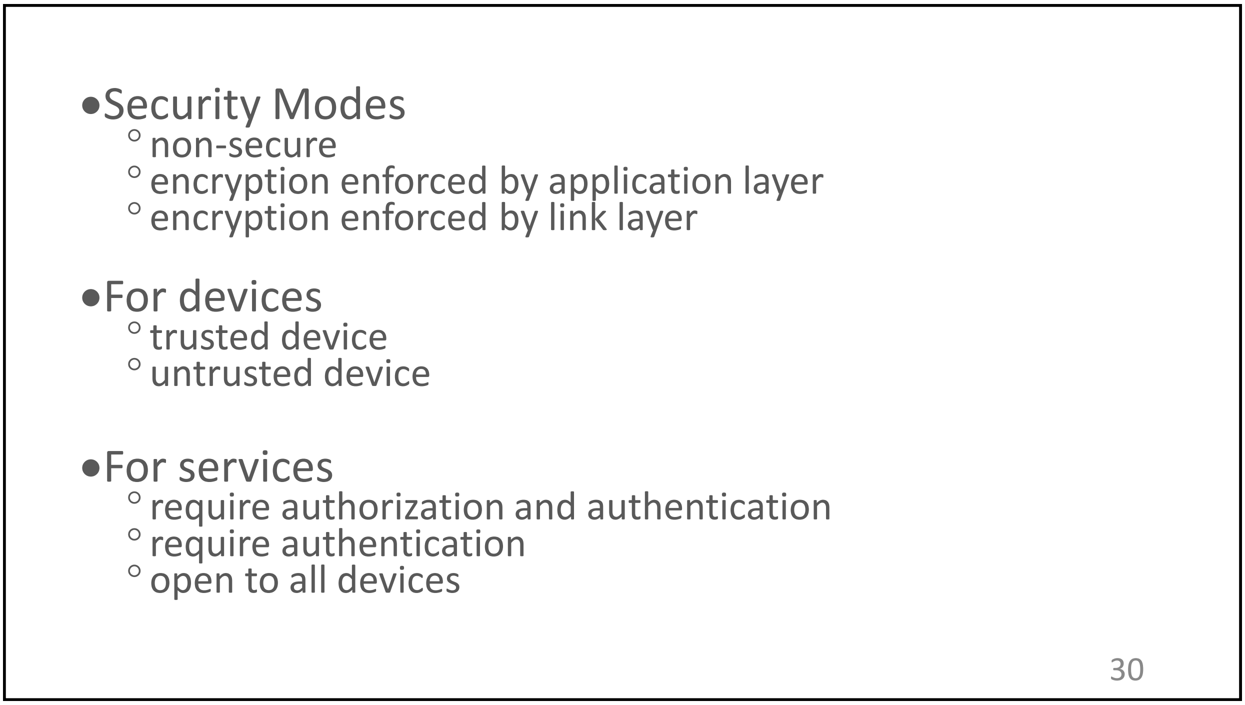
- A device will use 79 individual (pseudo)randomly chosen frequencies, changing from one to another on a regular basis.
- Communication between devices switches between available channels. The frequency hopping is done at a rate of 1600 times a second. This:
  - Allows more devices to use the limited time slice
  - Reduces the chance of two transmitters being on the same frequency at the same time

Baseband Layer

- The physical layer of the Bluetooth that provides
  - Error correction
  - Flow control
  - Hopping sequence
  - Security
- Hopping through 79 channels
- Data is divided in packets
  - Access code: e.g. timing synchronization
  - Header: e.g. packet numbering, flow control, slave address
  - Payload: voice, data or both



- Connection Modes
  - STANDBY: not connected in a piconet
  - ACTIVE: active participation on the channel
- Power Saving Modes
  - SNIFF: slave listens to the channel at a reduced rate (decreasing of duty cycle) least power efficient
  - HOLD: data transfer is held for a specific time period, medium power efficient
  - PARK: synchronized to the piconet but does not participate in traffic



- Security Modes
  - non-secure
  - encryption enforced by application layer
  - encryption enforced by link layer
- For devices
  - trusted device
  - untrusted device
- For services
  - require authorization and authentication
  - require authentication
  - open to all devices

Audio

- Two codecs: PCM and CVSD
- Both at 64kbit/s
- Synchronous Connection Oriented (SCO) links
- Time-critical
- No retransmission
- Errors appear as background noise

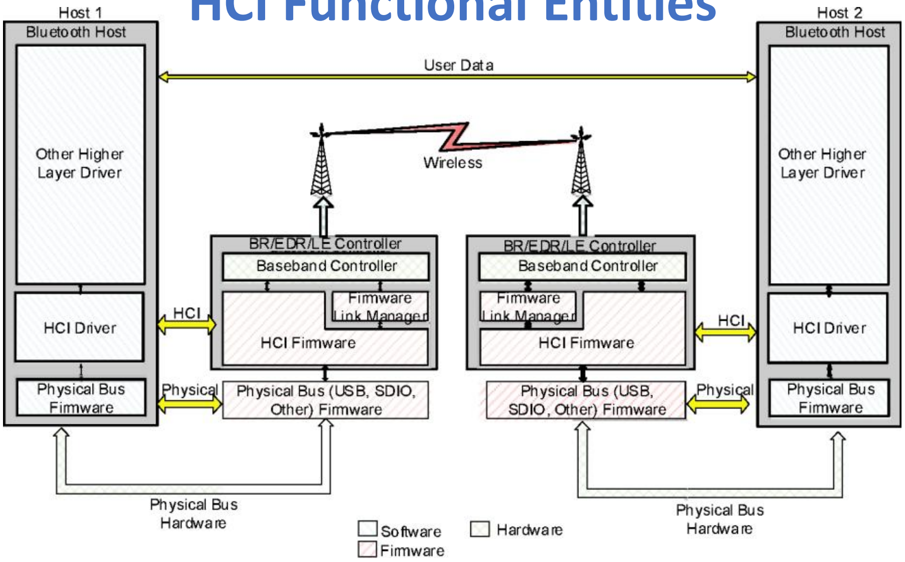
LMP (Link Manager Protocol)

- The Link Manager carries out link setup, authentication, link configuration and other protocols.
- It discovers other remote LM's and communicates with them via the Link Manager Protocol (LMP).
- To perform its service provider role, the LM uses the services of the underlying Link Controller (LC).

HCI (Host Controller Interface)

- HCI provides a command interface to baseband controller and link manager, and access to hardware status and control registers.
- Also, to hardware status, control and event registers
- Bluetooth defined Host Controller Transport Layers:
  - UART (HCI over serial interface)
  - RS232 (HCI over serial interface)
  - USB (HCI over USB interface e.g. USB dongle)

HCI Functional Entities



https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/
host-controller-interface/host-controller-interface-functional-specification.html

L2CAP (Logical Link Control and Adaptation Protocol)

- L2CAP is layered over the Baseband Protocol and resides in the data link layer
- L2CAP provides connection-oriented and connectionless data services to upper layer protocols with quality-of-service functions using multiplexing, segmentation and reassembly
- Two link types are supported for the Baseband layer:
  - Synchronous Connection-Oriented (SCO)
  - Asynchronous Connection-Less (ACL)

RFCOMM (Radio Frequency Communication)

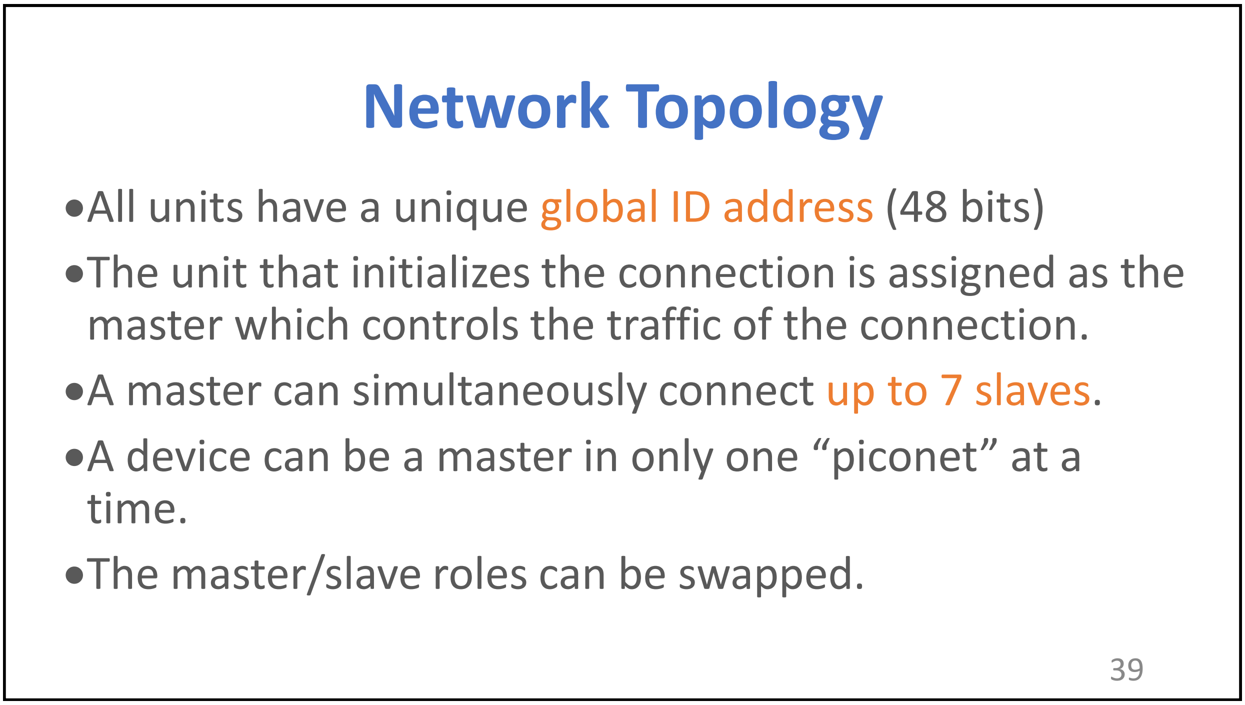
- Provides emulation of serial ports
- Supports up to 60 simultaneous connections
- Differentiates between two device types:
  - Type 1: communication end points (e.g. printer or headsets)
  - Type 2: devices which are part of communication (e.g. modems)
- But in the protocol itself no distinction is made, some information is for type 1 other for type 2

SDP (Service Discovery Protocol)

- Provides a means for applications to discover which services are available and to determine the characteristics of those available services
- Uses a request/response model where each transaction consists of one request protocol data unit (PDU) and one response PDU
- SDP is used with L2CAP
- Is optimized for the dynamic nature of bluetooth
- SDP does not define methods for accessing services

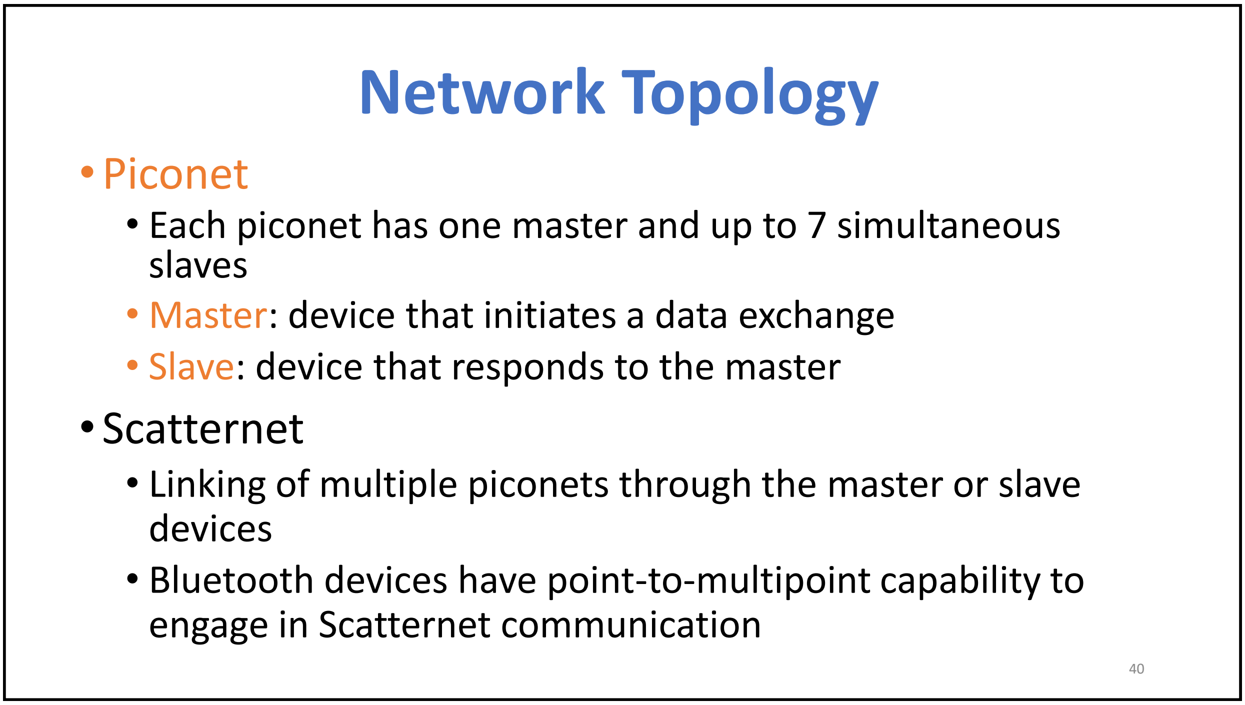
Outline

- BlueTooth
  - Motivation, releases
  - Introduction and Specs
  - Basic Idea
  - Protocol stack
  - Network topology
  - Security
  - Antennas
  - Bluetooth vs. Wi-Fi
- BlueTooth Modules
- Example Application + Demo



Network Topology

- All units have a unique global ID address (48 bits)
- The unit that initializes the connection is assigned as the master which controls the traffic of the connection.
- A master can simultaneously connect up to 7 slaves.
- A device can be a master in only one “piconet” at a time.
- The master/slave roles can be swapped.

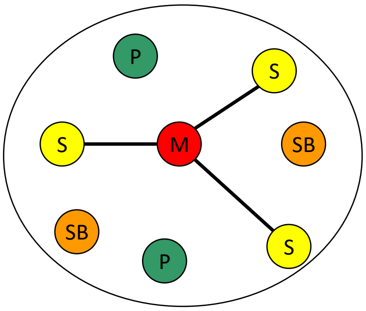


Network Topology

- Piconet
  - Each piconet has one master and up to 7 simultaneous slaves
  - Master: device that initiates a data exchange
  - Slave: device that responds to the master
- Scatternet
  - Linking of multiple piconets through the master or slave devices
  - Bluetooth devices have point-to-multipoint capability to engage in Scatternet communication

Piconet

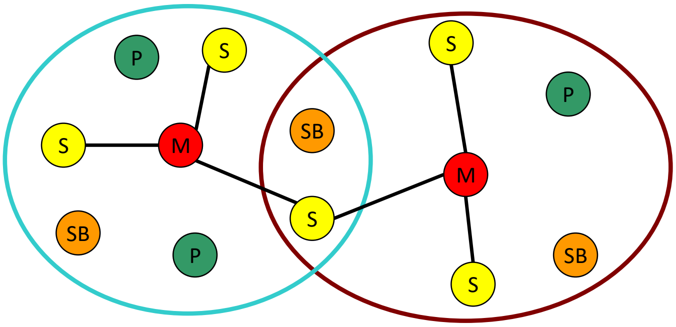
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
- Non-piconet devices are in standby

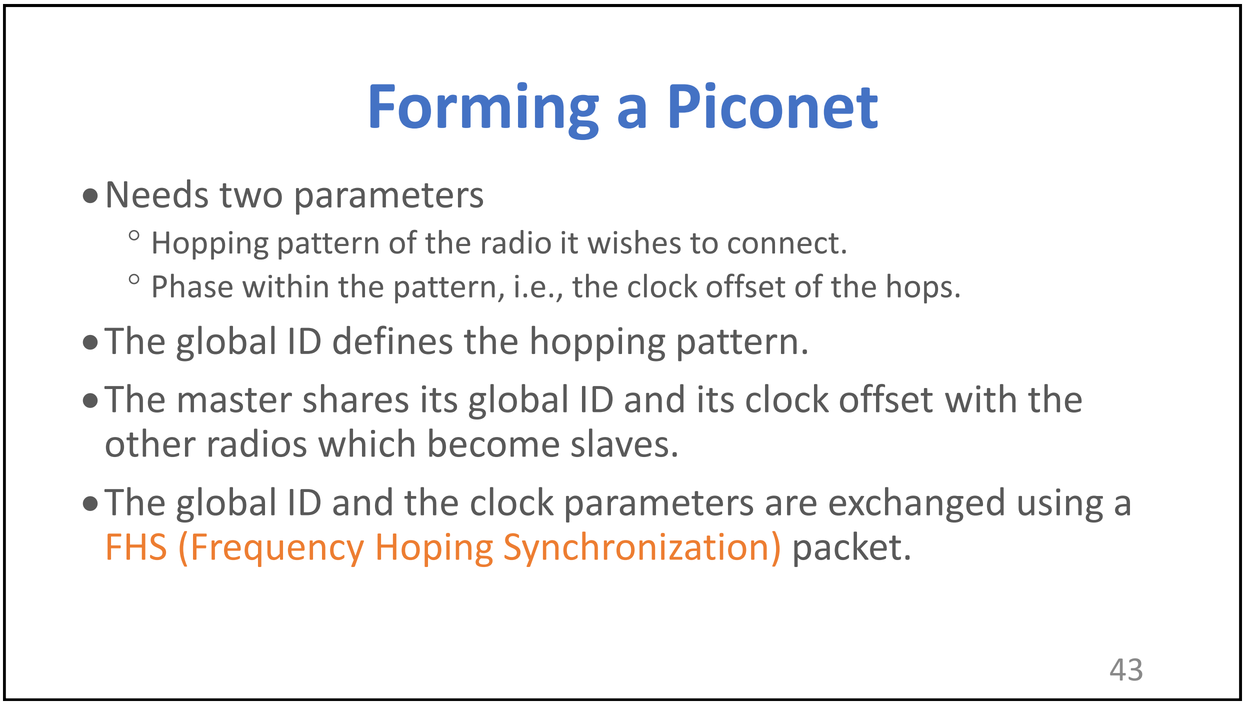


M = Master
P = Parked
S = Slave
SB = Standby

Scatternet

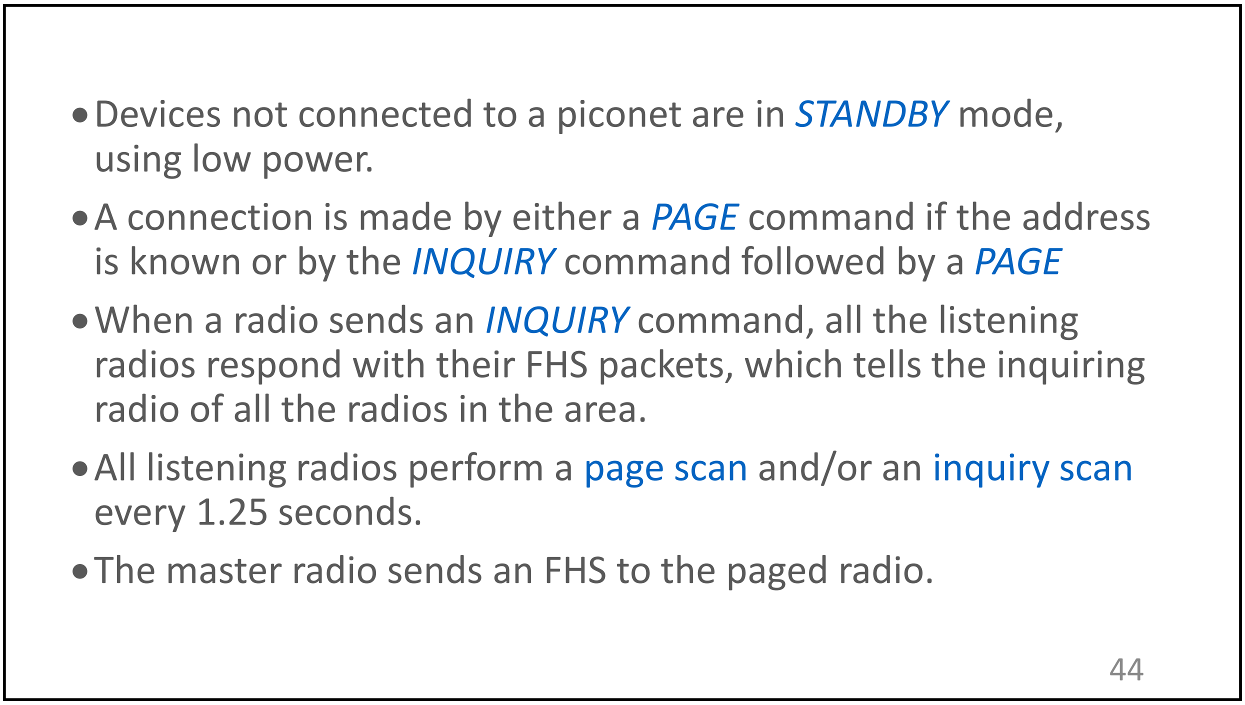
- Devices can be slave in one piconet and master of another





Forming a Piconet

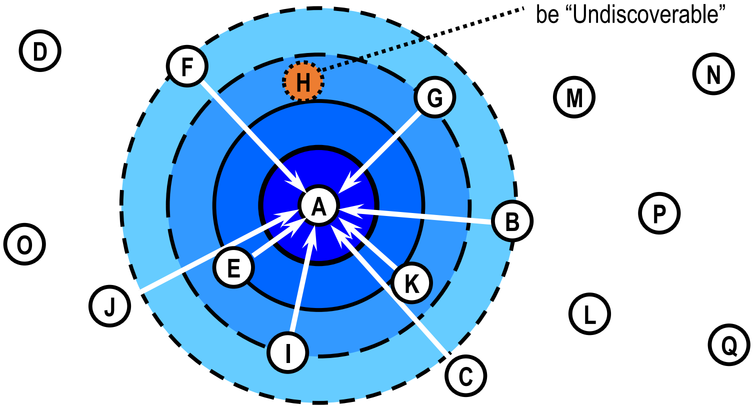
- Needs two parameters
  - Hopping pattern of the radio it wishes to connect.
  - Phase within the pattern, i.e., the clock offset of the hops.
- The global ID defines the hopping pattern.
- The master shares its global ID and its clock offset with the other radios which become slaves.
- The global ID and the clock parameters are exchanged using a FHS (Frequency Hoping Synchronization) packet.



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

- When a radio joins a piconet, it is assigned a 3 bit *Active Member Address (AMA).*
- Once the piconet has eight radios, the master can put/assign a radio into the *PARK* mode.
- This is one of the low power states, in which the radio releases its AMA for a 8 bit *PMA* (Passive Member Address).
- The freed AMA can be assigned to another radio wishing to join the piconet.
- Though up to 256 radios can actively reside on a piconet, only 8 of them with AMA's can transfer data.

Device Discovery Illustrated



Note that a device can be "Undiscoverable"

10 meters

After inquiry procedure, A knows about others within range

- Once a radio joins the piconet and has an AMA it can direct data to other devices on the piconet.
- In order to remain in the connected state within a piconet, the radio needs to maintain the frequency hopping pattern and offset while consuming low power.
- To achieve this the connected radios can be placed in either *PARK*, *HOLD* or *SNIFF* modes.

PARK MODE

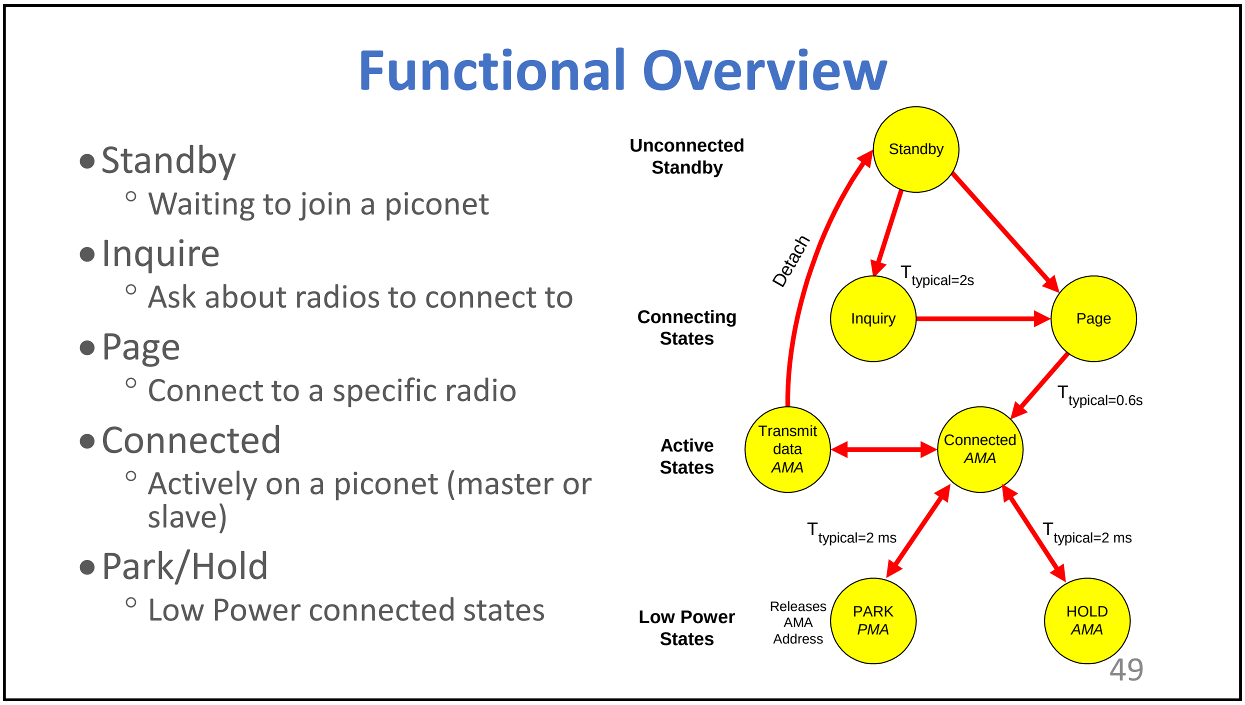
- ➢ The device has given up the AMA and has become passive.
- ➢ The parked device will occasionally listen to see if the master has sent any broadcast data asking it to become active.

HOLD MODE

- When data needs to be transmitted very infrequently, thus conserving power.
- In this mode only an internal timer is running.
- No data is transferred when in HOLD mode.
- The master can put slaves on HOLD mode.

SNIFF MODE

- ❖A slave device listens to the piconet at a reduced rate.
- ❖The SNIFF interval is programmable.
- ❖In both the HOLD and SNIFF states the device retains its AMA.



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

Unconnected Standby

Connecting States

Active States

Low Power States

Standby

Detach

Inquiry

$T_{typical=2s}$

Page

$T_{typical=0.6s}$

Transmit data *AMA*

Connected *AMA*

$T_{typical=2 ms}$

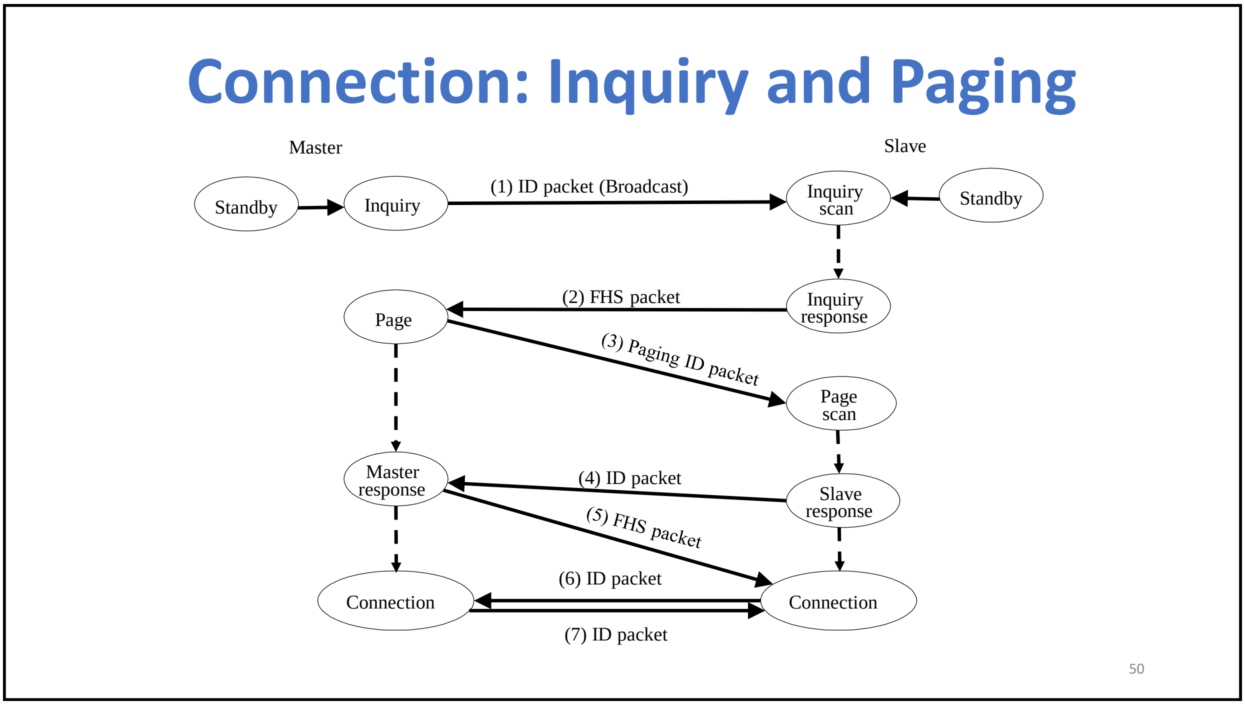
$T_{typical=2 ms}$

Releases AMA Address

PARK *PMA*

HOLD *AMA*

49



Connection: Inquiry and Paging

Master

Slave

Standby

Inquiry

(1) ID packet (Broadcast)

Inquiry scan

Standby

Page

(2) FHS packet

Inquiry response

(3) Paging ID packet

Page scan

Master response

(4) ID packet

Slave response

(5) FHS packet

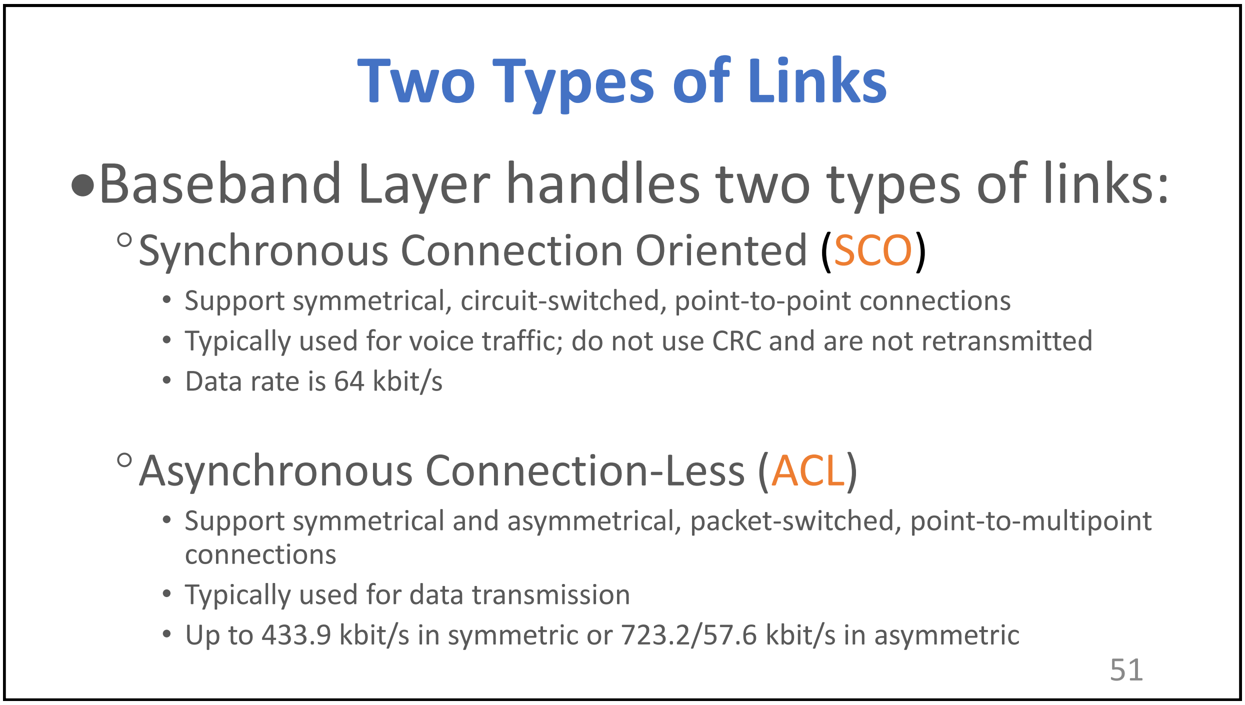
Connection

(6) ID packet

Connection

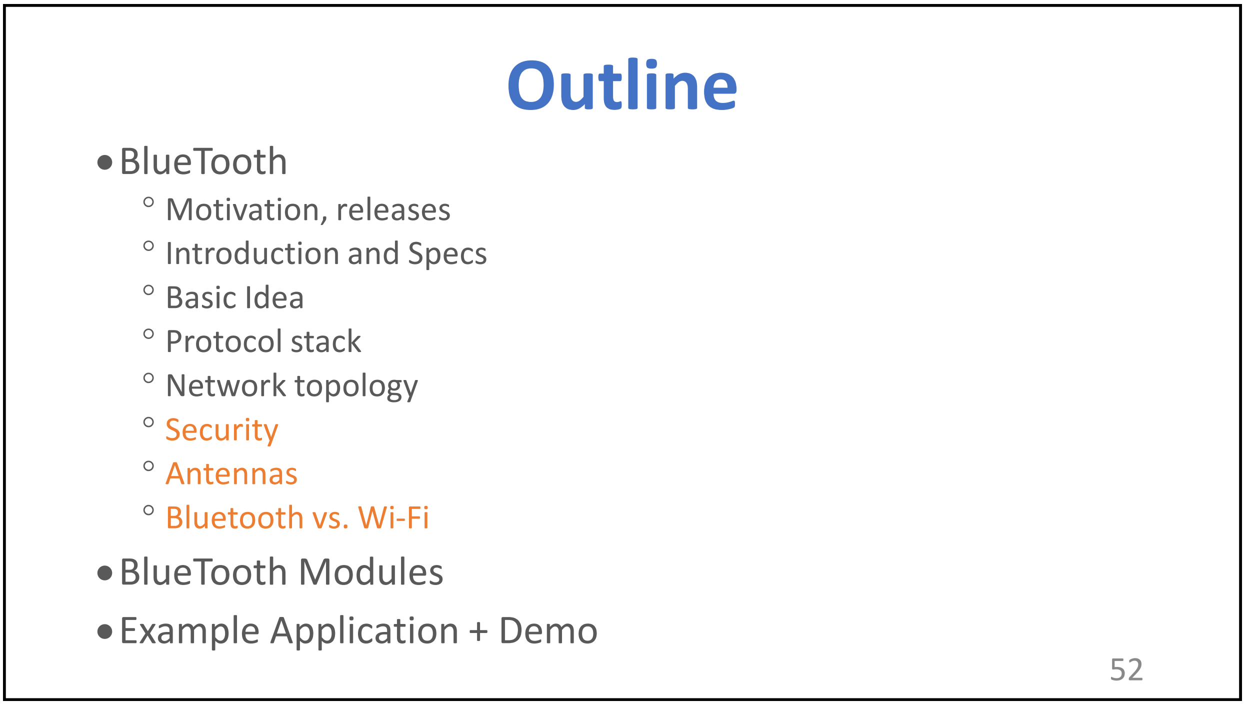
(7) ID packet

50



Two Types of Links

- Baseband Layer handles two types of links:
  - Synchronous Connection Oriented (SCO)
    - Support symmetrical, circuit-switched, point-to-point connections
    - Typically used for voice traffic; do not use CRC and are not retransmitted
    - Data rate is 64 kbit/s
  - Asynchronous Connection-Less (ACL)
    - Support symmetrical and asymmetrical, packet-switched, point-to-multipoint connections
    - Typically used for data transmission
    - Up to 433.9 kbit/s in symmetric or 723.2/57.6 kbit/s in asymmetric



Outline

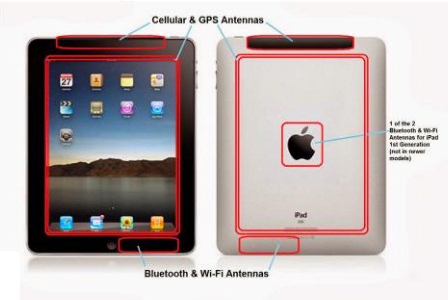
- BlueTooth
  - Motivation, releases
  - Introduction and Specs
  - Basic Idea
  - Protocol stack
  - Network topology
  - Security
  - Antennas
  - Bluetooth vs. Wi-Fi
- BlueTooth Modules
- Example Application + Demo

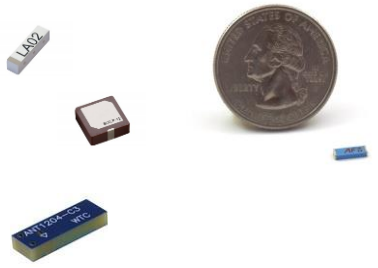
Security

- Bluetooth relies on PIN codes to establish trusted relationships between devices
- Supports Unidirectional or Mutual Encryption based on a secret link Key (128 bit) shared between two devices
- Security defined in 3 modes
  - Mode1 - No security
  - Mode 2 - Service level security: not established before channel is established at L2CAP
  - Mode 3 - Link level security: device initiates security before LMP (link management protocol) link is setup
- Devices and Services can be Set for Different Levels of Security
  - Two Trust Levels are Set for Devices
    - Trusted Device: Fixed Relationship and Unrestricted Access to All Services
    - Untrusted: No Permanent relationship and Restricted Services

Antennas

- Internal antennas
- External antennas


Cellular & GPS Antennas
1 of the 2 Bluetooth & Wi-Fi Antennas for iPad 1st Generation (not in newer models)
Bluetooth & Wi-Fi Antennas



BlueTooth vs. Wi-Fi

- Similar applications
  - Setting up networks, printing, or transferring files
- Bluetooth
  - Intended for portable equipment and its applications (wireless personal area network, WPAN); ad-hoc connections
  - Also works for fixed location applications such as smart energy functionality in homes (thermostats, etc.)
  - Usually symmetrical, between two Bluetooth devices
  - Simple applications: headsets, remote controls, etc.
- Wi-Fi
  - Intended as replacement for high-speed cabling (wireless local area networks, WLAN)
  - Usually access point-centered, with asymmetrical client-server connection with all traffic routed through the access point
  - Applications where high speeds are required, especially for network access

BlueTooth vs. Wi-Fi

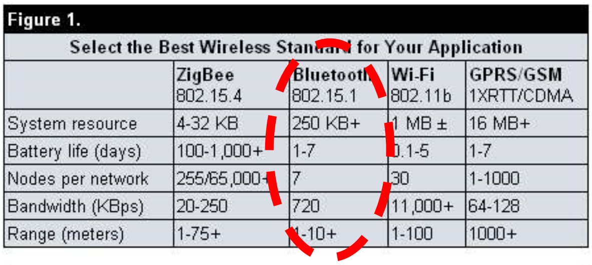


Figure 1.

Select the Best Wireless Standard for Your Application

	ZigBee 802.15.4	Bluetooth 802.15.1	Wi-Fi 802.11b	GPRS/GSM 1XRTT/CDMA
System resource	4-32 KB	250 KB+	1 MB ±	16 MB+
Battery life (days)	100-1,000+	1-7	0.1-5	1-7
Nodes per network	255/65,000+	7	30	1-1000
Bandwidth (KBps)	20-250	720	11,000+	64-128
Range (meters)	1-75+	1-10+	1-100	1000+

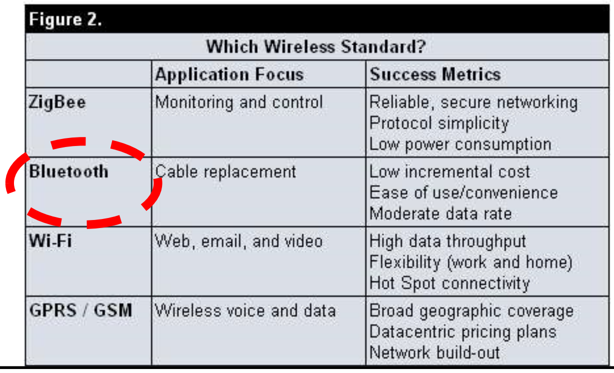


Figure 2.

Which Wireless Standard?

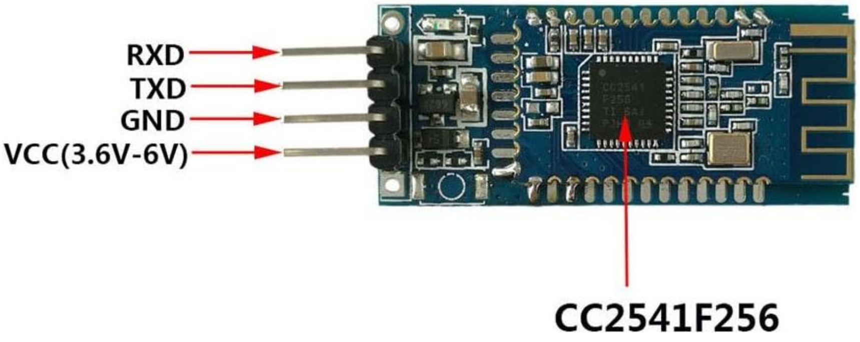
	Application Focus	Success Metrics
ZigBee	Monitoring and control	Reliable, secure networking Protocol simplicity Low power consumption
Bluetooth	Cable replacement	Low incremental cost Ease of use/convenience Moderate data rate
Wi-Fi	Web, email, and video	High data throughput Flexibility (work and home) Hot Spot connectivity
GPRS / GSM	Wireless voice and data	Broad geographic coverage Datacentric pricing plans Network build-out

Outline

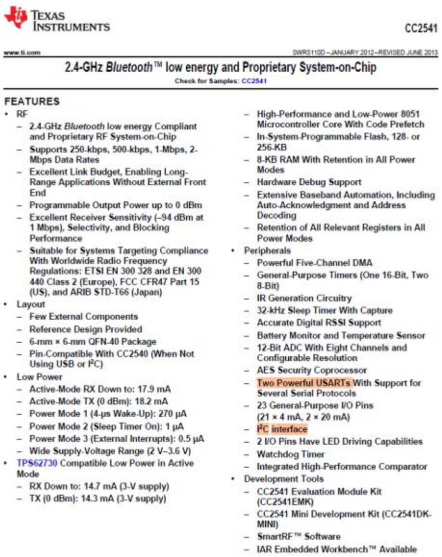
- BlueTooth
- BlueTooth Modules
- Example Application + Demo

Bluetooth Modules: HM-10

- HM-10 Bluetooth Module
  - https://www.deshide.com/product-details.html?pid=344851&_t=1665210577
- Bluetooth Specification v4.0 BLE (can be discovered by iPhone)



Texas Instruments BLE Chip – CC2541



TEXAS INSTRUMENTS

CC2541

www.ti.com

SWRS110D – JANUARY 2012 – REVISED JUNE 2013

2.4-GHz *Bluetooth*™ low energy and Proprietary System-on-Chip

Check for Samples: CC2541

FEATURES

- RF
  - – 2.4-GHz *Bluetooth* low energy Compliant and Proprietary RF System-on-Chip
  - – Supports 250-kbps, 500-kbps, 1-Mbps, 2-Mbps Data Rates
  - – Excellent Link Budget, Enabling Long-Range Applications Without External Front End
  - – Programmable Output Power up to 0 dBm
  - – Excellent Receiver Sensitivity (–94 dBm at 1 Mbps), Selectivity, and Blocking Performance
  - – Suitable for Systems Targeting Compliance With Worldwide Radio Frequency Regulations: ETSI EN 300 328 and EN 300 440 Class 2 (Europe), FCC CFR47 Part 15 (US), and ARIB STD-T66 (Japan)
- Layout
  - – Few External Components
  - – Reference Design Provided
  - – 6-mm × 6-mm QFN-40 Package
  - – Pin-Compatible With CC2540 (When Not Using USB or I²C)
- Low Power
  - – Active-Mode RX Down to: 17.9 mA
  - – Active-Mode TX (0 dBm): 18.2 mA
  - – Power Mode 1 (4-µs Wake-Up): 270 µA
  - – Power Mode 2 (Sleep Timer On): 1 µA
  - – Power Mode 3 (External Interrupts): 0.5 µA
  - – Wide Supply-Voltage Range (2 V–3.6 V)
- TPS62730 Compatible Low Power in Active Mode
  - – RX Down to: 14.7 mA (3-V supply)
  - – TX (0 dBm): 14.3 mA (3-V supply)
  - – High-Performance and Low-Power 8051 Microcontroller Core With Code Prefetch
  - – In-System-Programmable Flash, 128- or 256-KB
  - – 8-KB RAM With Retention in All Power Modes
  - – Hardware Debug Support
  - – Extensive Baseband Automation, Including Auto-Acknowledgment and Address Decoding
  - – Retention of All Relevant Registers in All Power Modes
- Peripherals
  - – Powerful Five-Channel DMA
  - – General-Purpose Timers (One 16-Bit, Two 8-Bit)
  - – IR Generation Circuitry
  - – 32-kHz Sleep Timer With Capture
  - – Accurate Digital RSSI Support
  - – Battery Monitor and Temperature Sensor
  - – 12-Bit ADC With Eight Channels and Configurable Resolution
  - – AES Security Coprocessor
  - – Two Powerful USARTs With Support for Several Serial Protocols
  - – 23 General-Purpose I/O Pins (21 × 4 mA, 2 × 20 mA)
  - – I²C interface
  - – 2 I/O Pins Have LED Driving Capabilities
  - – Watchdog Timer
  - – Integrated High-Performance Comparator
- Development Tools
  - – CC2541 Evaluation Module Kit (CC2541EMK)
  - – CC2541 Mini Development Kit (CC2541DK-MINI)
  - – SmartRF™ Software
  - – IAR Embedded Workbench™ Available

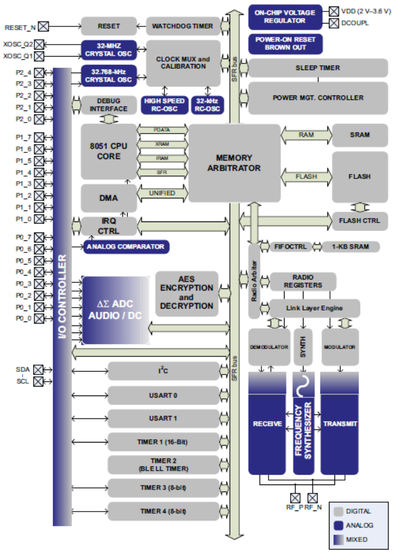


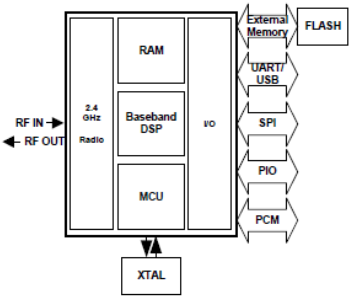
Figure 1. Block Diagram

Bluetooth Modules: HC-06

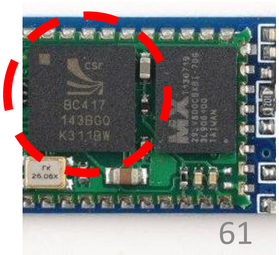
- JY-MCU BT_BOARD V1.07 - referred to as HC-06 Module
  - – Manual: http://www.ram-e-shop.com/ds/general/Bluetooth_TRx_Module_New.pdf
  - – There are many similar others (including HC-03, HC-04, and HC-05)
- Wireless Bluetooth Transceiver Module – uses Bluetooth Specification v2.0 (not supported by iPhones)
- Can work either as a master or a slave
- Built around the BC417 Bluetooth-to-Serial chip

BC417 BlueTooth-to-Serial Chip

- Single chip radio and baseband IC for Bluetooth 2.4 GHz systems
  - Datasheet: https://cdn.sparkfun.com/datasheets/Wireless/Bluetooth/CSR-BC417-datasheet.pdf
- Enhanced data rates (EDR) to 3Mbps
- Loaded with features
  - 1.8V core, 1.8 to 3.6V I/O
  - UART interface with programmable baud rate up to 3M baud
  - Low Power 1.8V operation
  - USB and Dual UART Ports
  - By default, it works as a Slave, 9600 baudrate, N, 8, 1, and Pincode 1234



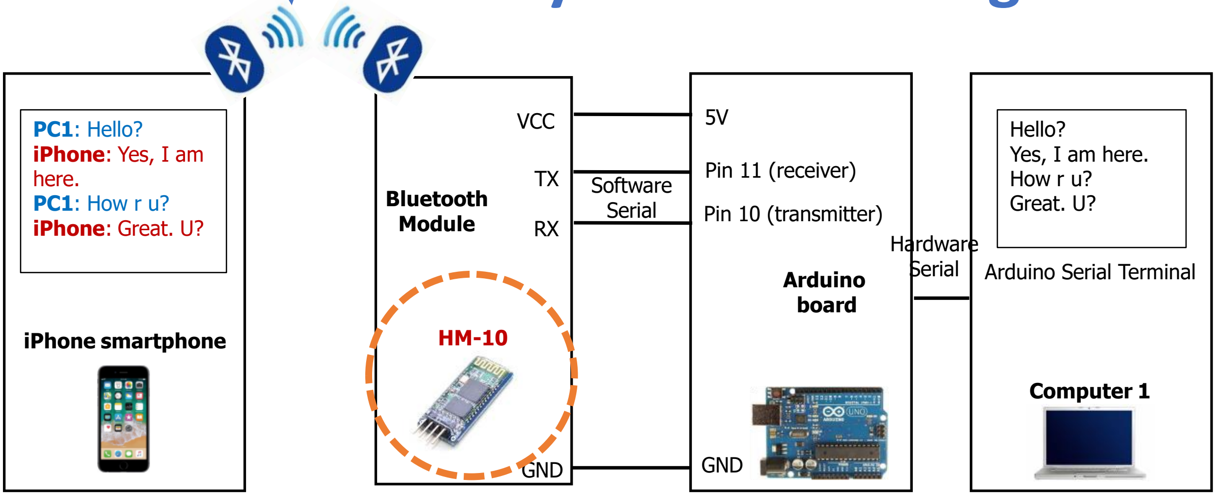
System Architecture



Outline

- BlueTooth
- BlueTooth Modules
- Example Application + Demo

Chat System – System Level Diagram



PC1: Hello?
iPhone: Yes, I am here.
PC1: How r u?
iPhone: Great. U?

Hello?
Yes, I am here.
How r u?
Great. U?

Credits and References

- https://en.wikipedia.org/wiki/Bluetooth
- https://www.bluetooth.com/learn-about-bluetooth/tech-overview/
- http://www.radio-electronics.com/info/wireless/bluetooth/bluetooth_overview.php
- https://www.bluetooth.com/wp-content/uploads/Files/Specification/HTML/Core-54/out/en/host-controller-interface/host-controller-interface-functional-specification.html