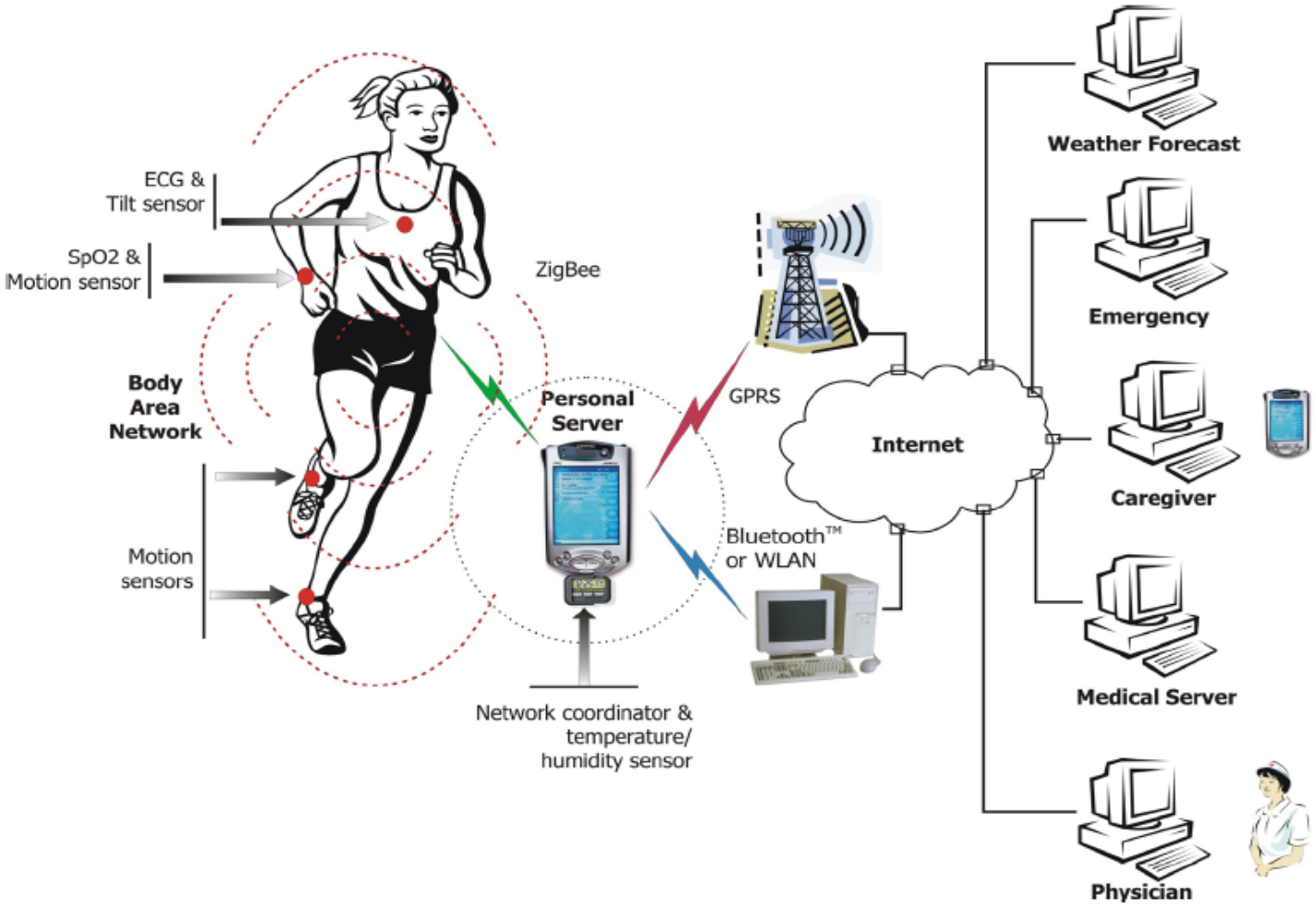
Selected Topics Communications and Mobile Computing (Smart Health)

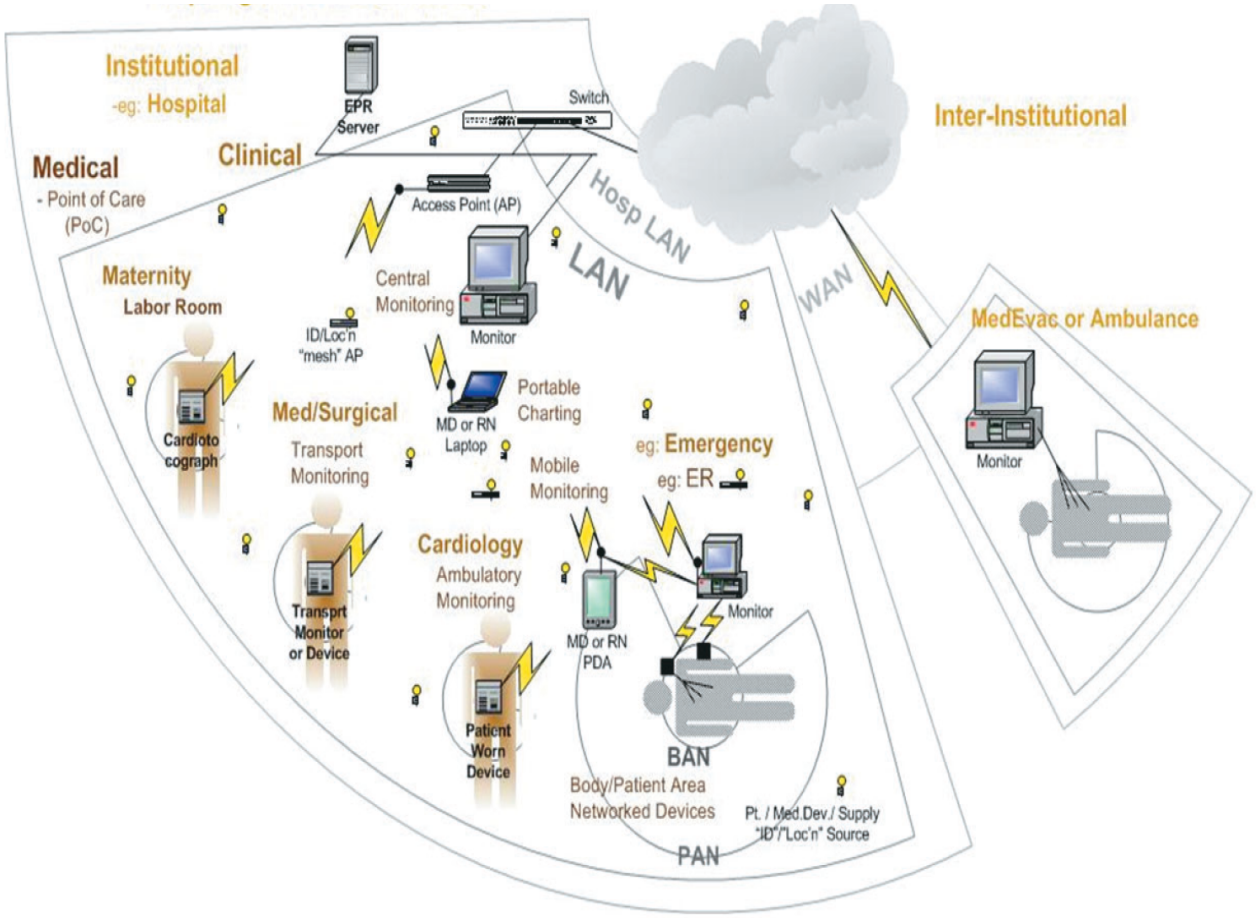
TU Graz

University of Notre Dame

Wireless Body Area Network



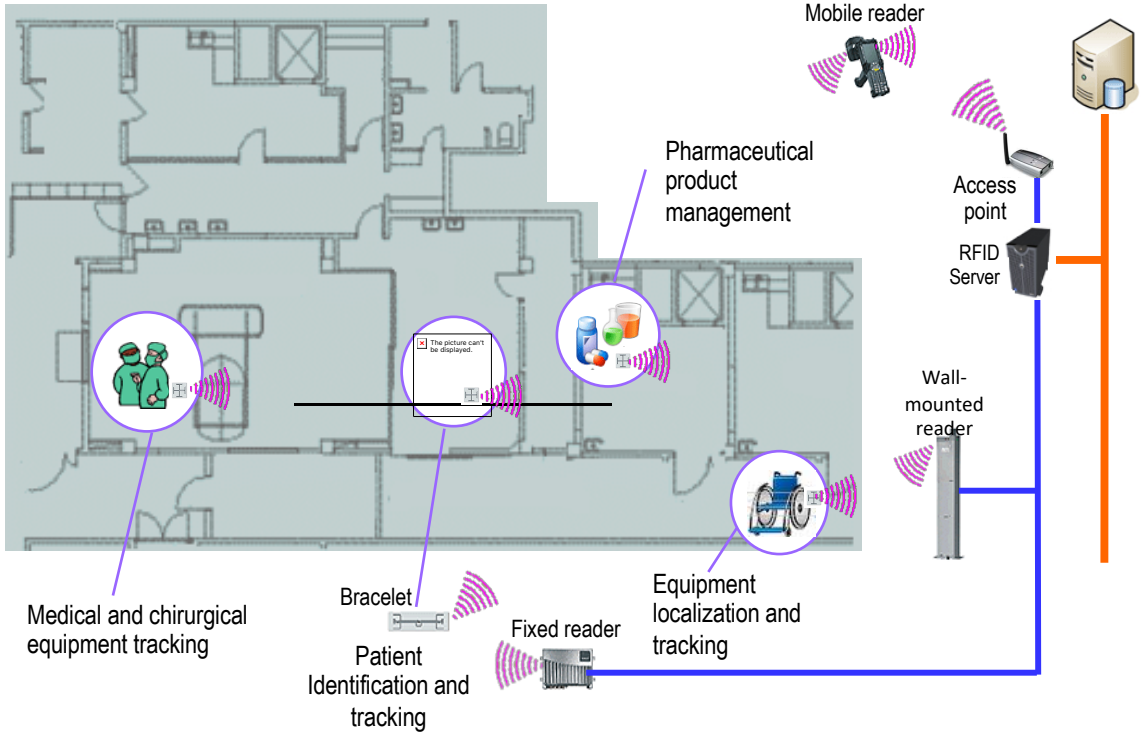
Wireless Networks in Health Care



- Each day more and more equipment is going "wireless" from pulse-oximeters to more complex patient vital signs monitors and ventilators
- Environments must scale from a few clients to 100s on a single subnet
- External factors such as nearby TV and radio stations can affect overall performance
- Interoperability profiles and standards are required to ensure plug-and-play operation in heterogeneous environments

Radio Frequency Identification (RFID)

- Facilitates management of assets (wheel chairs, scanners, ambulatory equipment)
- Improves patient localization and helps caregivers to provide services without delays
- Enhances process of drug administration (identification, distribution, localization, returns and disposal)
- Facilitates automatic data capture and the follow-up of blood and biological samples



Computer Network Terminology

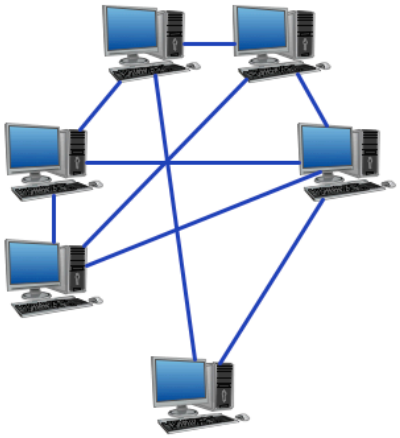
- **Network:** group of computers and associated devices that are connected by communication facilities
- **Wide Area Network (WAN)**: world-wide (Internet)
- **Metropolitan Area Network (MAN):** city-scale
- **Local Area Network (LAN):** laboratory/office-scale (Ethernet)
  - **WLAN:** wireless LAN (Wi-Fi)
  - **WPAN:** wireless personal area network (Bluetooth)
  - **WBAN:** wireless body area network

Networking Basics

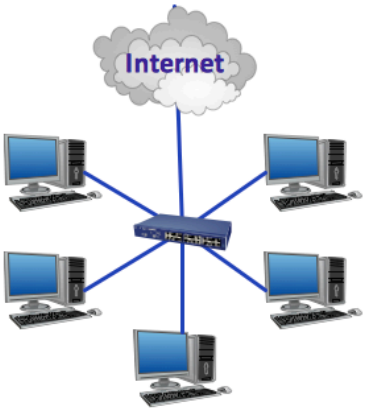
- Standards:
  - IEEE (Institute of Electrical and Electronics Engineers): Project 802
  - Three dominant standards:
    - 802.3 (Ethernet)
    - 802.5 (Token Ring)
    - 802.11 (Wireless)
  - Ethernet:
    - Most popular LAN technology, uses bus architecture
    - Easy to install, inexpensive
    - Data is broken into packets

Network Topologies

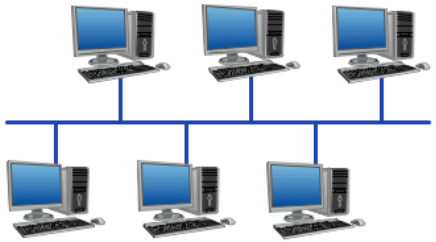
Fully Connected Network Topology



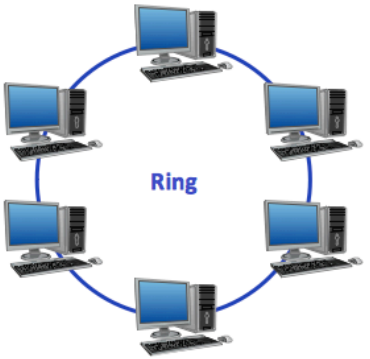
Mesh Network Topology



Star Network Topology



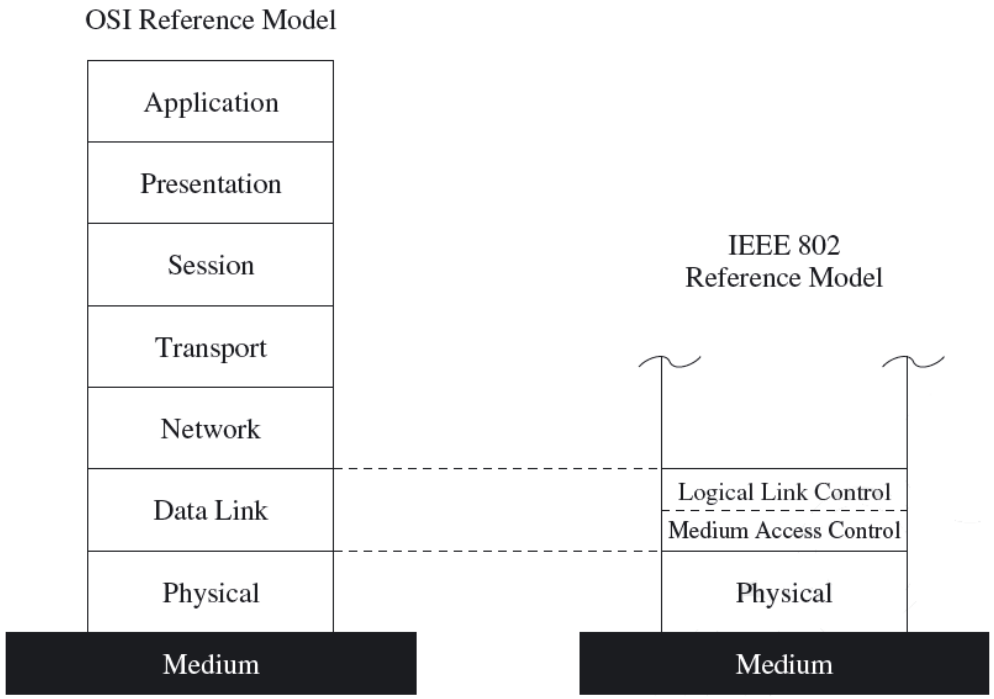
Common Bus Topology



Ring Network Topology

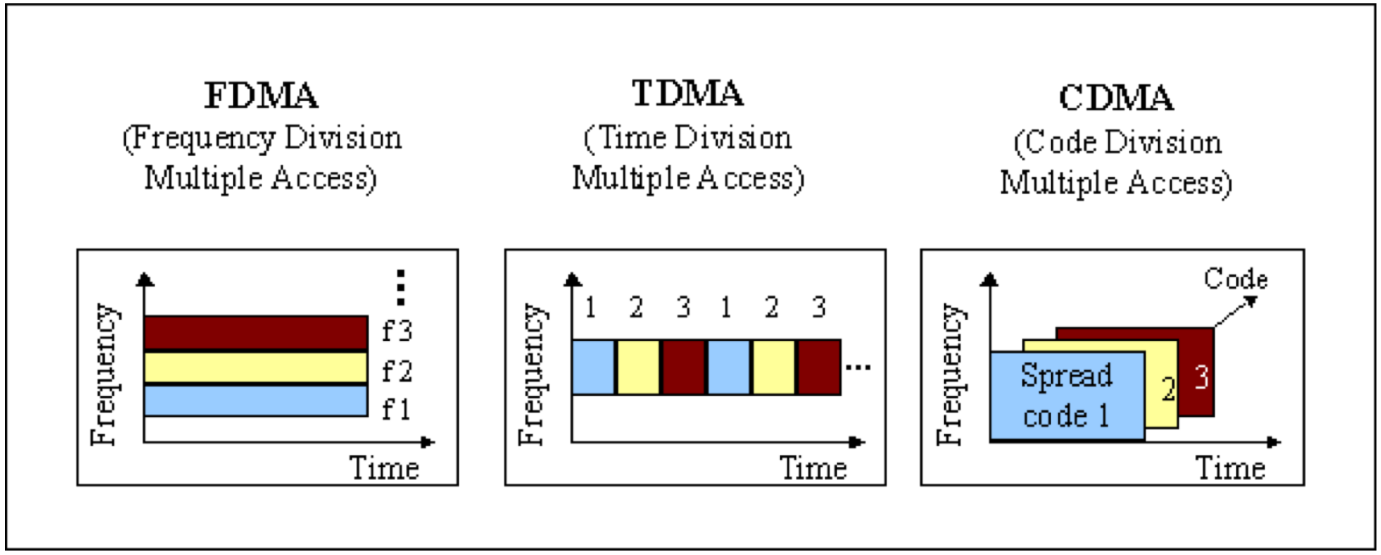
OSI Reference Model

- Responsibilities of **Data Link** layer include:
  - decide when a node accesses a shared medium
  - resolve any potential conflicts between competing nodes
  - correct communication errors occurring at the physical layer
  - perform other activities such as framing, addressing, and flow control



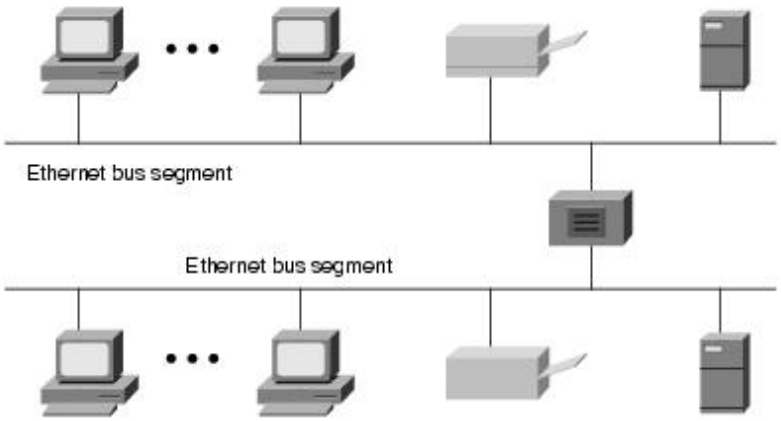
Data Link Layer (Layer 2)

- **Defines when/how medium will be accessed for transmission**
- Units typically called “frames”; error detection/correction; divided into sublayers, including: **MAC = Medium Access Control** (MAC address 6f:00:2b:23:1f:32)
- Cell phone example:



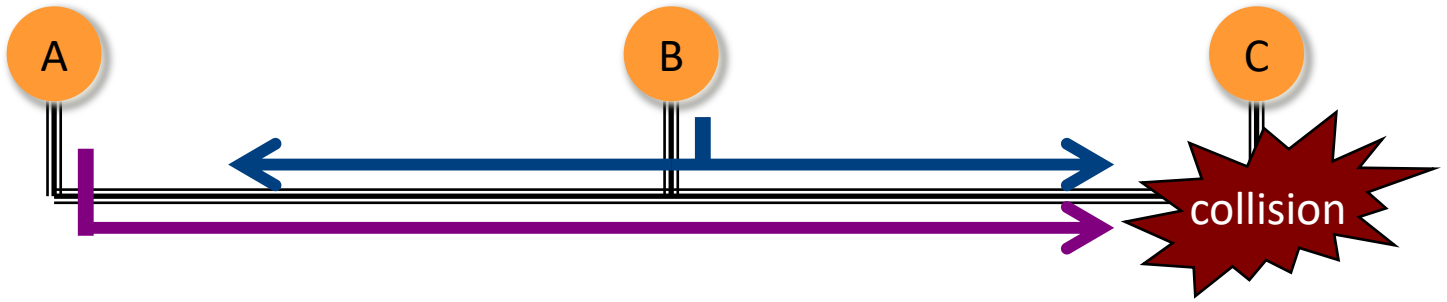
Example: Ethernet (802.3)

- Most popular LAN technology, uses bus architecture
- Easy to install, inexpensive
- Data is broken into **packets**

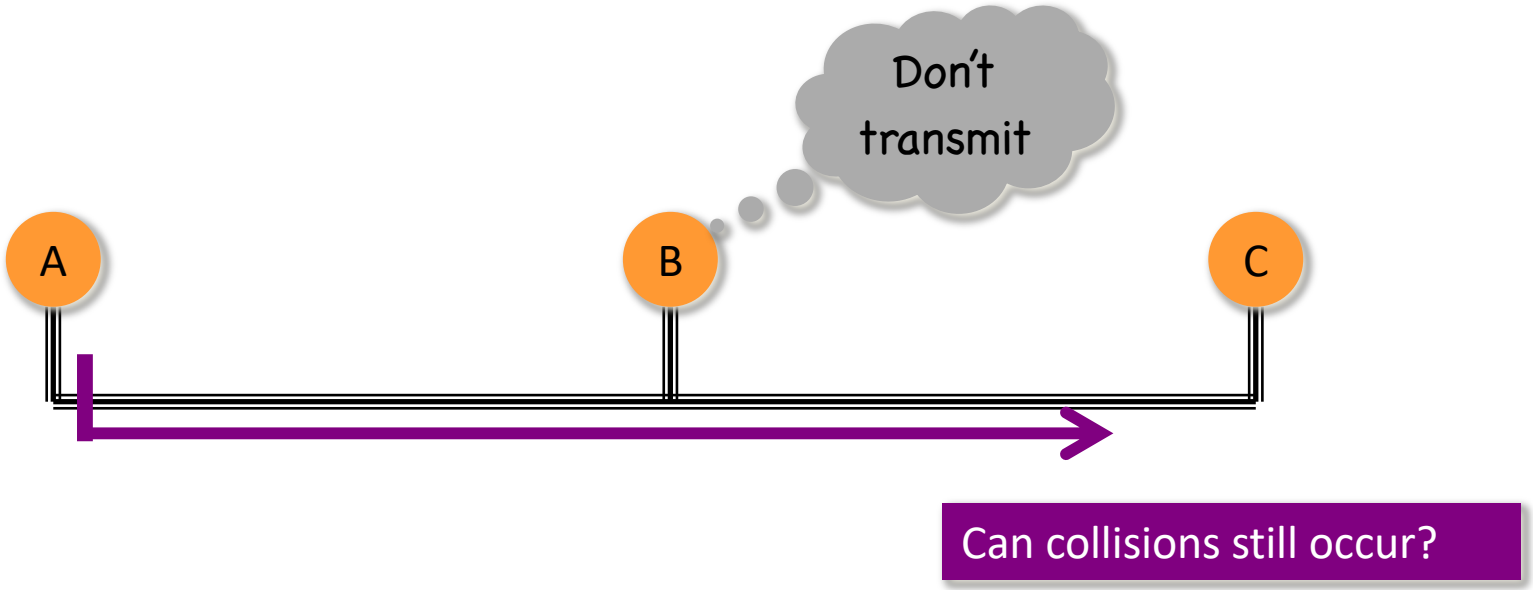


Example: Ethernet

- Medium Access Control (MAC) protocol
- **CSMA/CD** Protocol
  - **C**arrier **S**ense
  - **M**ultiple **A**ccess
  - **C**ollision **D**etection



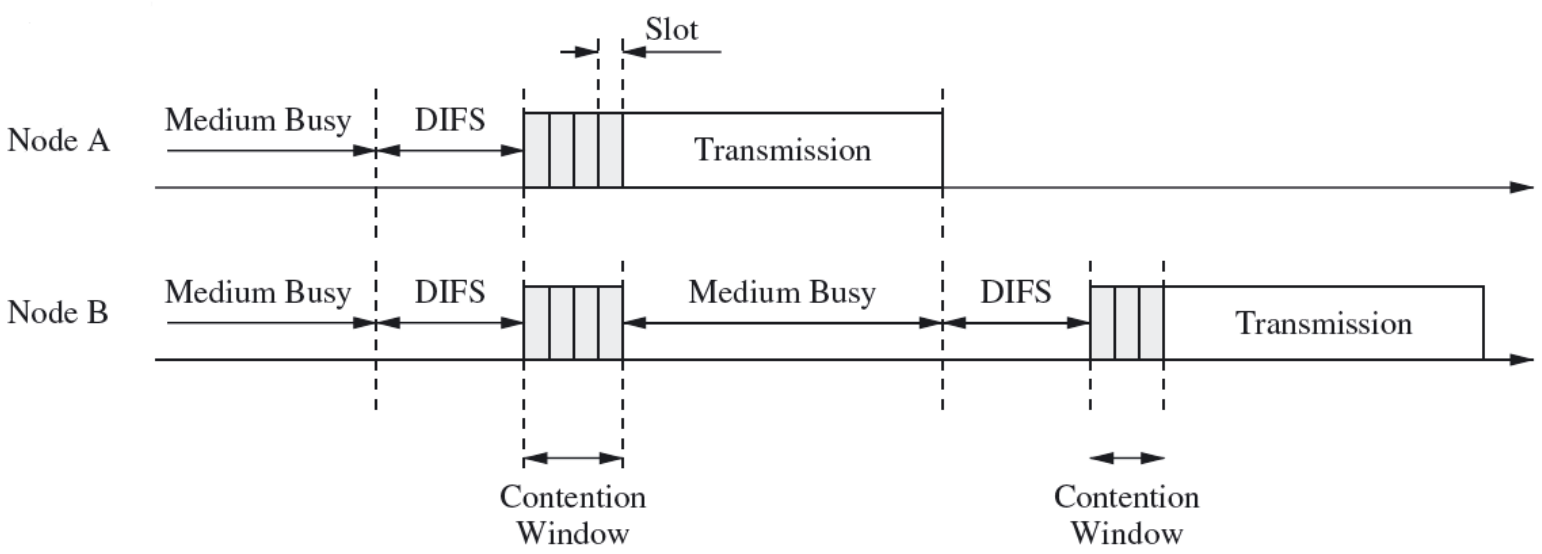
Example: Ethernet



- "Sense" (listen) carrier ("is anyone else talking right now?")
- If "busy": wait; if "idle": transmit
- CD: Keep listening while transmitting
  - If collision detected: retry at a later time

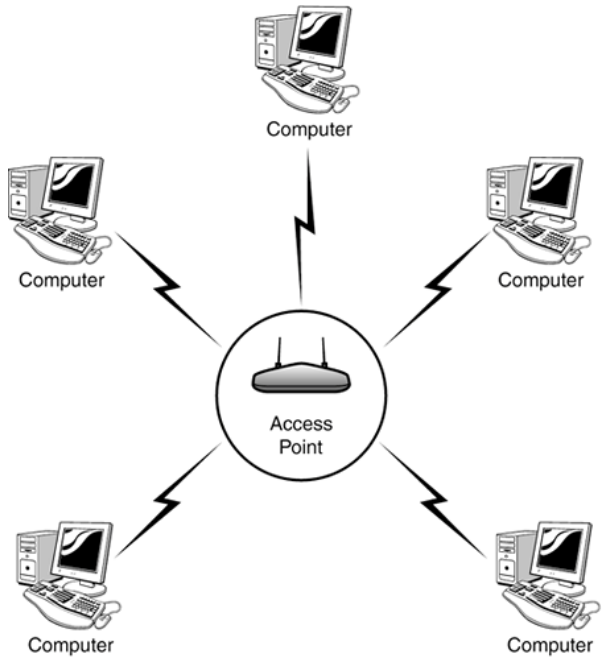
CSMA/CD

- Carrier Sense Multiple Access / Collision Detection
  - Carrier Sense: listen for inactivity on bus before transmitting
  - Multiple Access: multiple devices share same bus (wire)
  - Collision Detection: device detects if own transmission was corrupted (collision) and can retransmit at later time



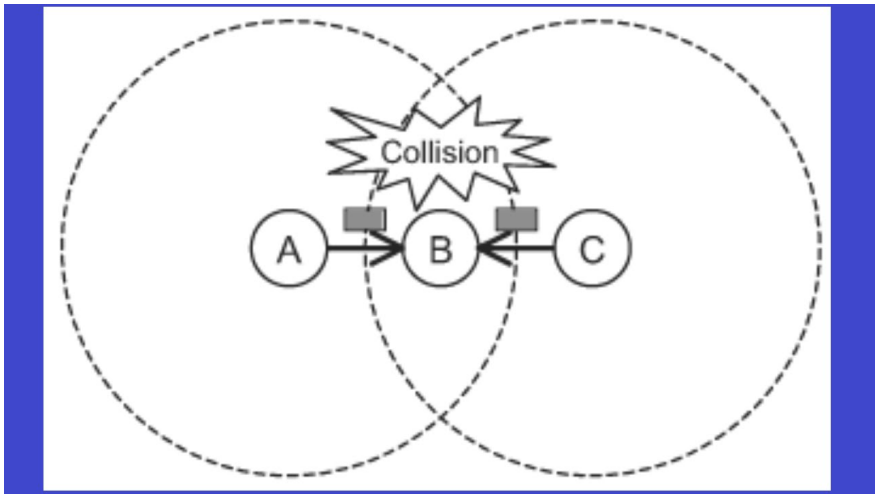
Example: Wi-Fi (802.11)

- Most popular wireless LAN architecture



Access point
Wi-Fi router
Base station
Hotspot

Example: Wi-Fi (802.11)

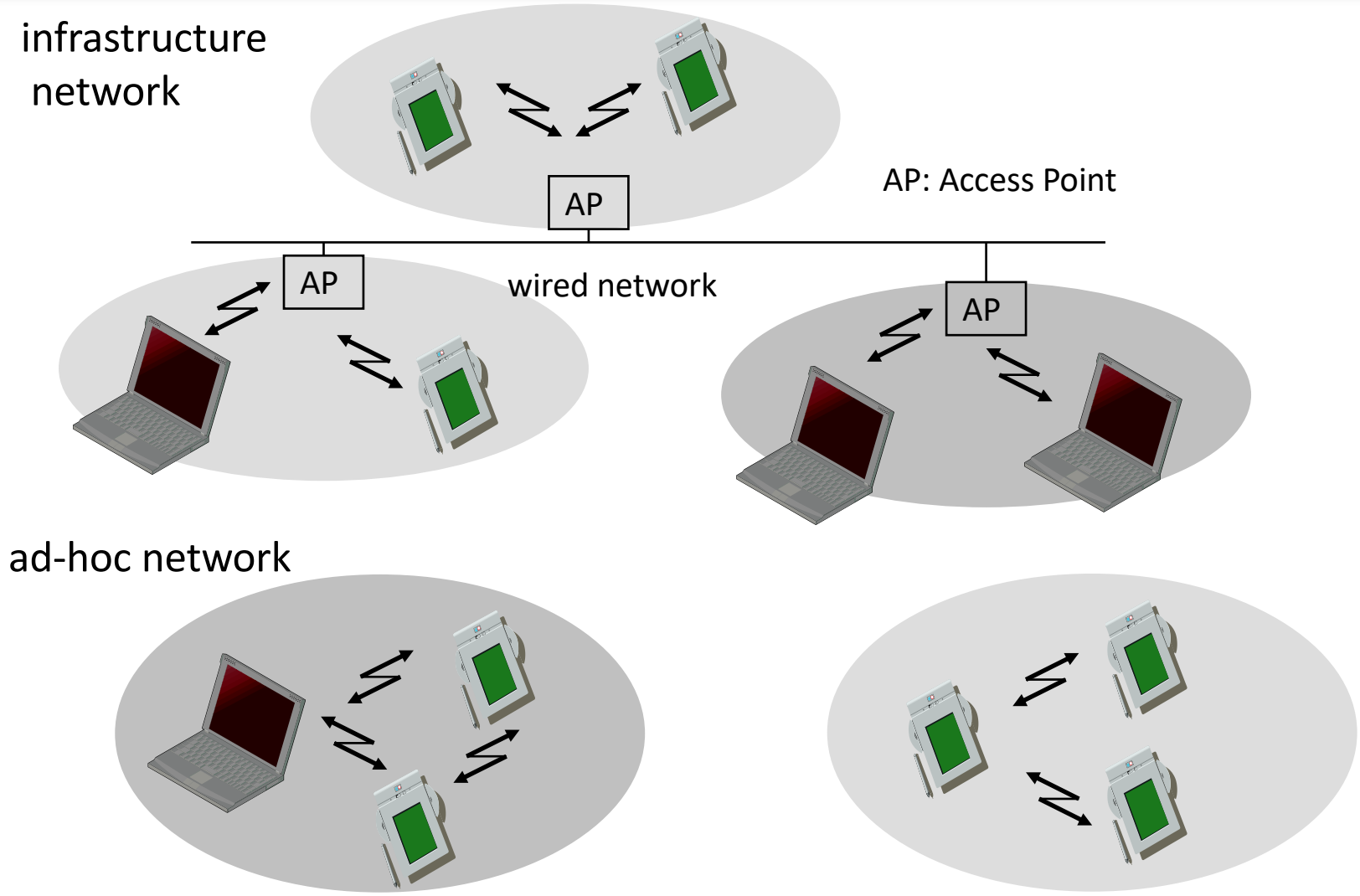


- **CSMA/CA** Protocol
  - **C**arrier **S**ense
  - **M**ultiple **A**ccess
  - **C**ollision **A**voidance
    - Channel reservations:
      - Transmitter sends request-to-send (RTS)
      - Receiver sends clear-to-send (CTS)
    - Advantages:
      - Nodes hearing RTS and/or CTS keep quiet
      - If collision, only small RTS or CTS packets are lost

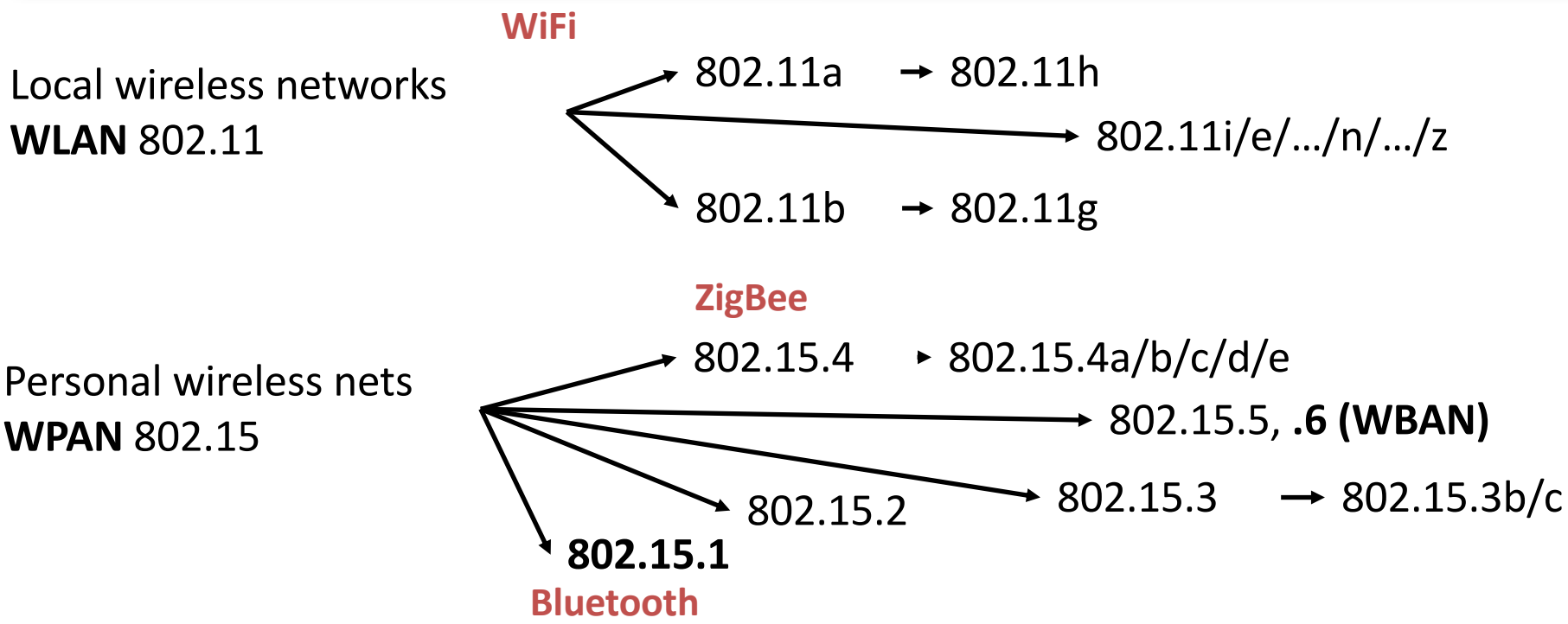
IEEE 802.11

- Published in 1999 by the Institute of Electrical and Electronics Engineers (IEEE)
  - specifies the physical and data link layers of the OSI model for wireless connections
- Often referred to as Wi-Fi
  - certification given by Wi-Fi Alliance, a group that ensures compatibility between hardware devices that use the 802.11 standard
- Wi-Fi roughly based on CSMA/CA

Infrastructure versus Ad-hoc Mode



Wireless Technologies (IEEE)



Wireless distribution networks

WMAN 802.16 (Broadband Wireless Access)

WiMAX

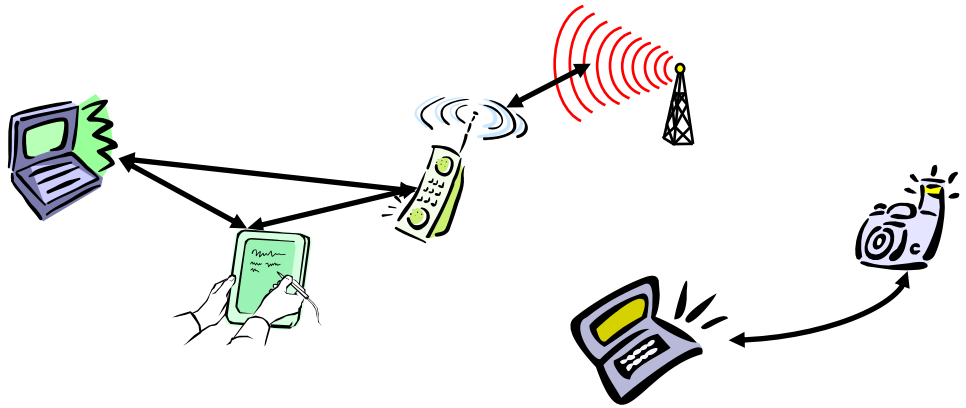
+ Mobility

[802.20 (Mobile Broadband Wireless Access)]

802.16e (addition to .16 for mobile devices)

Bluetooth

- Basic idea
  - Universal radio interface for ad-hoc wireless connectivity
  - Interconnecting computer and peripherals, handheld devices, PDAs, cell phones – replacement of IrDA
  - Embedded in other devices, very cheap
  - Short range (10m), low power consumption, license-free 2.4 GHz ISM
  - Voice and data transmission, approx. 1 Mbit/s data rate



Bluetooth

- History
  - 1994: Ericsson (Mattison/Haartsen), “MC-link” project
  - Renaming of the project: Bluetooth according to Harald “Blåtand” Gormsen [son of Gorm], King of Denmark in the 10th century
  - 1998: foundation of Bluetooth SIG, www.bluetooth.org
  - 2001: first consumer products for mass market, spec. version 1.1 released
  - 2005: 5 million chips/week

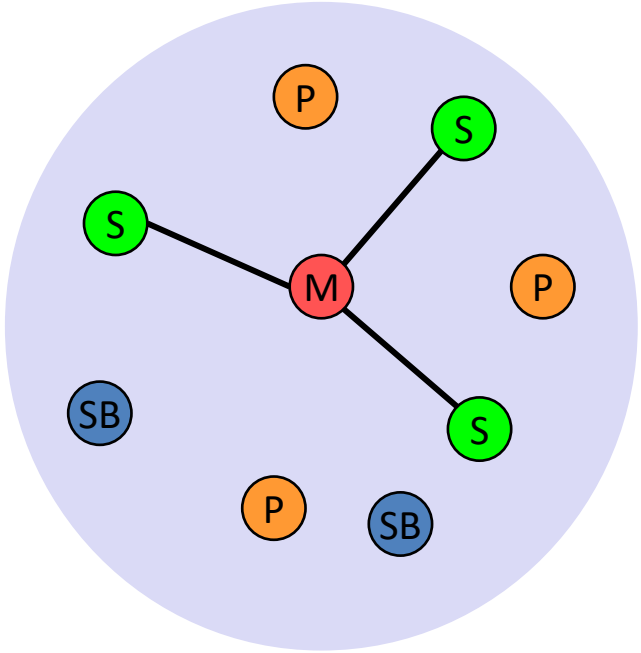
- Special Interest Group
  - Original founding members: Ericsson, Intel, IBM, Nokia, Toshiba
  - Added promoters: 3Com, Agere (was: Lucent), Microsoft, Motorola
  - > 10000 members
  - Common specification and certification of products

Characteristics

- **2.4 GHz** ISM band, **79 RF channels**, 1 MHz carrier spacing
  - Channel 0: 2402 MHz … channel 78: 2480 MHz
  - GFSK modulation, 1-100 mW transmit power
- FHSS and TDD
  - **Frequency hopping** (spread spectrum) with 1600 hops/s
  - Hopping sequence in a pseudo random fashion, determined by a master
  - Time division duplex for send/receive separation
- **Voice link – SCO** (Synchronous Connection Oriented)
  - **FEC (forward error correction)**, no retransmission, 64 kbit/s duplex, point-to-point, circuit switched
- **Data link – ACL** (Asynchronous Connection Less)
  - Asynchronous, acknowledgments, point-to-multipoint, up to 433.9 kbit/s symmetric or 723.2/57.6 kbit/s asymmetric, packet switched
- Topology
  - Overlapping piconets (stars) forming a scatternet

Piconet

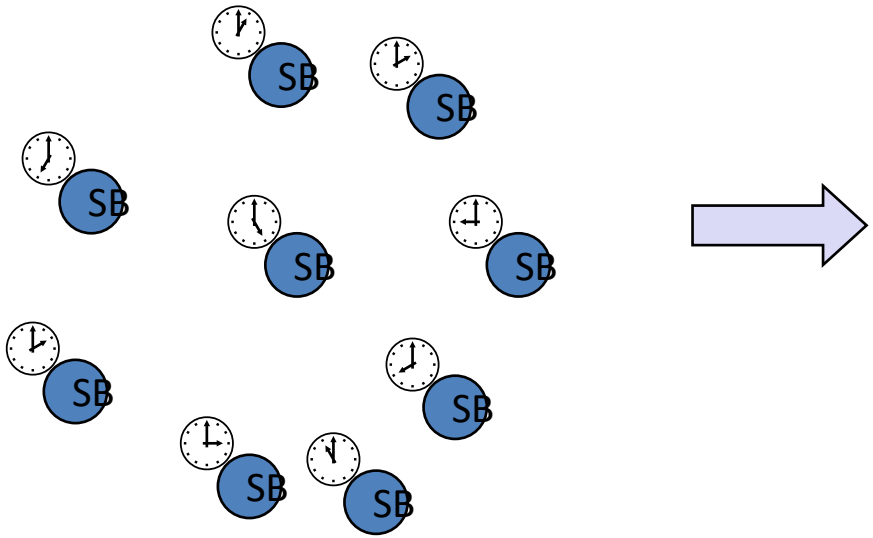
- Collection of devices connected in an ad hoc fashion
- One unit acts as master and the others as slaves for the lifetime of the piconet
- Master determines hopping pattern, slaves have to synchronize
- Each piconet has a unique hopping pattern
- Participation in a piconet = synchronization to hopping sequence
- Each piconet has one master and up to 7 simultaneous slaves (> 200 could be parked)

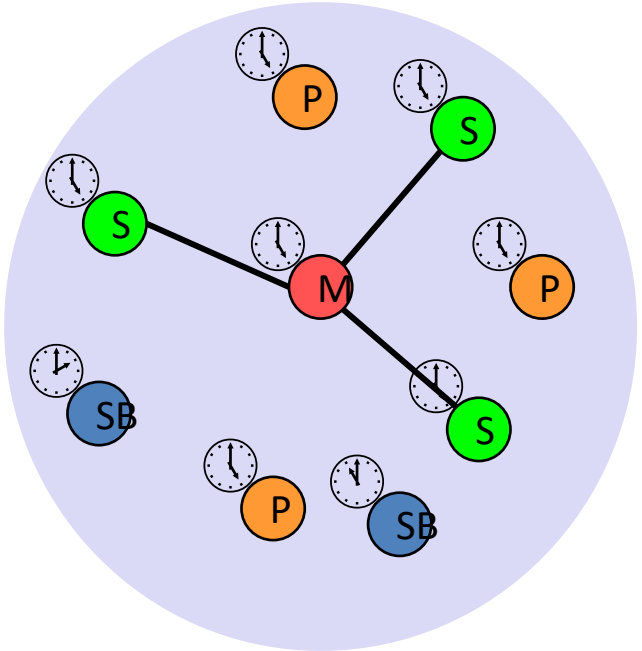


M=Master
S=Slave
P=Parked
SB=Standby

Piconet

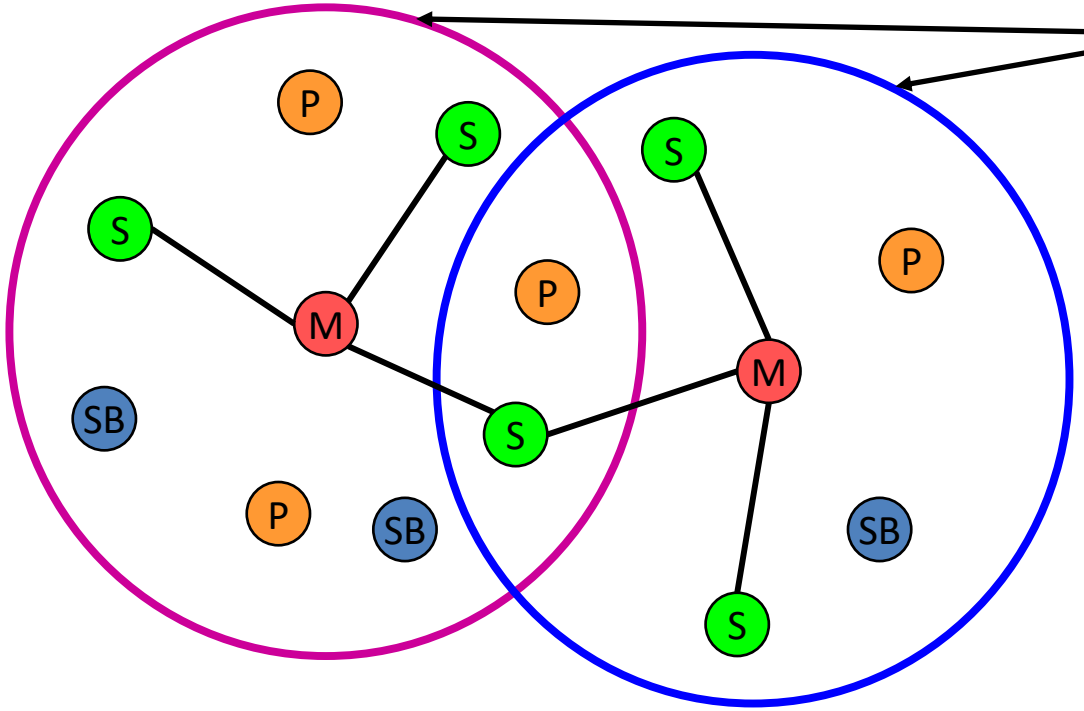
- All devices in a piconet hop together
  - Master gives slaves its clock and device ID
    - Hopping pattern: determined by device ID (48 bit, unique worldwide)
    - Phase in hopping pattern determined by clock
- Addressing
  - Active Member Address (AMA, 3 bit)
  - Parked Member Address (PMA, 8 bit)





Scatternet

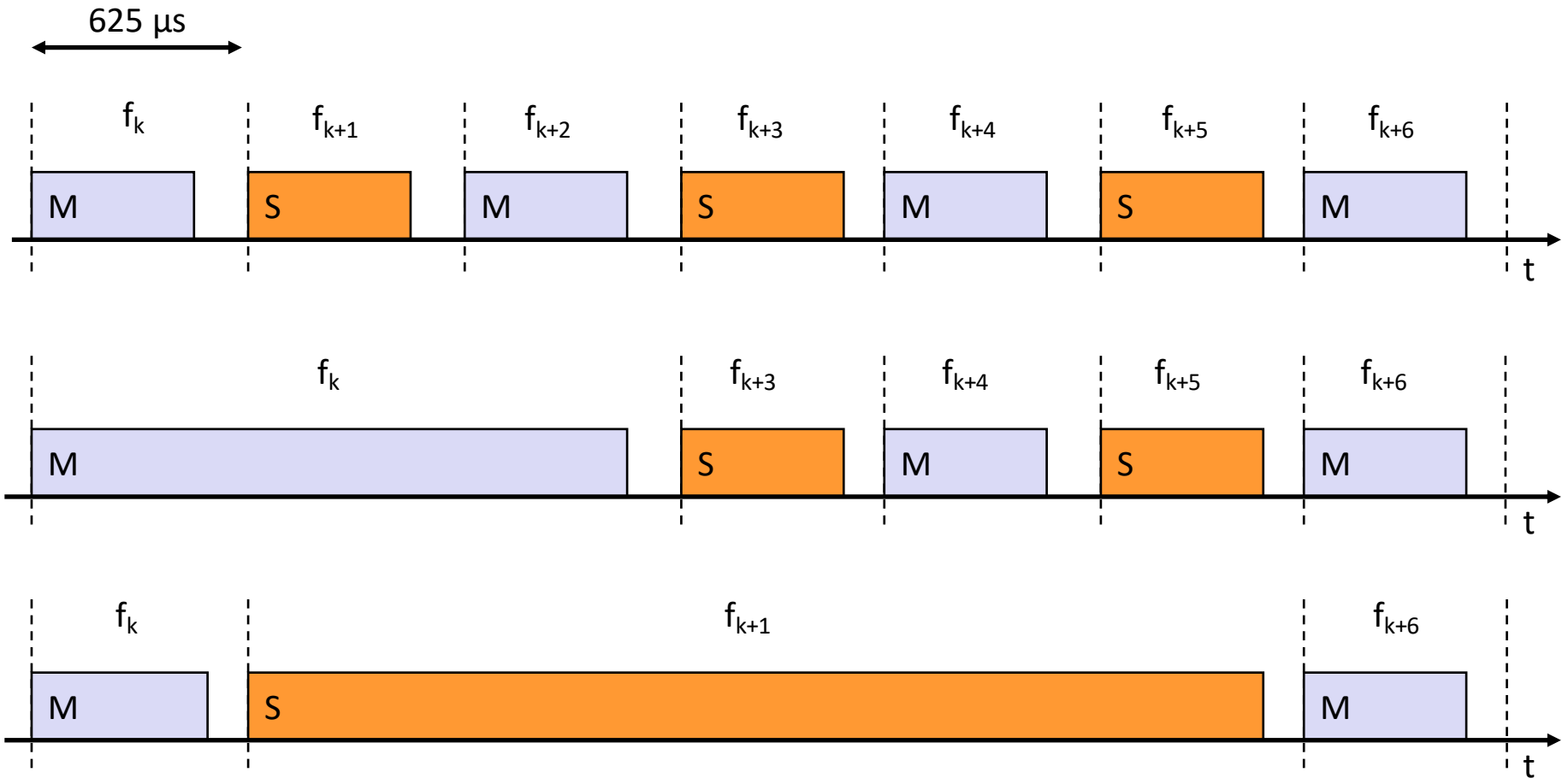
- Linking of multiple co-located piconets through the sharing of common master or slave devices
  - Devices can be slave in one piconet and master of another
- Communication between piconets
  - Devices jumping back and forth between the piconets



Piconets (each with a capacity of 720 kbit/s)

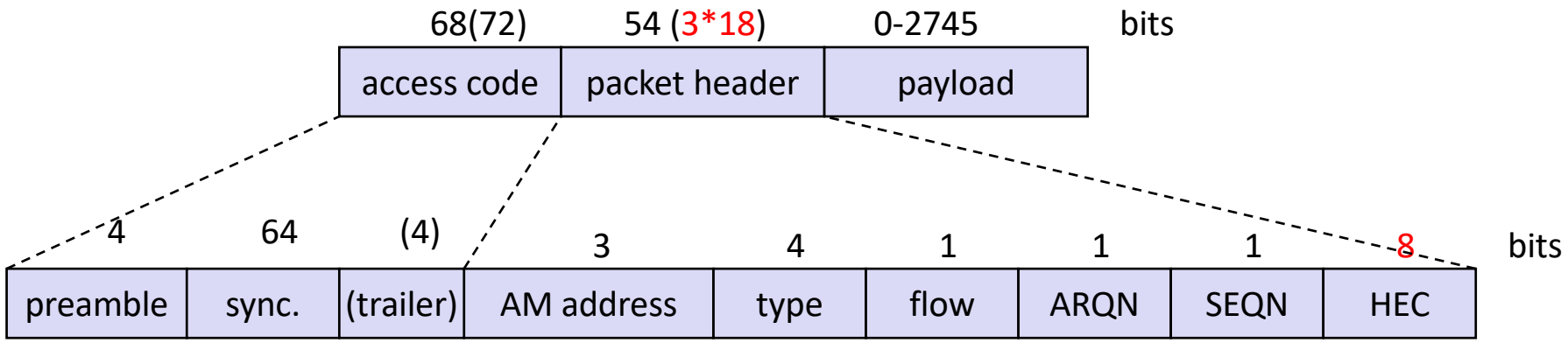
M=Master
S=Slave
P=Parked
SB=Standby

Communication

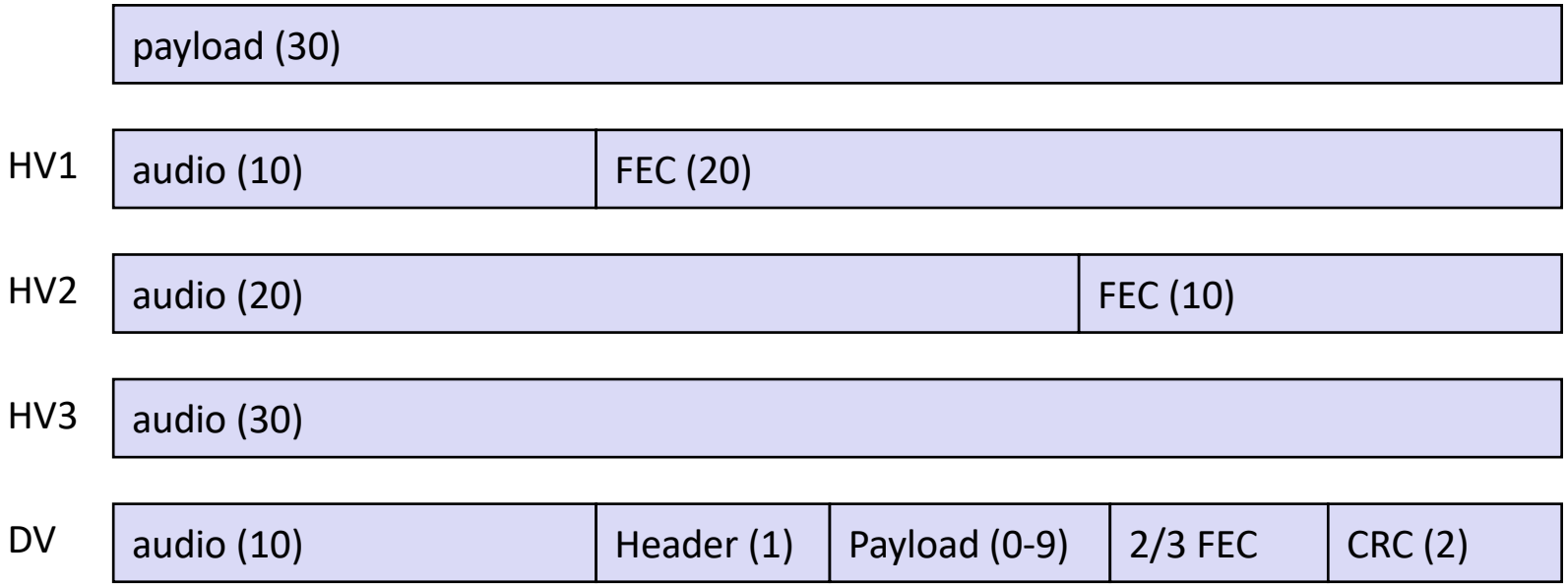


Bluetooth Packets

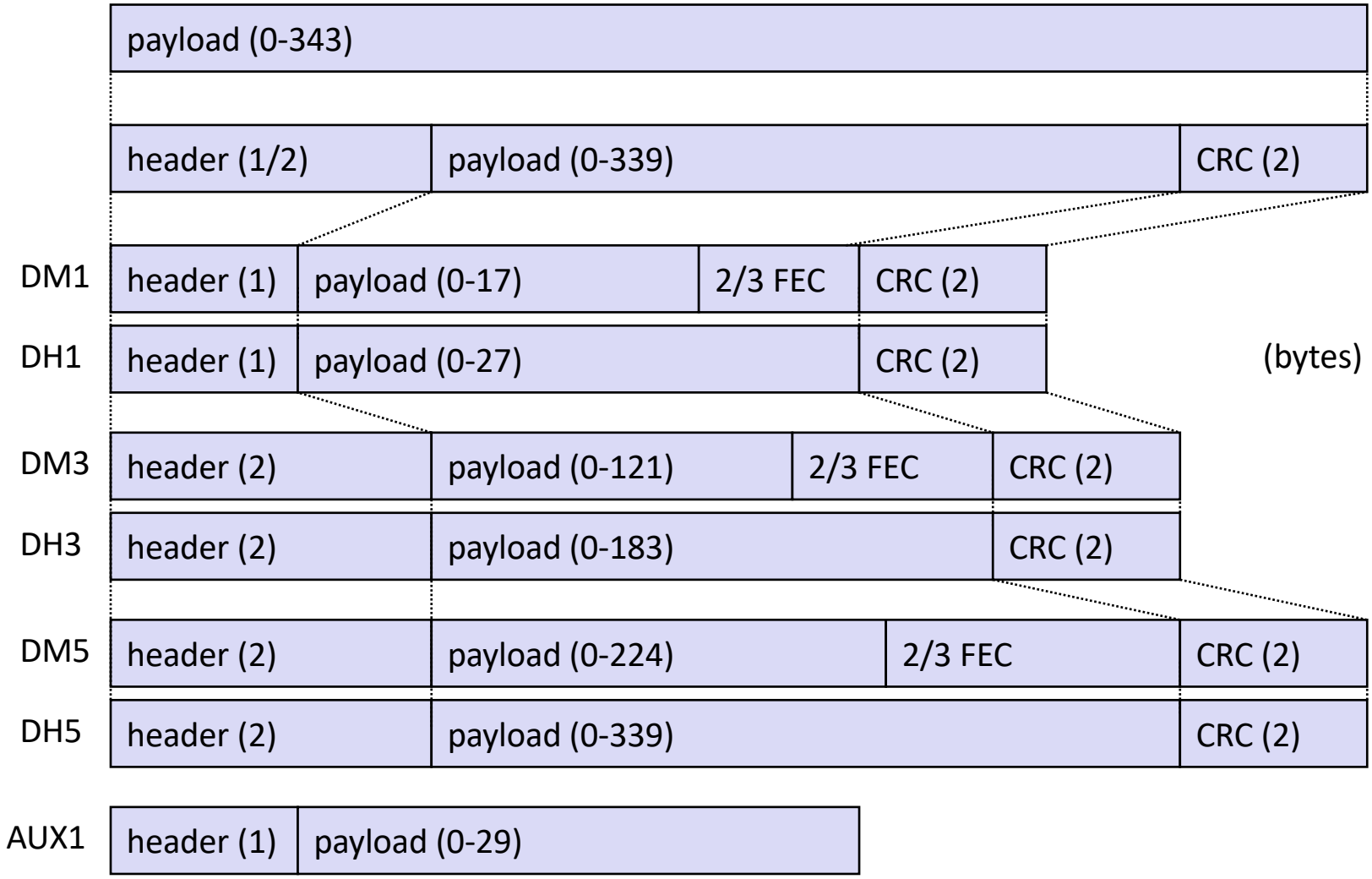
- Packet structure
  - Access code
    - Channel, device access, e.g., derived from master
  - Packet header
    - active member address (broadcast + 7 slaves), link type, alternating bit ARQ/SEQ, checksum



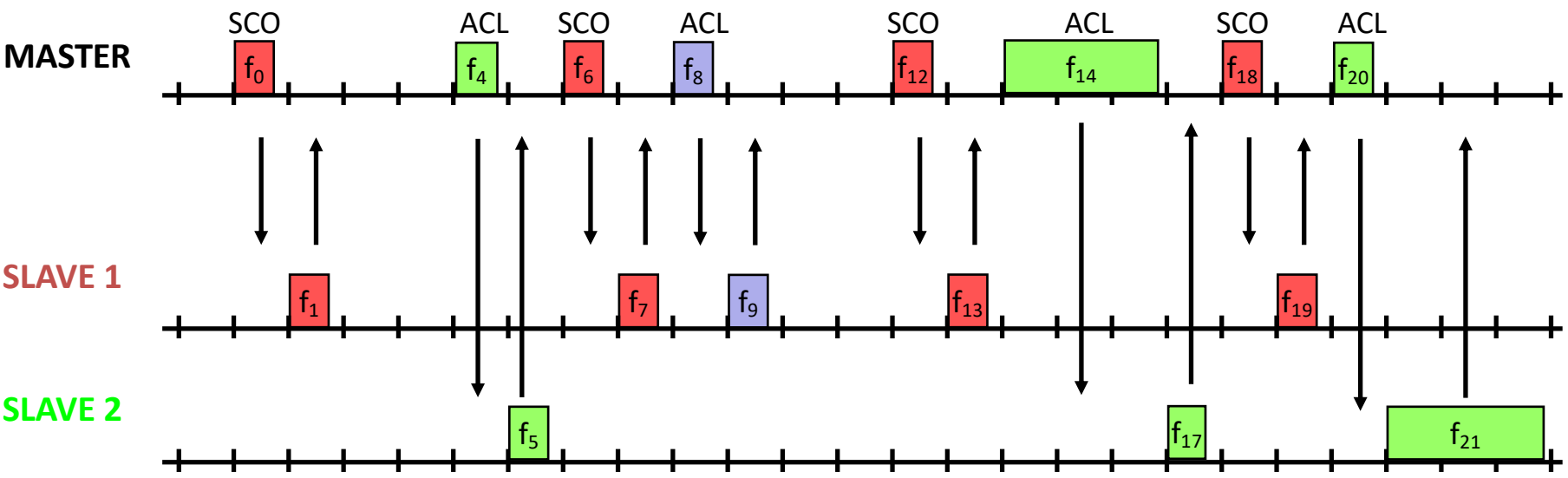
SCO Payload Types



ACL Payload Types



Communication Example



Bluetooth Versions

- Bluetooth 1.1
  - also IEEE Standard 802.15.1-2002
  - initial stable commercial standard
- Bluetooth 1.2
  - also IEEE Standard 802.15.1-2005
  - eSCO (extended SCO): higher, variable bitrates, retransmission for SCO
  - AFH (adaptive frequency hopping) to avoid interference
- Bluetooth 2.0 + EDR (2004, no more IEEE)
  - EDR (enhanced date rate) of 3.0 Mbit/s for ACL and eSCO
  - lower power consumption due to shorter duty cycle
- Bluetooth 2.1 + EDR (2007)
  - better pairing support, e.g., using NFC
  - improved security

Bluetooth Versions

- Bluetooth 3.0 + HS (2009)
  - speeds up to 24Mbps (using co-located Wi-Fi link!)
- Bluetooth 4.0
  - Classic Bluetooth
  - Bluetooth High Speed
  - Bluetooth Low Energy
- Bluetooth Low Energy (BLE):
  - Marketed as Smart Bluetooth
  - Lower power, lower cost
  - Use in healthcare, fitness, security, entertainment devices
  - 40 channels

- Bluetooth Profiles (different types of applications)

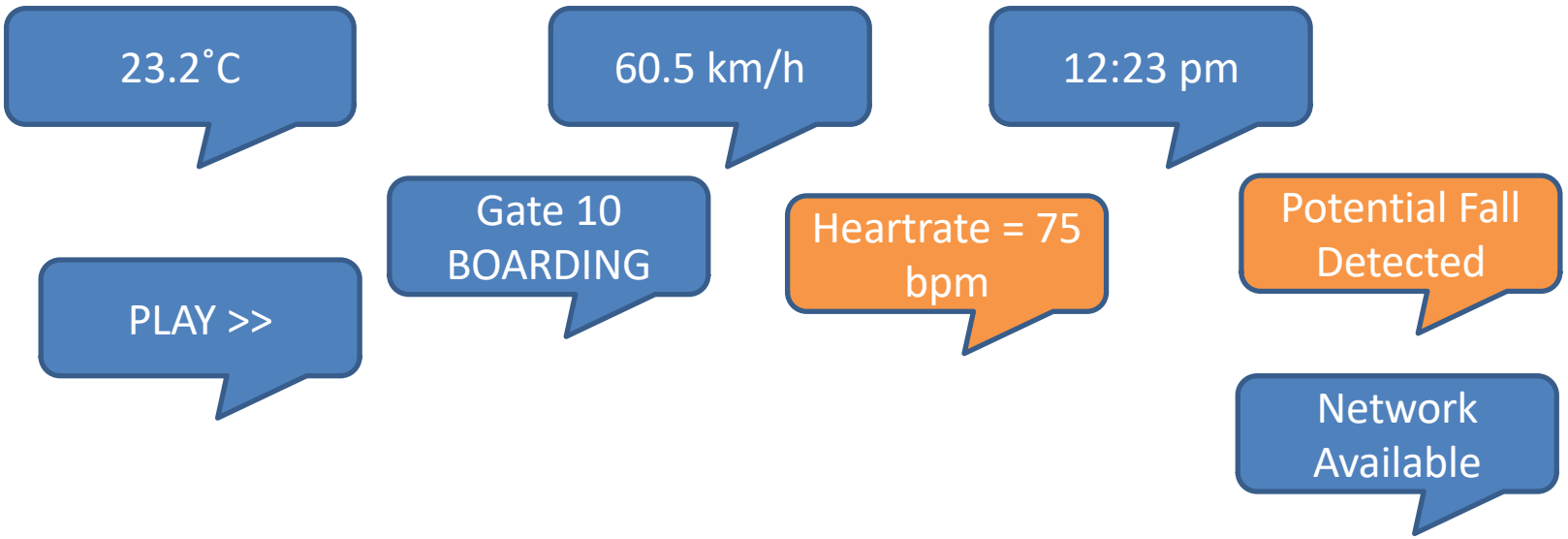
Energy Consumption in Classic BT

- Traditional Bluetooth is **connection oriented**. When a device is connected, a link is maintained, even if there is no data flowing
- **Sniff modes** allow devices to sleep, reducing power consumption to give months of battery life (e.g., wake up every 100ms)
- Peak transmit current is typically around 25mA
- Even though it has been independently shown to be lower power than other radio standards, it is still not low enough for **coin cells** and energy harvesting applications

Bluetooth Low Energy (BLE)

- Bluetooth low energy is a new, open, short range radio technology
  - Blank sheet of paper design
  - Different to Bluetooth classic (BR/EDR)
  - Optimized for ultra low power
  - Enable coin cell battery use cases
    - < 20mA peak current
    - < 5uA average current

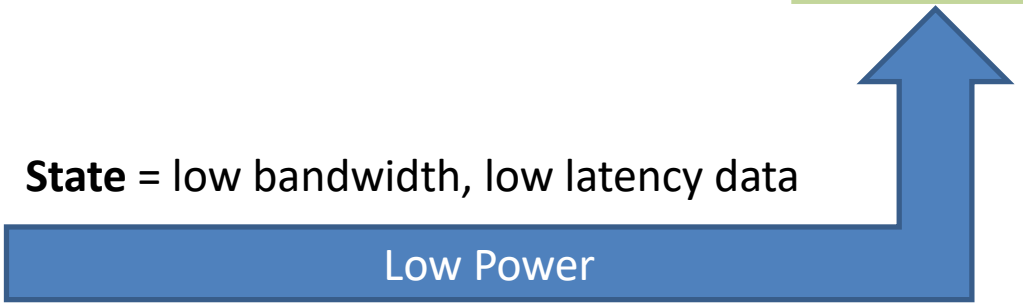
“Exposing State”



- Good at small, discrete data transfers
- Data can triggered by local events
- Data can be read at any time by a client
- Interface model is very simple (GATT)

Short Range Wireless Application Areas

	Voice	Data	Audio	Video	State
Bluetooth ACL/HS	x	Y	Y	x	x
Bluetooth SCO/eSCO	Y	x	x	x	x
Bluetooth low energy	x	x	x	x	Y
Wi-Fi	(VoIP)	Y	Y	Y	x
Wi-Fi Direct	Y	Y	Y	x	x
ZigBee	x	x	x	x	Y
ANT	x	x	x	x	Y



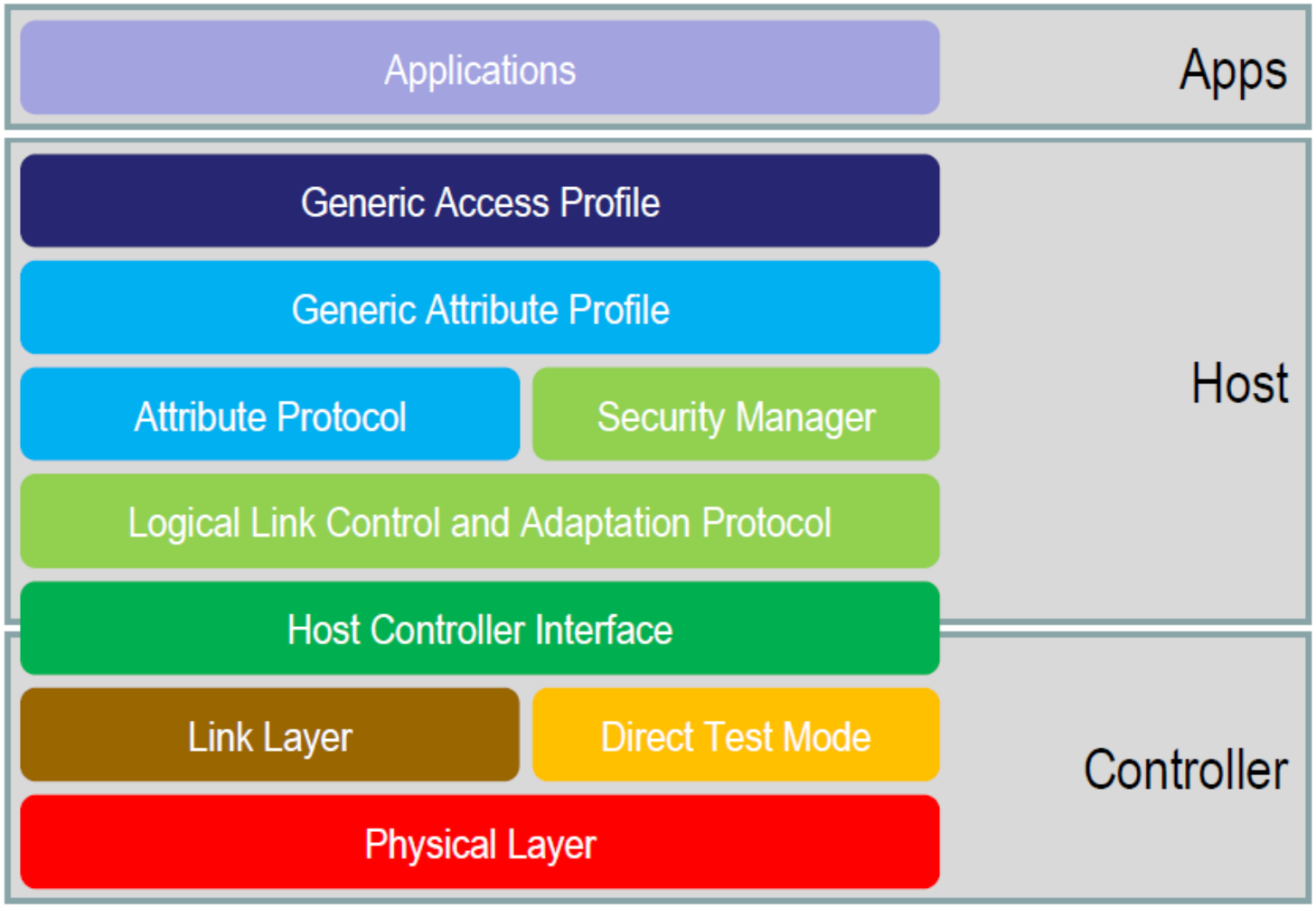
BLE Basic Concepts

- Everything is optimized for lowest power consumption
  - Short packets reduce TX peak current
  - Short packets reduce RX time
  - Fewer RF channels to improve discovery and connection time
  - Simple state machine
  - Single protocol
  - …

BLE Fact Sheet

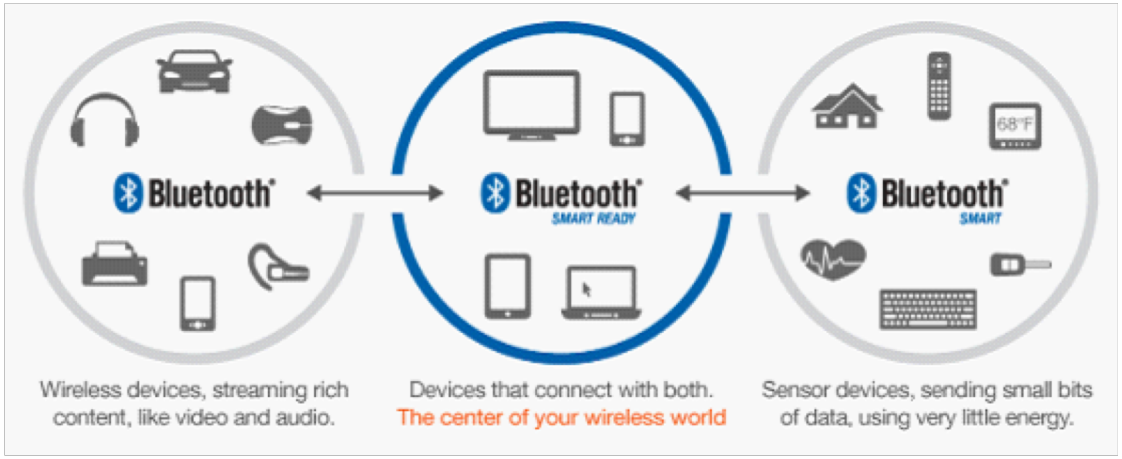
Range:	~ 150 meters open field
Output Power:	~ 10 mW (10dBm)
Max Current:	~ 15 mA
Latency:	3 ms
Topology:	Star
Connections:	> 2 billion
Modulation:	GFSK @ 2.4 GHz
Robustness:	Adaptive Frequency Hopping, 24 bit CRC
Security:	128bit AES CCM
Sleep current:	~ 1µA
Modes:	Broadcast, Connection, Event Data Models, Reads, Writes

BLE Architecture



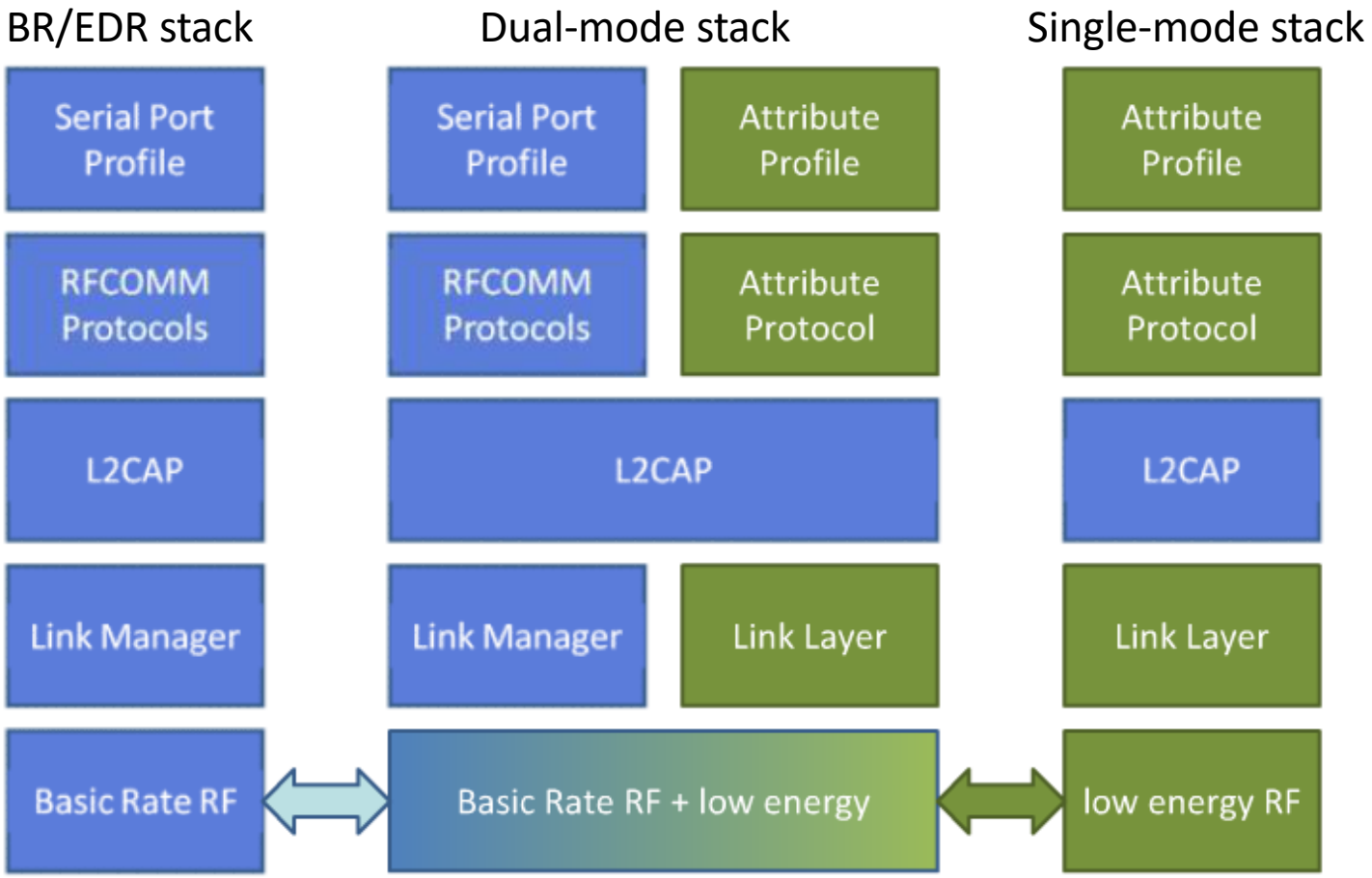
BLE Device Modes

- Dual Mode
  - Bluetooth BR/EDR and LE
  - Used anywhere BR/EDR is used today
- Single Mode
  - Implements only Bluetooth Low Energy
  - Will be used in new devices/applications



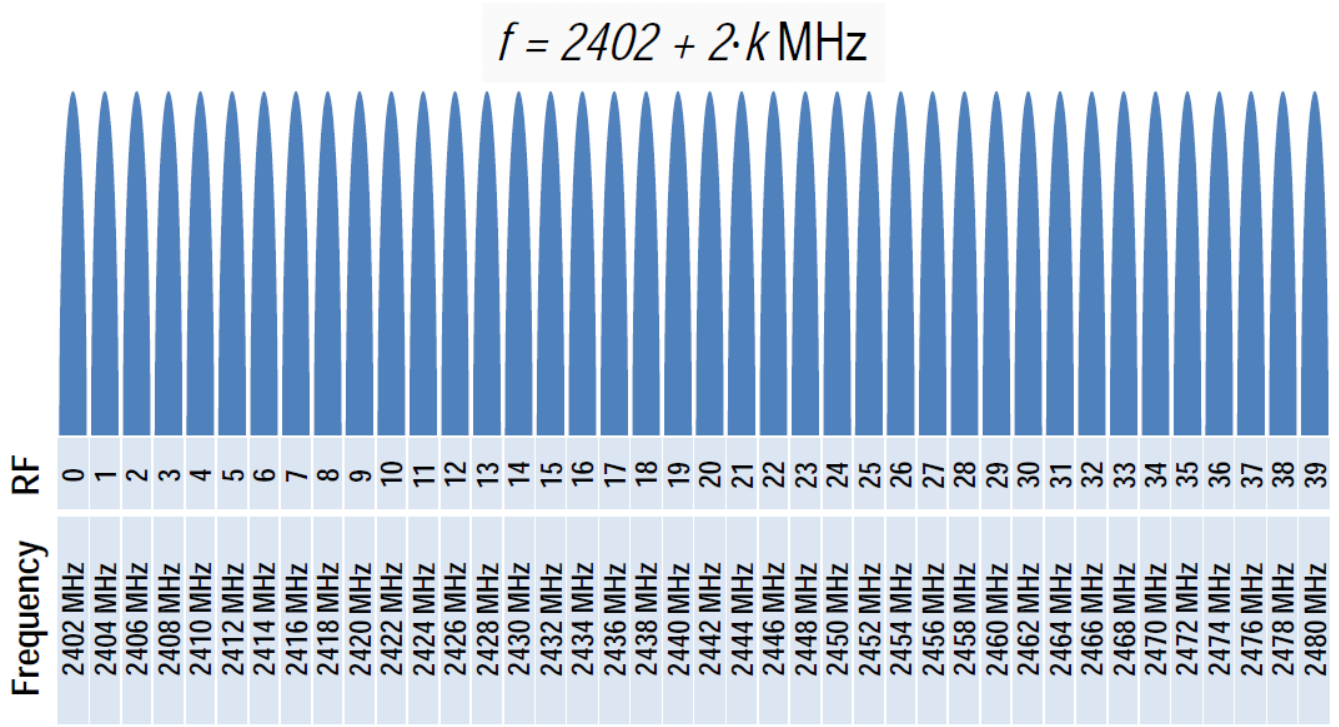
BLE Device Modes

- Dual mode + single modes



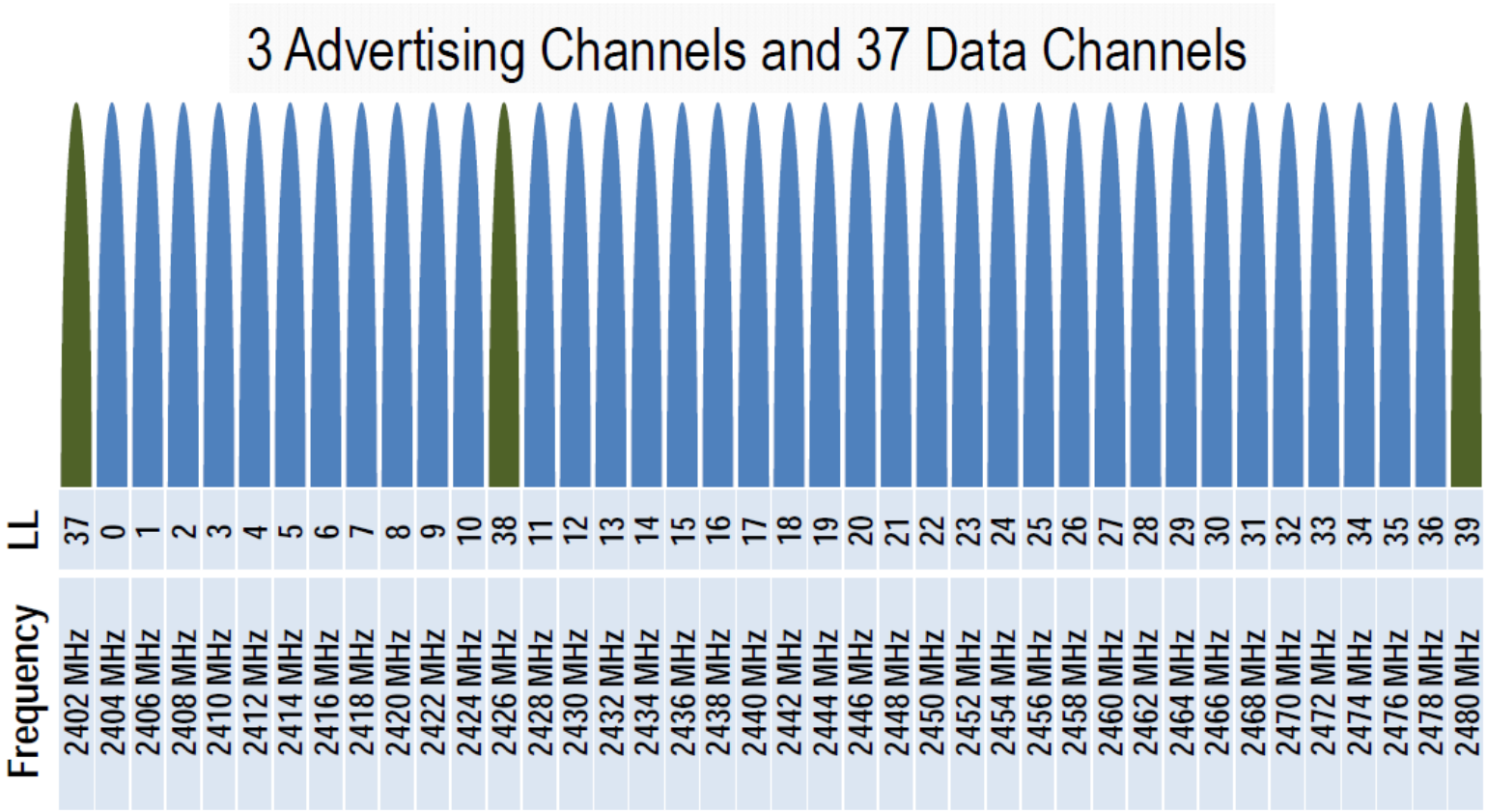
BLE Physical Layer

- 2.4 GHz ISM band
- 1Mbps GFSK
- 40 Channels on 2 MHz spacing



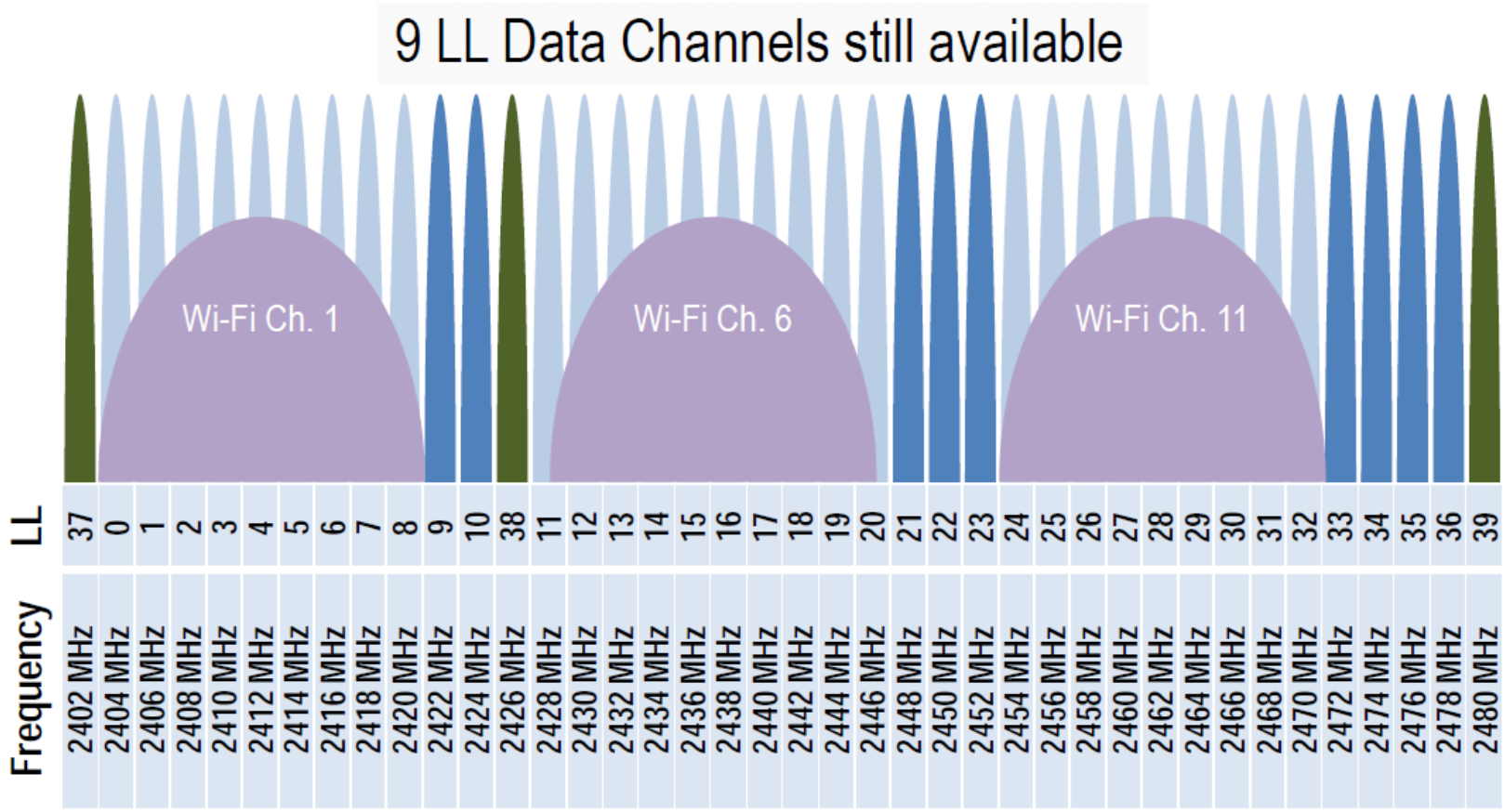
BLE Physical Layer

- Two types of channels



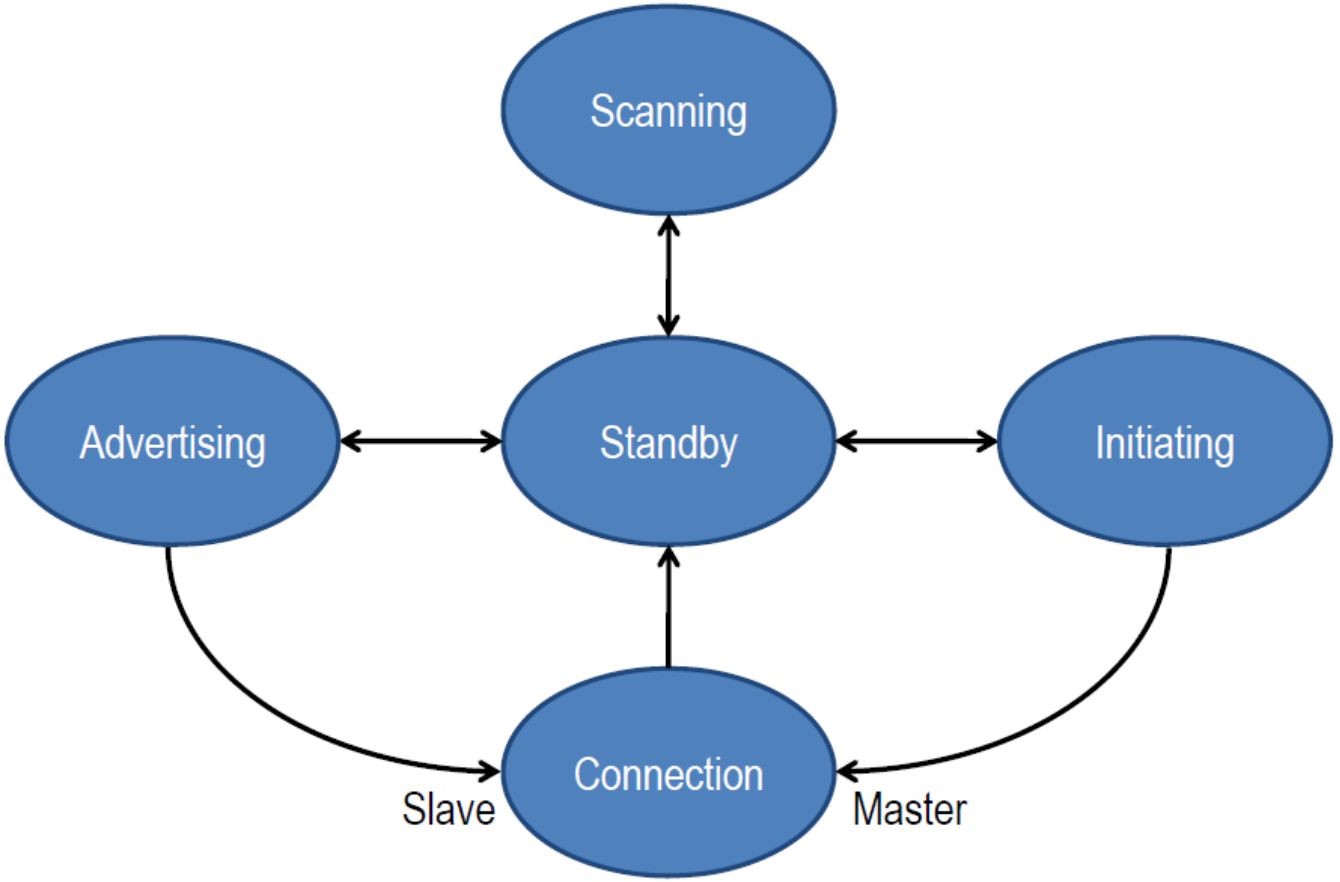
BLE Physical Layer

- Advertising channels avoid 802.11

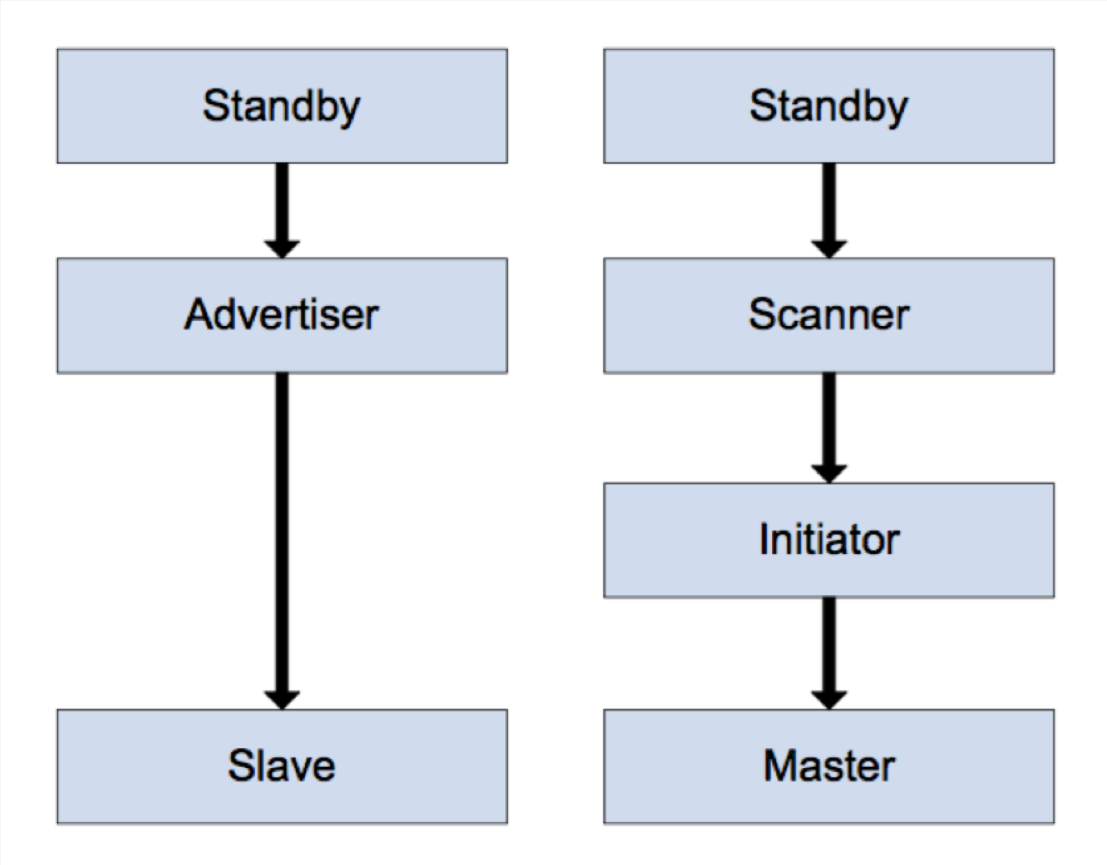


BLE Link Layer

- Link Layer state machine



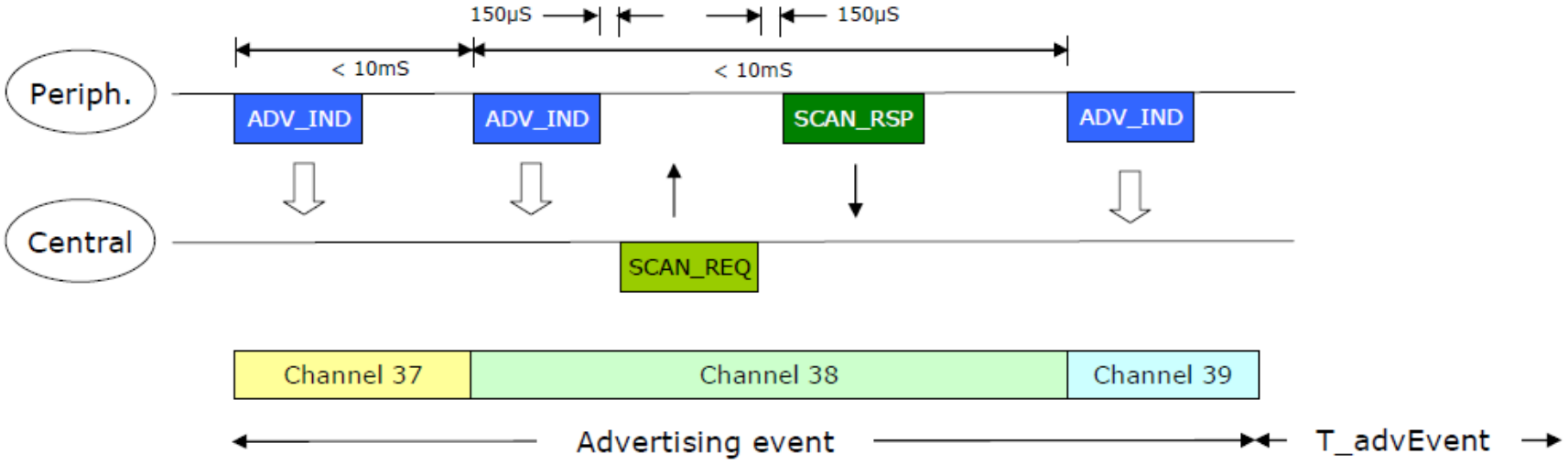
BLE Link Layer



BLE Link Layer

- Possible states:
  - **Standby**: not transmitting or receiving any data, and is not connected to any other device
  - **Advertiser**: periodically broadcasting advertisements
  - **Scanner**: actively looking for advertisers
  - **Initiator**: actively trying to initiate a connection with another device
  - **Master**: connected to another device as a master
  - **Slave**: connected to another device as a slave

BLE Advertising

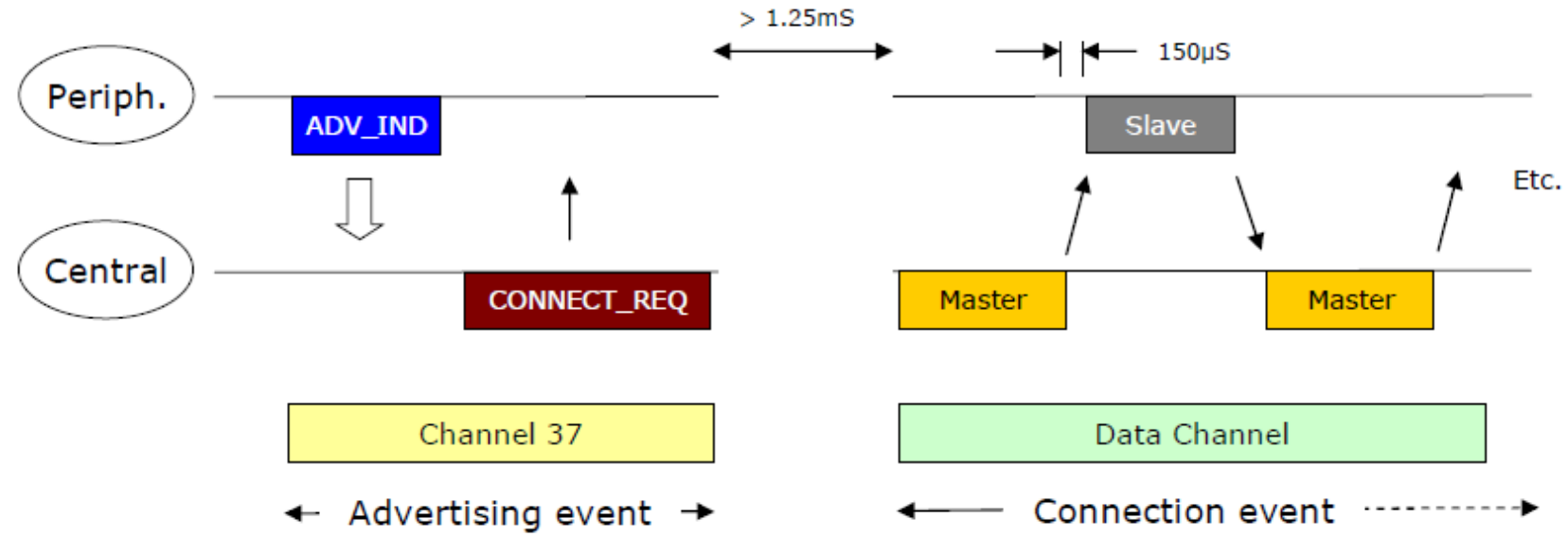


- Devices can advertise for a variety of reasons:
  - To broadcast promiscuously
  - To transmit signed data to a previously bonded device
  - To advertise their presence to a device wanting to connect
  - To reconnect asynchronously due to a local event

BLE Advertising

- Four types of advertisements:
  - **Connectable undirected**: any scanner device can initiate a connection with this advertiser
  - **Connectable directed**: only one specific device can initiate a connection with this advertiser
  - **Non-connectable undirected**: no devices can initiate a connection with this advertiser; primarily used for general broadcast of data (up to 31 bytes of payload)
  - **Discoverable undirected**: any scanner device can request more information from the advertising device, but no devices can initiate a connection with it

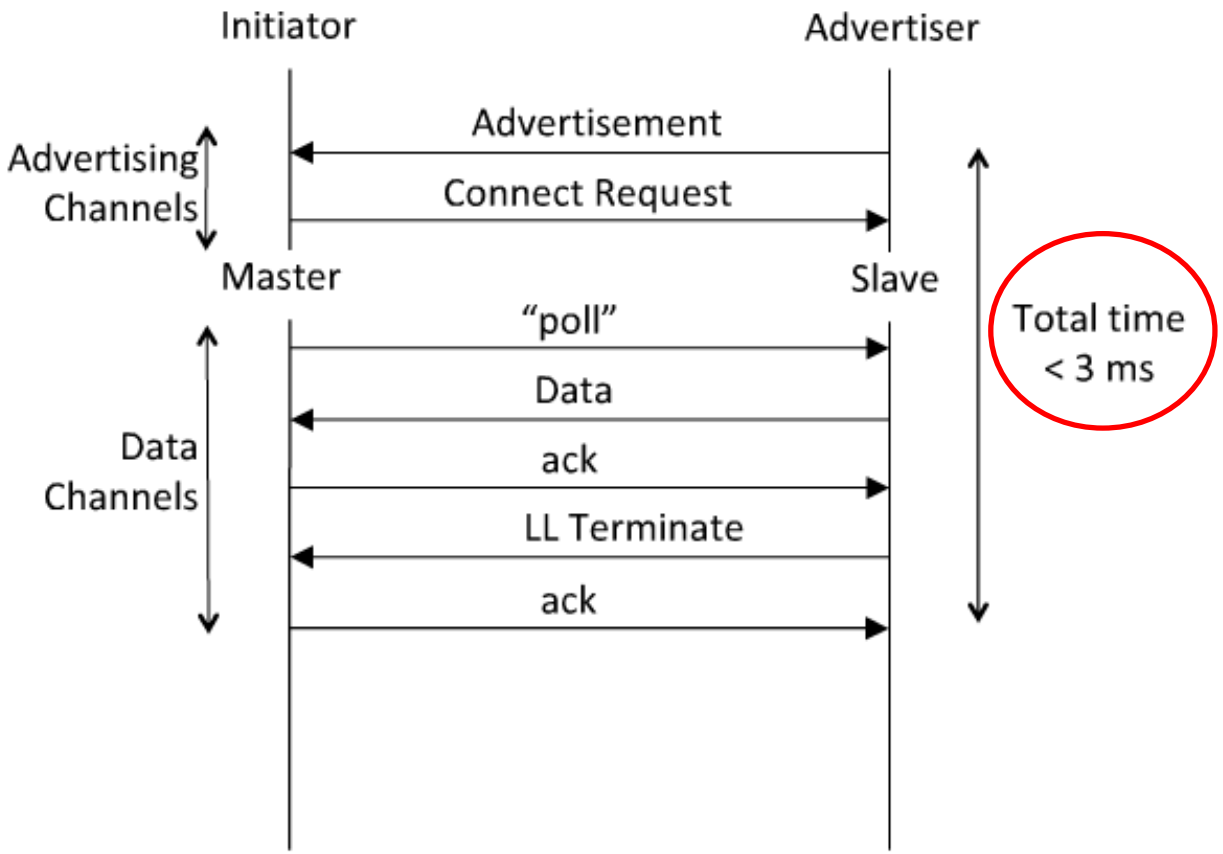
BLE Data Transfer



- Once a connection is made:
  - Master informs slave of hopping sequence and when to wake up
  - All subsequent transactions are performed on the 37 data channels
  - Transactions can be encrypted
  - Both devices can go into deep sleep between transactions

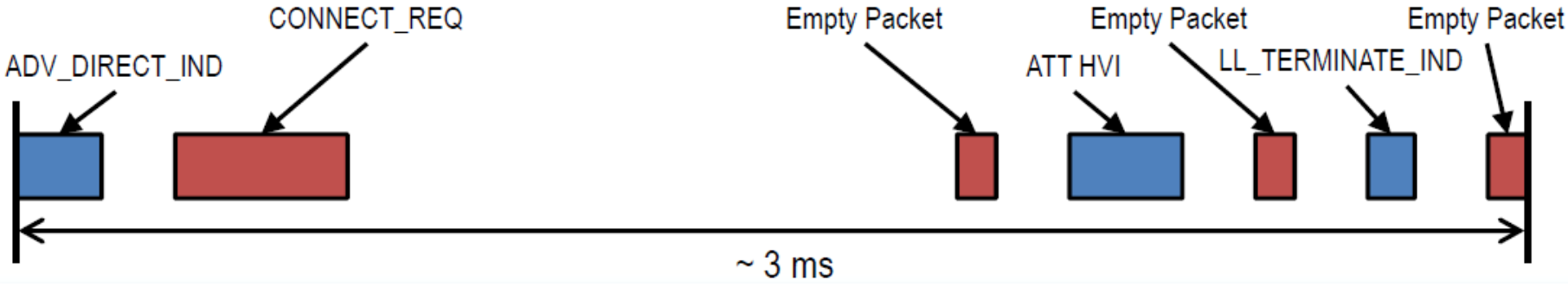
Link Layer Connections

- Very low latency connection



Link Layer Connections

Time (us)	Master Tx	Radio Active (us)	Slave Tx
0		176	ADV_DIRECT_IND
326	CONNECT_REQ	352	
1928	Empty Packet	80	
2158		144	Attribute Protocol Handle Value Indication
2452	Empty Packet (Acknowledgement)	80	
2682		96	LL_TERMINATE_IND
2928	Empty Packet (Acknowledgement)	80	



BLE Energy Characteristics

- From the previous slide, calculate energy per transaction
  - Assume an upper bound of 3ms per minimal transaction
  - Estimated TX power is 15mW (mostly TX power amp for 65nm chips)
  - For 1.5V battery, this is 10mA. 0.015W * 0.003 sec = 45 uJ
- How long could a sensor last on a battery?
  - An example battery: Lenmar WC357, 1.55v, 180mAh, $2-5
  - 180mAh/10mA = 18Hr = 64,800 seconds = 21.6M transactions
  - Suppose this sensor sends a report every minute = 1440/day
  - For just the BT LE transactions, this is 15,000 days, or > 40 years
  - This far exceeds the life of the battery and/or the product
- This means that battery will cost more than the electronics
  - This sensor could run on scavenged power, e.g., ambient light

BLE Use Cases

- Proximity
- Time
- Emergency
- Network availability
- Personal user interface
- Simple remote control
- Browse over Bluetooth
- Temperature sensor
- Humidity sensor
- HVAC
- Generic I/O (automation)
- Battery status
- Heart rate monitor
- Physical activity monitor
- Blood glucose monitor
- Cycling sensors
- Pulse oximeter
- Body thermometer

BLE Use Cases

- It can enable proximity detection
  - I’m in the car
  - I’m in the office
  - I’m in the meeting room
  - I’m in the movie theater
- It can enable presence detection
  - Turn the lights on when I walk around the house
  - Automatically locks the door when I leave home
  - Turn the alarm off if I’m already awake

BLE and Smart Health

My pulse is …

My blood glucose is …

My temperature is …

BLE and GAP

- Generic Access Profile (GAP)
  - GAP defines a base profile which all Bluetooth devices implement, which ties all the various layers together to form the basic requirements for a Bluetooth device
  - GAP also defines generic procedures for connection-related services:
    - Device Discovery
    - Link Establishment
    - Link Management
    - Link Termination
    - Initiation of security features

BLE and GAP

- The GAP layer works in one of four profile roles:
  - **Broadcaster**: an advertiser that is non-connectable
  - **Observer**: scans for advertisements, but cannot initiate connections
  - **Peripheral**: an advertiser that is connectable and can operate as a slave in a single link layer connection
  - **Central**: scans for advertisements and initiates connections; operates as a master in a single or multiple link layer connections

BLE and GAP

Temperature Sensor (Broadcaster) → Temperature Display (Observer)

Figure 1 – Temperature Sensor (Broadcaster)

Figure 2 – Temperature Display (Observer)

Watch (Peripheral) ← → Mobile Phone (Central)

Figure 3 - Watch (Peripheral)

Figure 4 – Mobile Phone (Central)

BLE and GAP – Discoverable Modes

- GAP supports three different discoverable modes:
  - Non-discoverable Mode: No advertisements
  - Limited Discoverable Mode: Device advertises for a limited amount of time before returning to the standby state
  - General Discoverable Mode: Devices advertises continuously
- GAP manages the data that is sent out in advertisement and scan response packets

BLE and GAP - Pairing

- Pairing can be initiated by either the central or peripheral device
- The two devices generate and exchange short-term keys (STK) which can be used to decrypt data packets
- Either device can request to enable “bonding” to create a long-term relationship between the two devices
  - A long-term key (LTK) is generated, exchanged, and stored allowing device to re-encrypt the link quickly upon re-connection, without going through the complete pairing process once again
  - Profile / Service configuration data is remembered, so that the user does not need to re-configure the device every time they re-connect

BLE and GAP - Pairing

- Each device also states its input/output capabilities from among these options:
  - DisplayOnly – no way user can input anything into device, but it can output data
  - DisplayYesNo – user can input “yes” or “no” but nothing else; can also display data
  - KeyboardOnly – user can input a password or PIN, but no display
  - NoInputNoOutput – device has no means for user input, and has no display
  - KeyboardDisplay – device has a means for display as well as for input

BLE and GAP - Pairing

- Based on the combination of the capabilities of the two devices, one of two methods of pairing will be used:
  - Passkey entry – one device will display a randomly generator passkey, while the other will require the user to input the passkey. This allows for an authenticated link (MITM protection)
  - "Just Works" – the pairing process completes without requiring a passkey to be entered. The link will not be authenticated, but is encrypted
- If either one of the two devices does not require authentication, then Just Works will be used by default, allowing the user to skip passkey entry

Bluetooth in Health Care

- Workgroup formed in 2006 to develop standard to support existing and emerging medical devices and to bring compatibility and interoperability
- Medical device manufacturers, silicon suppliers, and other supporters of the Bluetooth standard worked together to produce a **Health Device Profile** that was approved in 2008

BT Health Device Profile

- The Bluetooth Health Device Profile works with Bluetooth chips that support streaming data rates of up to 2.1Mbps
- That means that it can support medical devices as complex as ECGs, which need to stream data
- It is equally applicable for simple devices such as weight scales that only need to transmit small quantities of information

Capabilities

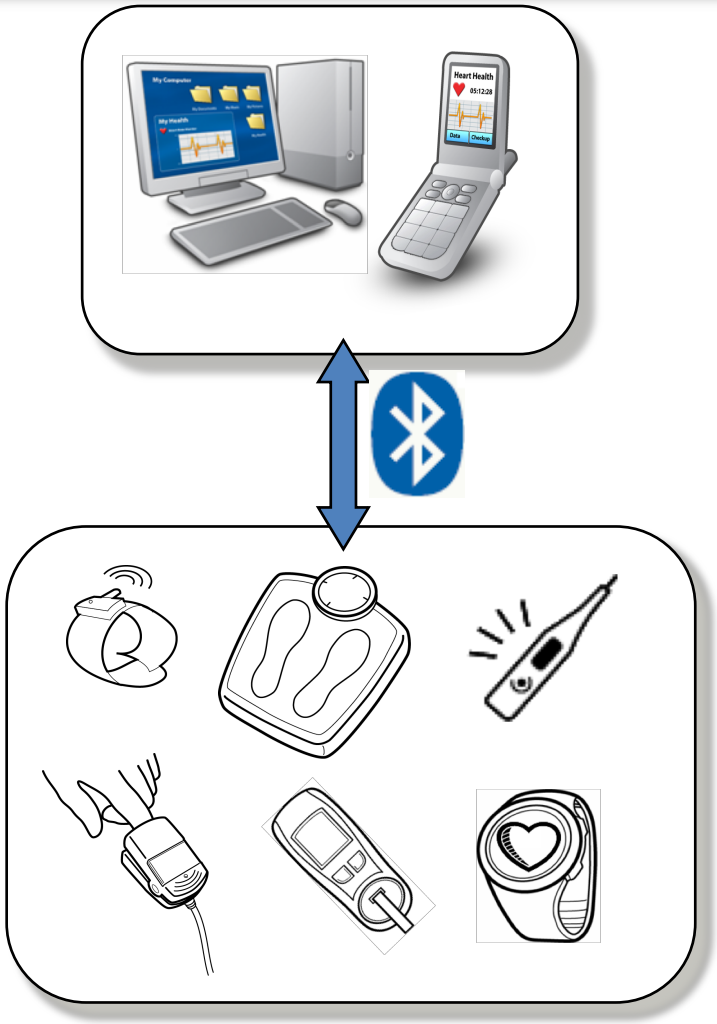
It builds on the underlying capabilities of the Bluetooth standard, which include:

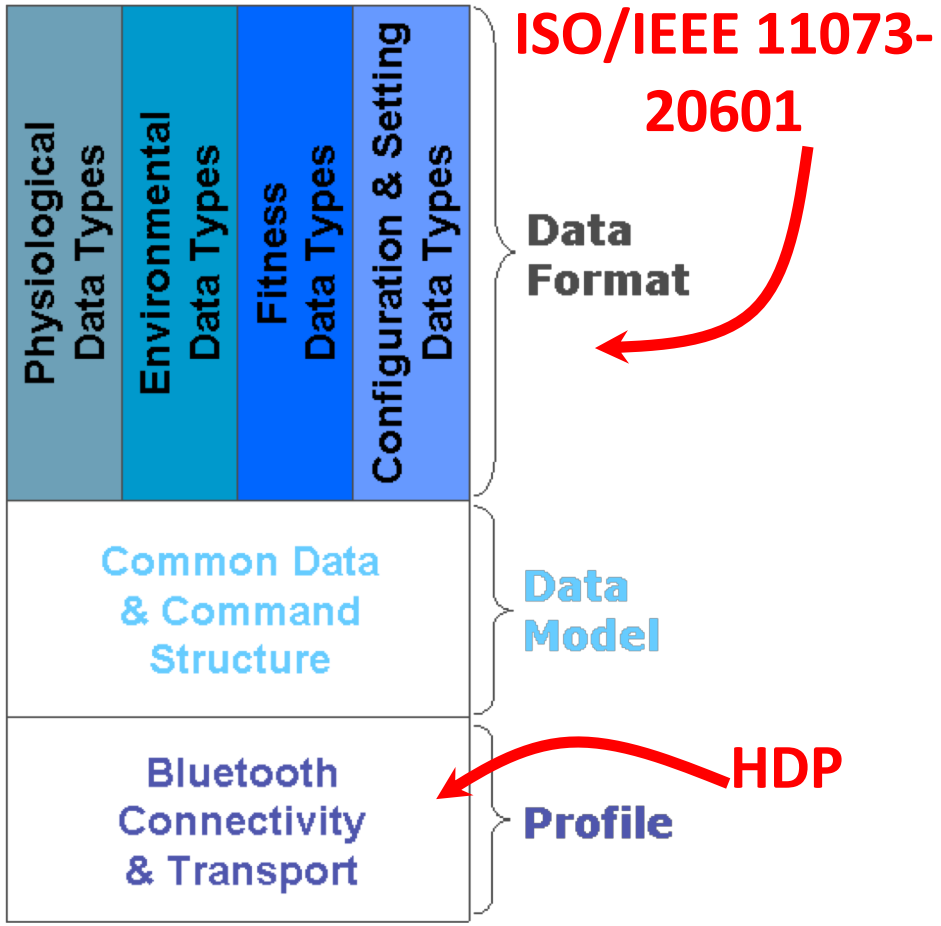
- excellent resistance to interference from wireless LANs, through the use of adaptive frequency hopping
- best-in-class security, including immunity from “man-in-the-middle” attacks, by utilizing public key cryptography
- low power consumption (devices frequently enter low power sleep states)
- a rigorous qualification program to ensure interoperability
- excellent range – up to 1km range products are available
- global applicability, using the 2.4GHz band
- low cost

Device Standards

- **IEEE11073** is a standard that describes how data is represented by medical devices and how these devices connect to each other
- Real-time: data from multiple devices can be retrieved, time correlated, displayed, and processed in fractions of a second
- Plug-and-play: devices detect, configure, and communicate without human interaction

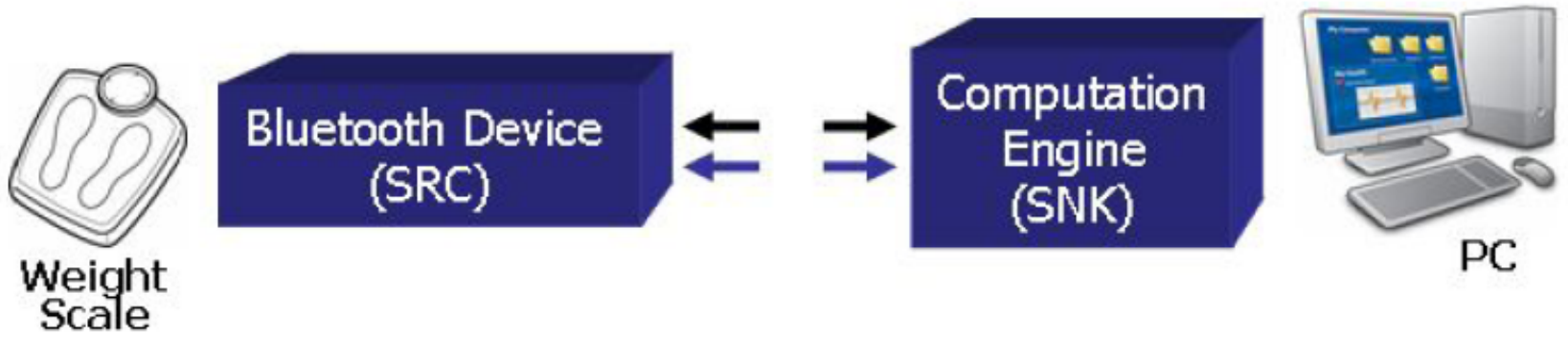
Bluetooth Health Device Profile





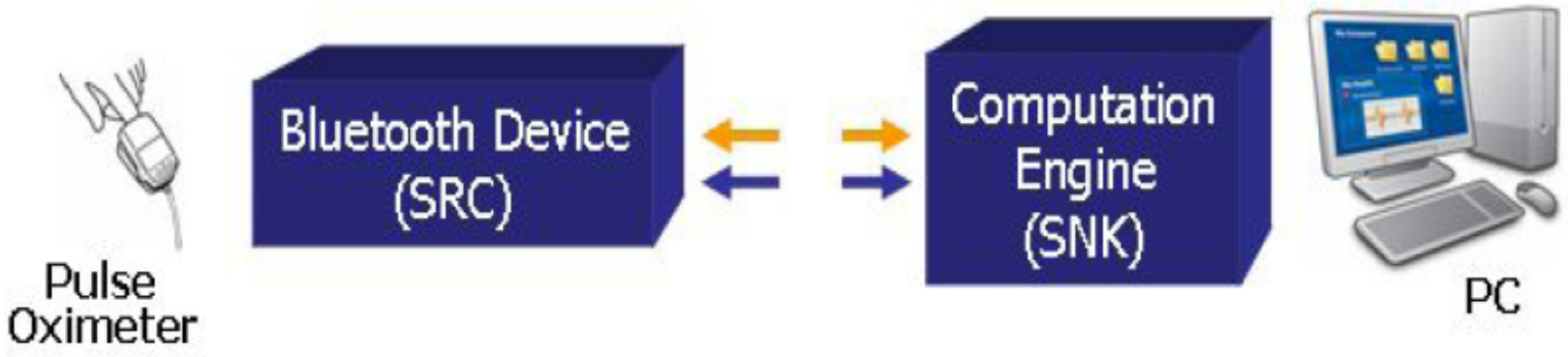
Configurations

SCENARIO 1: NON-STREAMING DATA



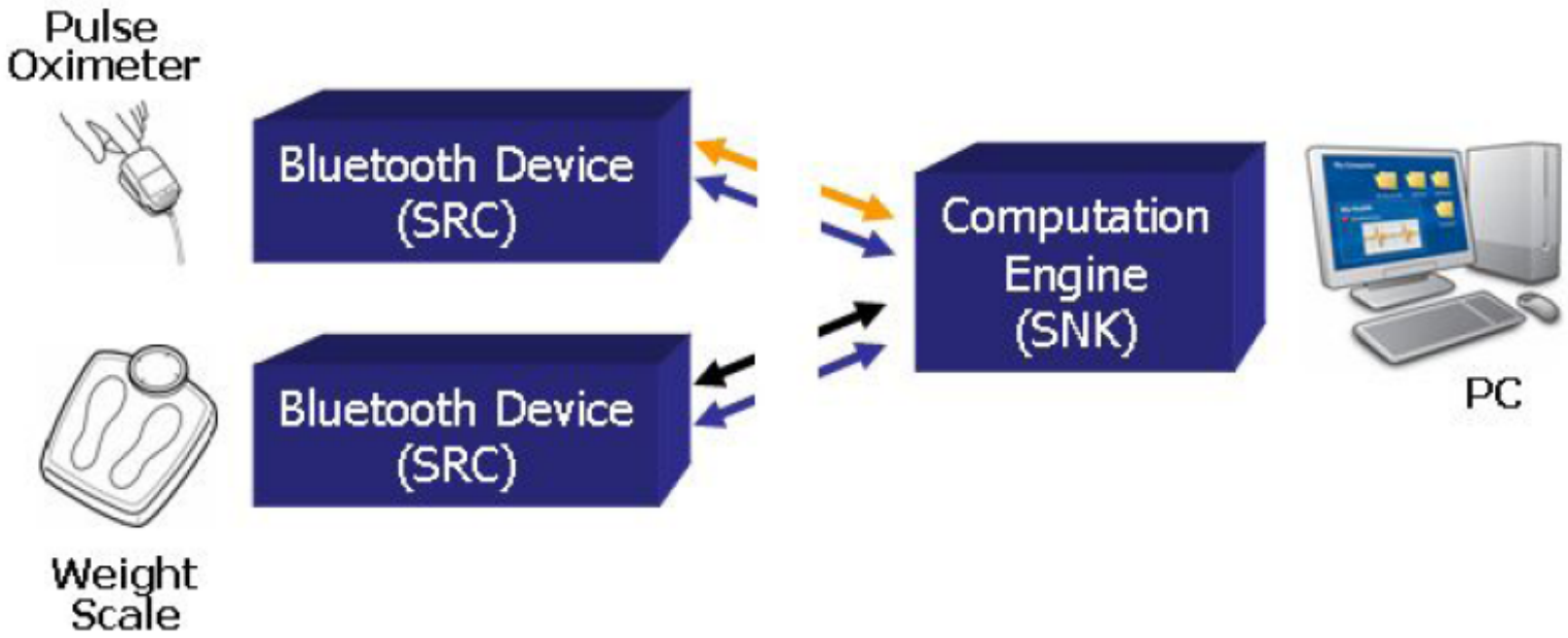
Configurations

SCENARIO 2: STREAMING DATA



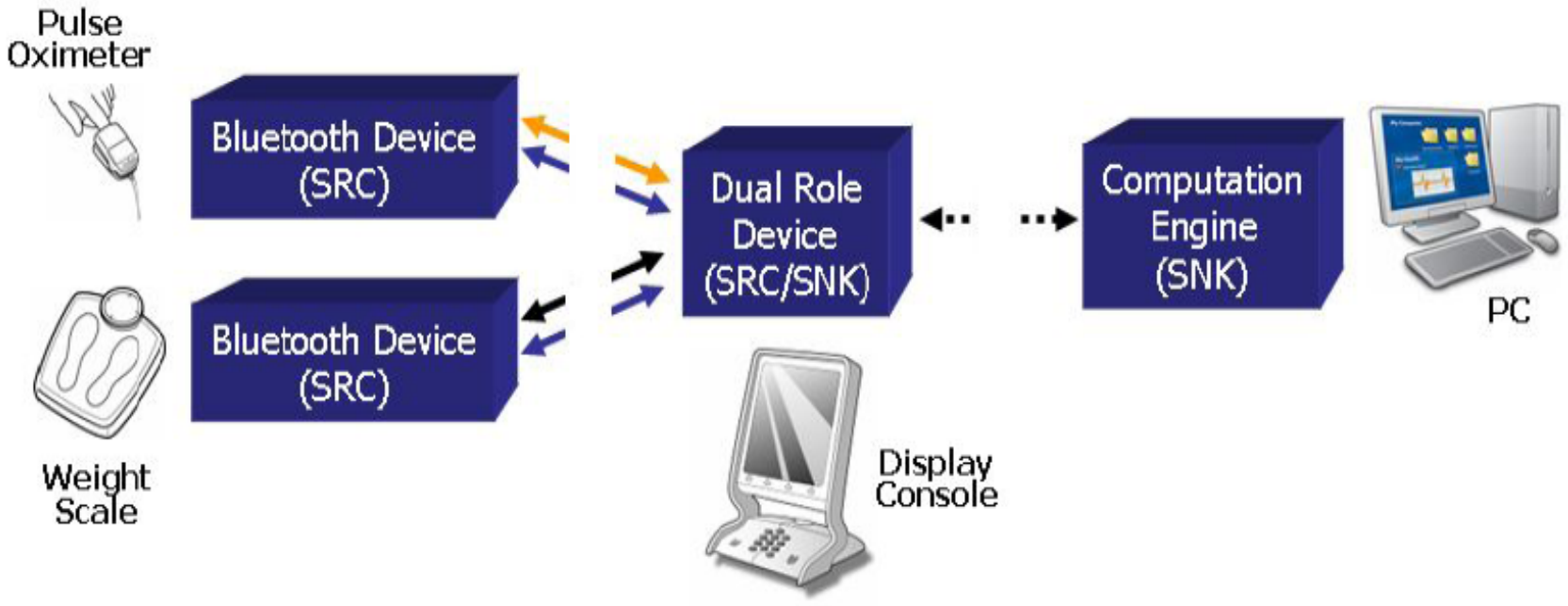
Configurations

SCENARIO 3: CONCURRENT STREAMING AND NON-STREAMING DATA



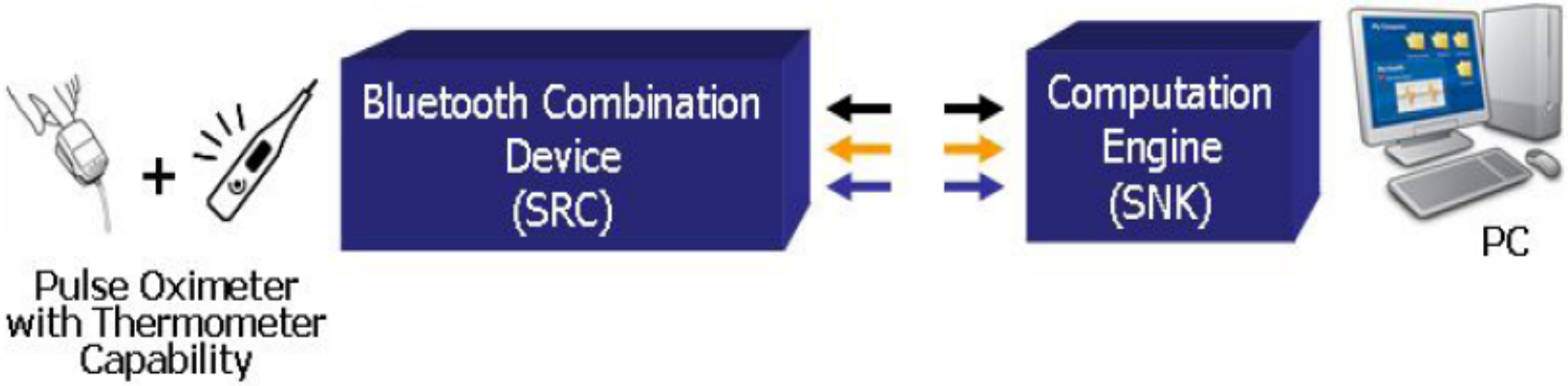
Configurations

SCENARIO 4: DUAL ROLE DEVICE



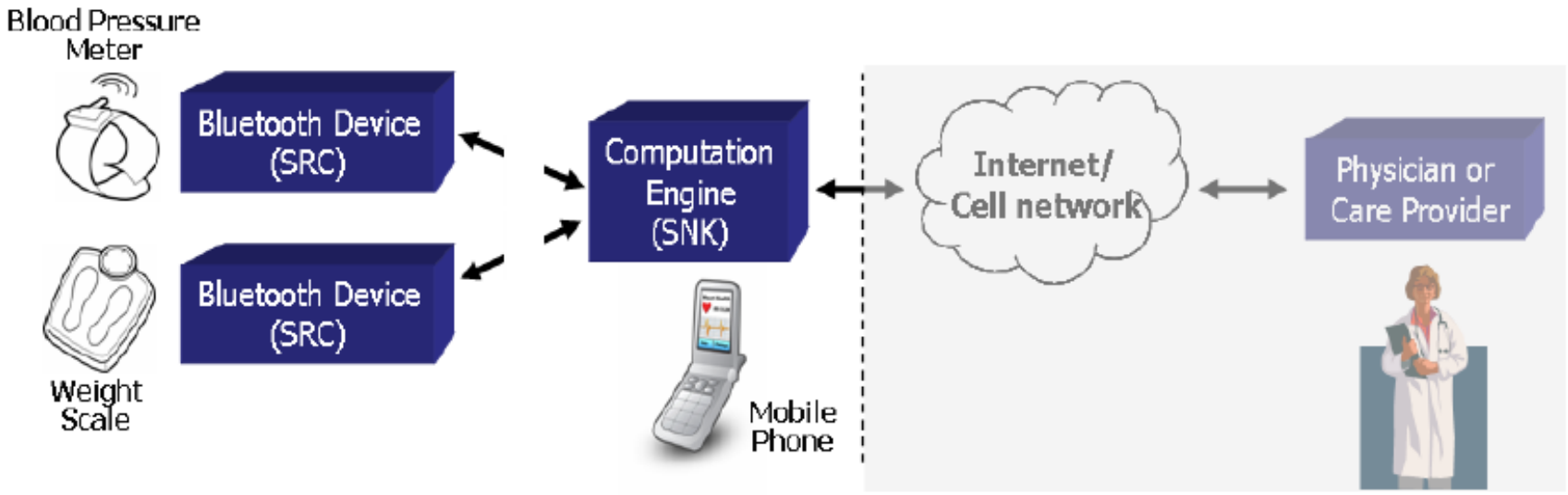
Configurations

SCENARIO 5: COMBINATION DEVICE



Configurations

SCENARIO 6: SHARING OF DATA WITH REMOTE CARE PROVIDER



Not Part of Profile Spec, but requires coordination with other standards bodies

ZigBee

- IEEE 802.15.4 (similar to Bluetooth and IEEE 802.15.1)
- Pushed by Chipcon (now TI), Ember, Freescale (Motorola), Honeywell, Mitsubishi, Motorola, Philips, Samsung…
- More than 260 members
  - about 15 promoters, 133 participants, 111 adopters
  - must be member to commercially use ZigBee spec
- ZigBee platforms comprise
  - IEEE 802.15.4 for layers 1 and 2
  - ZigBee protocol stack up to the applications

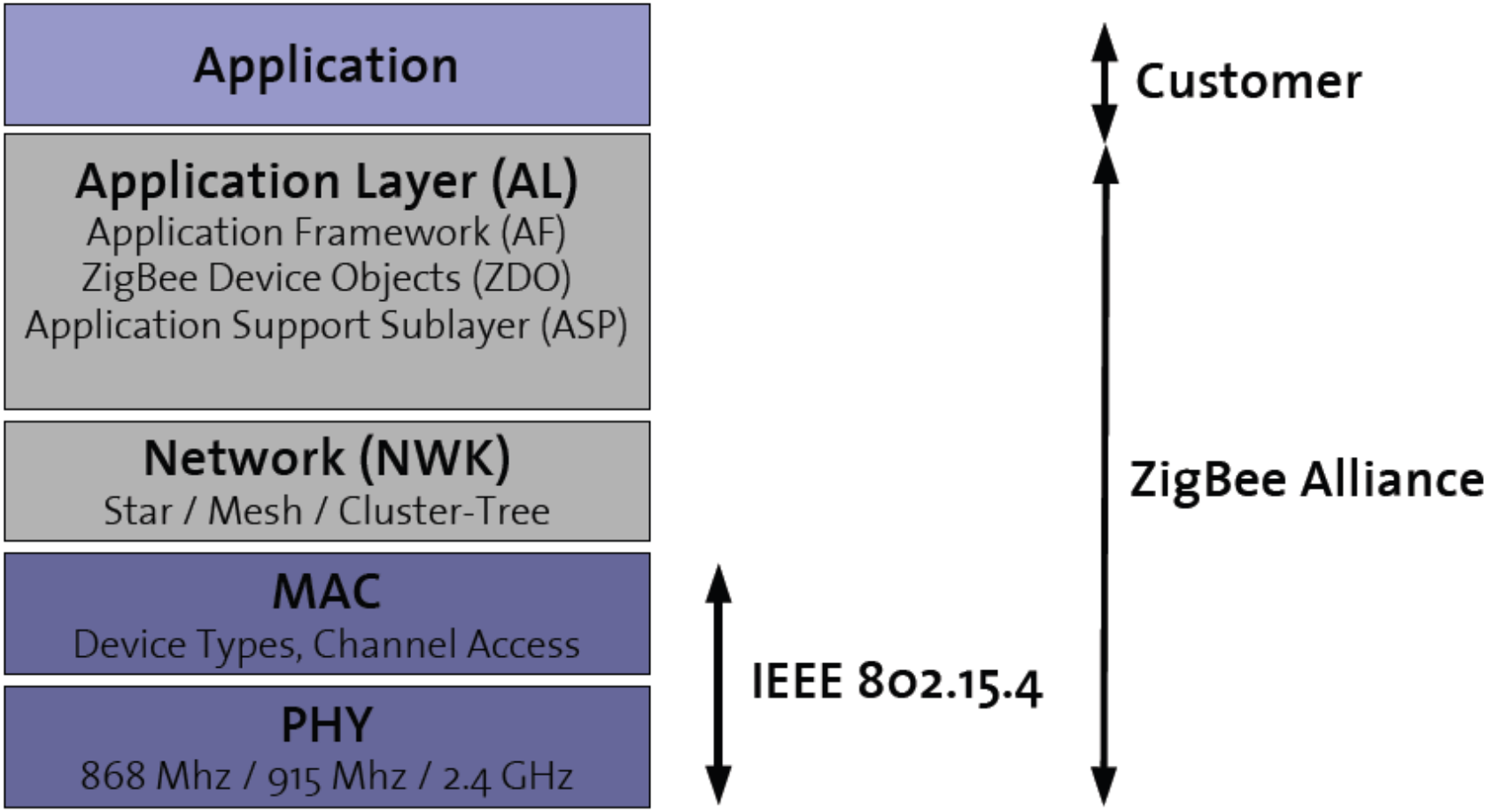
ZigBee

- Design goal
  - Low power consumption
  - Simple Design
  - Low cost
- History
  - ZigBee-style networks began ~1998
  - IEEE 802.15.4 was first completed in 2003
  - ZigBee Alliance was established in 2002

ZigBee Core Market

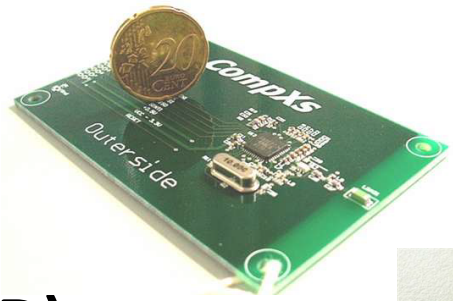
- **Industrial and Commercial**
  - Monitors
  - Movement sensors
  - Automation
- **Personal Healthcare**
  - Patient monitors
  - Remote diagnosis
  - Data loggers
- **Building Automation**
  - Security
  - Lighting
  - Fire and safety systems
- **Automotive**
  - Service controls
  - Inventory tracking

ZigBee Protocol Stack

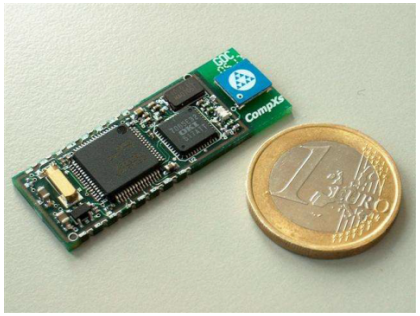


Device Type

- **Full Function Device (FFD)**
  - Network router function
  - Any topology

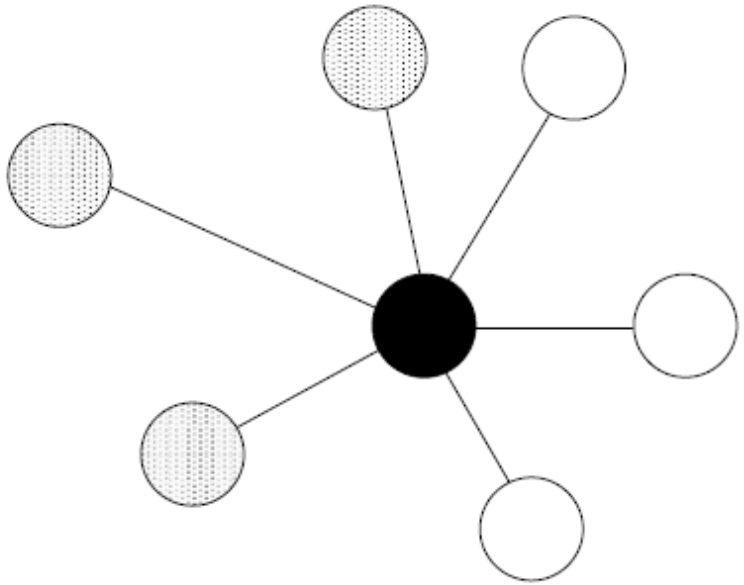


- **Reduced Function Device (RFD)**
  - Easy and cheap to implement
  - Limited to star topology



- **Personal Area Network (PAN) Coordinator**
  - Maintains overall network knowledge
  - Needs most memory and computing power

Basic Topology



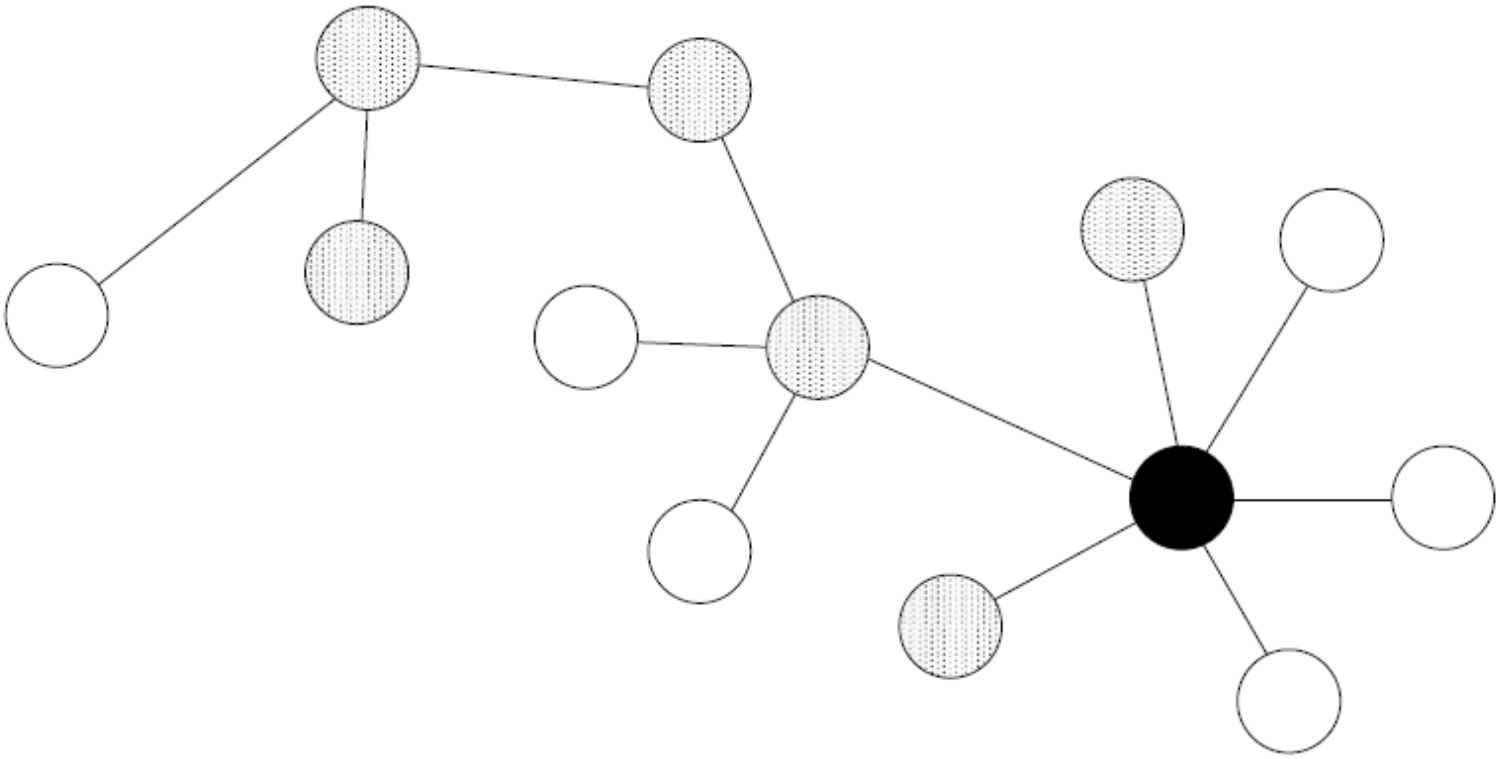
Star Network

RFD / EndPoint

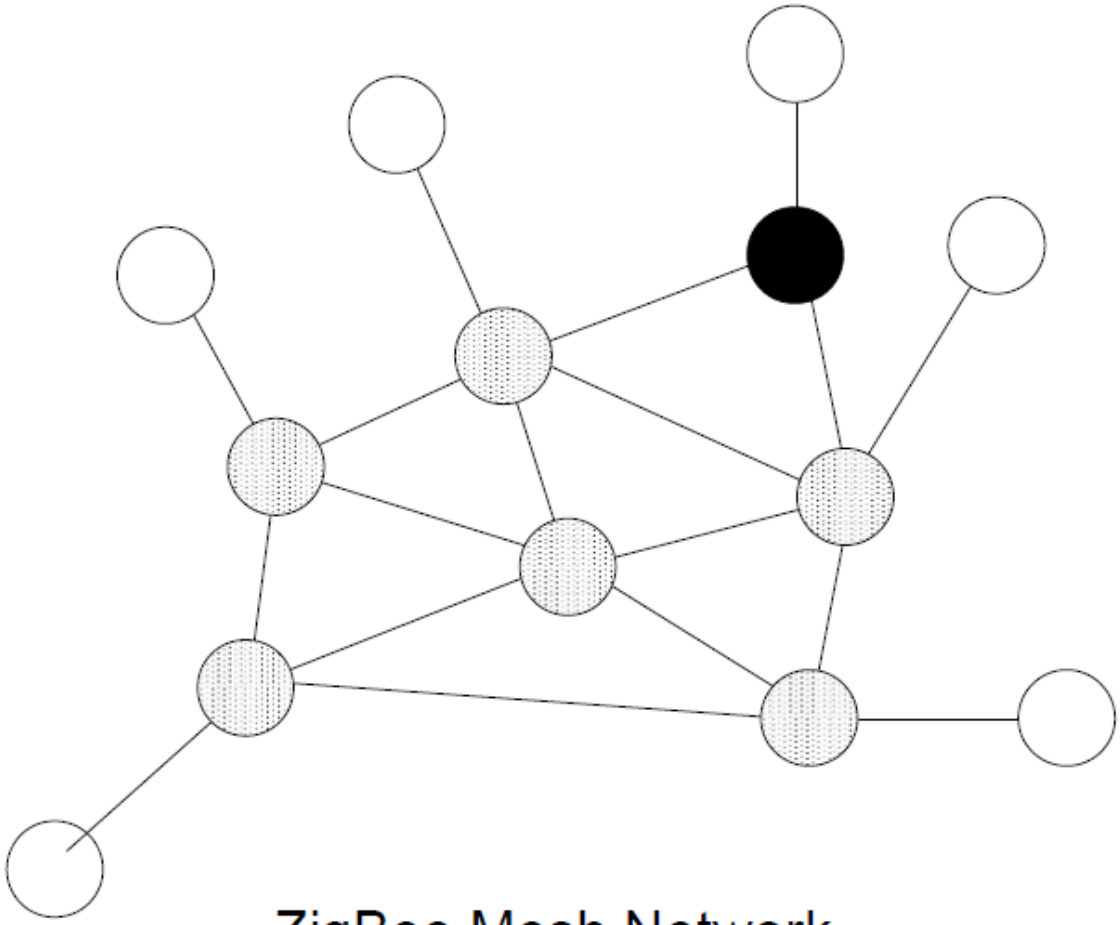
FFD / Router

Coordinator

Cluster Tree Network



ZigBee PRO: Mesh Network



ZigBee Mesh Network

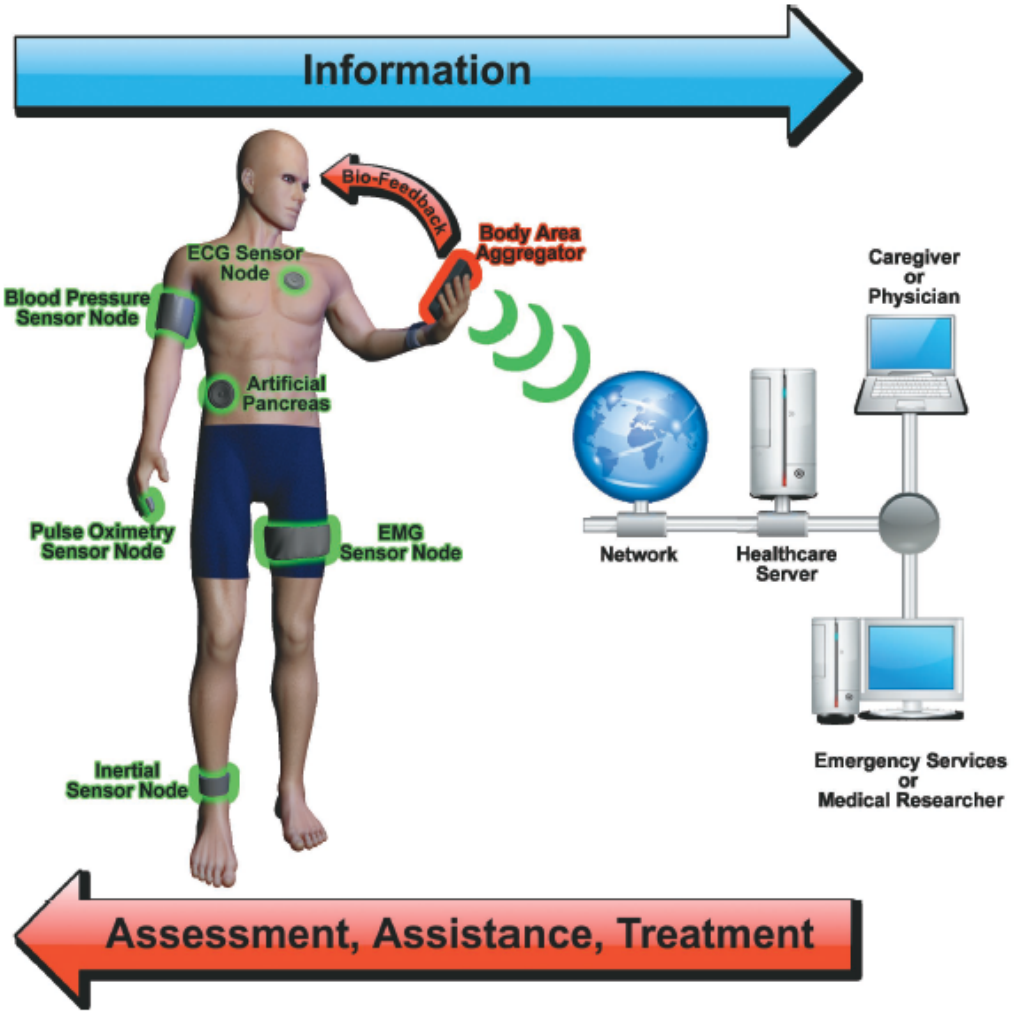
Comparison

Technology	Classic *Bluetooth* technology (BR/EDR)[1]	*Bluetooth* low energy technology[2]	ZigBee
Radio Frequency	2.4 GHz	2.4 GHz	2.4 GHz
Distance / Range	10 to 100 meters[3]	10 to 100 meters[3]	10 to 200 meters[4]
Over the air Data Rate	1-3Mbps	1Mbps	250kbps at 2.4 GHz.
Application Throughput	0.7-2.1 Mbps	0.2 Mbps	<0.1 Mbps
Nodes/Active Slaves	7 / 16777184[5]	Unlimited[6]	65535[7]
Security	64b/128b and applications layer user defined	128b AES and application layer user defined	128b AES and application layer user defined
Robustness	Adaptive fast frequency hopping, FEC, fast ACK	Adaptive fast frequency hopping	DSSS, Uses only 16 ch. in ISM band, optional mesh topology has long recovery time
Latency (from a non connected state)			
Total time to send data (det.battery life)[8]	100ms	<3ms	<10ms
Government Regulation	Worldwide	Worldwide	Worldwide
Certification Body	Bluetooth SIG	Bluetooth SIG	ZigBee Alliance
Voice capable	Yes	No	No
Network topology	Scatternet	Star-bus	Star or Mesh
Power Consumption	1 as the reference	0.01 to 0.5(depending on use-case)	2 (router) / 0.1 (end point)
Peak current consumption (max 15 mA to run on coin cell battery)	<30 mA	<15 mA	<15 mA
Service discovery	Yes	Yes	No
Profile concept	Yes	Yes	Yes
Primary Use Cases	Mobile phones, gaming, headsets, stereo audio streaming, automotive, PCs, consumer electronics, etc.	Mobile phones, gaming, PCs, watches, sports & fitness, healthcare, automotive, consumer electronics, automation, industrial, etc.	Fixed location industrial, building & home automation, AMI/SmartEnergy

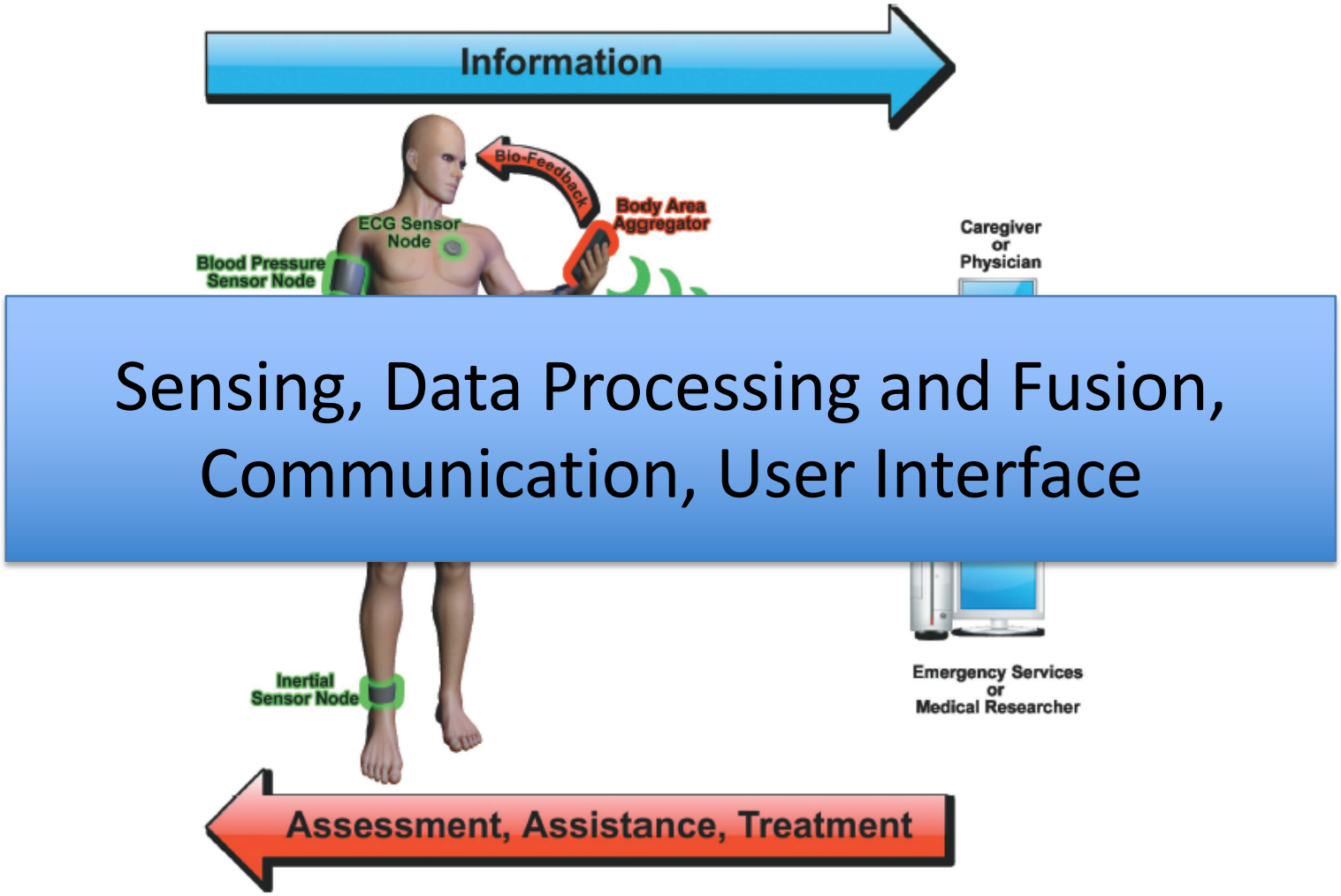
MICS

- Medical Implant Communication Service
  - 402-405MHz
  - Low power (25μW): reduce interference with other users
  - Low data rate
  - Couple of meters range (transceiver doesn't have to touch skin)

Body Area Sensor Network (BASN)



Key Components of BASN?

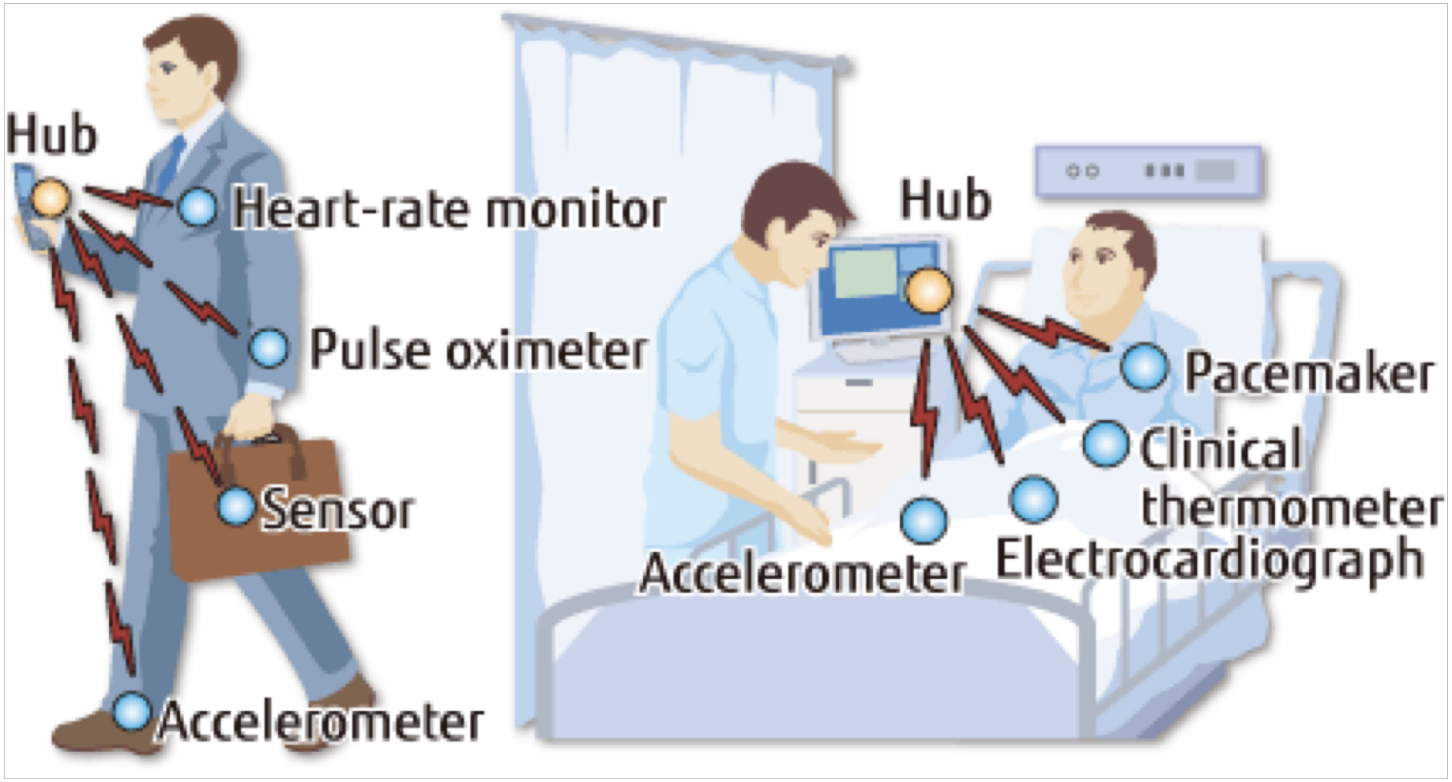


BASN Features

- **Extremely noninvasive**
  - Social acceptance
- **Tiny in size**
  - Small battery, limited resources, tradeoffs between energy and fidelity
- **Packaging and placement**
  - Neither prominent nor uncomfortable
- **Amortize nonrecurring costs**
  - Either significant volume in a single app or aggregate volume across apps
- **Emphasis on “value to user”**
  - Useful apps that deliver valuable information to users

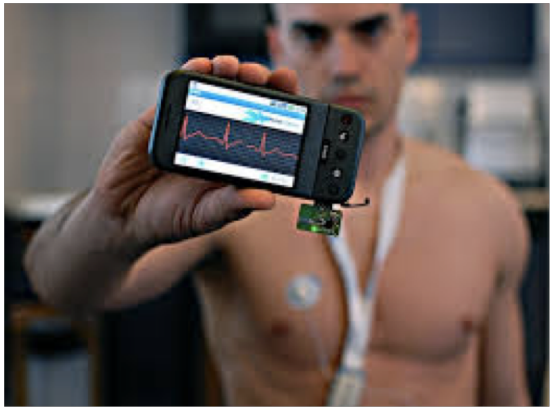
BASN Application Areas

- Healthcare Applications



BASN Application Areas

- Fitness Applications

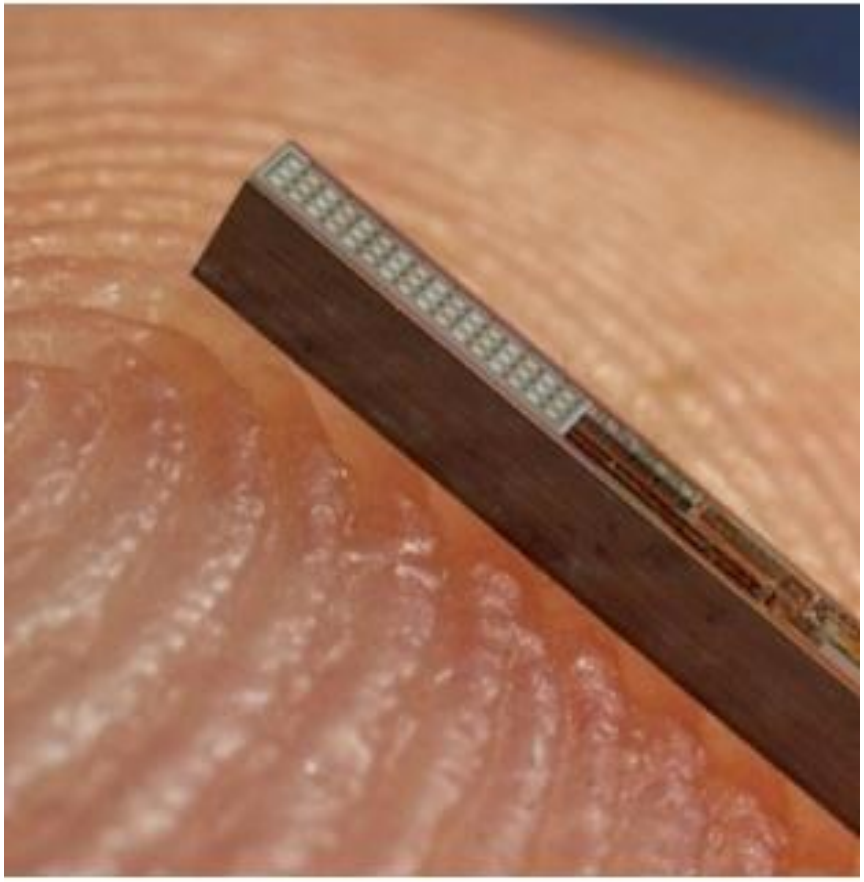


BASN Application Areas

- Entertainment Applications

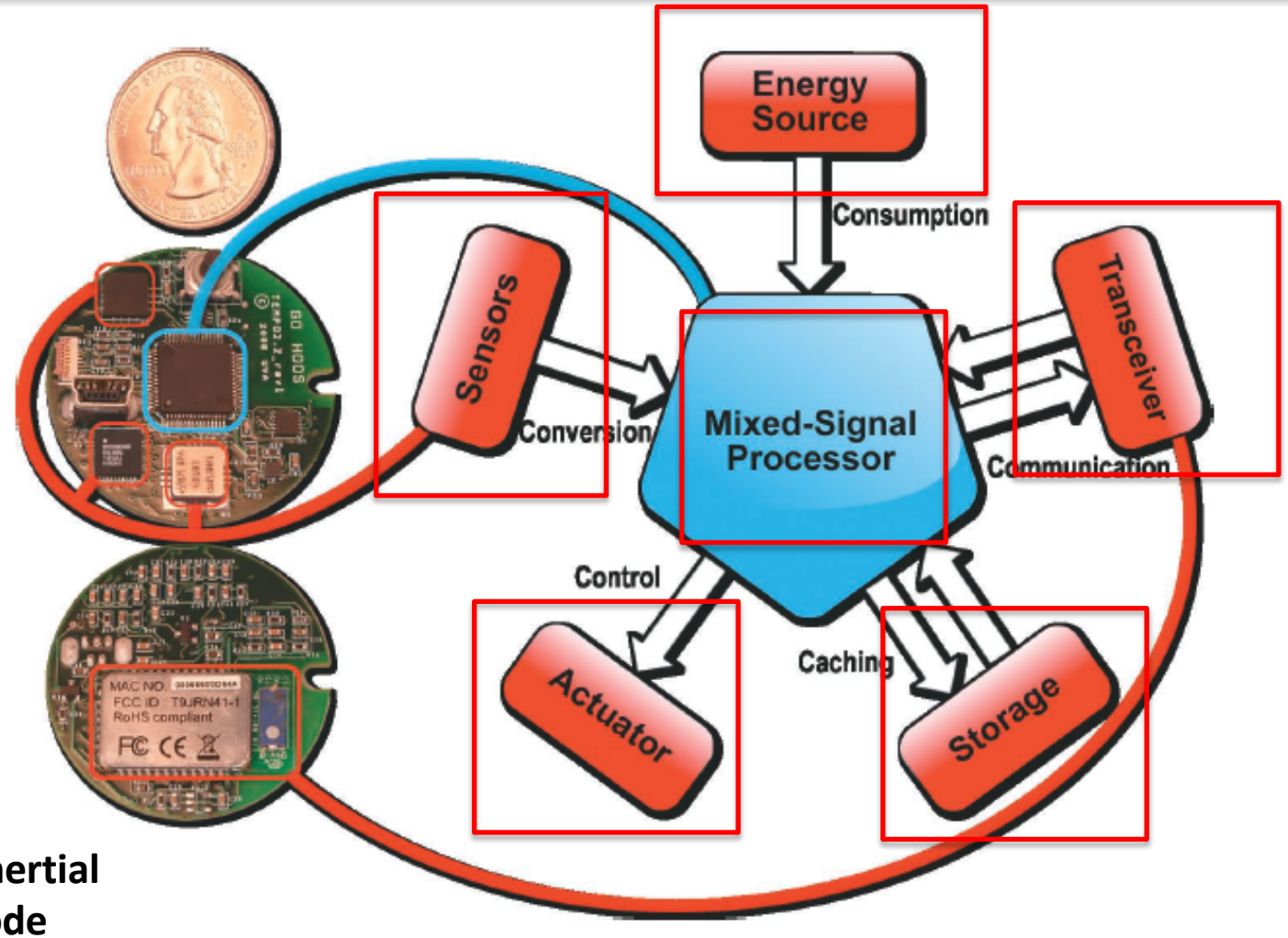
WBAN Sensors

In-Body Sensors



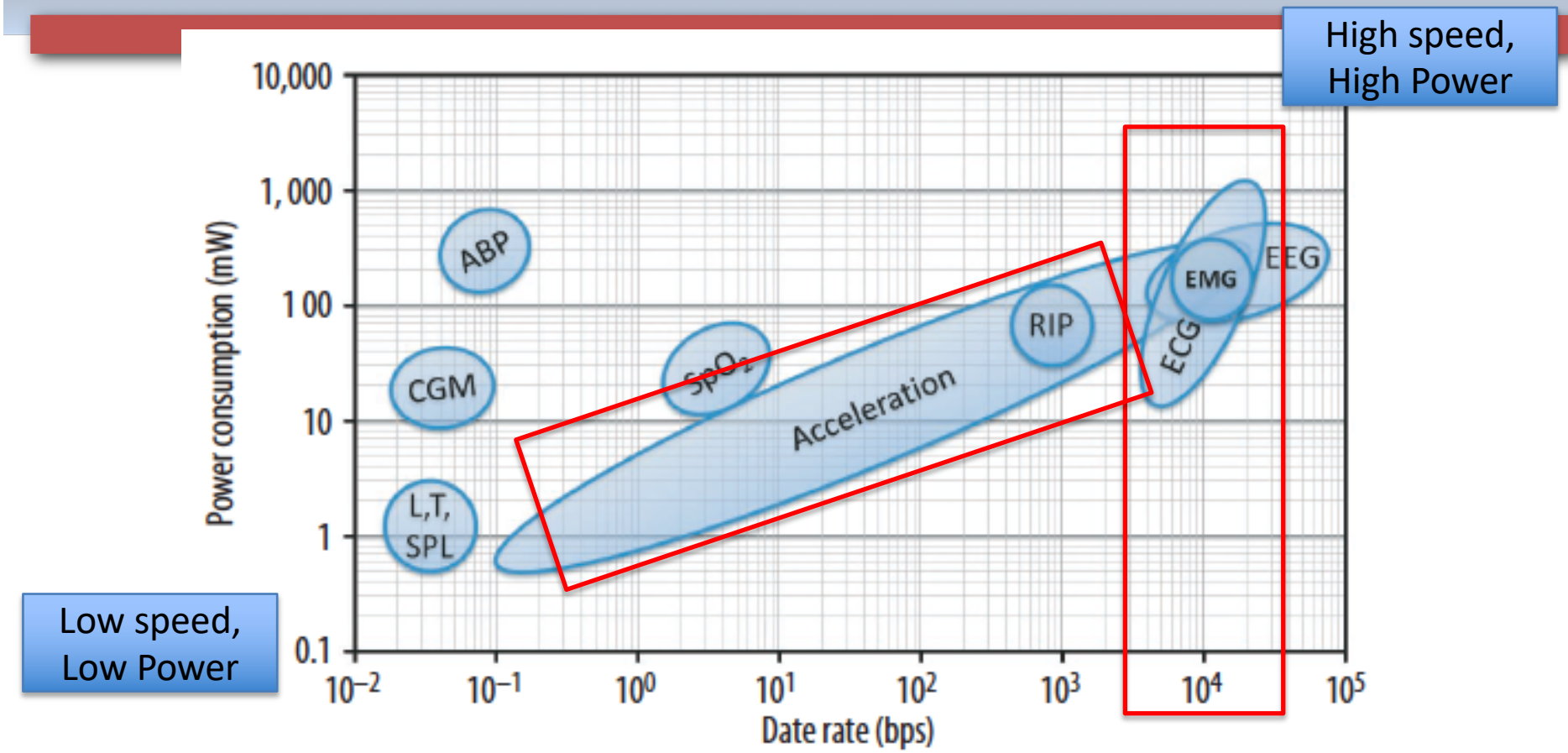
On-Body Sensors

BASN Components: Sensors



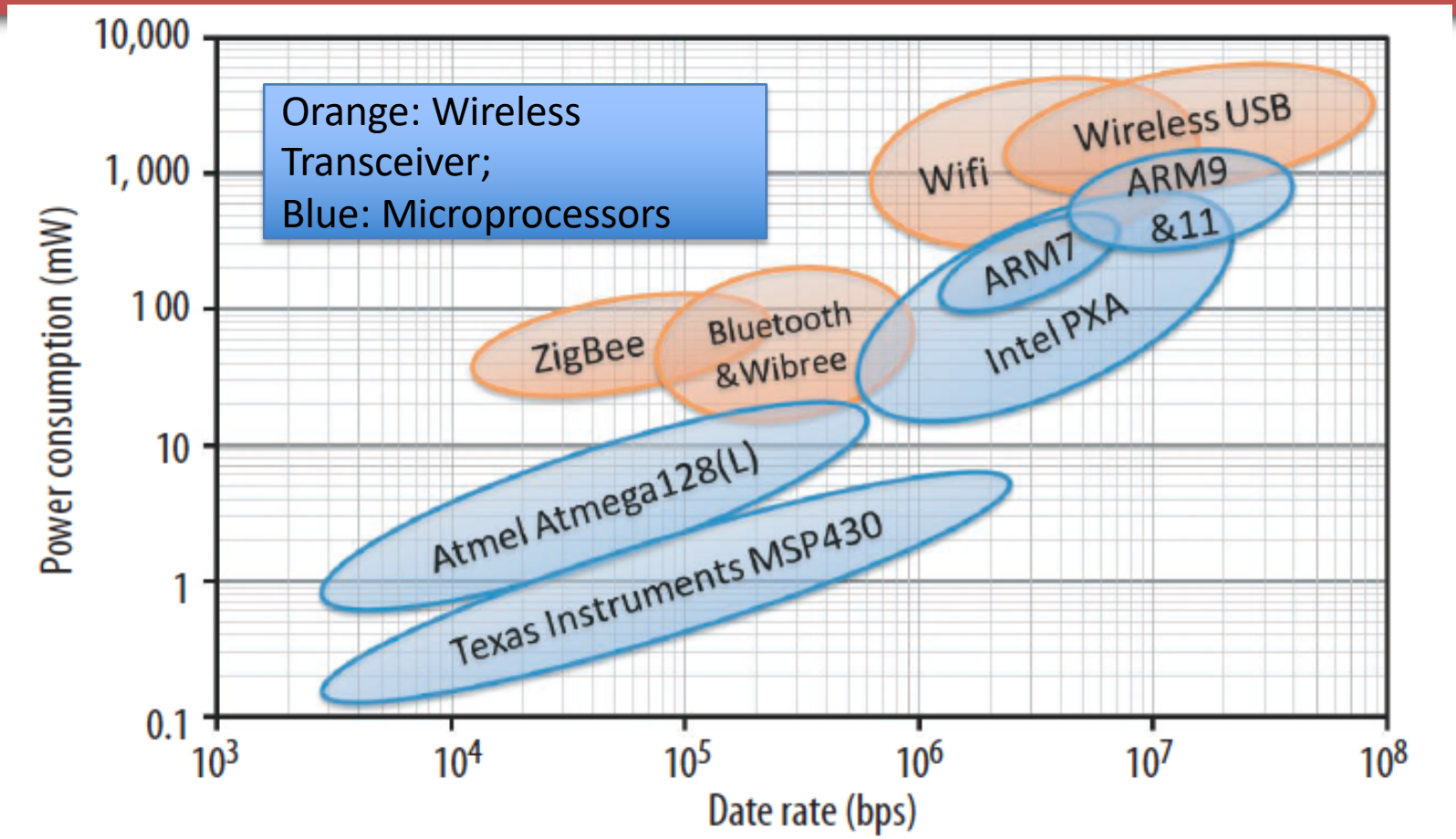
TEMPO inertial sensor node (UVA)

BASN Components: Sensors



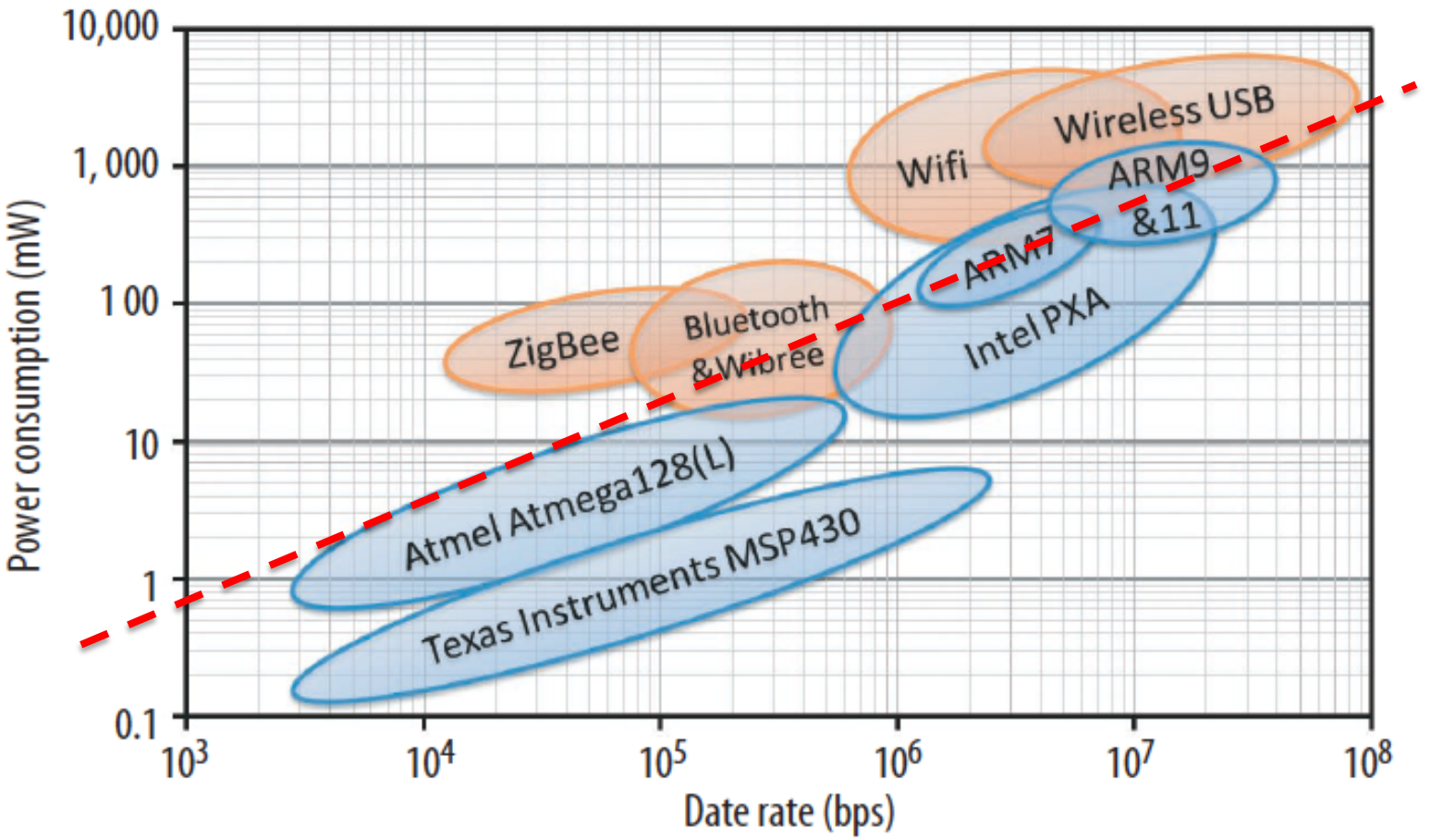
ABP: ambulatory blood pressure; **CGM:** continuous glucose monitoring;
L, T, SPL: light, temperature, sound pressure level;
SpO2: pulse oximetry; **RIP:** respiratory inductive plethysmography;
ECG: electrocardiography; **EMG:** electromyography;
EEG: electroencephalography.

BASN Components: Signal Processing



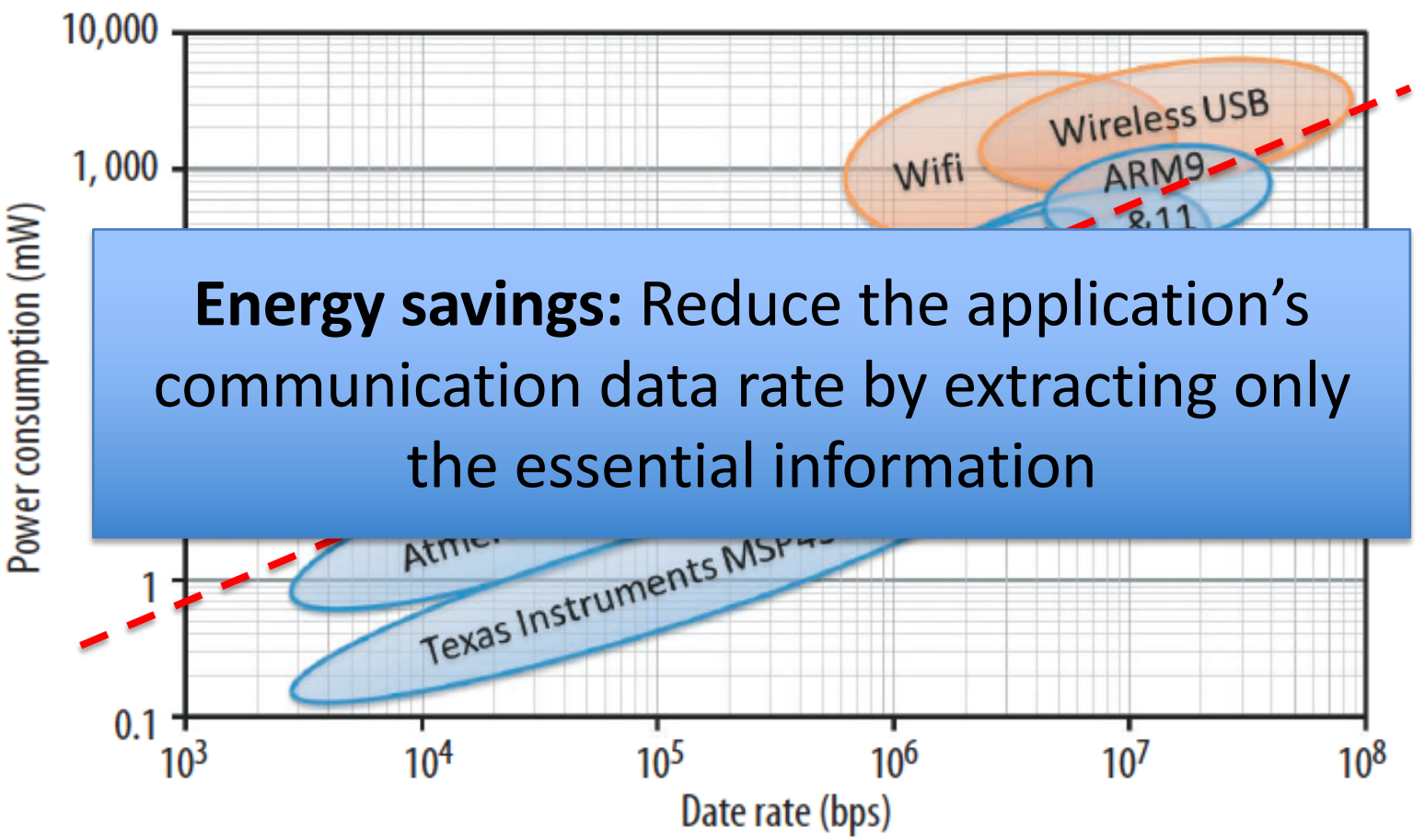
Q: What interesting observations can you get from this figure?

BASN Components: Signal Processing



Processing data at given rate consumes less power on average than transmitting the data

BASN Components: Signal Processing



Energy savings: Reduce the application's communication data rate by extracting only the essential information

Tradeoff: On-node Data Processing vs Wireless Communication

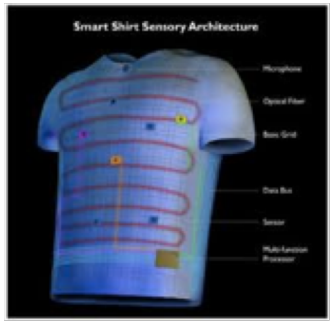
BASN Components: Communication

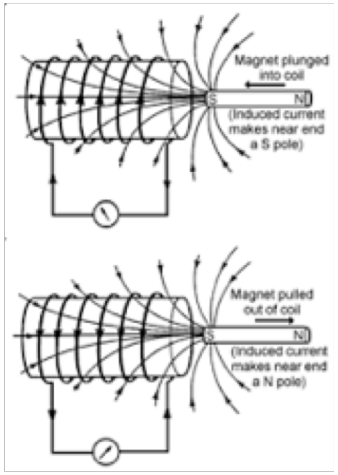
- Essential for node coordination
- Restrict the communication radius to the body's periphery
- RF channels: 850 MHz-2.4 GHz
- What are some key challenges of node communication in BASN?
- Big problem of **"body shadowing"**
  - Body's line of sight absorption of RF energy
  - Movements cause highly variable path

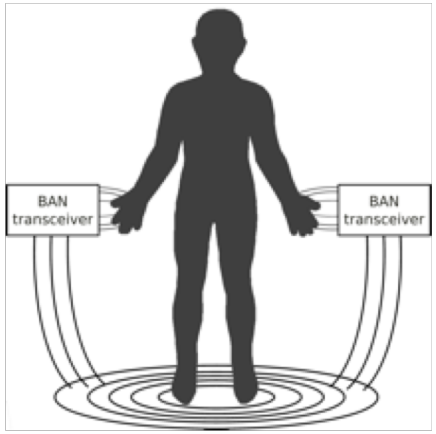
BASN Components: Communication

New/future communication methods:

- **Smart textiles**
  - Embed wires in clothing
- **Magnetic induction**
  - Use near field effect to communicate
- **Body-coupled communication**
  - Use human body as a channel
  - Highly stable, low energy
  - Safety is critical







Routing Related Characteristics

- **Bandwidth**
  - The available bandwidth is limited, shared, and can vary due to fading, noise, and interference. As a result, the overhead generated by the protocol should be limited.
- **Energy Sensitive**
  - The nodes that form the network can be very heterogeneous in terms of available energy or computing power.
- **Health Concerns**
  - An extremely low transmit power per node is needed to minimize interference to cope with health concerns and to avoid tissue heating.
- **Relative Mobility**
  - The devices are located on the human body that can be in motion. WBANs should therefore be robust against frequent changes in the network topology.

Routing Strategies in WBANs

- **Temperature Based Routing**
  - Avoid overheating (transmit power, paths)
- **Cluster Based Routing**
  - Spread energy dissipation

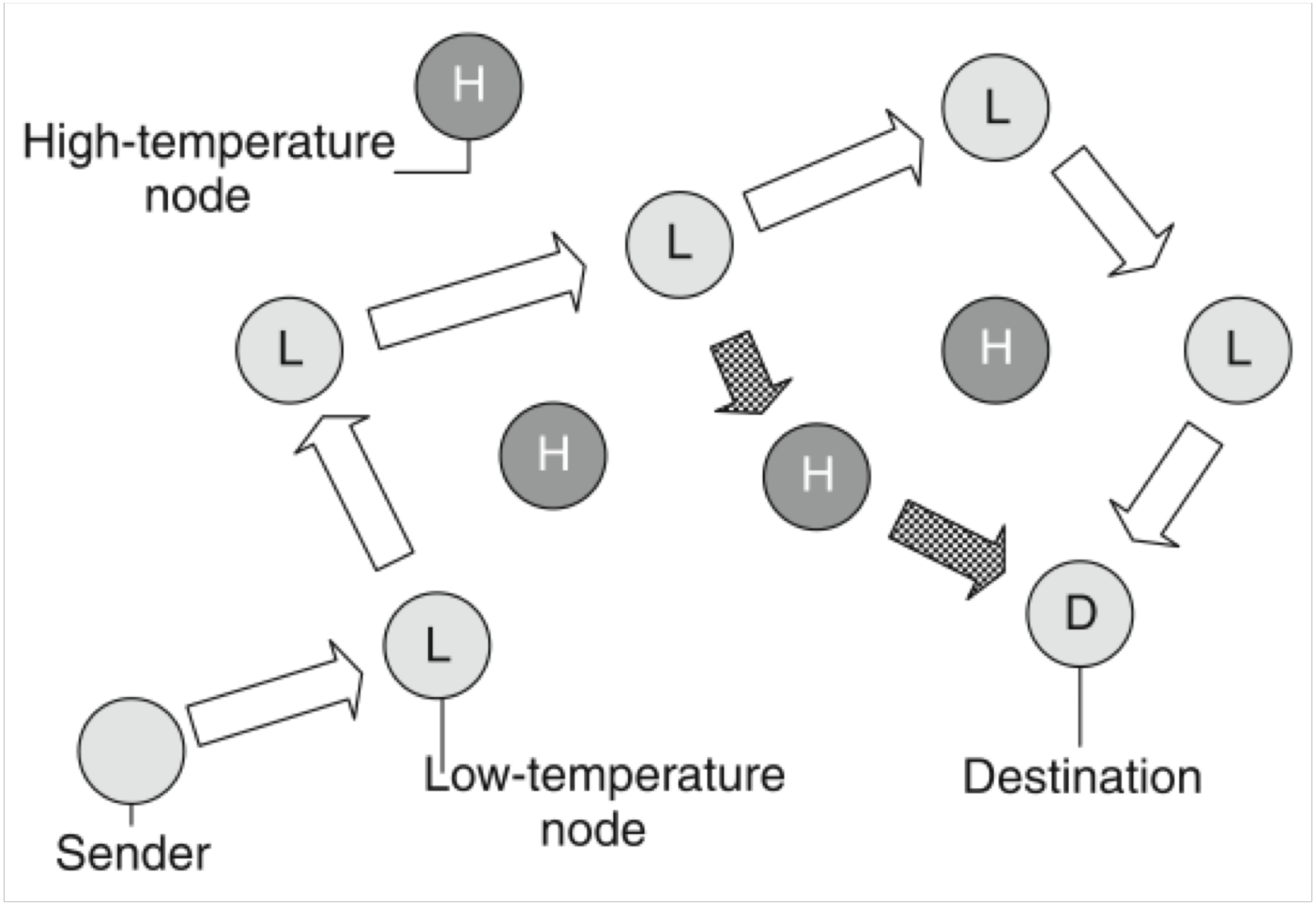
Thermal Aware Routing Algorithm (TARA)

- TARA
  - Routes data away from high temperature areas
  - Each node determines the current temperature of the neighbors by
    - Monitoring neighbors packet counts
    - Calculating the communication radiation and power consumption
  - If the temperature of a neighboring node > threshold
    - The packets will no longer be forwarded to the node but will be rerouted through alternate paths

Temperature Routing (cont.)

- Improvements of TARA are LTR and ALTR ((Adaptive) Least Temperature Routing)
  - Choose the neighboring node with the lowest temperature as the next hop for routing
  - Predefined maximum hop count is used
  - Loops are avoided by maintaining a list in the packet with the recently visited nodes
- Improvements of ALTR is Least Total Route Temperature (LTRT)
  - Selects the entire “least temperature route” instead of only considering the next hop

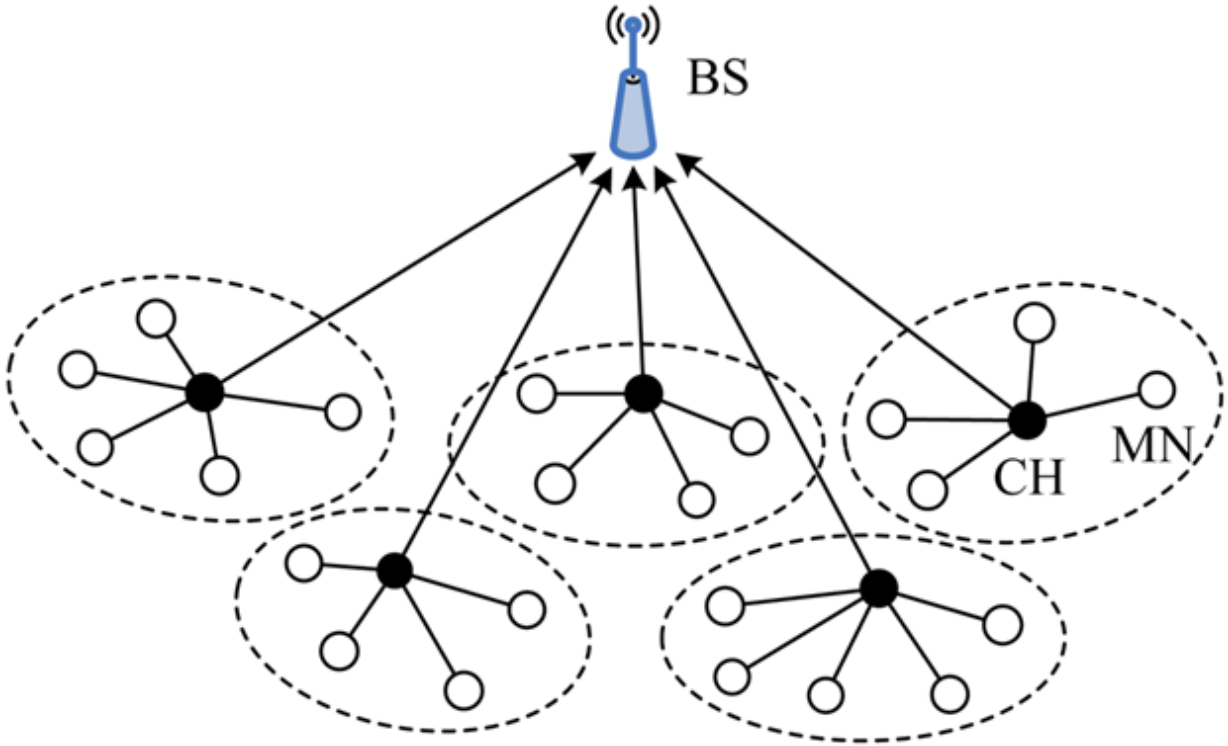
Temperature Routing (cont.)



Cluster Based Routing

- AnyBody (based on LEACH)
  - Randomly selects a cluster head at regular time intervals
  - Cluster head aggregates all data and sends data to a base station
  - Changes the cluster head selection and constructs a virtual backbone network of the cluster heads

Cluster Based Routing

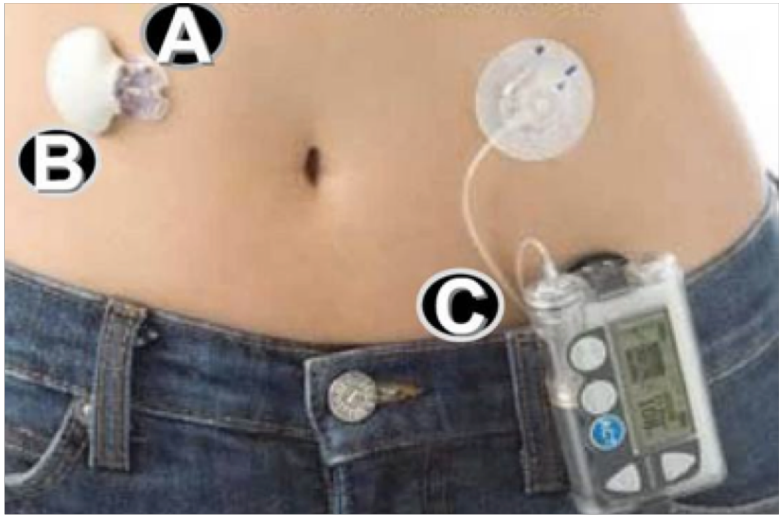


BASN Components: Storage

- **On-node storage:**
  - Low power nonvolatile storage
- **Cache data and wait for good channel conditions:**
  - Prolong battery life, decrease transmission error
- **Archive data for signal classification:**
  - Detect longitudinal trends (e.g., recovery from surgery)
  - Detect instantaneous events (e.g., falls)

BASN Components: Feedback Control

Prosthetics Devices



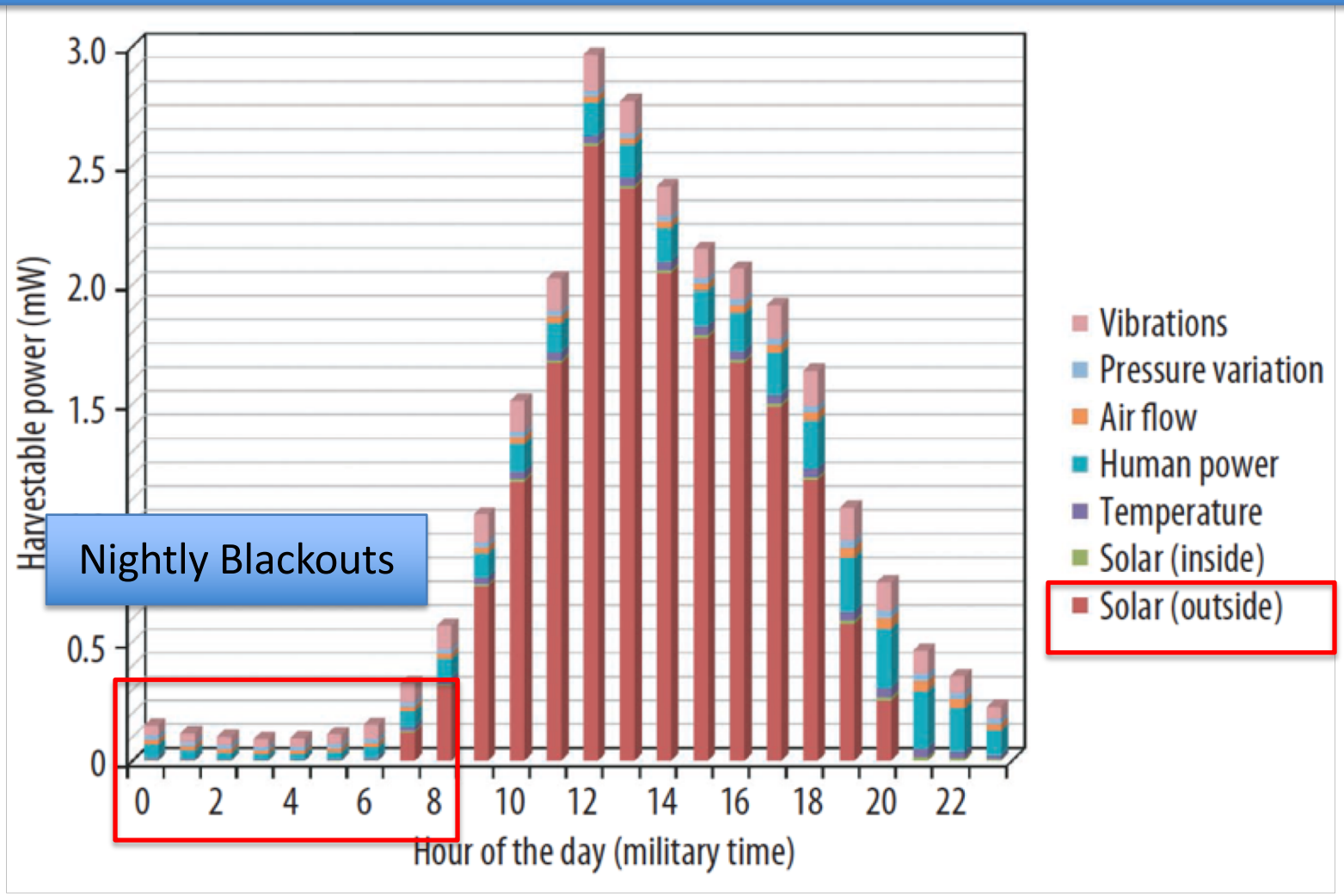
Diabetes Monitoring

EMG signals from the eyelid or jaw might be used to control prosthetics devices

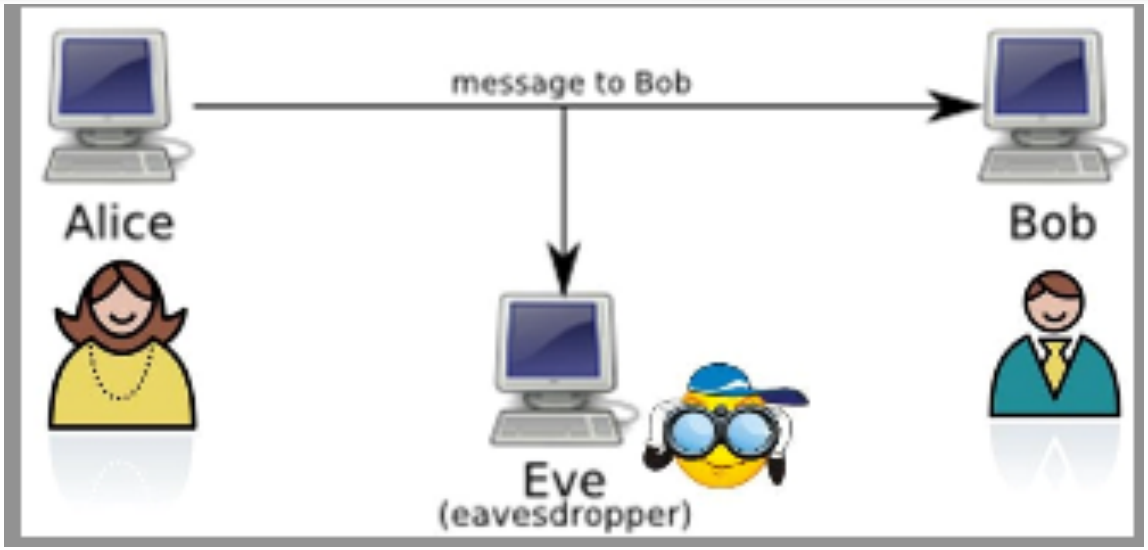
Use blood glucose measurements from biosensors to control insulin delivery

Energy Harvesting

Q: What can you observe from this figure?



Security in WBAN is CRUCIAL!



- “Shared” nature of wireless network; insecure channels
- Eve could break transmission
- More maliciously, Eve can modify the medical data
- Can lead to severe medical malpractice

Major security requirements	Description
Data storage security requirements	
Confidentiality	Patient-related data should be kept confidential during storage periods. Especially, its confidentiality should be robust against node compromise and user collusion.
Dynamical integrity assurance	Patient-related data must not be modified illegally during storage periods, which shall be checked and detected by a node dynamically.
Dependability	Patient-related data must be readily retrievable when node failure or data erasure happens.
Data access security requirements	
Access control (privacy)	A fine-grained data access policy shall be enforced to prevent unauthorized access to patient-related data generated by the WBAN.
Accountability	When a user of the WBAN abuses his/her privilege to carry out unauthorized actions on patient-related data, he/she should be identified and held accountable.
Revocability	The privileges of WBAN users or nodes should be deprived in time if they are identified as compromised or behave maliciously.
Non-repudiation	The origin of a piece of patient-related data cannot be denied by the source that generated it.
Other requirements	
Authentication	The sender of the patient-related data must be authenticated, and injection of data from outside the WBAN should be prevented.
Availability	The patient-related data should be accessible even under denial-of-service (DoS) attacks.

Open Questions

- What are the factors that will affect the widespread BASN adoption and diffusion (e.g., value, safety, privacy, compatibility, ease of use)?
- Who will be the stakeholders of BASN (e.g., users, emergency services, caregivers, researchers, etc.)?
- Who will pay for the BASN? Who will own the BASN data? How will access to data and information be granted? Who is liable for damages involving BASN?