Silica Wireless

FAE Friday

Wireless

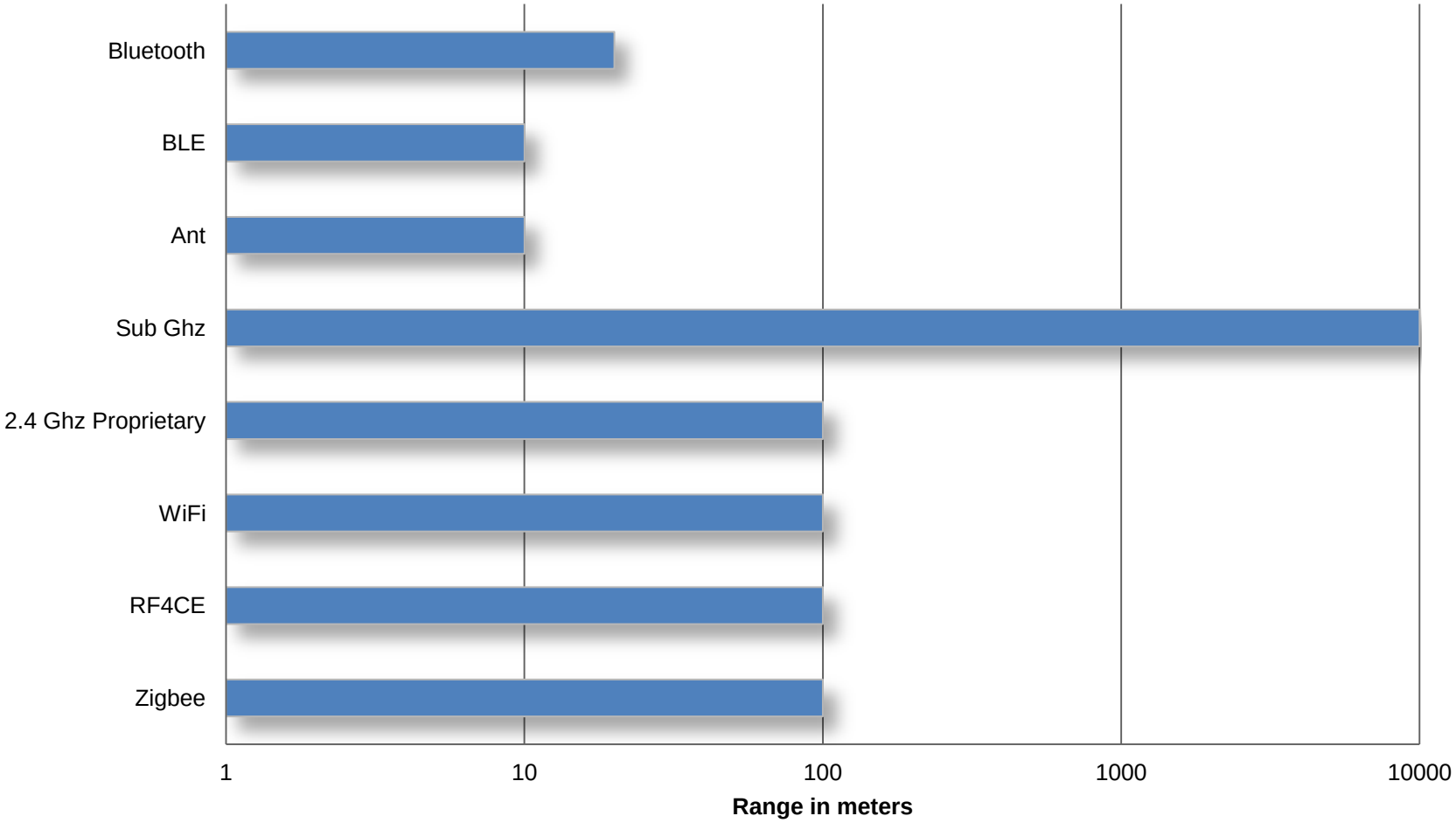
The big picture

Frequencies

Sub 1Ghz	2.4Ghz to 5Ghz		
W-Mbus 6LowPan Microchip MiWi TI SimpliciTI	ZigBee 6LoWPAN RF4CE TI SimpliciTI NXP Jennet	Bluetooth BLE	Wi-Fi
  	 	  	  
TI Microchip Anaren Analog Devices ST Rohm	TI Microchip Nxp ST Anaren Rohm LSR	TI Microchip ST Rohm LSR	TI Microchip ST LSR

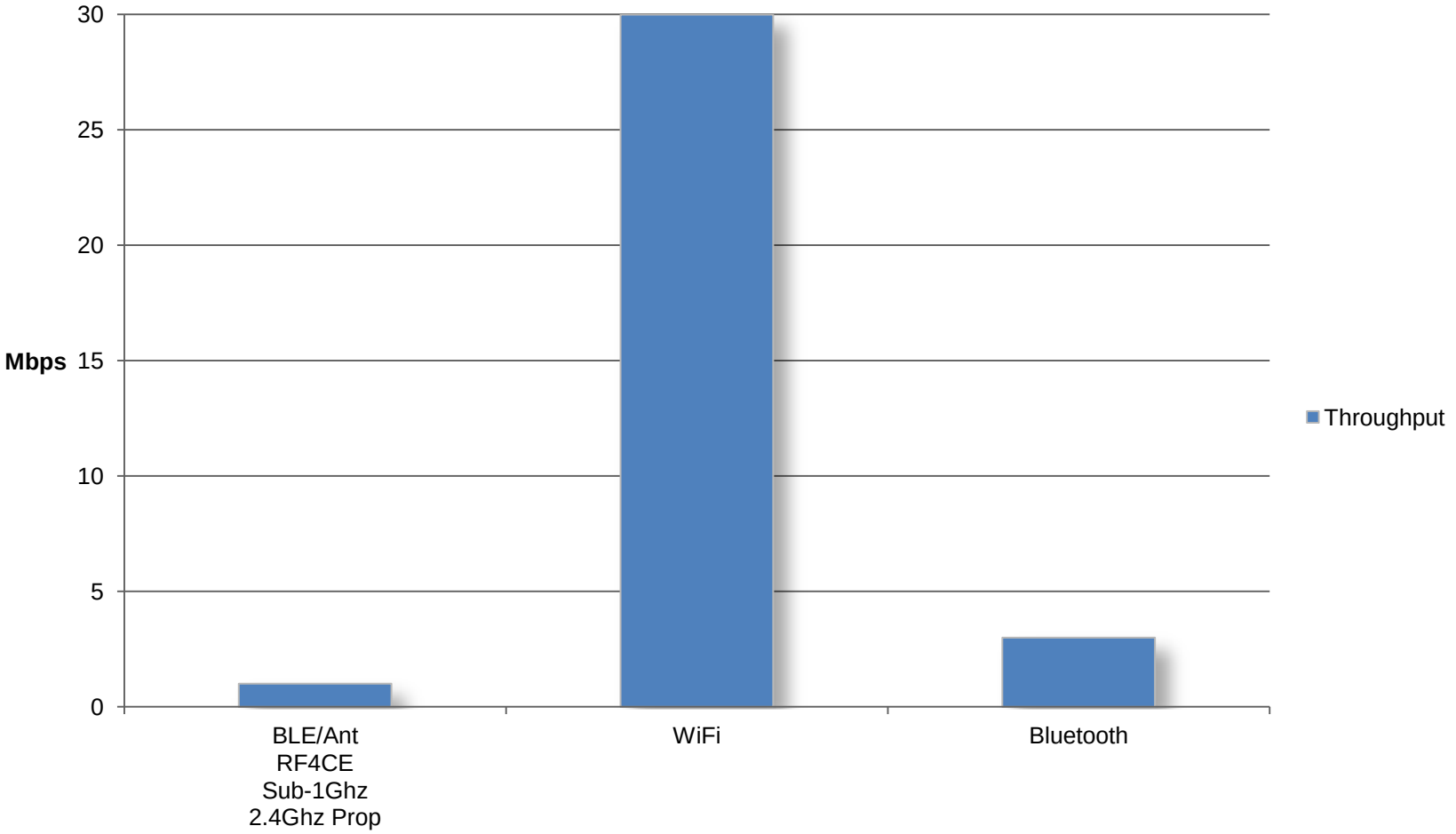
Choosing the frequency and protocol

I want to go far



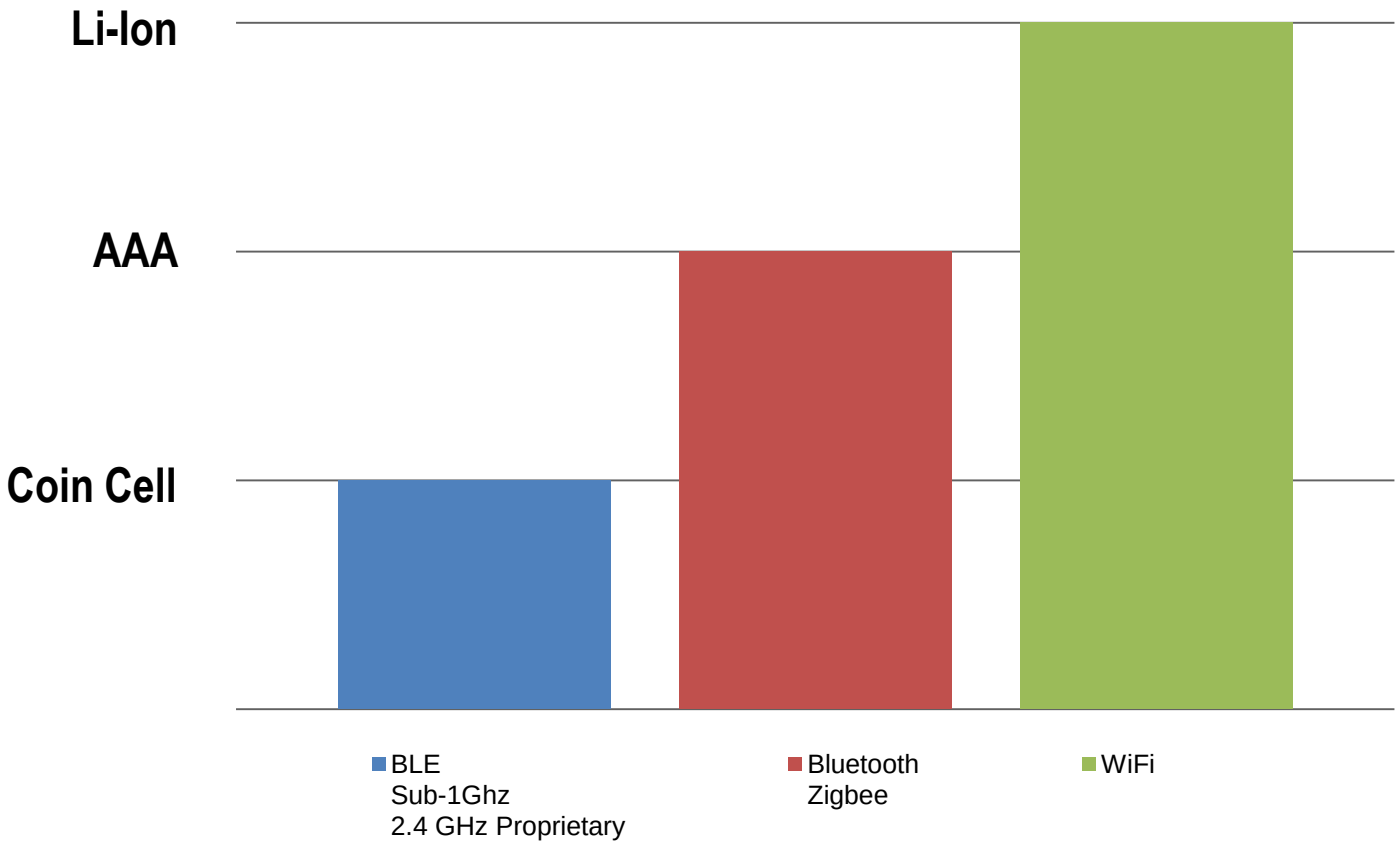
Choosing the frequency and protocol

I want to go fast

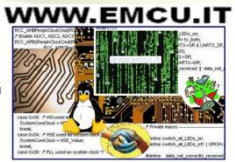


Choose the frequency and protocol

I want go low power



WiFi



Why WiFi?

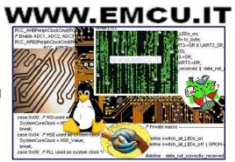
- Connect electronic devices to each other, to the Internet, and to wired networks –quickly and securely
- Most prominent wireless connectivity technology for computers and internet
- Real-world performance similar to wired networks
- High data rate, (>20Mbps throughput)
- Over 2.5 billion WiFiunits deployed in the market today; 1 billion units/year projected starting in 2011

IEEE802.11

- A set of standards for wireless local area network (WLAN) communication
- Protocols –amendments to the original standard, defined to offer improvements to 802.11 performance, frequency, bandwidth, or security

PHY Protocols	802.11b	802.11a	802.11g	802.11n
Standard approved by IEEE	1999	2000	2003	2007
Maximum data rate	11 Mbps	54 Mbps	54 Mbps	72 Mbps*
RF band	2.4 GHz	5 GHz	2.4 GHz	2.4 GHz and 5GHz
Channel width	20 MHz	20 MHz	20 MHz	20 MHz or 40 MHz

* 250Mbps is possible with multiple antennas (MIMO)



Wi-Fi

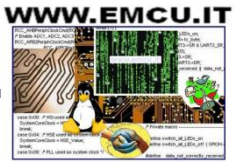
Wi-Fi Alliance

- Global non-profit industry association enabling widespread adoption of Wi-Fi worldwide
- The Wi-Fi brand was adopted for technologies based on 802.11
- The WiFiAlliance typically adopts a subset of the 802.11 standard, and sets the certification of 802.11 systems
- Enables interoperability around the standard (the only way to ensure that Wi-Fi devices will work together)

WiFi

Regulatory Certification

- **Wi-Fi operates in the unlicensed 2.4GHz and 5GHz bands, so licenses are not required to communicate between two devices. There are regulations however**
- **Wi-Fi is an intentional transmitter and therefore requires certification of the device**
  - FCC: The Federal Communications Commission is an independent agency of the US government
  - IC: Industry Canada is the Canadian Agency regulating the electronics industry
  - CE: The CE marking is a mandatory conformance mark on many products in the European Economic Area
  - ETSI: The European Telecommunications Standards Institute produces globally-applicable standards for Information and Communications
  - Telec: Telecommunications Engineering Center runs the Japanese equipment authorization program
- **FCC, IC, CE costs ~$25K for compliance testing**



Wi-Fi Certification

- To certify a product, become a member of the Wi-Fi Alliance, purchase the Wi-Fi test bed, and submit they end product for certification (~$10K)
- Upon passing certification, vendor can use the Wi-Fi CERTIFIED™ logo on that device
- IC/Modules + software can be pre-certified, but the end product needs to be certified in order to carry the Wi-Fi logo
- Wi-Fi CERTIFIED products are backwards compatible with previous generations

Frequency Bands

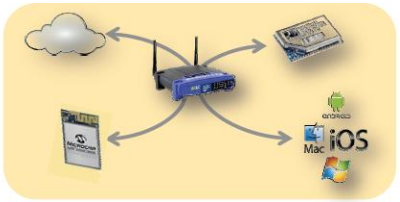
- **2.4GHz unlicensed ISM band**
  - 802.11 b,g,n–based products
  - Default band for regular consumer applications (microwave ovens, baby monitors, cordless phones, *Bluetooth and Zigbee applications)*
  - Crowded, noisy radio environment
  - Has 3 non–overlapping channels

- **5GHz unlicensed band**
  - 802.11 a,n–based products
  - Used in enterprise, controlled environments, mission critical or real-time applications
  - Consumer electronics products (such as iPad) are starting to embrace 5GHz
  - Relatively unused, less crowded so better performance against interference
  - Wide channel spacing
  - Has at least 20 non-overlapping channels (varies based on country)
  - Higher frequency degrades the range
  - Additional hardware required
  - Strict FCC regulations

Network Types

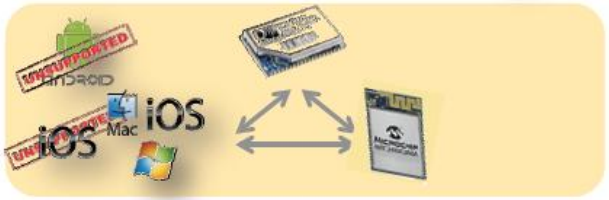
Infrastracture

- Client nodes communicate via an access point
- Most common, like connecting your PC to a home network



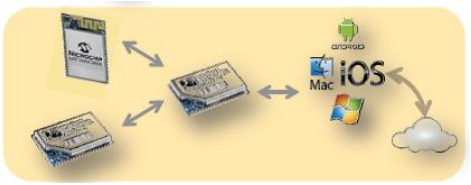
Adhoc/Wi-Fi Direct

- Point-to-Point connections
- Android unsupported (adhoc)
- Apple unsupported (Wi-Fi Direct)



SoftAP/LimitedAP

- Module “behaves” like limited AP
- AP module is network coordinator
- Same experience regardless of platform

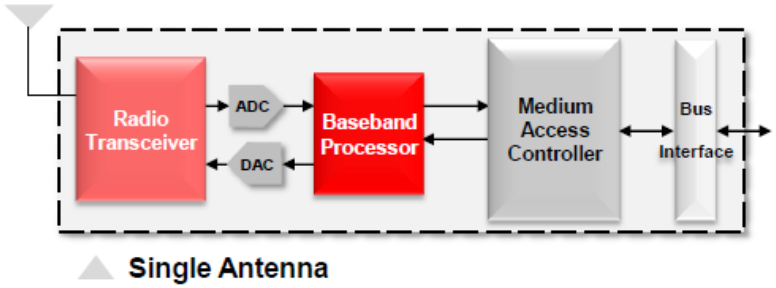


Wi-Fi Direct

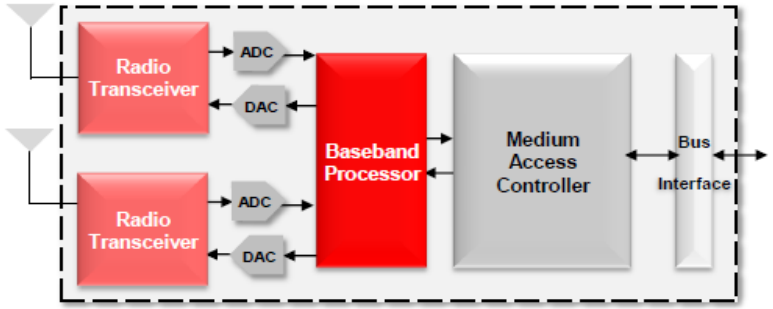
- A new standard which is just beginning to enter the market (most products will not feature Wi-Fi Direct until end of 2011)
- Allows wireless devices to directly communicate with each other (peer to peer)
- Do not need to join a traditional Wi-Fi infrastructure network like an access point/router
- One of the devices becomes group owner and acts like an access point
- Transfer content quickly and easily
- Make a one-to-one connection, or connect simultaneously to a group of devices
- All Wi-Fi Direct connections are protected by WPA2™ and WPS security

MIMO –Multiple-Input Multiple-Output

- Enables additional communication paths between devices
- Allows devices to send/receive 2x, 3x, or 4x the amount of data
- 802.11n allows up to 4x4
- Each data stream requires a discrete antenna at both the transmitter and the receiver along with a separate RF chain
- Translates to higher implementation costs and complexity compared to a single antenna system
- MIMO 2x2 chipsets have ~30% cost and size adder over single antenna chipsets
- Current MIMO chipsets draw a significant amount of power, impacting both battery-powered and line powered devices



Single Antenna



MIMO

Wi-Fi Security

- **The WLAN standards allows support for secure connection thus insuring a secure ecosystem.**
  - Authentication-controls who can connect to and configure your network and equipment.
  - Data Encryption-secures the data travelling across your network from unauthorized view –WEP, WPA, WPA2
- **Security splits into personal and enterprise.**
  - Personal security mechanisms enable secure connection without additional infrastructure or third-party authentication; it usually relies on some kind of shared secret.
  - Enterprise security is more robust and relies on a third party to support authentication and key generation.

WiFi Security Comparison

WEP

- 1999-2003, considered obsolete
- Prohibited by 'Payment Card Industry Security Standards Council' since 2008

WPAv1

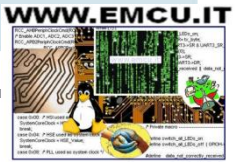
- A trimmed down 802.11i
- Same hardware as WEP
- Similar to WEP but uses a TKIP end-to-end encryption
- 8-64 Hexadecimal key, longer keys increase complexity
- Not recommended – but reasonable security

WPAv2

- Requires upgraded hardware
- AES-CCMP algorithm is mandatory 256bit key
- Considered very secure

WPA/WPA2 Enterprise

- Corporate level security additions to WPA/WPA2
- Complex implementation
- Users are qualified for network infrastructure and domain use
- Considered very secure



Stackless vs stack embedded chips

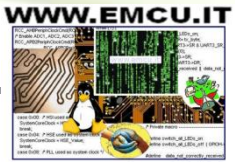
Stackless

- Tcp/IP, application layer protocols are not implemented in chip, but need to be implemented in host mcu/mpu
- These chips are lower cost, but they generally require an operating system (ie Linux)
- Examples are Texas Wilink Family, Microchip MRF24WB0MB

Stack embedded

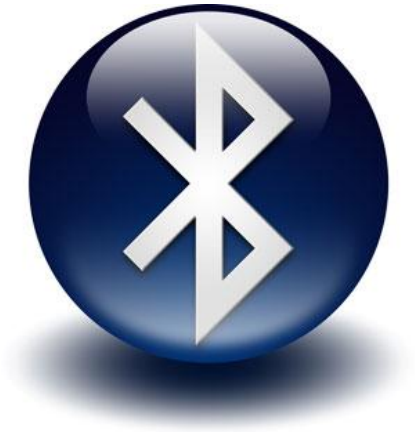
- Tcp/IP, application layer protocols (sometime application itself) is embedded in chip
- These chips are more expensive, but they can be easily used with any MCU with few line of code
- They are not the right choice for Linux or other advanced operating system
- Examples are STM WiFi module, Texas CC3000 or Microchip RN171

Bluetooh



Bluetooth

Why Bluetooth?



- **Simple Cable Replacement**
  - Original objective of Bluetooth
  - Easily make legacy wired devices – wireless
    - Barcode scanners
    - RS232 cable replacement
    - Industrial controllers
- **Smartphone and Tablet Apps**
  - Use the modern user interface of Android/IOS for your product
  - Apple has the‘cool’ factor
  - Becoming a lifestyle hub
    - Health/fitness
    - Automotive
    - Industrial control
    - Home automation
- **And now enabling low power sensors with Bluetooth Low Energy**

Bluetooth

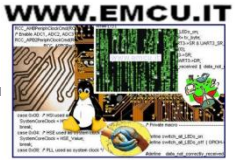
What is Bluetooth?

- **Bluetooth is a short range wireless protocol:**
  - A short-range 2.4GHz wireless technology aimed at simplifying communications among electronic products and creating Personal Area Network (PAN)
  - Enable users to automatically and easily connect a wide range of computing and telecommunication devices
    - Laptops
    - Smartphones
    - Printers
    - Keyboards
  - Use spread spectrum modulation techniques
  - Enable point-to-point or multipoint network
  - Handle both data and voice/audio transfer
- **Bluetooth protocol driven by Bluetooth SIG (Special Interest Group)**
  - Founding members are Ericsson, Nokia, IBM, Intel and Toshiba.

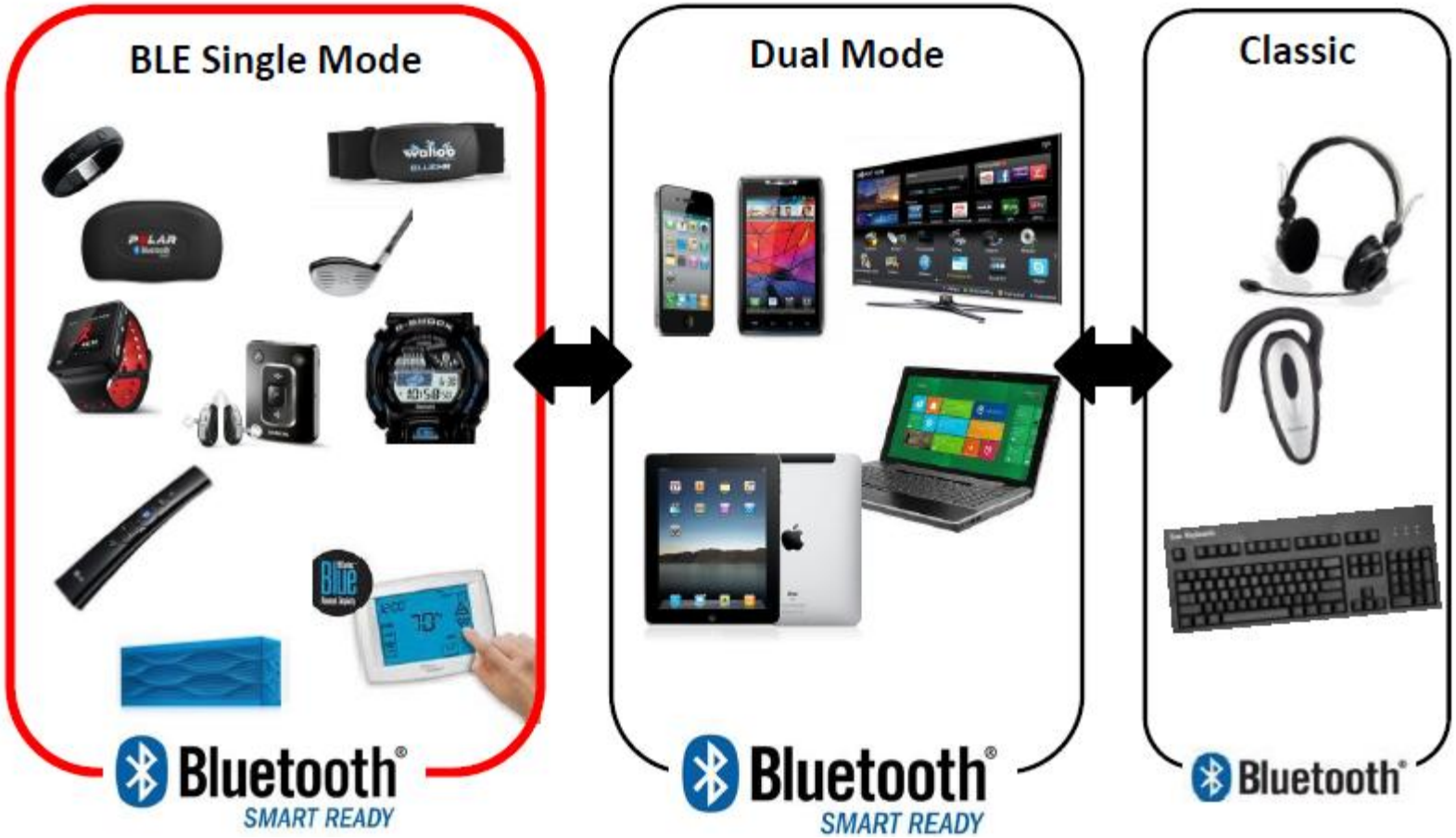
Bluetooth

What is Bluetooth low energy?

- **Part of Bluetooth Spec 4.0, July 2010**
  - Bluetooth low energy = Bluetooth SMART
    - **Bluetooth SMART Ready** indicates a dual-mode device - typically a laptop or smartphone - which operates with both Classic and LE Bluetooth peripherals.
    - **Bluetooth SMART** indicates an LE-only device - typically a battery-operated sensor - which requires either a SMART Ready or another SMART device in order to function.
  - BLE is not directly compatible with BR/EDR
- **Low bandwidth devices transmitting periodically or infrequently**
- **Targeted towards wireless applications with**
  - low-power
  - low-latency
  - low-throughput requirements
- **•Device lifetime based on role and communication interval (weeks to years)**



Blueooth 4.0 Ecosystem

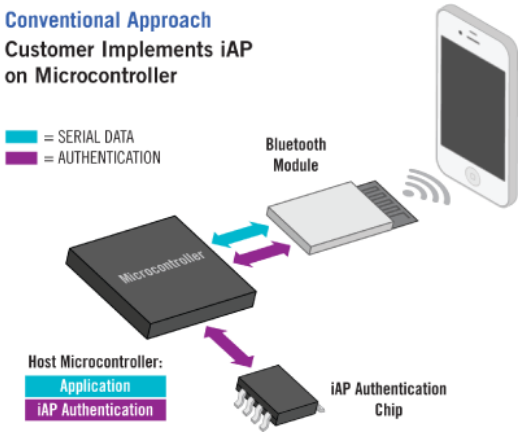


Bluetooth

Connecting to Smartphones

Bluetooth Classic

- Apple controls accessory linking to iPhone, iPad and iPod via Bluetooth and dock connector
- Customers are required to mount an Authentication Chip on their device to be able to communicate with IOS devices
- Some Bluetooth Modules make the development easier embedding the communication protocol (iAP) toward the Authentication Chip
- Exceptions are HID and Headset Profiles



Bluetooth Low Energy

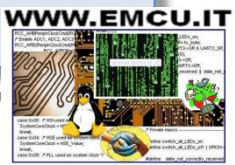
- Apple IOS Devices
  - Apple BLE connection DOESN'T require an Authentication Chip
- Android Devices
  - As April 2011 software stack is still missing from Android

Bluetooth

Profiles

- In order for two (or more) Bluetooth devices to be able to work together to accomplish a given task, such as file sharing, they need to both support the appropriate profiles.
- The Bluetooth SIG has defined countless profiles, such as Headset, A2DP Stereo, OBEX File Exchange, to name just a few.
- Profiles can be implemented in the MCU software or embedded in the module, making easier to develop applications
- Bluetooth LE profiles are much simpler than Bluetooth Classic profiles
  - Based on Generic Attribute Profile – basically consisting in a table of key/values

- Advanced Audio Distribution Profile (A2DP)
- Attribute Profile (ATT)
- Audio/Video Remote Control Profile (AVRCP)
- Basic Imaging Profile (BIP)
- Basic Printing Profile (BPP)
- Common ISDN Access Profile (CIP)
- Cordless Telephony Profile (CTP)
- Device ID Profile (DIP)
- Dial-up Networking Profile (DUN)
- Fax Profile (FAX)
- File Transfer Profile (FTP)
- Generic Audio/Video Distribution Profile (GAVDP)
- Generic Access Profile (GAP)
- Generic Attribute Profile (GATT)
- Generic Object Exchange Profile (GOEP)
- Hard Copy Cable Replacement Profile (HCRP)
- Health Device Profile (HDP)
- Hands-Free Profile (HFP)
- Human Interface Device Profile (HID)
- Headset Profile (HSP)
- Intercom Profile (ICP)
- LAN Access Profile (LAP)
- Message Access Profile (MAP)
- OBject EXchange (OBEX)
- Object Push Profile (OPP)
- Personal Area Networking Profile (PAN)
- Phone Book Access Profile (PBAP, PBA)
- Serial Port Profile (SPP)
- Service Discovery Application Profile (SDAP)
- SIM Access Profile (SAP, SIM, rSAP)
- Synchronization Profile (SYNCH)
- Video Distribution Profile (VDP)
- Wireless Application Protocol Bearer (WAPB)

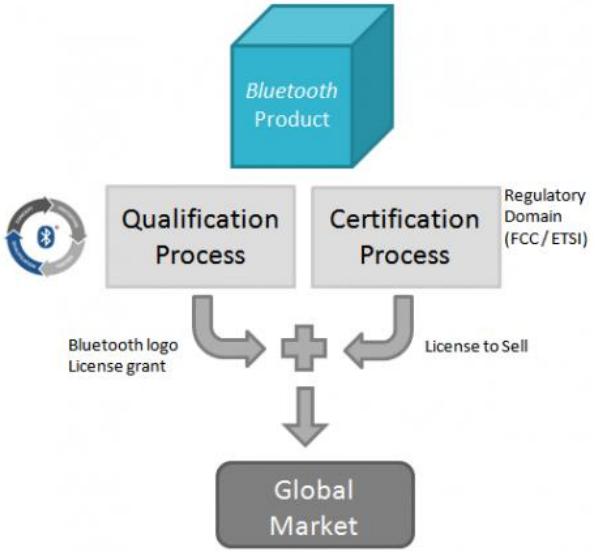


Bluetooth

Certification

Bluetooth Qualification

- Required if you want to use the Bluetooth logo on your product
- Only available to SIG members
- Consists of chip qualification, protocol stack qualification, profiles qualification, and product qualification
- The end product manufacturer must be signed up as a Bluetooth SIG Adopter (free of charge).
- Must perform profile(s) qualification and tests. Price will depend on the Bluetooth Qualification Test Facility.



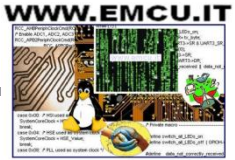
Regulatory Certification

- Operates on the unlicensed ISM band, meaning there are no licenses required to communicate between two devices. There are regulations however.
- Bluetooth is an intentional transmitter and therefore requires certification of the device (FCC, IC, CE)

Additional Notes

Documents and Contacts

- **For more info contact your SILICA local office**



Wireless Boards Under Development

ArchiTech
SILICA Design Tools

NXP Jennic Module for Seriz II

- Jennic Module 516X for Seriz II
- Enabling quick prototyping of Low-Power radio applications on Cortex M4 and RFID

ArchiTech WIFIxpresso – Microchip & NXP

- Microchip RN1** Wi-FI Module for NXP LPCXpresso
- Enabling WiFi Developing on NXP Cortex Family MCUs

ST Wi-Fi Module- Low Cost Development Kit

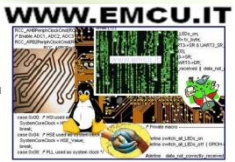
- Providing a low cost solution for developing with ST Wi-Fi Module and ST Discovery kits
- Prototypes ready and showed during ST Days in Italy

ArchiTech WiLux- Texas Instruments

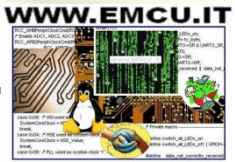
- Mood Lamp demo controlled remotely via Wi-Fi and Bluetooth Low Energy
- Under CE testing

Thank you!

Questions?



Backup Slides



WLAN Infrastructure Mode Networks

Access Point

- Networks are built to transfer data between stations
- Stations can access the Internet through the access point connected to a network
- AP's serve as the hub to relay all network communications, translating frames between a wireless medium and a wired medium
- AP's are given a service set identifier (SSID), which becomes the network name for the users
- AP sends out beacons to let stations know there is an access point they can connect to

Stations

- Computing devices with wireless network interfaces
- Stations associate with an AP to join a network
- Stations listen for beacons to understand if any traffic is available
- Because stations know when the next beacon is coming, they can go to sleep during this wait period and wake up in time for the next beacon

Soft Access Point

- Establish a WiFi connection without the need for a traditional Access Point
- Use a WiFi-enabled mobile handset to create a small local internet gateway, or ‘Soft Access Point (AP)’
- Wireless Gateway:
- Laptop connects to the phone through WiFi- where phone acts as an access point
- Phone provides access to the Internet through its 3G modem