An Introduction to Wireless Systems – Overview (Part 1)

Dr. Farid Farahmand

Updated: 9/8/14

Outline

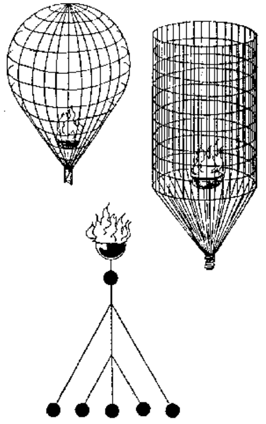
- Evolution of wireless technology
- Frequency spectrum allocation
- Wireless Network Categorization
- Wireless Network Technologies

Why Go Wireless?

Evolution of Wireless Technology

- Practical telecom started with telegraph and Morse code (1837)
  - *<u>tele</u>* (τηλε) = far and *graphein* (γραφειν) = write
  - Morse code is a type of character encoding that transmits telegraphic information using rhythm.
  - Created for Samuel F. B. Morse's electric telegraph in the early 1840s
- The invention of telephone (1876) later resulted in first switched network
  - Read The *Telephone Gambit* by Seth Shulman!
- Heinrich Hertz for the first time proved the existence of electromagnetic waves through lab experiment (1887)
  - RF signals ride on EM waves!
- Two major events had critical impact on wireless technology development
  - Sinking Titanic!
  - WWII – radar technology and FM
- Commercialization of 1-way/2-way radio
- Cellular technology in 1970

Wireless Telegraph



- The first wireless telegraph goes back to 1872 by Mahlon Loomis (the Dentist)
  - First to use a complete antenna and ground system
  - First experimental transmission of wireless telegraph signals.
  - The first use of balloons to raise an antenna wire.
  - Formulation of the idea of ‘waves’ traveling out from his antenna.
  - The first Patent for wireless telegraphy.
- Between 1895-1901 Marconi experimented with wireless telegraph systems
  - In 1901 he was able to send a character wirelessly over 1,600m across the Atlantic ocean
  - At the time there was no antenna concept or digital systems or even vacuum tube or

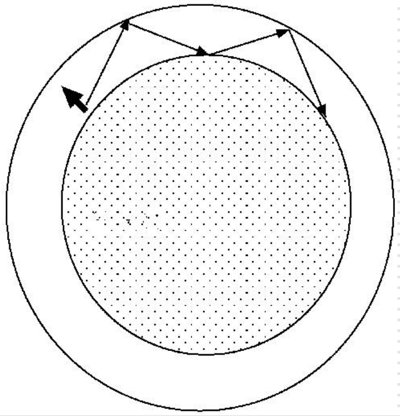
http://www.smecc.org/mhlon_loomis.htm

Wireless Continuous Waves

- In 1905 Fessenden in Mass. experimented with continuous waves
  - Continuous form of AM
  - Based on high-frequency (50kHz) – generated by a GE alternator
  - In 1906 this led to the first radio broadcasting
- In the early days U.S. Navy was very interested in the wireless technology applications
  - Titanic used wireless to send stress signals (SOS)
- WWI happened to be the major drive for development of wireless technology
- In 1920 Short-wave radio (or HF) development was underway
  - Shortwave radio operates between the frequencies of 3 MHz and 30 MHz
  - Called it shortwave because their wavelengths were shorter than other typical signals used at the time.

Wireless Transatlantic

- For transatlantic (long-range) communications high-frequency signals were required
  - Ionospheric layers (ionized by solar radiation) can be used to reflect high-frequency signals back to earth's surface
- In 1926 transatlantic wireless telephone calls became possible
- Eventually, in 1940, Microwave technology became very important
  - First Microwave system from Boston to NY was established in 1947 by AT&T

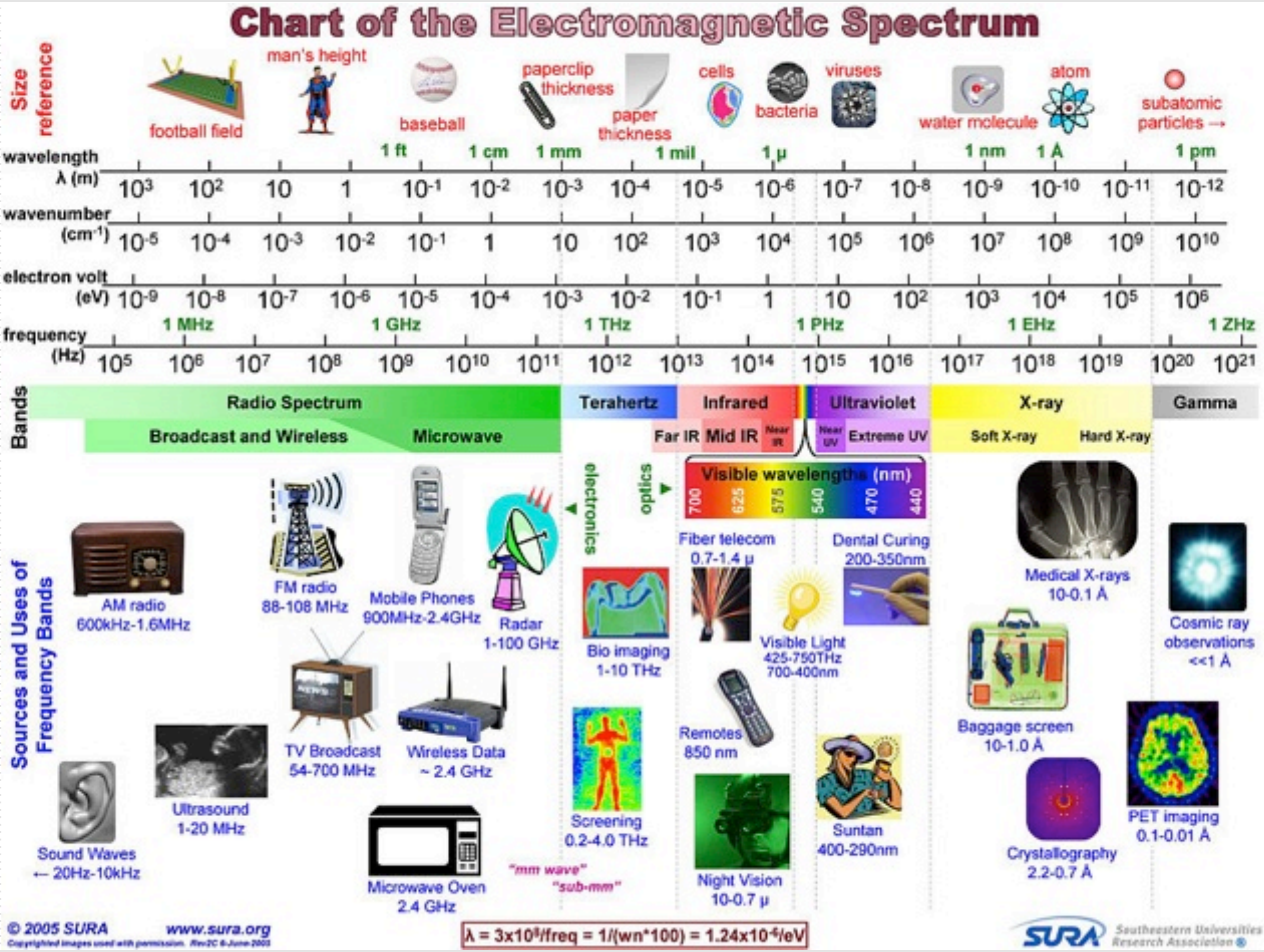


Mobile Technology was growing…..

Early Wireless Networks

- The first radio-telephone service was introduced in the US at the end of the 1940s,
  - Mainly for public fixed network
- In the 1960s, a new system launched by Bell Systems, called Improved Mobile Telephone Service (IMTS)
  - Offered many improvements like direct dialing and higher bandwidth
- The first analog cellular systems were based on IMTS and developed in the late 1960s and early 1970s

Frequency Allocations & Spectrum



http://www.jneuhaus.com/fccindex/spectrum.html

ISM Spectrum

- Data-oriented wireless network started in 1970
- In 1985 FCC opened a band for Industrial, Scientific, and Medical (ISM) applications (930 MHz – 5.856 GHz) for public
- In 1999 different industries came together to form a global non-profit organization with the goal of driving adoption of a single worldwide standard for high-speed WLAN
  - Wi-Fi Alliance http://www.wi-fi.org/
  - Certifies HW to match the standards (defined by IEEE)

Global Wireless Network – Standards….

- The key is implementing standards – standard bodies are in charge of creating such standards:

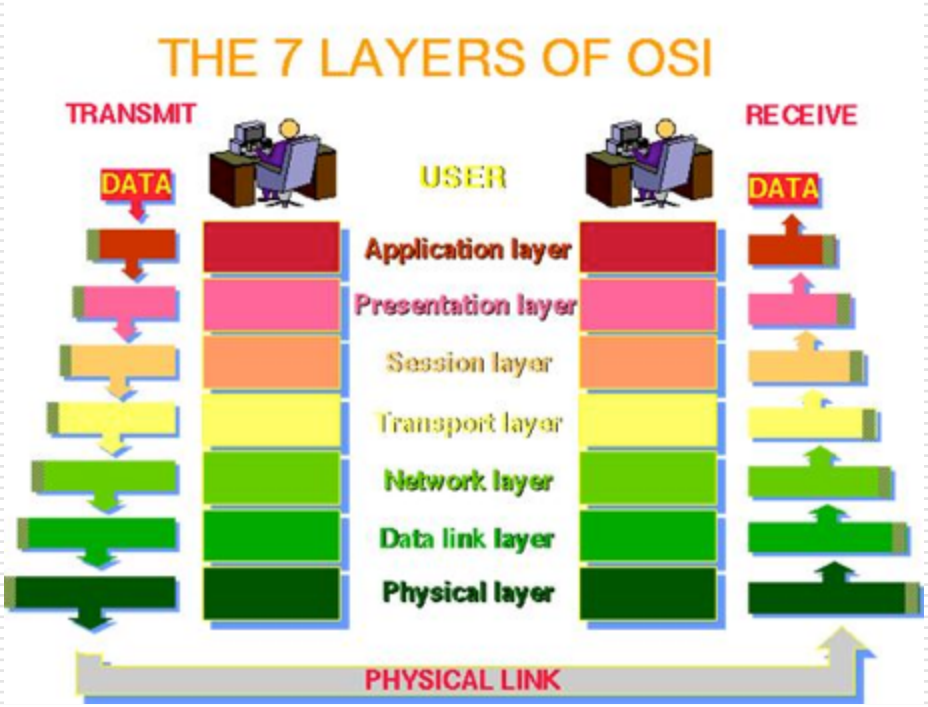
- ITU (International Telecommunications Union) has been developing International Mobile Communication standards
- WAP (Wireless Access protocol) Forum
  - Consolidated into the Open Mobile Alliance (OMA) http://www.openmobilealliance.org
  - Developing a common protocol for mobile devices with limited Internet access and display
- IETF (The Internet Engineering Task Force)
  - Developing a mobile IP standard that adopts ubiquitous IP protocol to work within a mobile environment

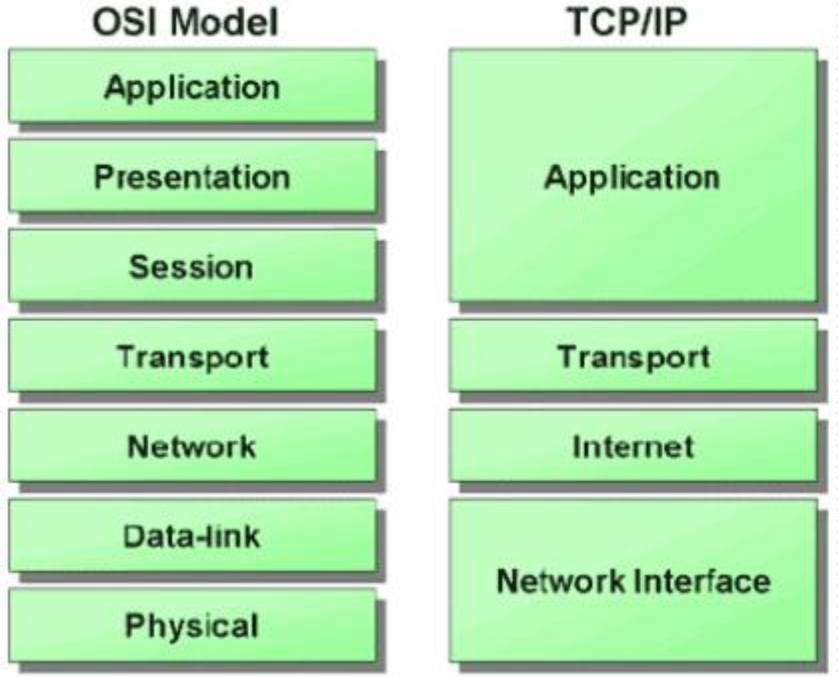
- FCC (Federal Communication Commission) - http://www.fcc.gov/
  - An independent (?) United States government agency
    - Serving public or corporate interest? http://pittsburgh.indymedia.org/
  - In charge of regulating interstate and international communications by radio, television, wire, satellite and cable
    - Power levels, frequencies, broadcast rules, ownerships, ….

Other Players: WHO IS WHO on the Internet

- Internet Corporation for Assigned Names and Numbers (ICANN)
  - It is contracted by the U.S. government to supply IANA (Internet Assigned Number Authority) – responsible for all IP addresses!
- Institute of Electrical and Electronics Engineers (IEEE)
- The European Computer Manufacturers Association (ECMA)
- The International Electro-technical Commission (IEC)
- The International Organization for Standardization (ISO)
- World Wide Web Consortium (*W3C*)
  - Develops technologies for www, including specifications, guidelines, and tools (HTML, DHTML, XML were all developed by W3C)
- The *Internet Engineering Task Force* (*IETF*)
  - Protocol engineering and development arm of the Internet
  - IETF's technical management is handled by IESG (Internet Engineering Steering Group)
  - the RFC repository maintained by the *IETF*
  - *RFC → IETF → Review →*
    - *If not accepted goes to the Repository "historical"*
    - *If accepted it become an standard*

Standards & OSI and TCP/IP Architecture



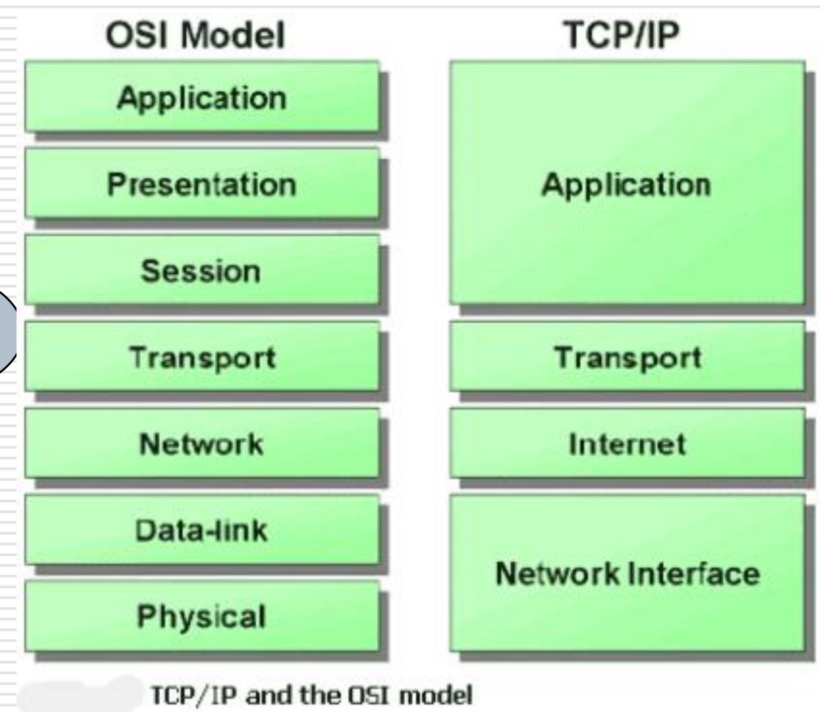


TCP/IP and the OSI model

Wireless Systems and Networks

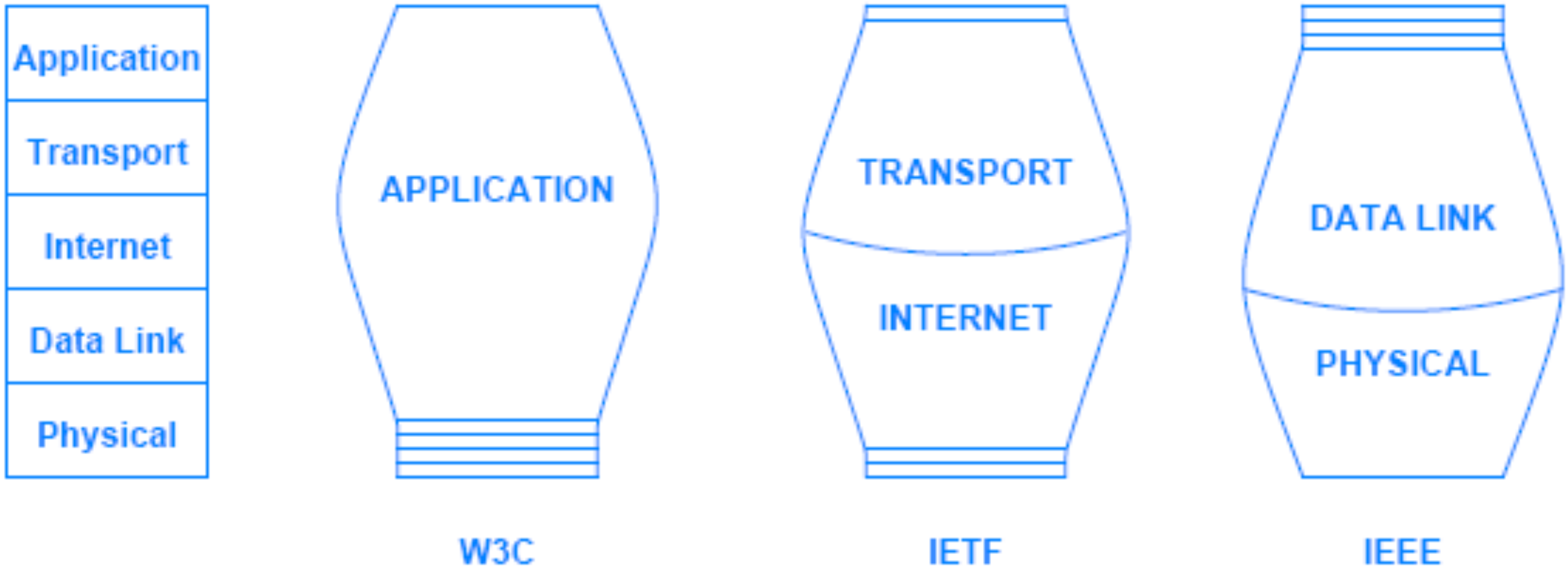
- Network Layer
  - Location management
  - Handoff process
  - Routing
- Link Layer
  - Power management
  - Rate allocation
  - Error control
  - Call admission
  - Scheduling
- Physical Later
  - TX/RX signal format
  - Channel properties
  - Radio interface

Our focus!



TCP/IP and the OSI model

Various Standard Emphasis



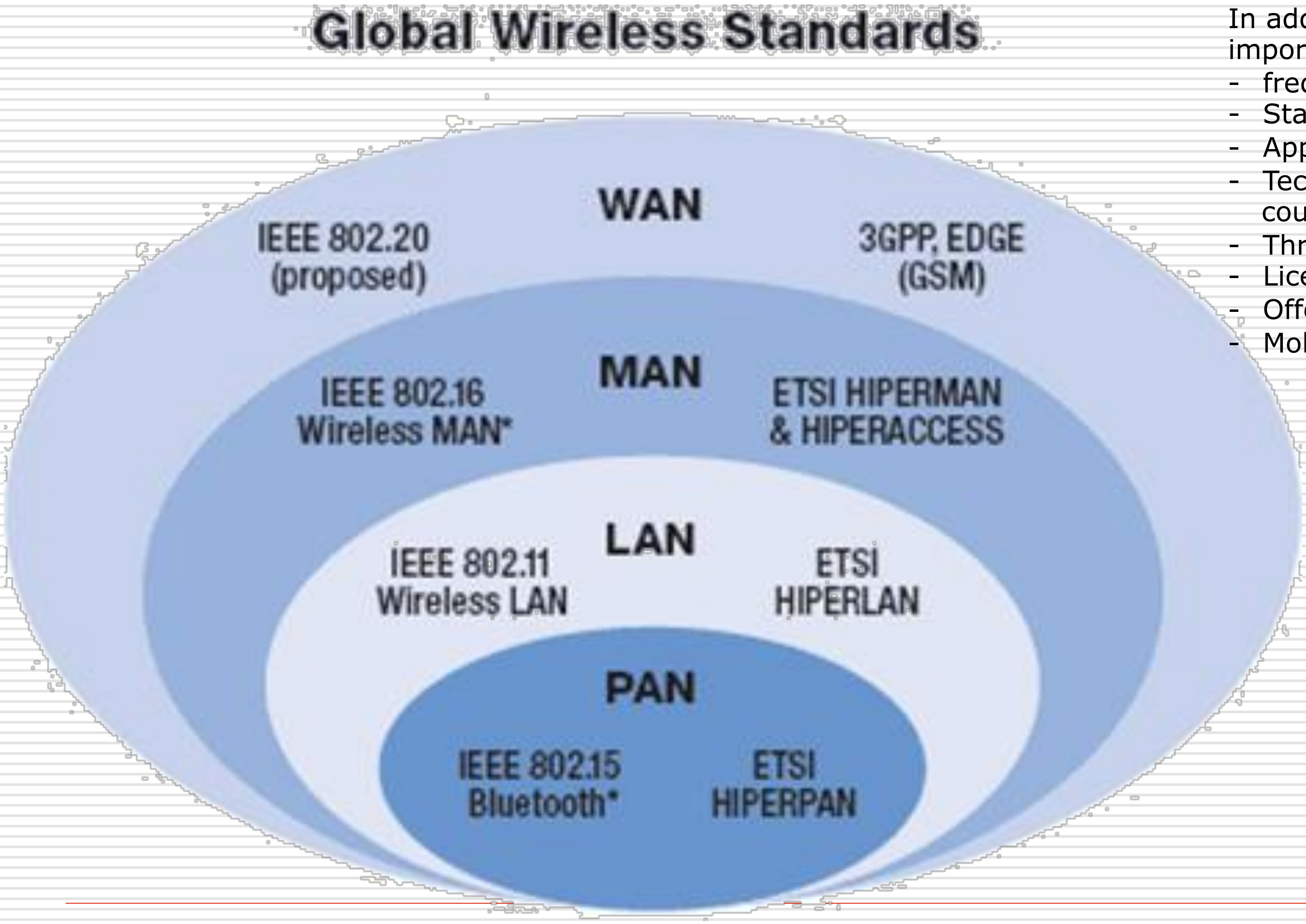
Institute of Electrical and Electronics Engineers

Wireless Networks

Categorization of Wireless Networks

- Wireless Wide Area Networks (WWANs)
  - Cellular Networks :
    - GSM, cdmaone (IS-95), UMTS, cdma2000 EVDO
  - Satellite Networks:
    - Iridium, Globalstar, GPS, etc.
- Wireless Metro Area Networks (WMANs)
  - IEEE 802.16 WiMAX
- Wireless Local Area Networks (WLANs)
  - IEEE 802.11, a, b, g, etc. (infrastructure, ad hoc, sensor)
- Wireless Personal Area Networks (WPANs)
  - IEEE 802.15 (Bluetooth), IrDa, Zigbee, sensor, etc.

Wireless Network Standards - Examples



In addition to their coverage, other important issues are:

- freq. of operation (spectrum)
- Standards
- Applications
- Technology variations in diff. countries
- Throughput (data rate)
- Licensed or unlicensed
- Offered Services
- Mobility (e.g., vehicular vs. office)

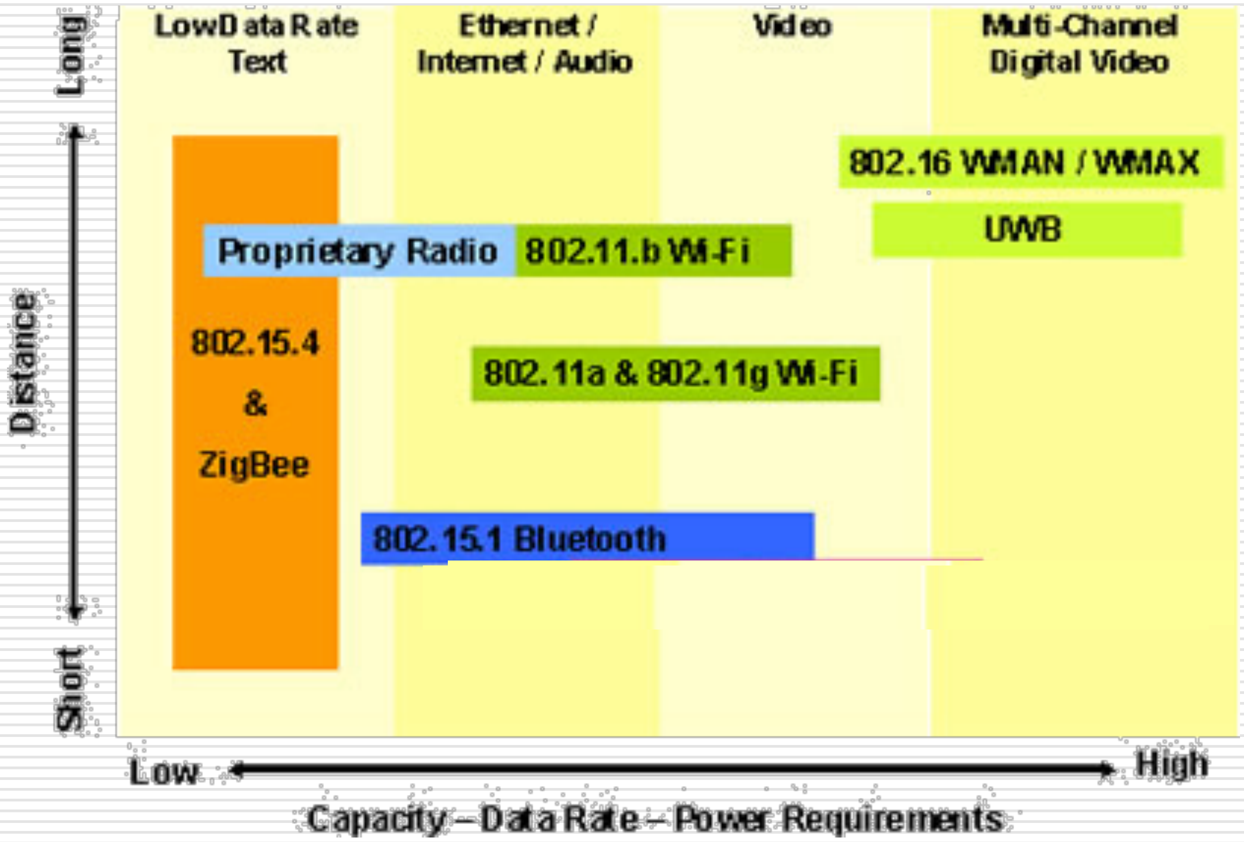
Wireless Networks

Network	Geographic Coverage	Typical Throughput	Standards
WWANs	National, Continent wide	2G: 9.6 – 45 Kbps, 2.5G: 50 -300 Kbps 3G : 50kbsp- 2Mbps 3.5G: .1 – 10 Mbps	2G: GSM, cdmaone 2.5G: GPRS, cdma 2000 1X-rtt 3G: UMTS, cdma2000 1x-EDVO 3.5G: HSPDA
WMANs	Metro, suburb, campus 1-15 km	2~100 Mbps	IEEE 802.16
WLANs	In building, campus wide, subdivision wide, Range ~ 100 M per AP	1-106 Mbps	IEEE 80211a, b, g, etc.
WPANs	5-10 M around device	.1 – 1Mbps	IEEE 802.15 IrDa, BlueTooth, Zigbee

Frequency Allocation For Different Standards

	Europe	USA	Japan
WWANs **Licensed**	**Cellular:** 453-457MHz, 463-467 MHz; **PCS:** 890-915 MHz, 935-960 MHz; 1710-1785 MHz, 1805-1880 MHz **3G:** 1920-1996 MHz 2110-2186 MHz	**Cellular** 824-849 MHz, 869-894 MHz; **PCS** 1850-1910 MHz, 1930-1990 MHz;	**Cellular** 810-826 MHz, 940-956 MHz; 1429-1465 MHz, 1477-1513 MHz **3G** 1918.1-1980 MHz 2110-2170 MHz
WMANs **Licensed** **Unlicensed**	**IEEE 802.16** 3.4-3.6 GHz SAME as WLANs	**IEEE 802.16** 2.5 – 2.6 GHz, 2.7-2.9GHz Same as WLANs	**IEEE 802.16** 4.8-5 GHz Same as WLANS
WLANs **Unlicensed**	**IEEE 802.11** 2400-2483 MHz 5.7-5.825 GHz **HIPERLAN 1** 5176-5270 MHz	**IEEE 802.11** 2400-2483 MHz (b, g) 5.7 – 5.825 GHz (a)	**IEEE 802.11** 2471-2497 MHz (b, g) 5.7-5.825 GHz (a)
WPANs **Unlicensed**	**IEEE 802.15** 2400-2483 MHz	**IEEE 802.15** 2400-2483 MHz	**IEEE 802.15** 2471-2497 MHz

Wireless Technologies Basic Characteristics



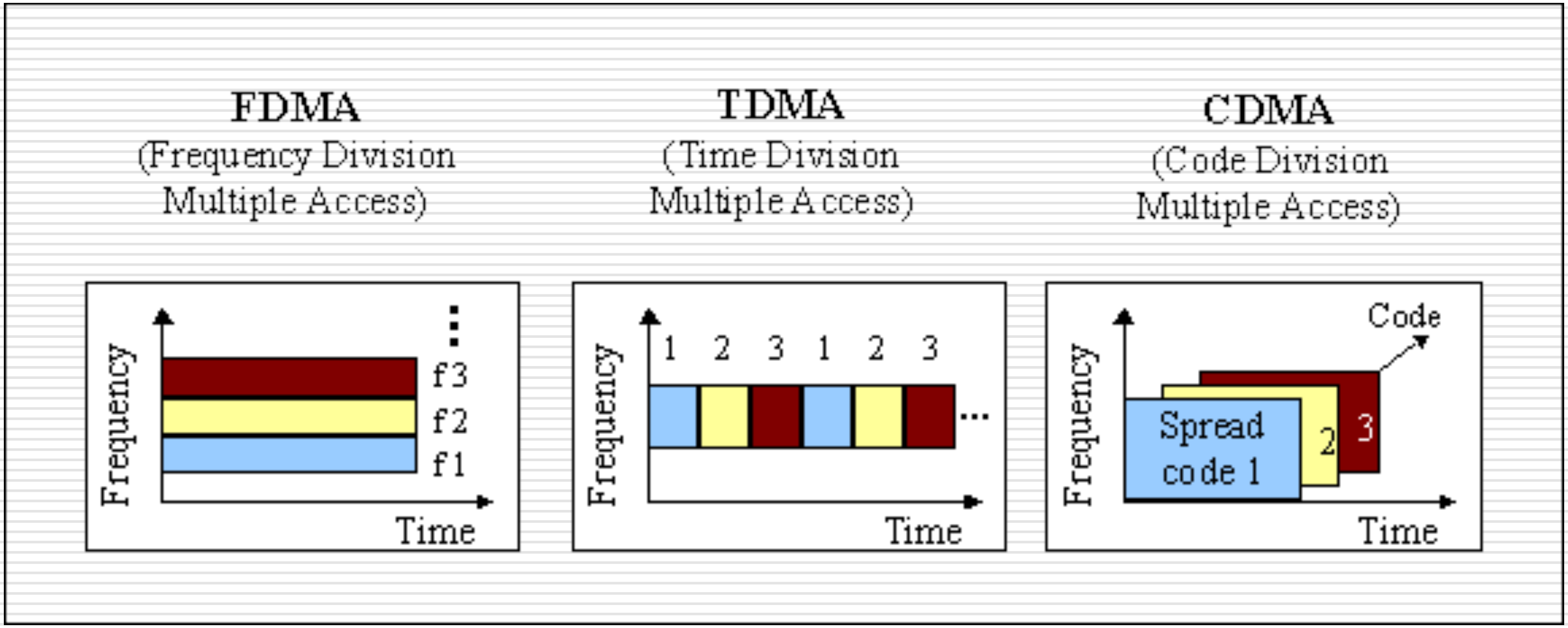
Wireless Access Technologies

Access Wireless Technologies

- **FDMA:** Frequency Division Multiple Access (FDMA)
  - The most common analog system
  - The spectrum is divided up into frequencies and then assigned to users
  - With FDMA, only one subscriber at any given time is assigned to a channel
- **TDMA:** Time Division Multiple Access (TDMA)
  - Improves spectrum capacity by splitting each frequency into time slots
  - TDMA allows each user to access the entire radio frequency channel for the short period of a call
  - Other users share this same frequency channel at different time slots
- **CDMA:** Code Division Multiple Access
  - Based on "spread" spectrum technology
  - Suitable for encrypted transmissions (useful for military)

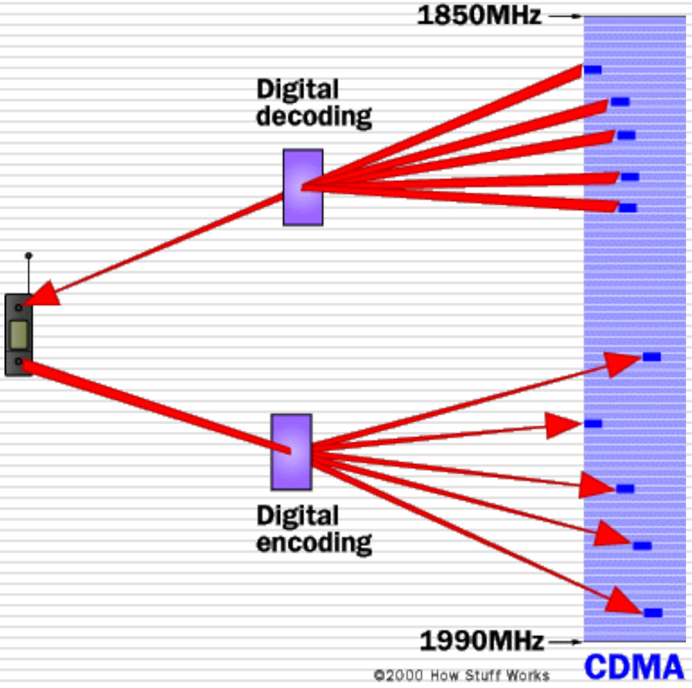
We will discuss these later in Chapter 7: Spread Spectrum & CDMA

Wireless ACCESS Technologies



More on CDMA

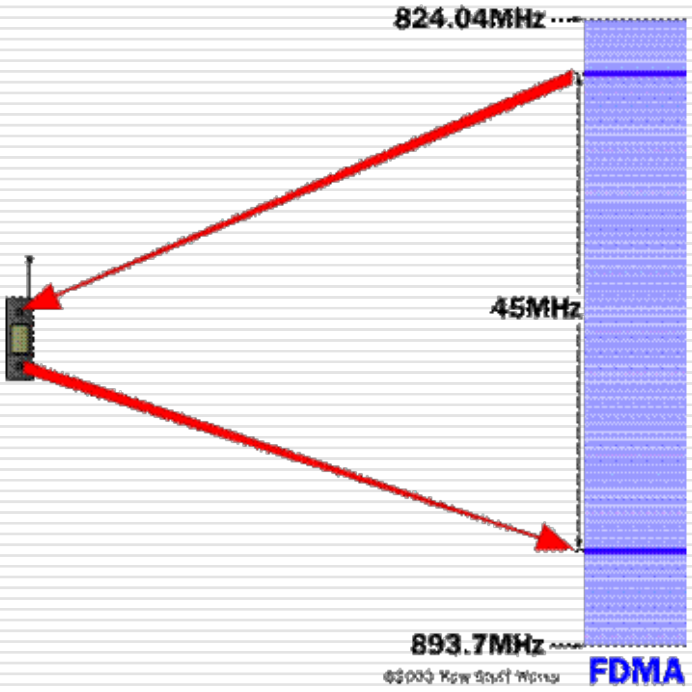
- CDMA is Code Division Multiple Access. When users make a call, CDMA spreads the data throughout the entire bandwidth.



http://classes.cecs.ucf.edu/\seecsseniordesign/fa2002sp2003/g05/Papers/Initial%20Project%20Paper.htm

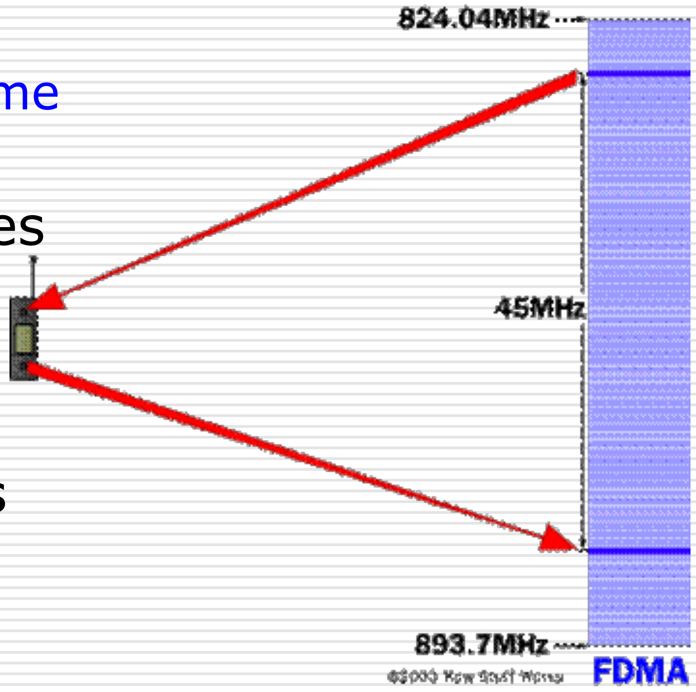
What about GSM?
Global System for Mobile Communications

- Considered as 2G Cellular Technology
- GSM uses TDMA and FDMA (Frequency Division Multiple Access) technology as two operations on one system
  - Each phone call is encrypted
  - This frequency is then divided into carrier frequencies
  - Using TDMA technology, each of these carrier frequencies are finally divided into time – this is different from spreading!
- It is the international standard and most used throughout the world
- Callers are assigned a frequency (FDMA)



GSM Frequency Operations

- In the United States, GSM operates on frequencies in the range of 850 MHz and 1.9 GHz and
- The 850 MHz range is also used in many other countries, such as Australia and some in South America.
- In Europe, GSM operates in the ranges of 900 MHz and 1.8 GHZ
- The ranges are not that important to consumers, who are generally more concerned about transmission speeds and reliability



Two main competing cellular networks

Global System for Mobile Communications (GSM)
Code Division Multiple Access (CDMA)

- GSM
  - Used by AT&T and T-Mobile in U.S.
  - Very good coverage in rural areas
  - Reliable international roaming (used in most other countries)
  - Uses a removable SIM card (Subscriber Identity Module) – SIM is tied to the network not the phone
    - Changing the phone is easier!
  - Quad-band phone (850/900/1800/1900) MHz
  - Extended capacity is provided by EDGE (Enhanced Data Rates for GSM Evolution) – 2.75/3G communication technology
    - Boasts data rates of up to 384 kbps with real world speeds reported closer to 70-140 kbps
- CDMA
  - Developed by Qualcomm
  - Used by Verizon and Sprint
  - Smaller users compared GSM (200 million vs 1 billion [*])
  - Extended capacity is provided by CDMAone, CDMA2000 1xRTT and/or EVDO
    - Replacing DSL
  - The phone is connected to the network
    - R-UIM (Removable User Identity Module) enabled phone removable cards
    - R-UIM card will work in GSM phones for roaming (with roaming agreement)

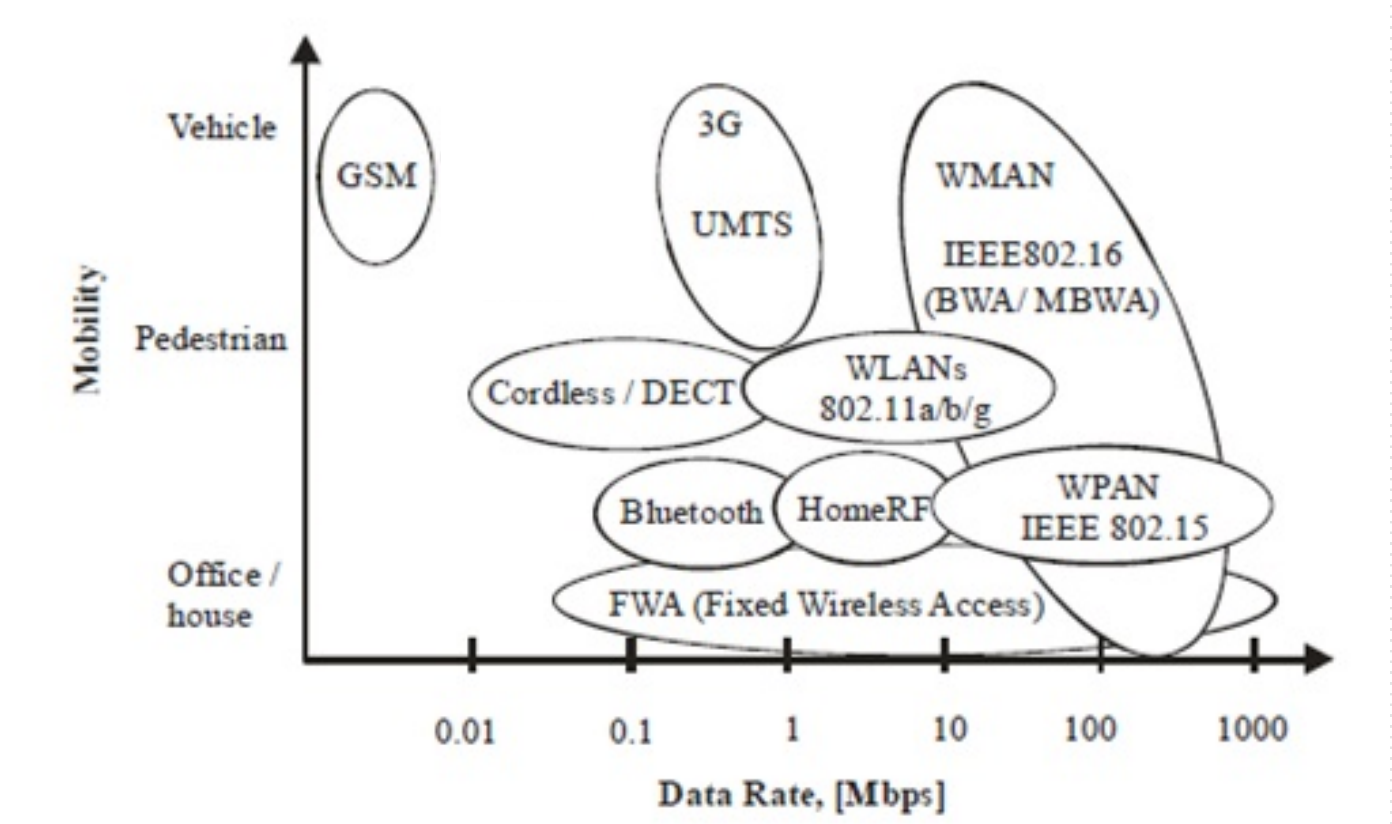
* http://www.wisegeek.com/what-is-the-difference-between-gsm-and-cdma.htm

Comparing Different Cellular Technologies

Technology Name	Access Technology Type	Characteristics	Peak Network Speed	Typical Downlink Speed	Typical Uplink Speed
GPRS	TDMA	General Packet Radio Service. First data service for GSM.	115 kbps	20 to 40 kbps	20 to 40 kbps
EDGE	TDMA	Enhanced Data Rates for GSM Evolution. Enhancement to GPRS.	473.6 kbps	70 kbps to 130 kbps	70 kbps to 130 kbps
WCDMA	CDMA	Wideband CDMA 3G technology providing voice and data capabilities. Current deployments use HSPA for data.	2 Mbps	200 to 300 kbps	200 to 300 kbps
HSPA	CDMA	High Speed Packet Access. Data enhancement for WCDMA.	14.4 Mbps	1 Mbps to 4 Mbps	500 kbps to 2 Mbps
HSPA+	CDMA	Evolution of HSPA.	42 Mbps	>5 Mbps expected	>3 Mbps expected
LTE	OFDMA	Long Term Evolution. New radio interface. All IP.	326 Mbps	> 10 Mbps expected	> 5 Mbps expected
LTE Advanced	OFDMA	Advanced version of LTE designed to meet IMT-Advanced requirements.	1 Gbps	TBD	TBD

The Universal Mobile Telecommunications System (UMTS) and Enhanced Data Rates for GSM Evolution (EDGE)
http://www.wirelessweek.com/Articles/2009/02/The-Shift-from-3G-to-4G/

Wireless Technologies – Mobility vs Data Rate



NEXT:

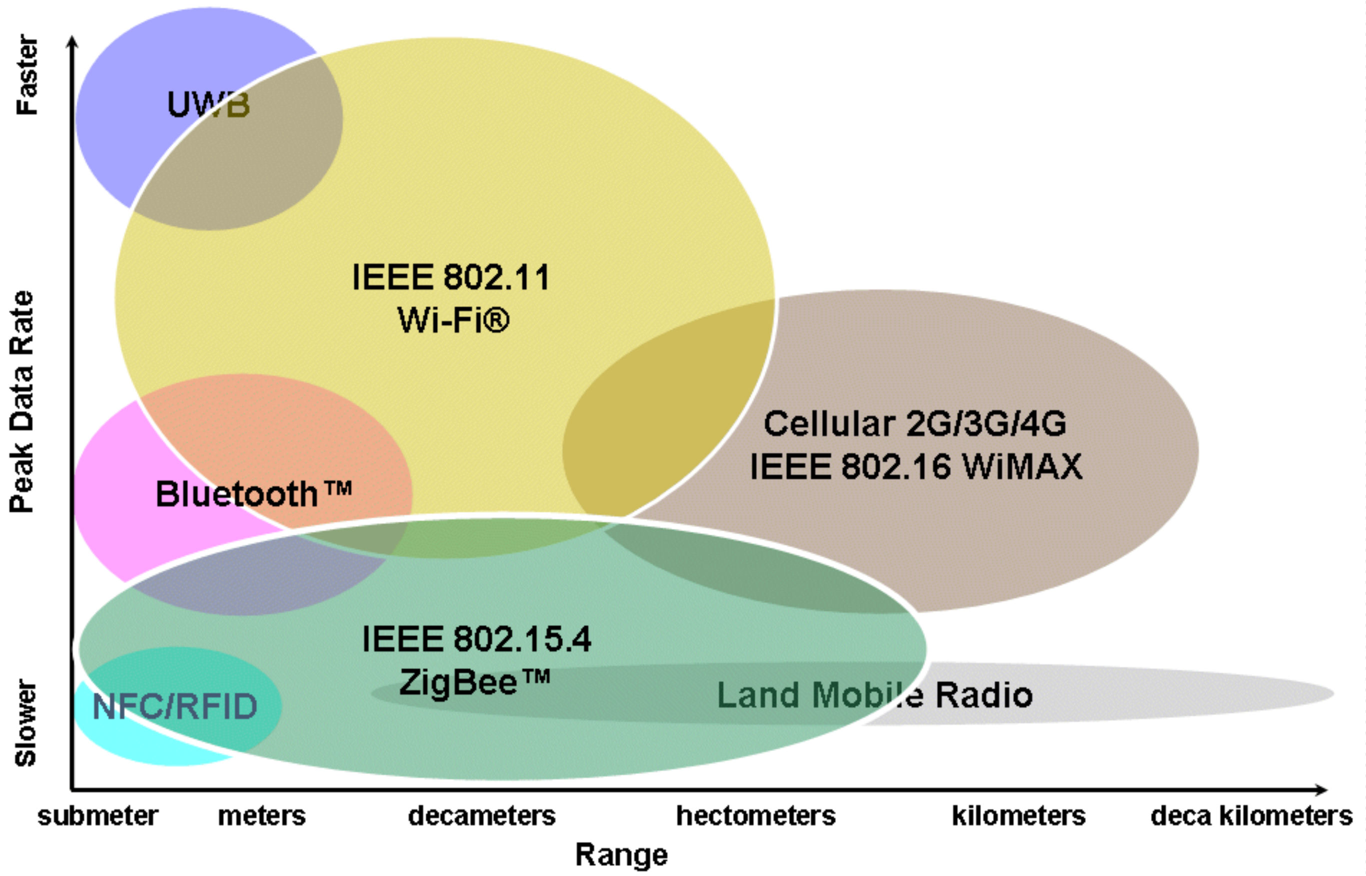
- We will talk about Cellphone Technologies and their difference later…..

Wireless MAN/LAN/PAN Networks & Their Related Technologies

Wireless LAN/MAN Network Standards (802)

Competing:

802.15.4
Z-Wave
Bluetooth
IEEE 802.11b



IEEE 802 Model

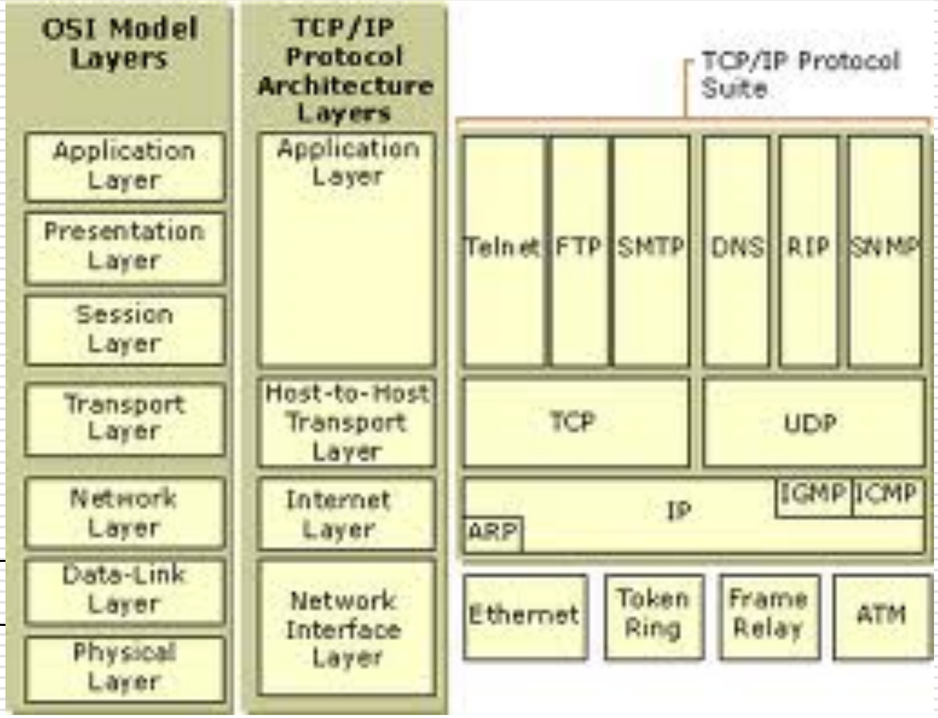
- IEEE divides Layer 2 of the protocol stack into two conceptual sub-layers
  - The Logical Link Control (LLC) ← IEEE 802.2 (Logic Link Control) Model
    - sublayer specifies addressing and the use of addresses for demultiplexing
  - The Media Access Control (MAC) ← IEEE 802.3 Ethernet
    - sublayer specifies how multiple computers share underlying medium

Sub-Layer	Expansion	Purpose
LLC	Logical Link Control	Addressing and demultiplexing
MAC	Media Access Control	Access to shared media

Presentation Slides:
http://www.sonoma.edu/users/f/farahman/sonoma/courses/es465/lectures/es465_fall2010/chapter15_v3.pdf

OSL Model
Reminder

Logic Link Control sublayer
MAC sublayer



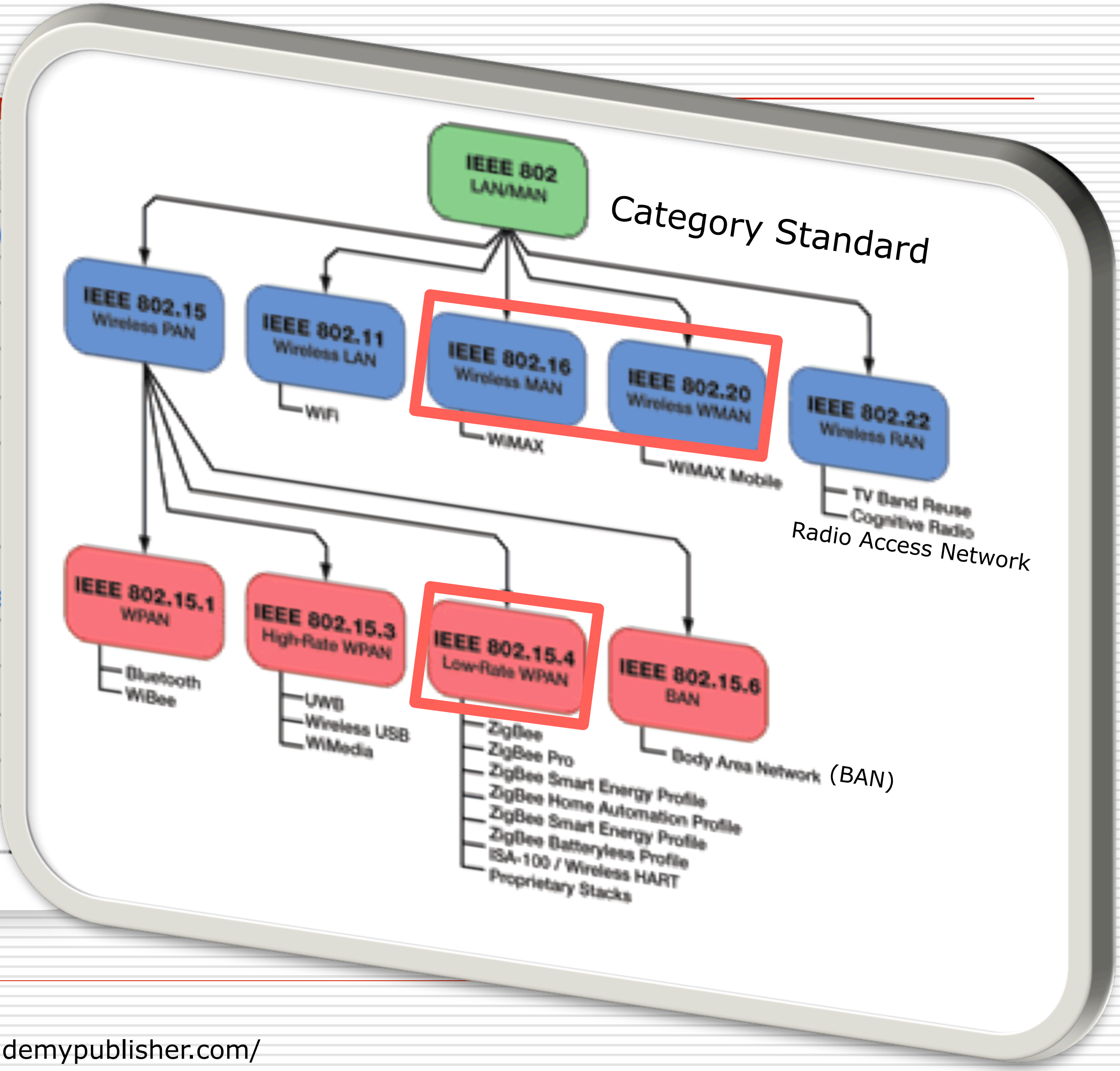
IEEE Standards

- IEEE assigns a multi-part identifier of the form XXX.YYY.ZZZ
  - XXX denotes the category of the standard
  - YYY denotes a subcategory
  - If a subcategory is large enough, a third level can be added

ID	Topic
802.1	Higher layer LAN protocols
802.2	Logical link control
802.3	Ethernet
802.4	Token bus (disbanded)
802.5	Token Ring
802.6	Metropolitan Area Networks (disbanded)
802.7	Broadband LAN using Coaxial Cable (disbanded)
802.9	Integrated Services LAN (disbanded)
802.10	Interoperable LAN Security (disbanded)
802.11	Wireless LAN (Wi-Fi)
802.12	Demand priority
802.13	Category 6 - 10Gb LAN
802.14	Cable modems (disbanded)
802.15	Wireless PAN 802.15.1 (Bluetooth) 802.15.4 (ZigBee)
802.16	Broadband Wireless Access 802.16e (Mobile) Broadband Wireless
802.17	Resilient packet ring
802.18	Radio Regulatory TAG
802.19	Coexistence TAG
802.20	Mobile Broadband Wireless Access
802.21	Media Independent Handoff
802.22	Wireless Regional Area Network

IEEE LAN, PAN, RAN and MAN Standards

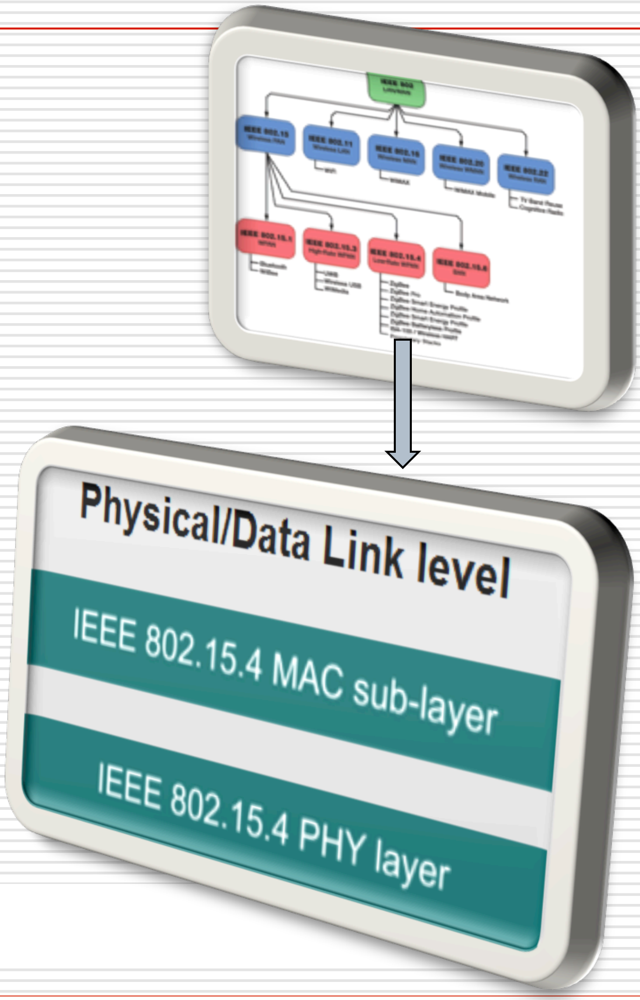
802.10	Interoperable LAN Security (disband
802.11	Wireless LAN (Wi-Fi)
802.12	Demand priority
802.13	Category 6 - 10Gb LAN
802.14	Cable modems (disbanded)
802.15	Wireless PAN 802.15.1 (Bluetooth) 802.15.4 (ZigBee)
802.16	Broadband Wireless Access 802.16e (Mobile) Broadband Wirele
802.17	Resilient packet ring
802.18	Radio Regulatory TAG
802.19	Coexistence TAG
802.20	Mobile Broadband Wireless Access
802.21	Media Independent Handoff
802.22	Wireless Regional Area Network



Read about Cognitive Radio: http://www.academypublisher.com/jcm/vol01/no01/jcm01013847.pdf

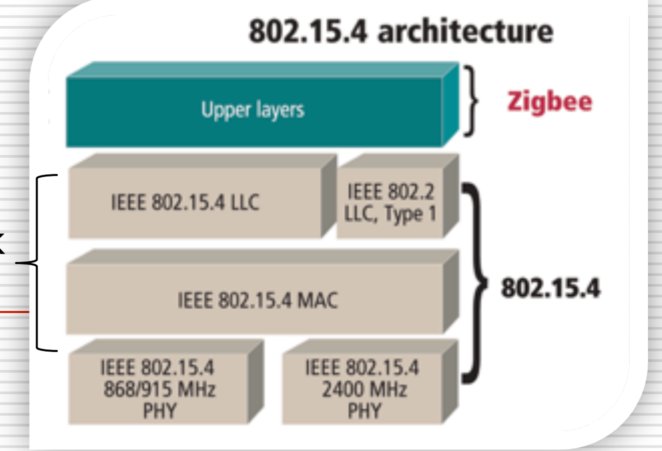
802.15.4
Physical and MAC

- Zigbee Standards
- 6LoWPAN Standards
- Wireless HART Standards
- MiWi
- … all use 802.15.4



802.15.4

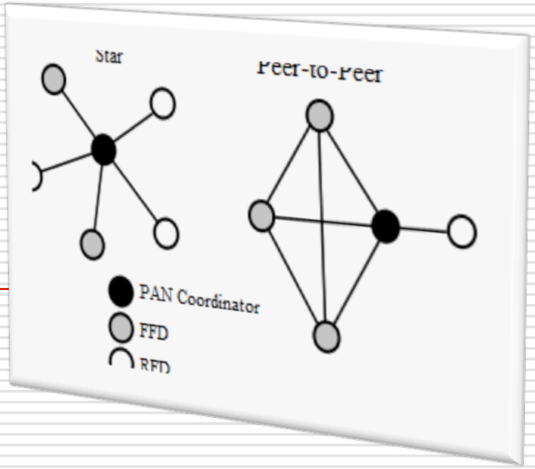
Data Link Layer

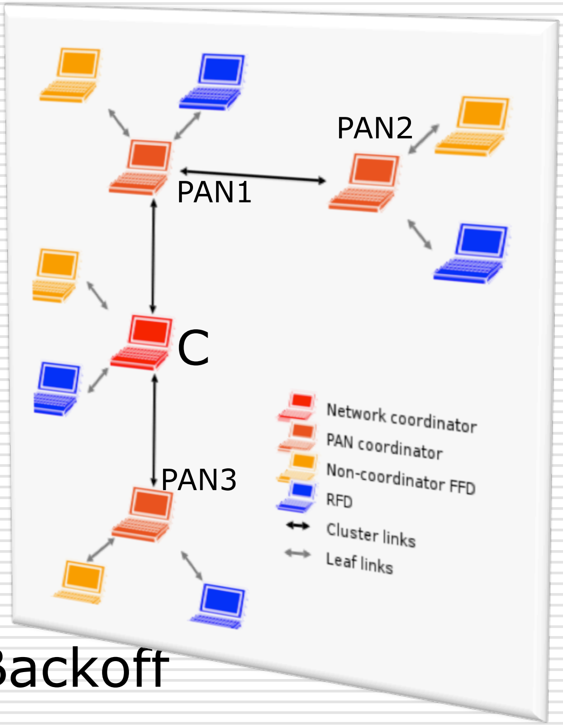


- Physical layer
  - Radio frequencies from 868MHz, 902-928MHz, 2.GHz
  - Uses direct sequence spread spectrum (DSSS)
  - Variations include a,c,d
    - Different frequencies and modulation techniques
- MAC Layer
  - Medium access
  - Data services
    - Node association and frame validation
  - Provides network beaconing

802.15.4
Network Model

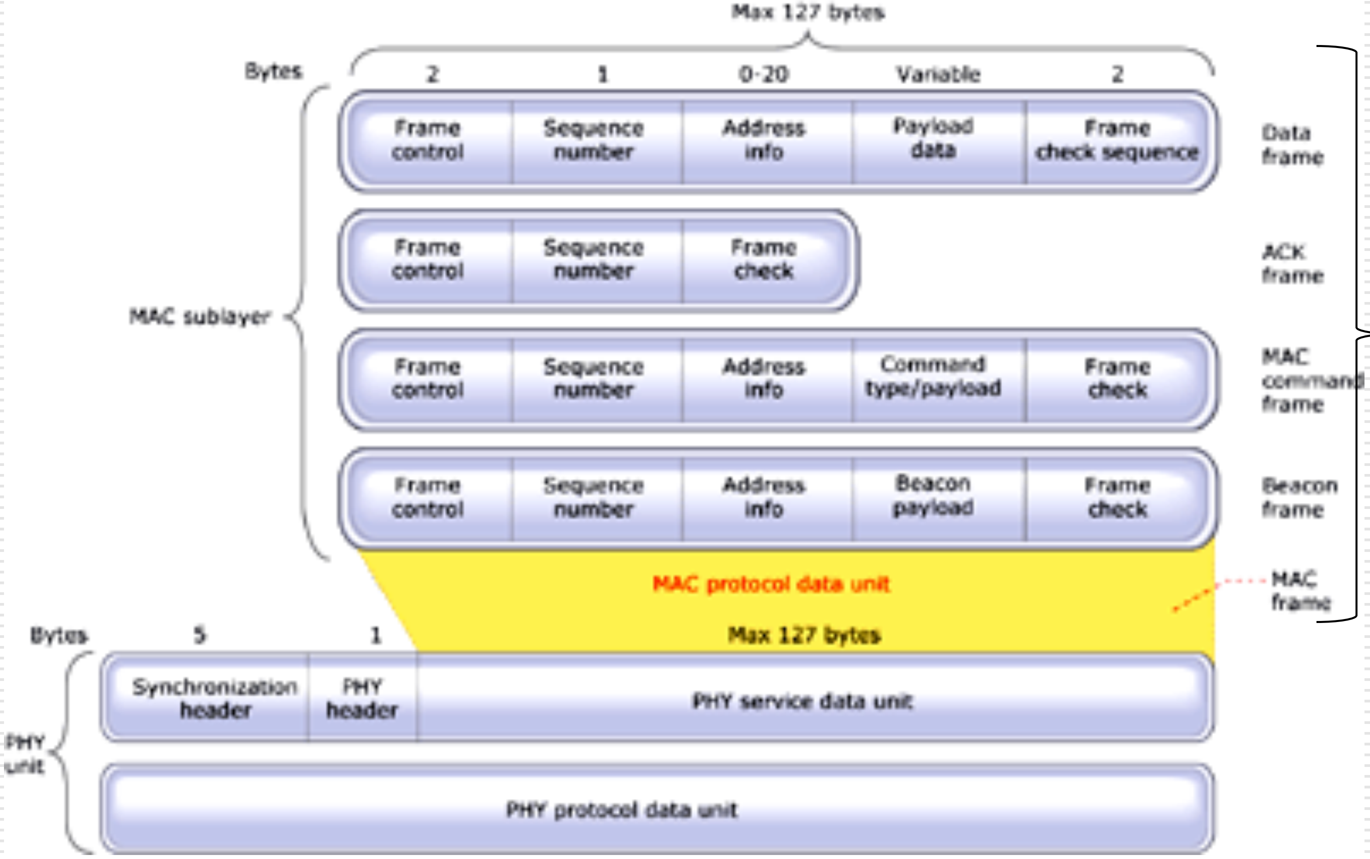
- Node type
  - Full function device (FFD)
    - Common node
    - Coordinator
  - Reduced function device (RFD)
    - Only communicate with FFD
    - Never becomes coordinator
- Topologies
  - P2P (Ad-Hoc), Star, Mesh (Cluster)
- Data frame architecture
  - CSMA/CA with Random Exponential Backoff
  - Timeout-based retransmission





Read about CSMA: http://www.sonoma.edu/users/f/farahman/sonoma/courses/es465/lectures/es465_fall2010/chapter15_v3.pdf

802.15.4
Protocol Stack



Diff.
Data frames are supported

Protocols using 802.15.4

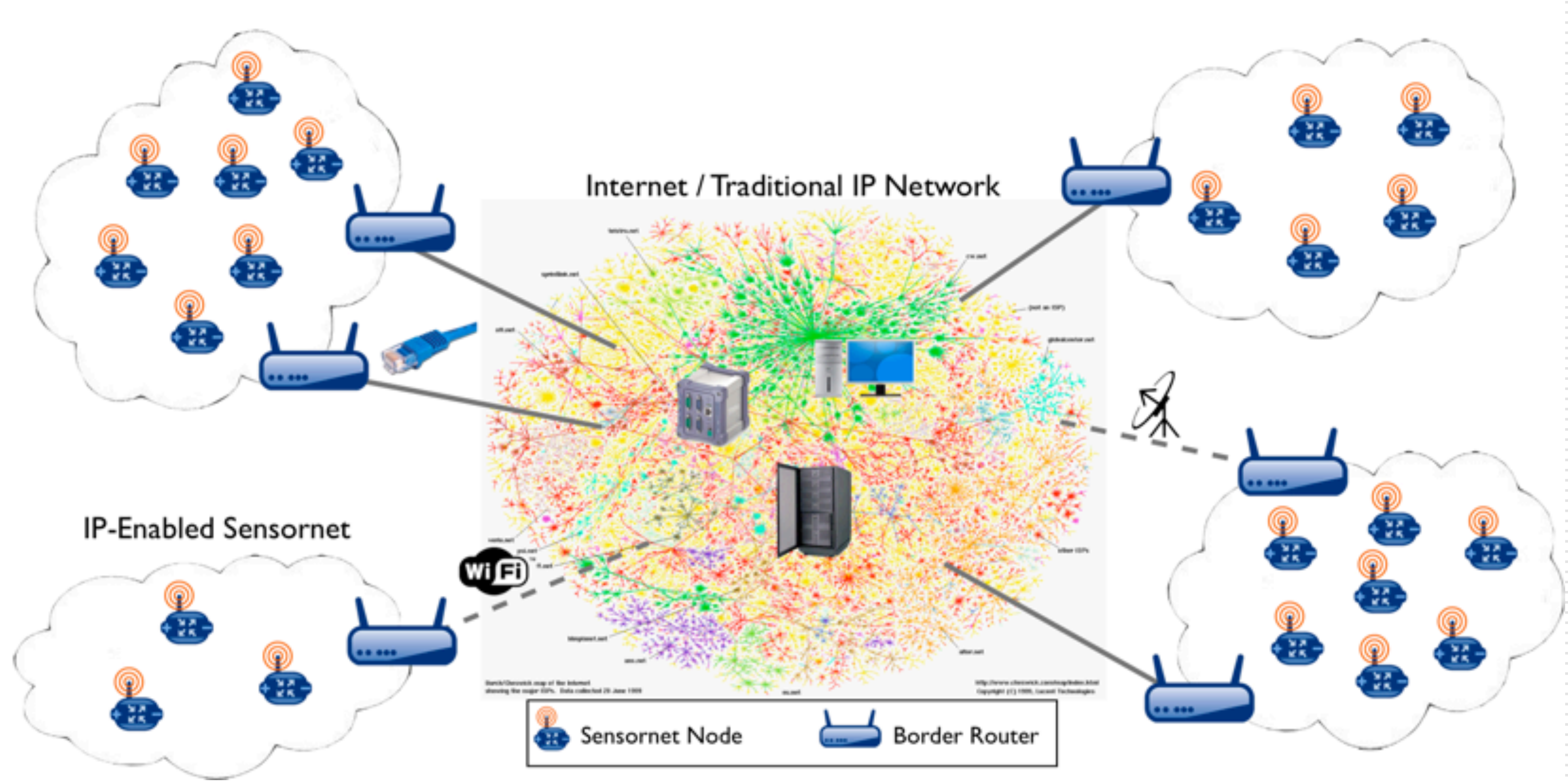
IP-Based 6LoWPAN

IPv6 over Low power WPAN

- IP for smart objects!
- Proposed in RFC4944 by IETF
- Transport IP packets using 802.15.4
- Low memory / processing requirement
- Uses IPv6 (IPv6 enabled)
  - 128-bit address space
  - Min. packet size is 1280 octets
  - Header size is 40 octet
  - Supports multicasting
- Several implementation including Berkeley (b6LoWPAN) using TinyOS
- Very useful if packet sizes are large and we need IP-enabled system

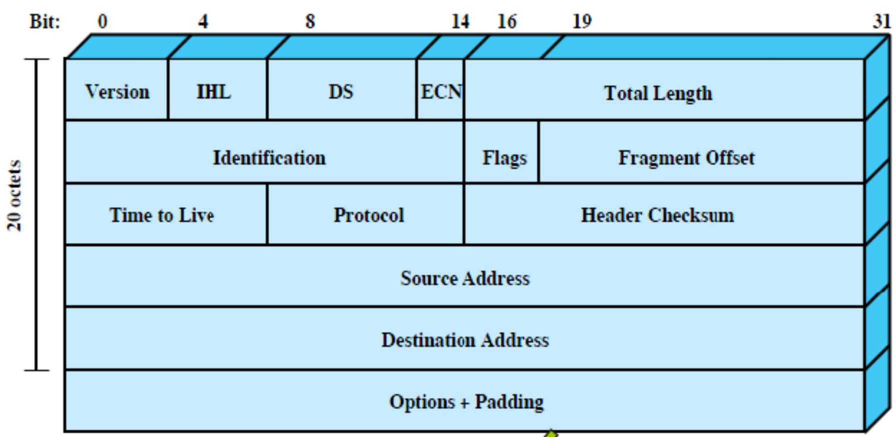
Watch the video: https://cisco.webex.com/cmp0306lb/webcomponents/jsp/docshow/closewindow.jsp

6LoWPAN
Extending the Internet Architecture



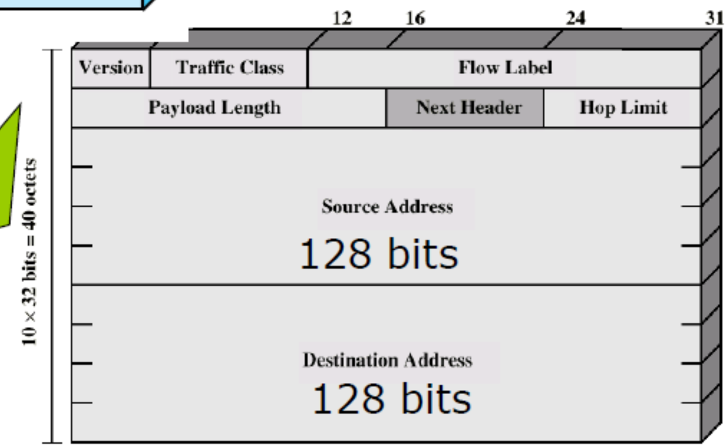
http://www.cs.berkeley.edu/~jwhui/6lowpan/IPSO-WP-3.pdf

A little about IPv4 vs. IPv6



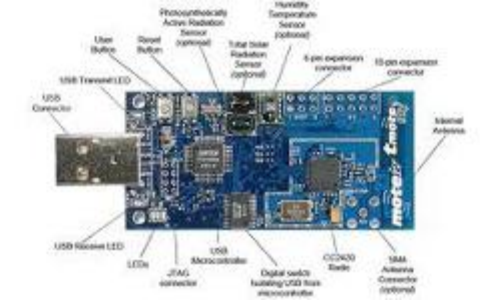
Note:
IPv5 used for Stream Protocol- IP-layer protocol that provides end-to-end guaranteed service across a network.

Features:
Extended address space
Improved option mechanism
Dynamic address assignment
Multicasting and anycasting
Flow routing



Presentation Slides: http://www.sonoma.edu/users/f/farahman/sonoma/courses/es465/lectures/es465_fall2010/ip_fragmentation.pdf

IPv6 over 802.15.4
How it is implemented



Telco Implementation

- Encapsulating IPv6 creates several issues
  - Standard IPv6 header is 40 bytes [RFC 2460] → Compression technique
  - Minimum Transmission Unit (MTU) of IP is 1280 bytes → requires almost TEN 802.15.4 frames! → Fragmentation
  - Establishing routing into and out of the WSN → may have different criteria (radio hops vs. IP hops)
  - Supporting multicasting in WSN → still under discussion
  - Neighbor discovery → how the routing should be handled in WSN
- General concerns
  - Security
  - Overhead: IP=40 bytes/ TCP=20/
  - IP addressing is too long for small networks!
  - WSN has many constraints
    - processors are typically 8/16-bit with several kB RAM/ROM, low speed 250 kbps
    - Power (limited memory size and processing power)
- Energy calculations and 6LoWPAN impact
  - This can impact routing / routing in WSN can be different from routing on WAN
- Allow IP routing over a mesh of 802.15.4 nodes
  - Localized internet of overlapping subnets

http://www1.cse.wustl.edu/~jain/cse567-08/ftp/7lowpan/index.html

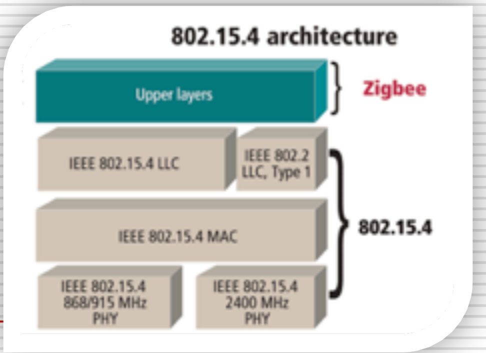
IPv6 over 802.15.4
How it is implemented

- Fragmentation
  - Adaptation layer is primarily in charge of fragmentation
  - IPv6 packets are fragmented into multiple link-level frames to accommodate the IPv6 minimum MTU requirement
- Header Compression
  - Reducing redundant or obvious bytes (version, class, address, etc.)
  - Compression can drastically reduce the power

The key is implementation of 6LoWPAN

http://www1.cse.wustl.edu/~jain/cse567-08/ftp/7lowpan/index.html

Zigbee



- Only defines communication between 15.4 nodes ("layer 2" in IP terms), not the rest of the network (other links, other nodes).
- Defines new upper layers, all the way to the application, similar to IRDA, USB, and Bluetooth, rather utilizing existing standards
- Specification in progress (some compatibility issues)
- Code size for full featured stack is 90KB vs. 30KB for 6LoWPAN
- Zigbee provides no end-to-end IP connection

http://www.cs.berkeley.edu/~jwhui/6lowpan/6LoWPAN-tutorial.pdf

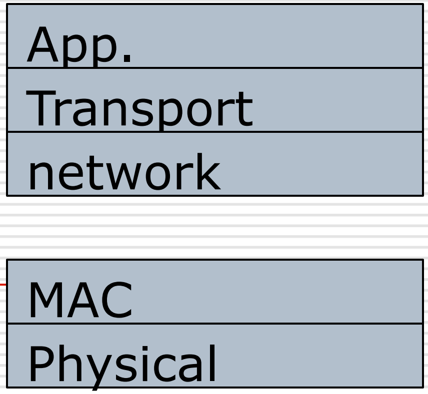
Review: 6LoWPAN vs. Zigbee

- Zigbee
  - Only defines communication between 15.4 nodes ("layer 2" in IP terms), not the rest of the network (other links, other nodes).
  - Defines new upper layers, all the way to the application, similar to IRDA, USB, and Bluetooth, rather utilizing existing standards
  - Specification in progress (some compatibility issues)
  - Code size for full featured stack is 90KB vs. 30KB for 6LoWPAN
- 6LoWPAN defines already established IP networking layers utilize the 15.4 link.
  - it enables 15.4 ←→15.4 and 15.4 ← →non-15.4 communication
  - It enables the use of a broad body of existing standards as well as higher level protocols, software, and tools.
  - It is a focused extension to the suite of IP technologies that enables the use of a new class of devices in a familiar manner
  - Lower overhead than Zigbee
    - ZigBee has a seven-byte header for communicating over a single hop and a 15-byte header when communicating over multiple hops, which is equal or larger to 6LoWPAN's compressed UDP/IPv6 header (lower overhead)
  - Zigbee provides no end-to-end IP connection

http://www.cs.berkeley.edu/~jwhui/6lowpan/6LoWPAN-tutorial.pdf

Wireless HART

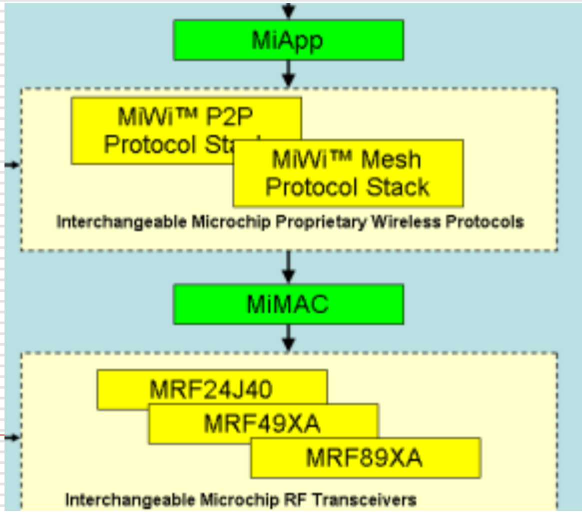
Highway Addressable Remote Transducer



- Industrial Forum (like Zigbee)
- FSK modulation
- Supports data rate up to 250kbps
- Wired/wireless (2.5GHz) physical layer
  - Supports 802.15.4
- Used in process controlling / monitoring / Master-Slave application
- Provides security
- High transmission power

MiWi

- Designed by Microchip (PIC)
- Supports proprietary MiWi Mesh and P2P
  - Short range wireless interfaces
- Uses IEEE 802.15.4
- Low data rate and short distance, low-power
  - Industrial monitoring
  - Home automations
  - Weather monitoring!!



http://ww1.microchip.com/downloads/en/AppNotes/01204a.pdf

Z-Wave

- Developed by Z-Wave alliance
- Operates at 900 MHz
- Does not Support 802.15.4
- Up to 40 kbps data rate
- FSK modulation / narrowband
- Supports MESH
  - Node addressing and cluster addressing
- Cheaper than Zigbee!

DASH 7

- Promoted by DASH7 Alliance
- Supported and funded by DoD in 2009
- A new wireless sensor networking technology using the ISO/IEC 18000-7 standard for active RFID
  - ISO/IEC 18000-7 is international standard that describes a series of diverse RFID technologies (radio interfaces, etc.)
- Operates at 433 MHz unlicensed spectrum, for applications such as
  - Item management
  - Tracking moving objects
  - Tag-to-tag communication
- Provides multi-year battery life, range of up to 2 km (potentially farther), low latency for
- Small protocol stack
- Supports sensors and security options
- Data transfer of up to 200 kbit/s
- Also supports IPv6

Video: http://www.dash7-alliance.org/why-dash7

DASH7 and Zigbee

Technology	Global standard used	Frequencies used	Globally available frequency(ies)?	Penetrates water	Penetrates concrete
DASH7	ISO/IEC 18000-7	433.92 MHz	Yes	Yes	Yes
ZigBee[2]	IEEE 802.15.4	2.4 GHz, 915 MHz, 868 MHz	2.4 GHz – yes; 915 MHz – no; 868 MHz – no	No	No

Technology	Range	Average power draw	Average latency	Device cost	Multi-hop capabilities	Sensor and Security support	Interference from 802.11n	Maximum bit rate
DASH7	1,000 m	30–60 µW	2 seconds worst case	$10+	Yes	Yes	No	200 kbit/s
ZigBee[2]	30–500 m	125–400 µW	varies from seconds to potentially minutes	$10+	Yes	Yes	Yes	250 kbit/s

Ultra-Low-Power Bluetooth (ULP)

- Originally called **Wibree**
- Short range
- Uses the same PHY layer (radio) as Bluetooth (2.5GHz ISM, unlicensed)
- No support for mesh
- Point-to-point communication
- Supports 40 channels with 2MHz channel spacing
- No QOS support
- Compatible with Bluetooth

Wireless Technology Comparison

Standard	Bandwidth	Power Consumption	Protocol Stack Size	Stronghold	Applications
Wi-Fi	Up to 54Mbps	400+mA TX, standby 20mA	100+KB	High data rate	Internet browsing, PC networking, file transfers
Bluetooth	1Mbps	40mA TX, standby 0.2mA	~100+KB	Interoperability, cable replacement	Wireless USB, handset, headset
ZigBee	250kbps	30mA TX, standby 3#&956;A	4"32KB	Long battery life, low cost	Remote control, battery-operated products, sensors

Critical Issues

- Power
- Operating Systems
- Hardware Characteristics

Energy Efficiency
Key to WSN

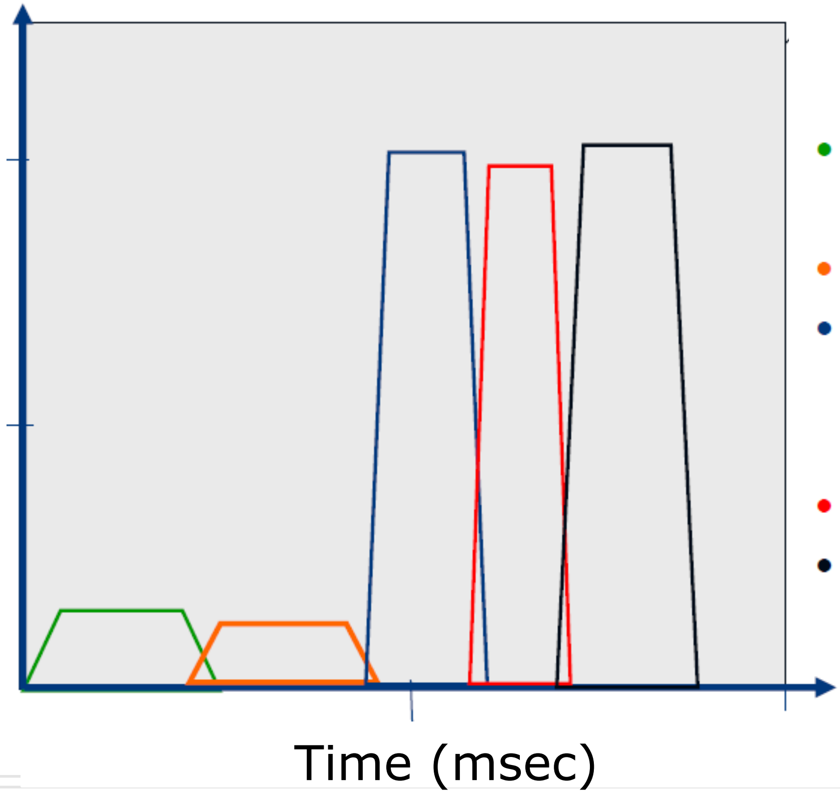
- Battery capacity typically rated in Amp-hours
  - Chemistry determines voltage (http://electronics.howstuffworks.com/battery4.htm)
  - AA Alkaline: ~2,000 mAh = 7,200,000 mAs (Milli-Amp Second)
  - D Alkaline: ~15,000 mAh = 54,000,000 mAs
- Unit of effort: mAs
  - multiply by voltage to get energy (joules)
- Lifetime
  - 1 year = 31,536,000 sec
  - Assuming the designed lifetime is a year, for AA Alkaline:
    - Average current = 228 uA-year (= 7,200,000/ 31,536,000)
  - With 72,000,000 packets TX or RX per year (~ 2 pkts /sec for a year) @ 100 uAs per TX or RX
    - → 72,000,000 pkt x 100 uAs/pkt = 7,200,000,000uAs = 7,200,000mAs = AA Alkaline: ~2,000 mAh (works fine!)

http://www.cs.berkeley.edu/~jwhui/6lowpan/6LoWPAN-tutorial.pdf

Node Power Profile

Sleep mode saves energy!

Various technologies are used to minimize TX/RX power and increase Sleep mode



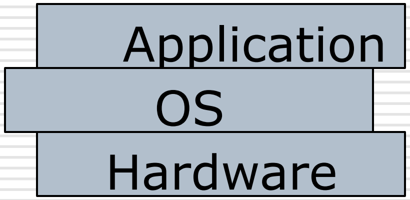
- Power up oscillator & radio
- Configure radio
- Clear Channel Assessment, Encrypt and Load TX buffer
- Transmit packet
- Switch to rcv mode, listen, receive ACK

Comparing Different OSes

- Different technologies and protocols in terms of supporting IPv6; Licenses, footprint, queue implementation, etc
  - TinyOS
  - Contiki
  - FreeRTOS
  - Mantis
  - …. and more

TinyOS

- TinyOS is an open-source event-driven operating system developed at UC Berkeley for very low power applications
- Designed for WSN – provides an specific approach to designing WSN
  - Also provides support for IPv6
  - Offers mesh network layers on top of 802.15.4
  - Open-source OS supported by TinyOS Alliance
  - The node is in IDLE mode most of the time!
- In WSN Sensor nodes may require large processing power to run the OS
  - OS is required to write particular application and manage resources
  - Large processing requirement needs large power
  - OS aims at providing low-power OS for sensor nodes
- Can be implemented on Zigbee application layer
  - Provides programming environment



- Uses nesC (network embedded C) programming language for developing applications

Typical HW supporting different OS

	Mica [6]	Telos [7]	SunSPOT [8]
Controller	AVR atmega88	TI MSP430	ARM 920T
Bus	8-bit	16-bit	32-bit
Memory	128k	10k	512k
Flash	512k	48k	4M
Radio Chip	variable	TI CC2420	TI CC2420
Sensors		humidity, temperature, luminosity	accelerometer, temperature, luminosity
Connectivity		16 ports	13 ports
Antenna	external	onboard	external

	Sensinode [9]	LiveNode [10]
Controller	TI 8051	ARM 7
Bus	8-bit	32-bit
Memory	8k	64k
Flash	128k	256k
Radio Chip	TI CC2420	Xbee Pro
Sensors	temp, luminosity	n.c.
Connectivity	21 ports	11 ports
Antenna	onboard	external

Telco Implementation:
http://www.cs.berkeley.edu/~culler/papers/spots05-telos.pdf

Paper: Comparisons of 6LoWPAN Implementations on Wireless Sensor Networks

Implementation of Open-Source 6LoWPAN Stack

How TinyOS is used!

- There are various implementations of 6LoWPAN using different operating systems and licensing agreements

Concept	Matus [19]	blip [20]	ηstack [9]	μIPv6 [21]
State	Unachiev	Compl.	Compl.	In dev.
Support OS	TinyOS AM	TinyOS	FreeRTOS	Contiki
License		LGPL	GPL	BSD
AM	X			
UDP	X	X	X	X
TCP				X
ICMP	X	X	X	X
Mesh-Rout.		X	X	
Frag.	X	X	X	X
Compress.	X	X	X	X
Broad. BC0	X	X	X	X
Neigh. Disc.		X		X
Radio chip	CC2420	CC2430	CC2430	CC2430
Unix tools	X	X	X	X
Monolithic	X	X	X	X
Start	2007	2000-08	2006	2008

UDP (User Datagram Protocol),
TCP (Transmission Control Protocol),
AM (Active Message)
ICMP (Internet Control Message Protocol)

BSD=Berkeley SW Distribution
GPL= The GNU General Public License is a free, copyleft (right to change) license for software and other kinds of works.
LGPL= GNU Lesser General Public License.

Licensing: http://www.gnu.org/copyleft/lesser.html
Paper: Comparisons of 6LoWPAN Implementations on Wireless Sensor Networks

Zigbee…..

- We discuss it later!
- Use these links:

http://www.media.mit.edu/resenv/classes/MAS961/readings/embeddedmag/zigbee.html

-

References (click on the link)

1. Very good and brief reference on development of cellular networks
   http://www.itu.int/osg/spu/ni/3G/technology/index.html
2. Radio transmitters and receivers
   http://sci-toys.com/scitoys/scitoys/radio/homemade_radio.html
3. Spark gap history
   http://www.vistech.net/users/w1fji/spark.html
4. Telecommunications Growth in Africa through the Multipurpose Community Telecenter
   www.telecentres.isoc.am/references/info/tc_africa.doc
5. A partial list of standard committees and organizations
   http://www.openmobilealliance.org/collaborating/index.html
6. Conversion tables:
   - http://www.hoptechno.com/nightcrew/sante7000/convert.cfm

Interesting Ideas

- Mobile Phone As Home Computer http://philip.greenspun.com/business/mobile-phone-as-home-computer
- Wearable Computers http://www.media.mit.edu/wearables/

Some Cools Stuff….

- Hacking your iPhone
  - Book: http://oreilly.com/catalog/9780596516642
  - Hack that phone (follow a flow chart!) http://www.hackthatphone.com/3x/3GS_flowchart.html
- Jailbreaking your iPhone
  - http://www.youtube.com/watch?v=V_MdkNzS1Uc
- Nokia 1260 (ATT, CDMA Phone – with no SIM card)
  - Position to the closes tower
  - http://www.youtube.com/watch?v=6wpDoM48DDk&feature=related
- Use Nokia 6230i Used as Bluetooth Mouse via camera
  - http://www.youtube.com/watch?v=yT1h_ITR0G0&feature=related
- Use a cell phone as a webcam using bluetooth
  - http://www.youtube.com/watch?v=COTHdrBv15I&NR=1
- Control your Roomba using your cell phone
  - http://hackingroomba.com/projects/build-a-roomba-bluetooth-adapter/
  - Video: http://www.youtube.com/watch?v=01vXftgGVsM