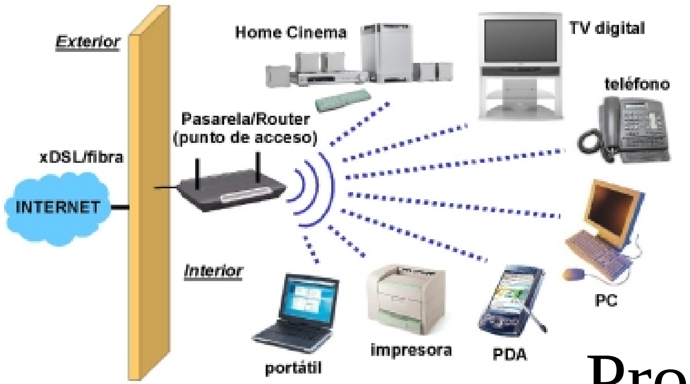
Wireless Personal Area Networks (WPANs)



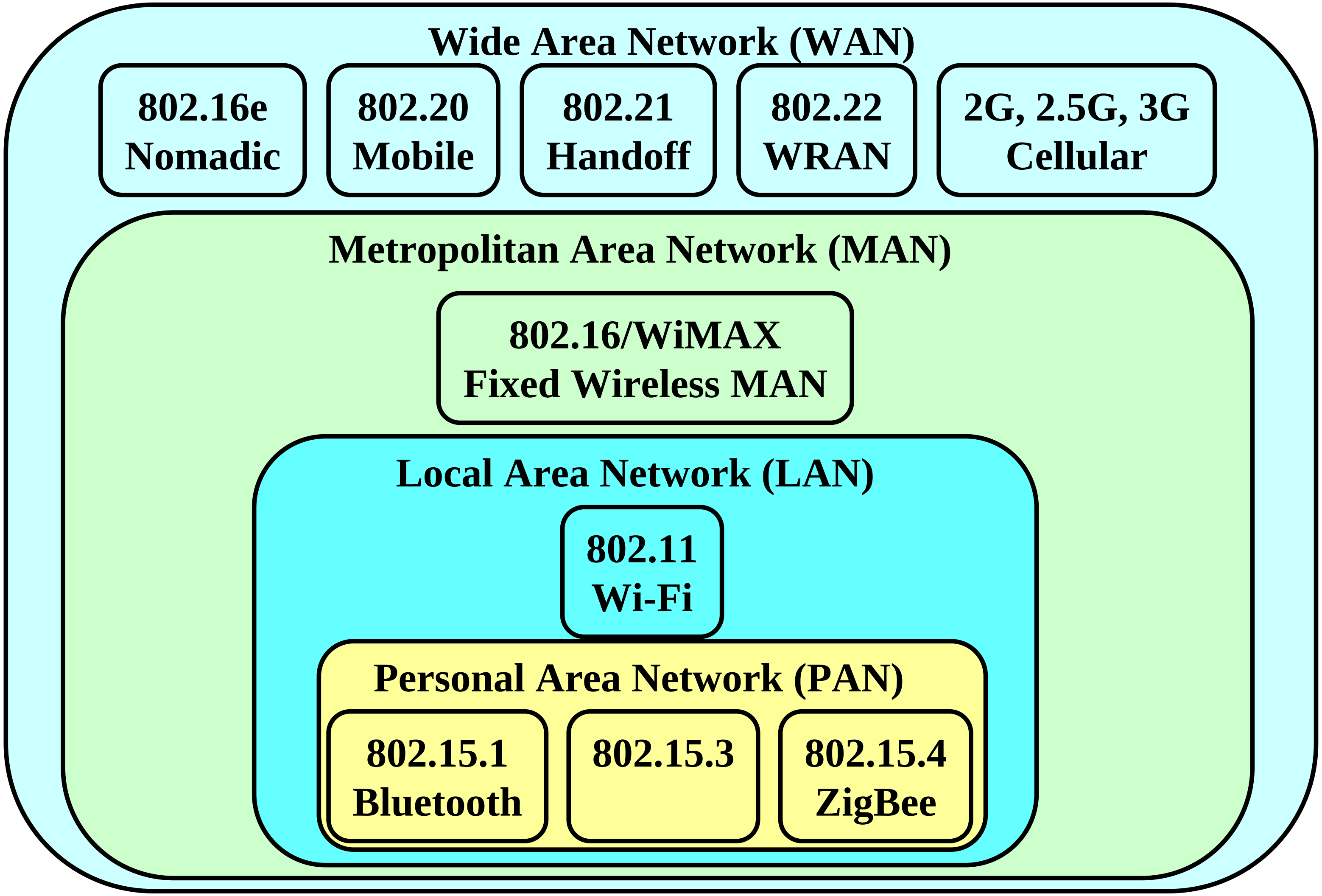
Raj Jain
Professor of CSE
Washington University in Saint Louis
Saint Louis, MO 63130
Jain@cse.wustl.edu

These slides are available on-line at:

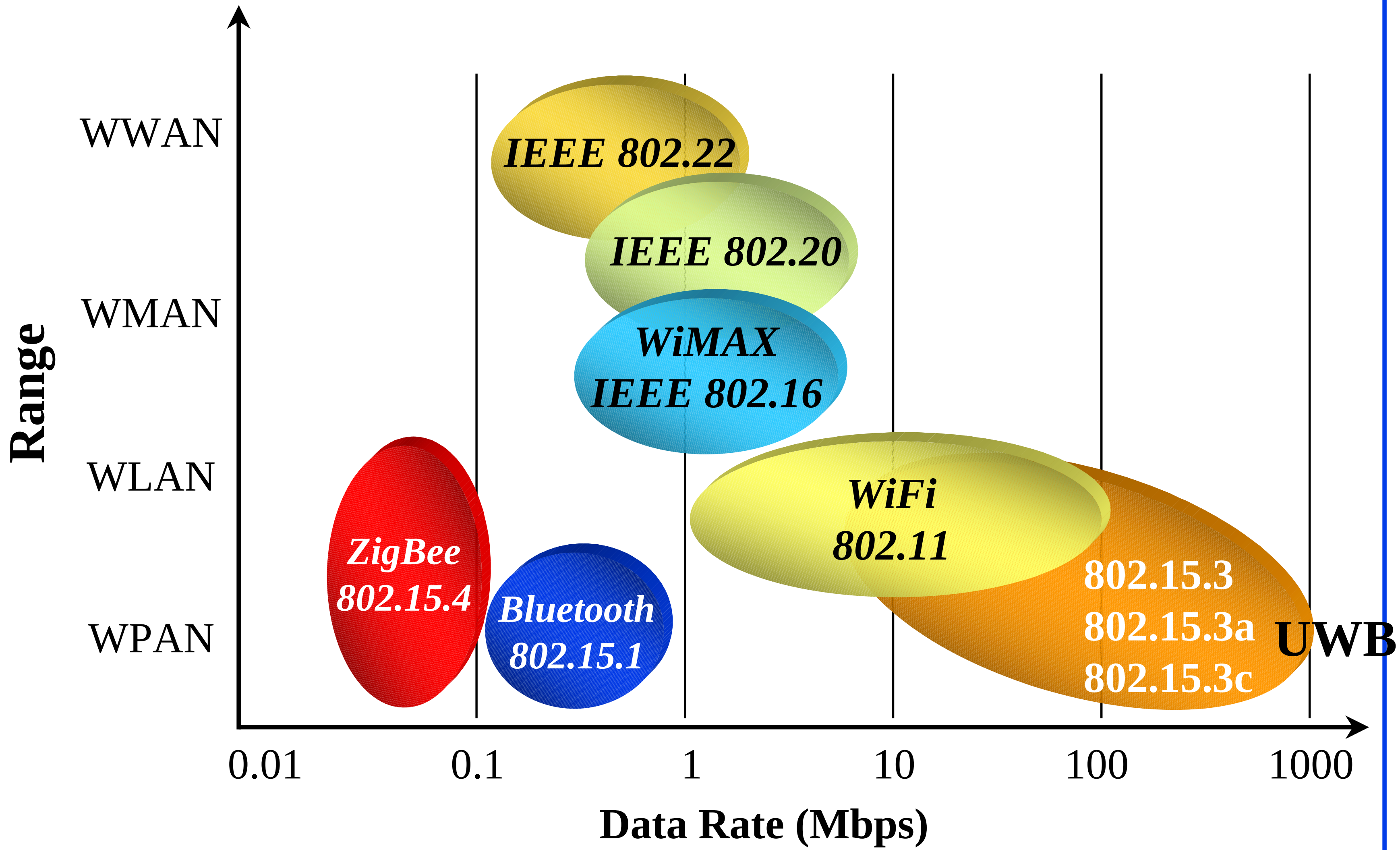
http://www.cse.wustl.edu/~jain/cse574-06/

- Wireless Standards Overview
- Bluetooth
- Ultra-Wideband
- ZigBee

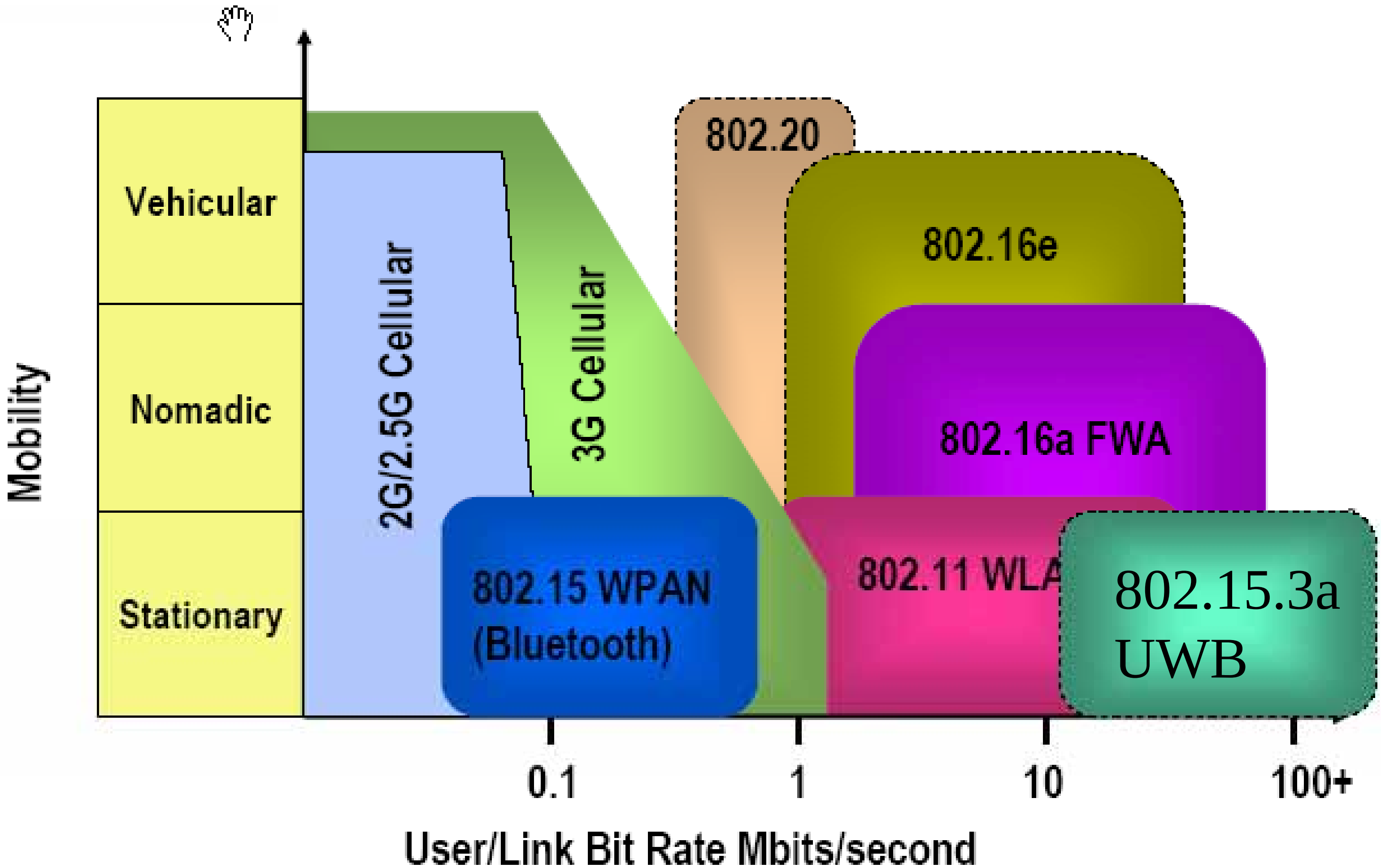
Wireless Standards



Distance vs. Data Rate



Mobility vs. Data Rate



Bluetooth Products

Headsets Audio Game Controller Keyboard GPS

- Printers, faxes, digital cameras…
- 720 kbps to 10m
- Competes with infrared, which has a range of 1m, requires line of sight and has a low data rate

Bluetooth

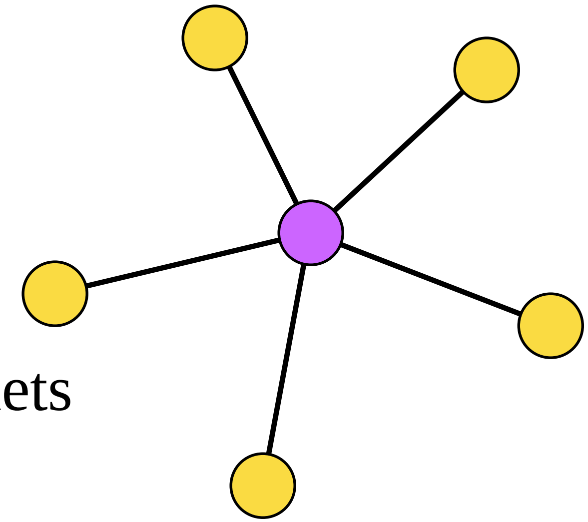
- Started with Ericsson's Bluetooth Project in 1994
- Named after Danish king Herald Blatand (AD 940-981) who was fond of blueberries
- Radio-frequency communication between cell phones over short distances
- Intel, IBM, Nokia, Toshiba, and Ericsson formed Bluetooth SIG in May 1998
- Version 1.0A of the specification came out in late 1999.
- IEEE 802.15.1 approved in early 2002 is based on Bluetooth
- Key Features:
  - Lower Power: 10 μA in standby, 50 mA while transmitting
  - Cheap: $5 per device
  - Small: 9 mm^2 single chips

Bluetooth: Details

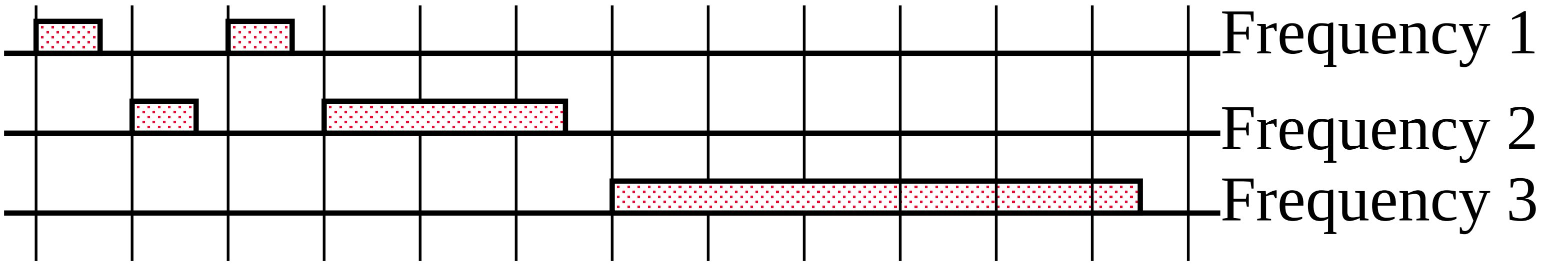
- **Frequency Range:** 2402 - 2480 MHz (total 79 MHz band) 23 MHz in some countries, e.g., Spain
- **Data Rate:**1 Mbps (Nominal) 720 kbps (User)
- **Channel Bandwidth:**1 MHz
- **Range:** Up to 10 m can be extended further
- **RF hopping:** 1600 times/s ⇒ 625 μs/hop
- **Security:** Challenge/Response Authentication. 128b Encryption
- **TX Output Power:**
  - Class 1: 20 dBm Max. (0.1W) – 100m
  - Class 2: 4 dBm (2.5 mW)
  - **Class 3**: 0 dBm (1mW) – 10m
- **Ref:** http://www.bluetooth.com/ http://www.bluetooth.org/ http://grouper.ieee.org/groups/802/15/index.html

Piconet

- Piconet is formed by a master and many slaves
  - Up to 7 active slaves.
    Slaves can only transmit when requested by master
  - Up to 255 Parked slaves
- Active slaves are polled by master for transmission
- Each station gets a 8-bit parked address
  $\Rightarrow$ 255 parked slaves/piconet
- The parked station can join in 2ms.
- Other stations can join in more time.
- A device can participate in multiple piconets
  $\Rightarrow$ complex schedule



Frequency Hopping Sequences



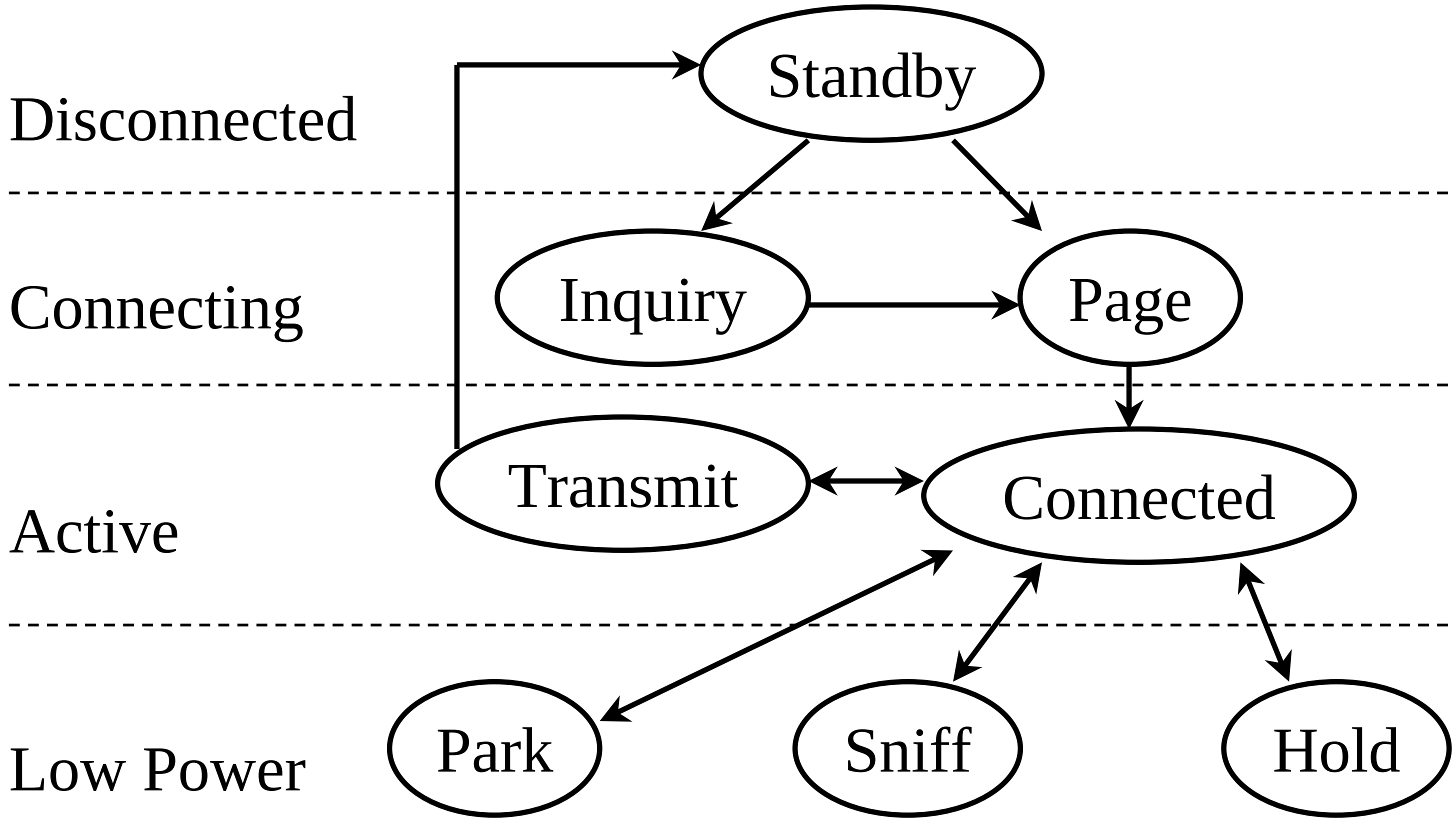
- 625 μs slots
- Time-division duplex (TDD)
  ⇒ Downstream and upstream alternate
- Master starts in even numbered slots only.
- Slaves start in odd numbered slots only
- *lsb* of the clock indicates even or odd
- Slaves can transmit in one slot right after receiving a packet from master
- Packets = 1 slot, 3 slot, or 5 slots long
- The frequency hop is skipped during a packet.

Bluetooth Packet Format

Access Code	Baseband/Link Control Header	Data Payload
72b	54b	0-2745b

- Packets can be up to five slots long. 2745 bits.
- Access codes:
  - Channel access code identifies the piconet
  - Device access code for paging requests and response
  - Inquiry access code to discover units
- Header: member address (3b), type code (4b), flow control, ack/nack (1b), sequence number, and header error check (8b) 8b Header is encoded using 1/3 rate FEC resulting in 54b
- Synchronous traffic has periodic reserved slots.
- Other slots can be allocated for asynchronous traffic

Bluetooth Operational States



Bluetooth Operational States (Cont)

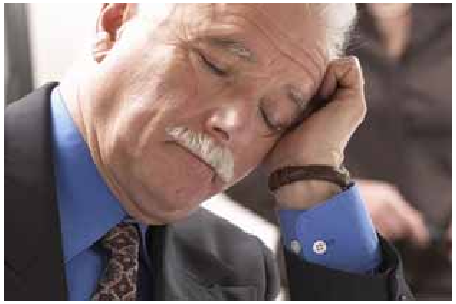
- **Standby**: Initial state
- **Inquiry**: Master sends an inquiry packet. Slaves scan for inquiries and respond with their address and clock after a random delay (CSMA/CA)
- **Page**: Master in page state invites devices to join the piconet. Page message is sent in 3 consecutive slots (3 frequencies). Slave enters page response state and sends page response including its device access code.
- Master informs slave about its clock and address so that slave can participate in piconet. Slave computes the clock offset.
- **Connected**: A short 3-bit logical address is assigned
- **Transmit**:

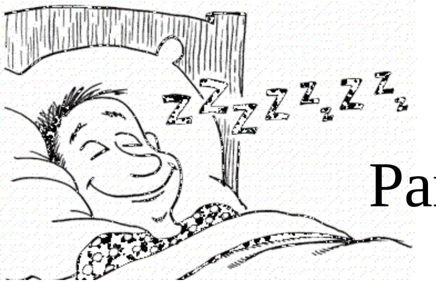
Energy Management in Bluetooth

Three inactive states:

- **Hold**: No ACL. SCO continues. Node can do something else: scan, page, inquire
- **Sniff**: Low-power mode. Slave listens only after fixed sniff intervals.
- **Park**: Very Low-power mode. Gives up its 3-bit active member address and gets an 8-bit parked member address.
- Packets for parked stations are broadcast to 3-bit zero address.

Sniff

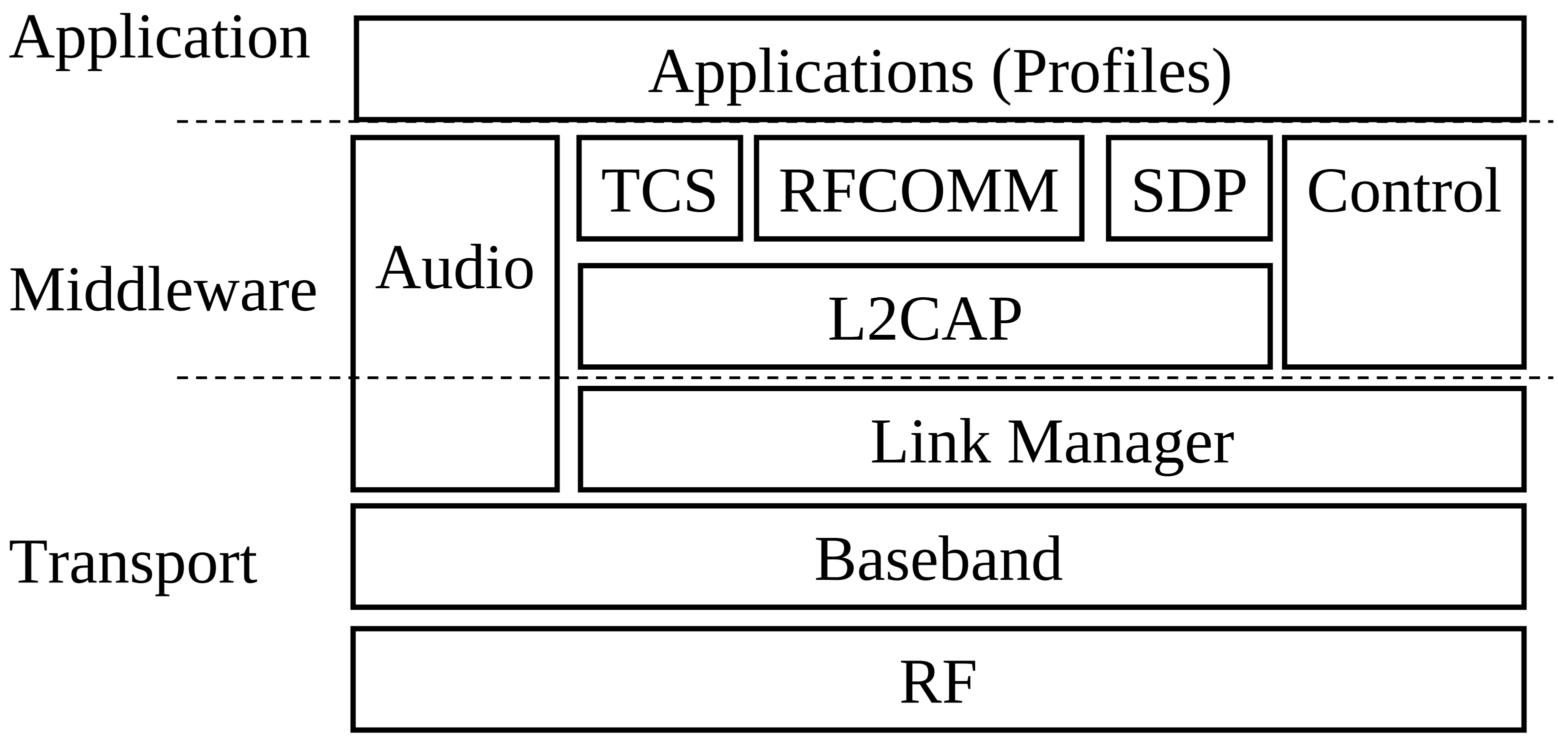




Park

Power per MB

Bluetooth Protocol Stack



- RF = Frequency hopping GFSK modulation
- Baseband: Frequency hop selection, connection, MAC

Baseband Layer

- Each device has a 48-bit IEEE MAC address
- 3 parts:
  - Lower address part (LAP) – 24 bits
  - Upper address part (UAP) – 8 bits
  - Non-significant address part (NAP) - 16 bits
- UAP+NAP = Organizationally Unique Identifier (OUI) from IEEE
- LAP is used in identifying the piconet and other operations
- Clock runs at 3200 cycles/sec or 312.5 μs (twice the hop rate)

Upper Address Part	Non-sig. Address Part	Lower Address Part
8b	16b	24b

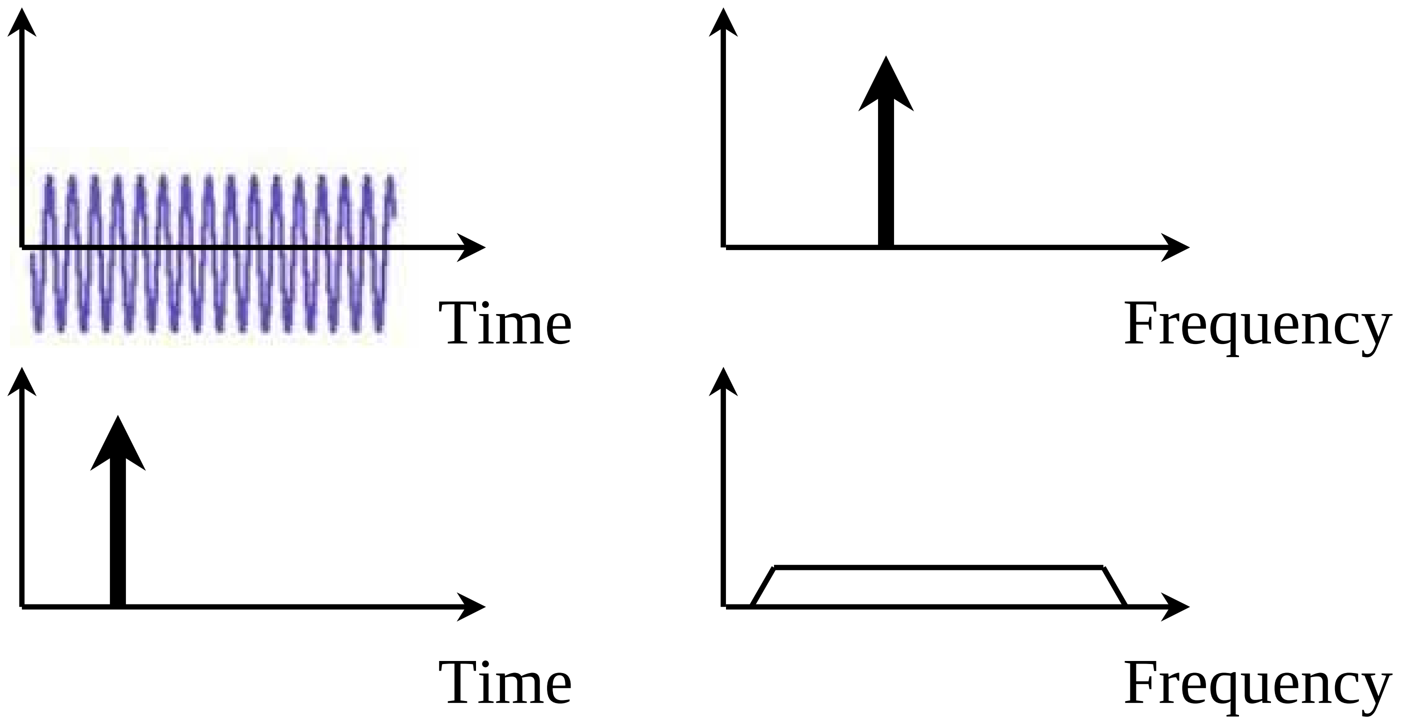
Bluetooth Protocol Stack (Cont)

- Logical Link Control and Adaptation Protocol (L2CAP)
  - Protocol multiplexing
  - Segmentation and reassembly
  - Controls peak bandwidth, latency, and delay variation
- Host Controller Interface
- RFCOMM Layer:
  - Presents a virtual serial port
  - Sets up a connection to another RFCOMM
- Service Discovery Protocol (SDP): Each device has one SDP which acts as a server and client for service discovery messages
- IrDA Interoperability protocols: Allow existing IrDA applications to work w/o changes

Bluetooth Protocol Stack (Cont)

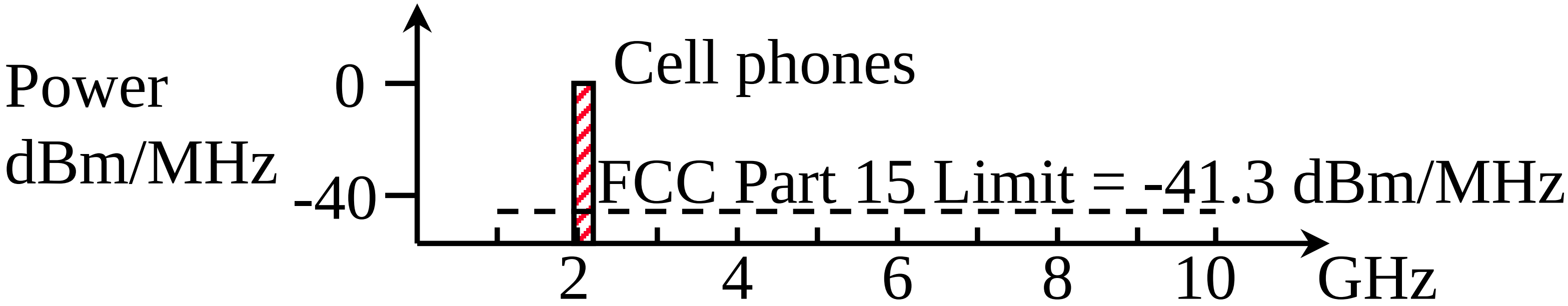
- IrDA object Exchange (IrOBEX) and Infrared Mobile Communication (IrMC) for synchronization
- Audio is carried over 64 kbps over SCO links over baseband
- Telephony control specification binary (TCS-BIN) implements call control including group management (multiple extensions, call forwarding, and group calls)
- Application Profiles: Set of algorithms, options, and parameters. Standard profiles: Headset, Cordless telephony, Intercom, LAN, Fax, Serial line (RS232 and USB).

Ultra-Wideband



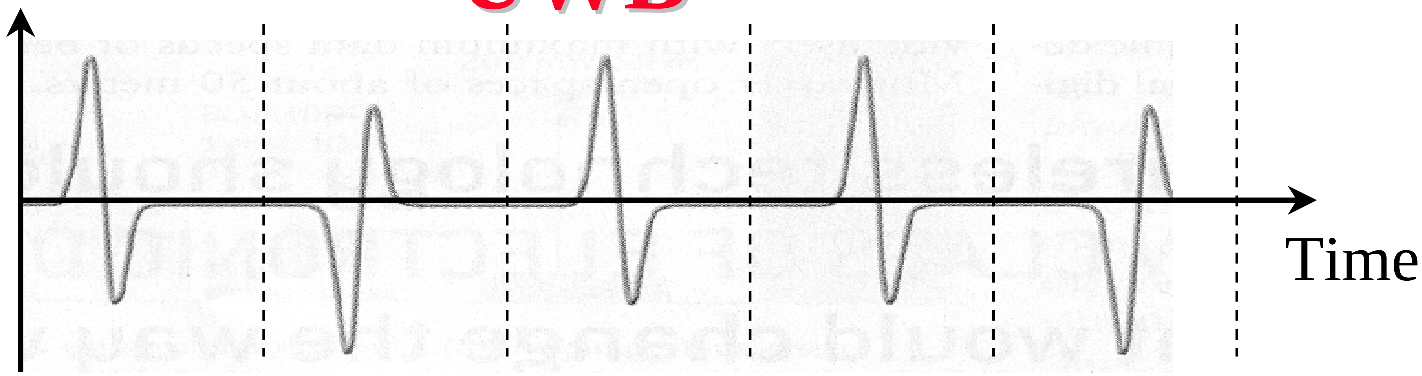
- An impulse in time domain results in a ultra wide spectrum in frequency domain and essentially looks like a white noise to other devices

Ultra-Wideband (UWB)



- FCC rules restrict the maximum noise generated by a wireless equipment (0 dBm = 1mW, -40 dBm = 0.1 μW)
- It is possible to generate very short (sub-nano sec) pulses that have spectrum below the allowed noise level
  ⇒ Possible to get Gbps using 10 GHz spectrum
- FCC approved UWB operation in 2002
- UWB will be used for high-speed over short distances
  ⇒ Wireless USB
- UWB can see through trees and underground (radar)
  ⇒ collision avoidance sensors, through-wall motion detection
- Position tracking: cm accuracies. Track high-value assets

UWB



- Sub-nanosecond impulses are sent many million times per second
- Became feasible with high-speed switching semiconductor devices
- Pulse width = 25 to 400 ps
- Impulses may be position, amplitude, or polarity modulated
- 0.25 ns Impulse $\Rightarrow$ 4 B pulses/sec $\Rightarrow$ 100's Mbps
- Two leading proposals: DS-UWB and MB-OFDM

Advantages of UWB

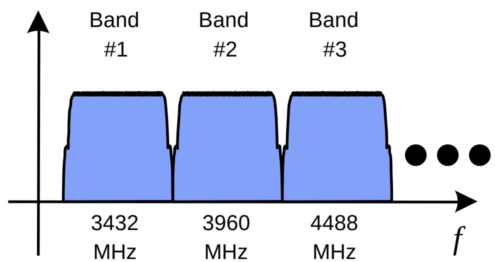
- Very low energy consumption: Good Watts/Mbps
- Line of sight not required. Passes through walls.
- Sub-centimeter resolution allows precise motion detection
- Pulse width much smaller than path delay
  $\Rightarrow$ Easy to resolve multipath
  $\Rightarrow$ Can use multipath to advantage
- Difficult to intercept (interfere)
- All digital logic $\Rightarrow$ Low cost chips
- Small size: 4.5 mm2 in 90 nm process for high data rate designs

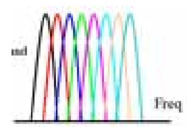
Direct sequence (DS-UWB)

- Championed by Motorola/XtremeSpectrum
- Uses CDMA with multiple chips per bit
- Chips are encoded using pulse
- 2 frequency bands: 3.1-4.85GHz, 6.2-9.7GHz
- Spectrum shaping filter can be used to meet differing spectrum requirements worldwide

Multi-Band OFDM

- From MB-OFDM Alliance (MBOA):
- Originally proposed by TI. Now many companies
- Divide the 3.1-10.6 GHz spectrum in 14x528 MHz bands (FCC requires min 500 MHz use for UWB)



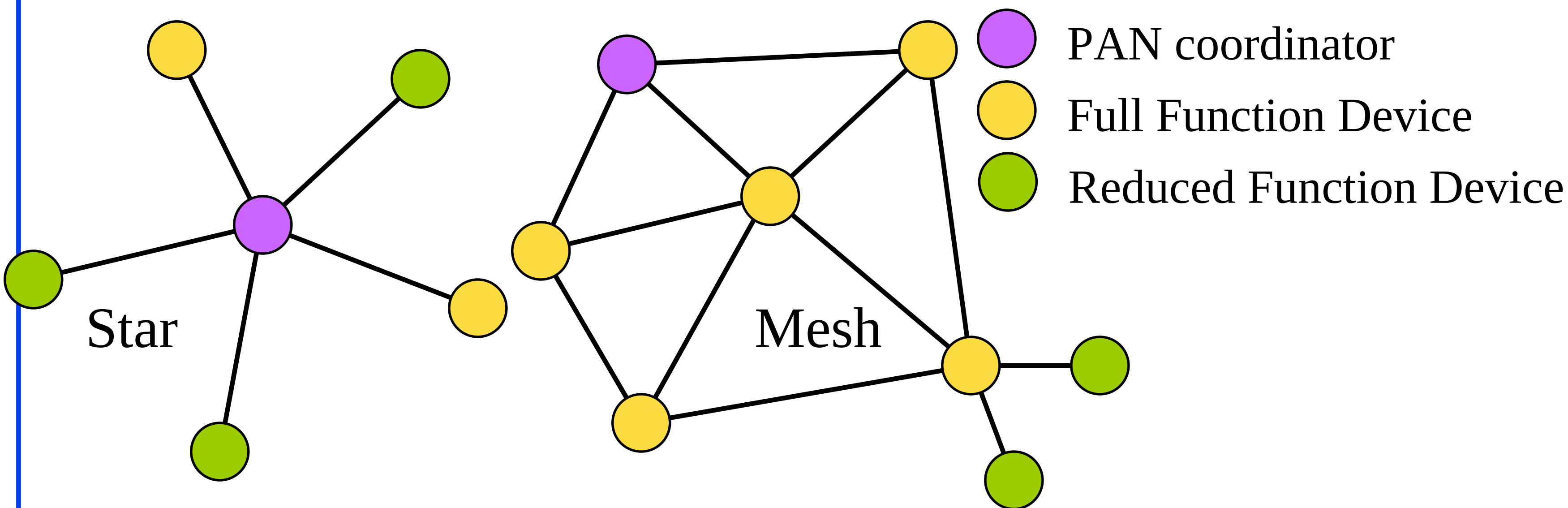


- Simple devices need to support 3 lowest bands
- Spectrum shaping flexibility for international use
   Move off the band if interference
- Use OFDM with 128 subcarriers in a band:
  Similar in nature to 802.11a/g
- Disable a few sub-carriers if required to meet local laws

ZigBee

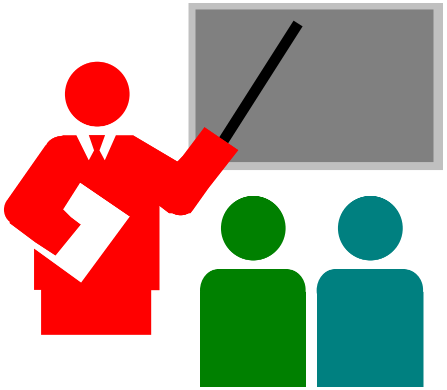
- Ultra-low power, low-data rate, industrial monitoring and control applications requiring small amounts of data, turned off most of the time (<1% duty cycle),
  e.g., wireless light switches, meter reading, patient monitoring
- IEEE 802.15.4
- Less Complex. 32kB protocol stack vs 250kB for Bluetooth
- Range: 1 to 100 m, up to 65000 nodes.
- Tri-Band:
  - 16 Channels at 250 kbps in 2.4GHz ISM
  - 10 Channels at 40 kb/s in 915 MHz ISM band
  - One Channel at 20 kb/s in European 868 MHz band
- Ref: ZigBee Alliance, http://www.ZigBee.org

Network Topology



- Two types of devices:
  - Full Function Devices (FFD) for network routing and link coordination
  - Reduced Function Devices (RFD): Simple send/receive devices

Summary



- Wireless personal area networks are used for 1-10m communications
- Medium rate: Bluetooth – 720 kbps, uses Frequency hopping, has application specific profiles
- High rate: UWB – 480 Mbps, 528 MHz bands, OFDM or DS-UWB
- Low rate: ZigBee – 20 kbps, longer distance, includes routing

Reading Assignment

- Read Sections 2.1, 2.2, 2.5-2.7 of Murthy and Manoj.
- Try problems 24 thru 30.

Homework 4

- Submit answer to the following Problem:
  Assume that in one slot in Bluetooth 256 bits of payload could be transmitted. How many slots are needed if the payload size is (a) 512 bits, (b) 728 bits, and (c) 1024 bits. Assume that the non-payload portions do not change.