Syllabus:
Smart Objects: The "Things" in IoT, Sensors, Actuator, and Smart Objects, Sensor Networks, Connecting Smart Objects, Communications Criteria, IoT Access Technologies.

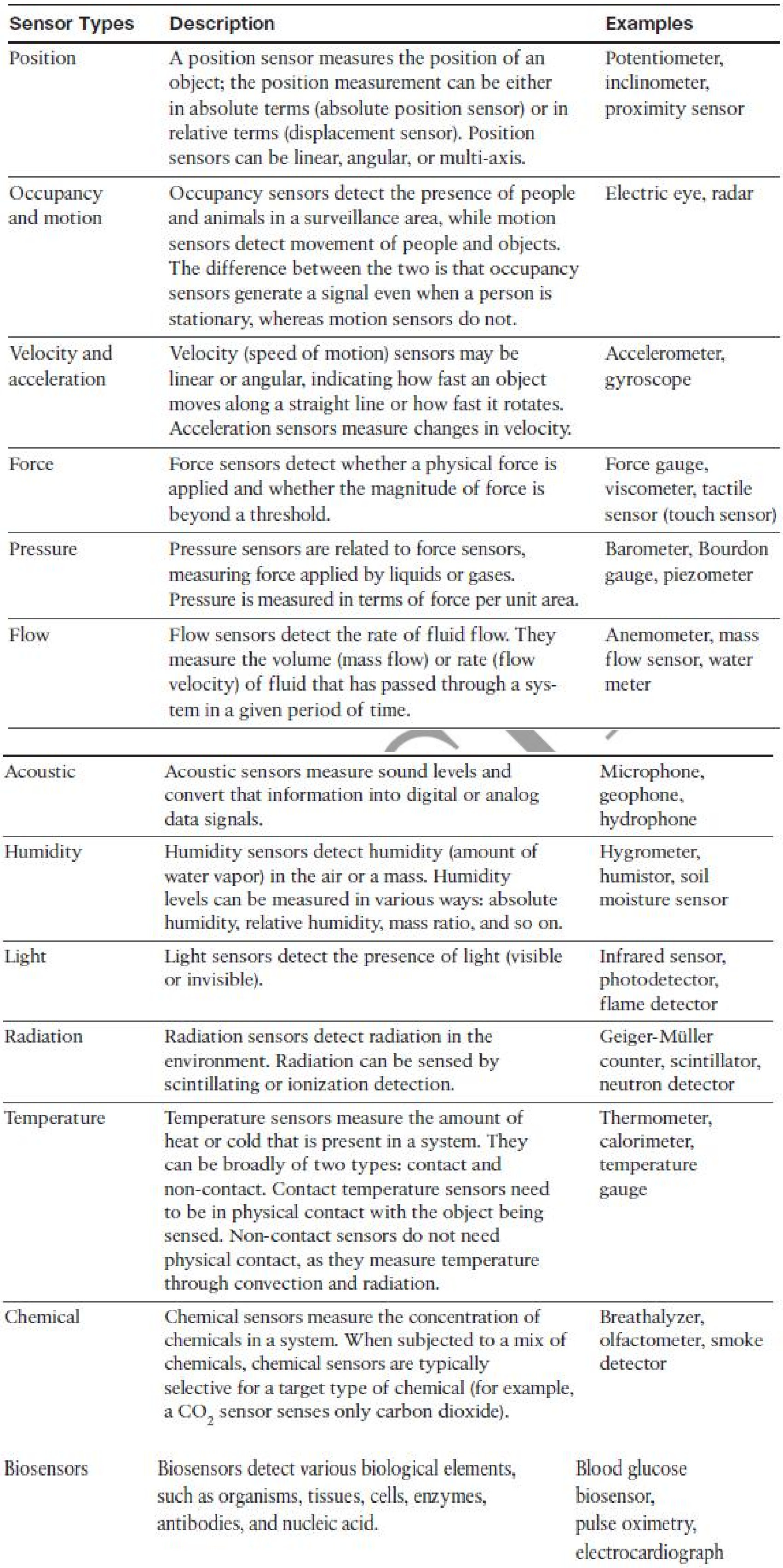
1. List and explain the number of ways to group and cluster sensors into different categories.

Answer: Ways to group and cluster sensors into different categories are:

- **Active or passive:** Sensors can be categorized based on whether they produce an energy output and typically require an external power supply (active) or whether they simply receive energy and typically require no external power supply (passive).
- **Invasive or non-invasive:** Sensors can be categorized based on whether a sensor is part of the environment it is measuring (invasive) or external to it (non-invasive).
- **Contact or no-contact:** Sensors can be categorized based on whether they require physical contact with what they are measuring (contact) or not (no-contact).
- **Absolute or relative:** Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).
- **Area of application:** Sensors can be categorized based on the specific industry or vertical where they are being used.
- **How sensors measure:** Sensors can be categorized based on the physical mechanism used to measure sensory input (for example, thermoelectric, electrochemical, piezo resistive, optic, electric, fluid mechanic, photo elastic
- **What sensors measure:** Sensors can be categorized based on their applications or what physical variables they measure.).

2. List and explain sensor types.

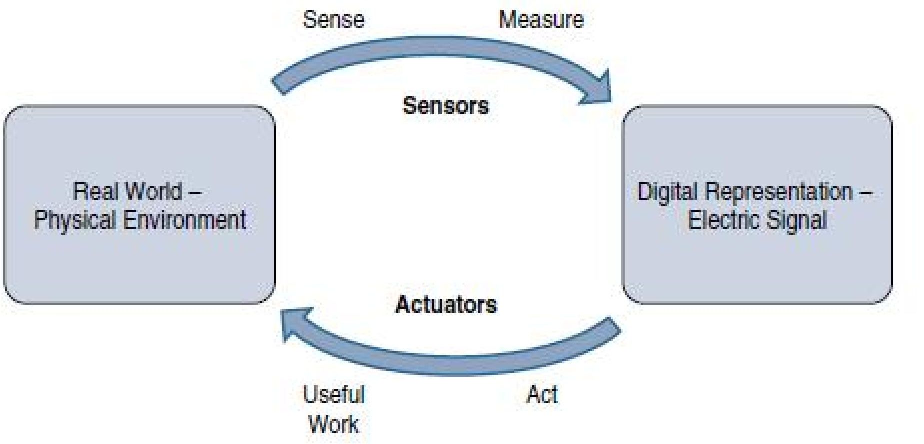
Answer:



Sensor Types	Description	Examples
Position	A position sensor measures the position of an object; the position measurement can be either in absolute terms (absolute position sensor) or in relative terms (displacement sensor). Position sensors can be linear, angular, or multi-axis.	Potentiometer, inclinometer, proximity sensor
Occupancy and motion	Occupancy sensors detect the presence of people and animals in a surveillance area, while motion sensors detect movement of people and objects. The difference between the two is that occupancy sensors generate a signal even when a person is stationary, whereas motion sensors do not.	Electric eye, radar
Velocity and acceleration	Velocity (speed of motion) sensors may be linear or angular, indicating how fast an object moves along a straight line or how fast it rotates. Acceleration sensors measure changes in velocity.	Accelerometer, gyroscope
Force	Force sensors detect whether a physical force is applied and whether the magnitude of force is beyond a threshold.	Force gauge, viscometer, tactile sensor (touch sensor)
Pressure	Pressure sensors are related to force sensors, measuring force applied by liquids or gases. Pressure is measured in terms of force per unit area.	Barometer, Bourdon gauge, piezometer
Flow	Flow sensors detect the rate of fluid flow. They measure the volume (mass flow) or rate (flow velocity) of fluid that has passed through a system in a given period of time.	Anemometer, mass flow sensor, water meter
Acoustic	Acoustic sensors measure sound levels and convert that information into digital or analog data signals.	Microphone, geophone, hydrophone
Humidity	Humidity sensors detect humidity (amount of water vapor) in the air or a mass. Humidity levels can be measured in various ways: absolute humidity, relative humidity, mass ratio, and so on.	Hygrometer, humistor, soil moisture sensor
Light	Light sensors detect the presence of light (visible or invisible).	Infrared sensor, photodetector, flame detector
Radiation	Radiation sensors detect radiation in the environment. Radiation can be sensed by scintillating or ionization detection.	Geiger-Müller counter, scintillator, neutron detector
Temperature	Temperature sensors measure the amount of heat or cold that is present in a system. They can be broadly of two types: contact and non-contact. Contact temperature sensors need to be in physical contact with the object being sensed. Non-contact sensors do not need physical contact, as they measure temperature through convection and radiation.	Thermometer, calorimeter, temperature gauge
Chemical	Chemical sensors measure the concentration of chemicals in a system. When subjected to a mix of chemicals, chemical sensors are typically selective for a target type of chemical (for example, a CO_2 sensor senses only carbon dioxide).	Breathalyzer, olfactometer, smoke detector
Biosensors	Biosensors detect various biological elements, such as organisms, tissues, cells, enzymes, antibodies, and nucleic acid.	Blood glucose biosensor, pulse oximetry, electrocardiograph

3. How Sensors and Actuators Interact with the Physical World. Explain

Answer:


Sense
Measure
Sensors
Real World – Physical Environment
Digital Representation – Electric Signal
Actuators
Useful Work
Act

Sensors and Actuators Interact with the Physical World

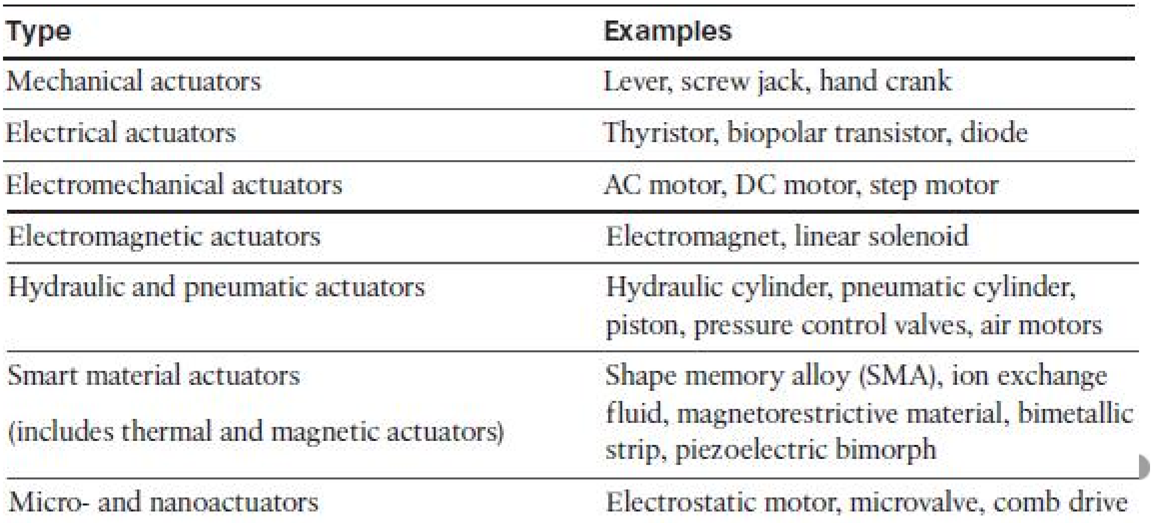
- Sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements into electric signals or digital representations that can be consumed by an intelligent agent. Actuators, receive some type of control signal that triggers a physical effect, usually some type of motion, force.
- IoT sensors are devices that sense and measure the physical world and signal their measurements as electric signals sent to some type of microprocessor or microcontroller for additional processing.
- A processor can send an electric signal to an actuator that translates the signal into some type of movement (linear, rotational, and so on) or useful work that changes or has a measurable impact on the physical world.

4. Explain the ways to classify Actuators.

Answer:

- **Type of motion:** Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).
- **Power:** Actuators can be classified based on their power output (for example, high power, low power, micro power).
- **Binary or continuous:** Actuators can be classified based on the number of stable-state outputs.
- **Area of application:** Actuators can be classified based on the specific industry or vertical where they are used.
- **Type of energy:** Actuators can be classified based on their energy type.

Classifications of actuators based on energy are:



Type	Examples
Mechanical actuators	Lever, screw jack, hand crank
Electrical actuators	Thyristor, biopolar transistor, diode
Electromechanical actuators	AC motor, DC motor, step motor
Electromagnetic actuators	Electromagnet, linear solenoid
Hydraulic and pneumatic actuators	Hydraulic cylinder, pneumatic cylinder, piston, pressure control valves, air motors
Smart material actuators (includes thermal and magnetic actuators)	Shape memory alloy (SMA), ion exchange fluid, magnetorestrictive material, bimetallic strip, piezoelectric bimorph
Micro- and nanoactuators	Electrostatic motor, microvalve, comb drive

5. Explain the Characteristics of a Smart Object.

Answer:

Four defining characteristics of smart objects are:

- **Processing unit:** A smart object has some type of processing unit for acquiring data, processing and analyzing sensing information received by the sensor(s), coordinating control signals to any actuators, and controlling a variety of functions on the smart object, including the communication and power systems. The specific type of processing unit that is used can vary greatly, depending on the specific processing needs of different applications. The most common is a microcontroller because of its small form factor, flexibility, programming simplicity, ubiquity, low power consumption, and low cost.
- **Sensor(s) and/or actuator(s):** A smart object is capable of interacting with the physical world through sensors and actuators. As described in the previous sections, a sensor learns and measures its environment, whereas an actuator is able to produce some change in the physical world. A smart object does not need to contain both sensors and actuators. In fact, a smart object can contain one or multiple sensors and/or actuators, depending upon the application.
- **Communication device:** The communication unit is responsible for connecting a smart object with other smart objects and the outside world (via the network). Communication devices for smart objects can be either wired or wireless. Overwhelmingly, in IoT networks smart objects are wirelessly interconnected for a number of reasons, including cost, limited infrastructure availability, and ease of deployment.
- **Power source:** Smart objects have components that need to be powered. The most significant power consumption usually comes from the communication unit of a smart object. As with the other three smart object building blocks, the power requirements also vary greatly from application to application. Typically, smart objects are limited in power, are deployed for a very long time, and are not easily accessible. Smart object relies on battery power, requires power efficiency, judicious power management, sleep modes, ultra-low power consumption hardware.

6. List and explain the trends in smart objects impacting IOT.
Answer:

- **Size is decreasing:** Some smart objects are so small they are not even visible to the naked eye. This reduced size makes smart objects easier to embed in everyday objects.
- **Power consumption is decreasing:** The different hardware components of a smart object continually consume less power. This is especially true for sensors, many of which are completely passive
- **Processing power is increasing:** Processors are continually getting more powerful and smaller. This is a key advancement for smart objects, as they become increasingly complex and connected.
- **Communication capabilities are improving:** IoT is driving the development of more and more specialized communication protocols covering a greater diversity of use cases and environments.
- **Communication is being increasingly standardized:** There is a strong push in the industry to develop open standards for IoT communication protocols. There are more and more open source efforts to advance IoT.

6. Explain Design Constraints for Wireless Smart Objects.

OR

Explain Wireless Sensor Networks: design Constraints for Wireless Smart Objects

Answer:

- Limited processing power
- Limited memory
- Lossy communication
- Limited transmission speeds
- Limited power

These limitations greatly influence how WSNs are designed, deployed, and utilized. Individual sensor nodes are deployed in very large numbers.

7. Write short notes on Data Aggregation in Wireless Sensor Networks

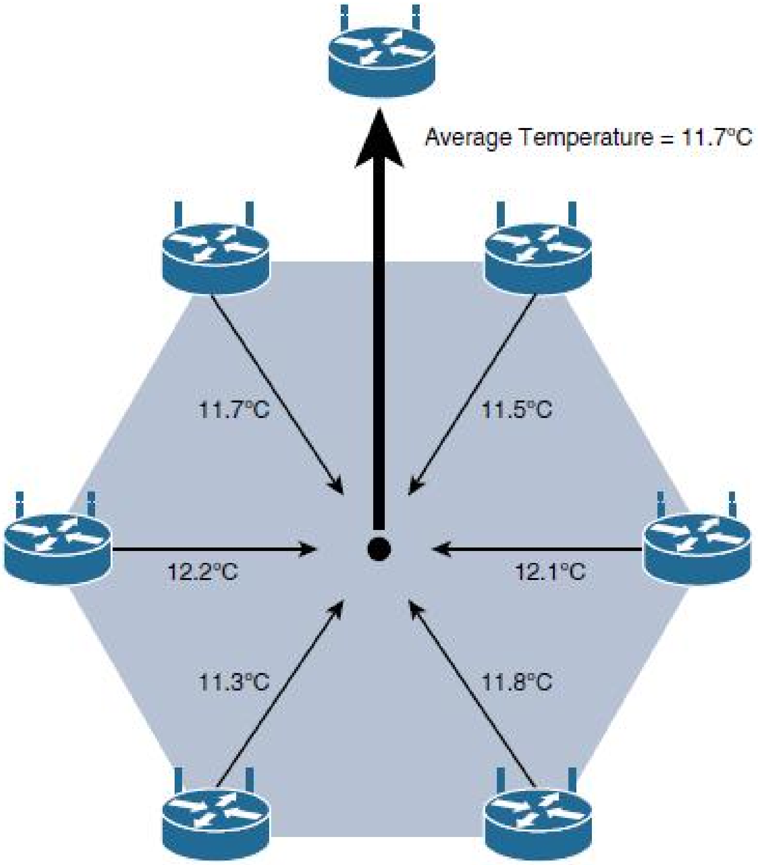
OR

Explain Wireless Sensor Networks: Data Aggregation in Wireless Sensor Networks

Answer:

- Large numbers of sensors permit the introduction of hierarchies of smart objects. Hierarchy provides, among other organizational advantages, the ability to aggregate similar sensor readings from sensor nodes that are in close proximity to each other.

- These data aggregation techniques are helpful in reducing the amount of overall traffic. This data aggregation at the network edges is where fog and mist computing.
- Wirelessly connected smart objects generally have one of the following two communication patterns:
    - **Event-driven:** Transmission of sensory information is triggered only when a smart object detects a particular event or predetermined threshold.
    - **Periodic:** Transmission of sensory information occurs only at periodic intervals.



Data Aggregation in Wireless Sensor Networks

Figure shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.

8. List advantages and disadvantages that a wireless-based solution offers.

Answer:

Advantages:

- Greater deployment flexibility (especially in extreme environments or hard-to-reach places)
- Simpler scaling to a large number of nodes
- Lower implementation costs
- Easier long-term maintenance
- Effortless introduction of new sensor/actuator nodes
- Better equipped to handle dynamic/rapid topology changes

Disadvantages:

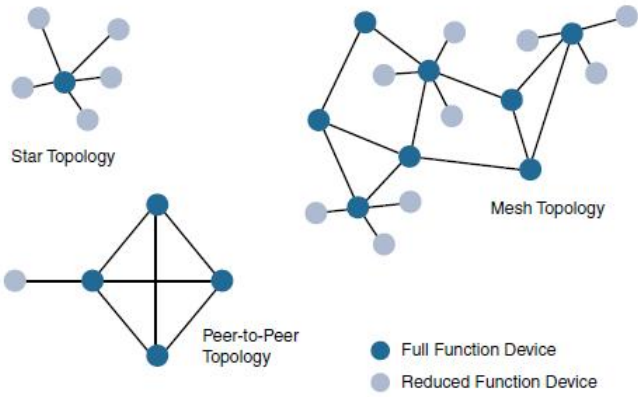
- Potentially less secure (for example, hijacked access points)
- Typically lower transmission speeds
- Greater level of impact/influence by environment

9. Explain the **Communications Criteria** in connecting smart objects in IOT

Answer:

- **Range:**
  - **Short range:** The classical wired example is a serial cable. Wireless short-range technologies are often considered as an alternative to a serial cable, supporting tens of meters of maximum distance between two devices. Examples of short-range wireless technologies are IEEE 802.15.1 Bluetooth and IEEE 802.15.7 Visible Light Communications (VLC).
  - **Medium range:** This range is the main category of IoT access technologies. In the range of tens to hundreds of meter. The maximum distance is generally less than 1 mile between two devices. Example: IEEE 802.11 Wi-Fi,
  - **Long range:** Distances greater than 1 mile between two devices require long-range technologies. These technologies are therefore ideal for battery-powered IoT sensors.Example:2G, 3G, and 4G.
- **Frequency Bands:** In IoT access technologies, the frequency bands leveraged by wireless communications are split between licensed and unlicensed bands. Licensed spectrum is generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services broadcasters, and utilities.

  For IoT access, these are the most well-known ISM bands:
  - 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi
  - IEEE 802.15.1 Bluetooth
  - IEEE 802.15.4 WPAN
- **Power Consumption:** A powered node has a direct connection to a power source, and communications are not limited by power consumption criteria. Ease of deployment of powered nodes is limited by the availability of a power source. Battery-powered nodes bring much more flexibility to IoT devices. These nodes are classified by the required lifetimes of their batteries. IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes. This has led to the evolution of a new wireless environment known as Low-Power Wide-Area (LPWA).
- **Topology:**



For medium-range technologies, a star, peer-to-peer, or mesh topology is common. Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other. Peer-to-peer topologies rely on multiple full-function devices. Peer-to-peer topologies enable more complex formations, such as a mesh networking topology. Mesh topology requires a properly optimized implementation for battery-powered nodes. Battery-powered nodes are often placed in a "sleep mode" to preserve battery life when not transmitting.

- **Constrained Devices:**

Devices are categorized into classes of IoT nodes with computing, memory, storage, power, and networking.

Class	Definition
Class 0	This class of nodes is severely constrained, with less than 10 KB of memory and less than 100 KB of Flash processing and storage capability. These nodes are typically battery powered. They do not have the resources required to directly implement an IP stack and associated security mechanisms.
Class 1	While greater than Class 0, the processing and code space characteristics (approximately 10 KB RAM and approximately 100 KB Flash) of Class 1 are still lower than expected for a complete IP stack implementation. They cannot easily communicate with nodes employing a full IP stack. However, these nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP).
Class 2	Class 2 nodes are characterized by running full implementations of an IP stack on embedded devices. They contain more than 50 KB of memory and 250 KB of Flash, so they can be fully integrated in IP networks.

Constrained-Node Networks:

Constrained-node networks are often referred to as low-power and lossy networks. *Low-power* in the context of LLNs refers to the fact that nodes must cope with the requirements from powered and battery powered constrained nodes. *Lossy networks* indicate that network performance may suffer from interference and variability due to harsh radio environments. Layer 1 and Layer 2 protocols that can be used for constrained-node networks must be evaluated in the context of the following characteristics for use-case applicability: data rate and throughput, latency and determinism, and overhead and payload.

- Data Rate and Throughput: Understanding the bandwidth requirements of a particular technology, its applicability to given use cases, the capacity planning rules, and the expected real throughput are important for proper network design and successful production deployment. Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints The IoT access technologies developed for constrained nodes are optimized for low power consumption, but they are also limited in terms of data rate, which depends on the selected frequency band, and throughput. Majority of them initiate the communication. Upstream traffic toward an application server is usually more common than downstream traffic from the application server.
- Latency and Determinism: Latency expectations of IoT applications should be known when selecting an access technology. This is true for wireless networks, where packet loss and retransmissions due to interference, collisions, and noise are normal behaviours. On constrained networks, latency may range from a few milliseconds to seconds, and applications and protocol stacks must cope with these wide-ranging values.
- Overhead and Payload: When considering constrained access network technologies, it is important to review the MAC payload size characteristics required by applications and should be aware of any requirements for IP. The minimum IPv6 MTU size is expected to be 1280 bytes. Therefore, the fragmentation of the IPv6 payload has to be taken into account by link layer access protocols with smaller MTUs. Most LPWA technologies offer small payload sizes. These small payload sizes are defined to cope with the low data rate and time over the air or duty cycle requirements of IoT nodes and sensors.

10. Write a short note on Classes of Constrained Nodes, as Defined by RFC 7228

Answer:

Note: write the content of question 9 point 5: Constrained devices

11. Write a note on IEEE 802.15.4 technology

Answer:

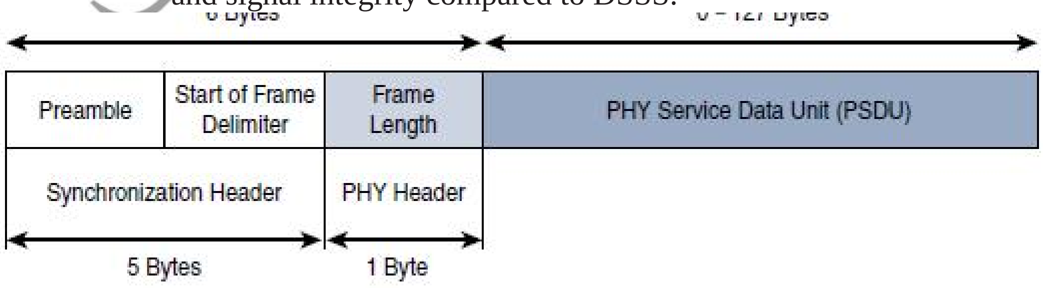
- **IEEE 802.15.4:** IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries. In addition to being low cost and offering a reasonable battery life, this access technology enables easy installation using a compact protocol stack while remaining both simple and flexible. IEEE 802.15.4 is commonly found in the following types of deployments:

  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls
- **Standardization and Alliances:** IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN). Protocol Stacks Utilizing IEEE 802.15.4 are

Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components) as well as application profiles. Common profiles include building automation, home automation, and healthcare.
6LoWPAN	6LoWPAN is an IPv6 adaptation layer defined by the IETF 6LoWPAN working group that describes how to transport IPv6 packets over IEEE 802.15.4 layers.
ZigBee IP	ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as “Wireless Systems for Industrial Automation: Process Control and Related Applications.”
WirelessHART	WirelessHART, promoted by the HART. Communication Foundation, is a protocol stack that offers a time-synchronized, self-organizing, and self-healing mesh architecture, leveraging IEEE 802.15.4-2006
Thread	Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home.

- **Physical Layer:** The 802.15.4 standard supports an extensive number of PHY options that range from 2.4 GHz to sub-GHz frequencies in ISM bands.
  - 2.4 GHz, 16 channels, with a data rate of 250 kbps
  - 915 MHz, 10 channels, with a data rate of 40 kbps.
  - 868 MHz, 1 channel, with a data rate of 20 kbps

  IEEE 802.15.4-2015 introduced additional PHY communication options. They are:
  - **OQPSK PHY:** This is DSSS PHY, employing offset quadrature phase-shift keying (OQPSK) modulation. OQPSK is a modulation technique that uses four unique bit values that are signalled by phase changes.
  - **BPSK PHY:** This is DSSS PHY, employing binary phase-shift keying (BPSK) modulation. BPSK specifies two unique phase shifts as its data encoding scheme.
  - **ASK PHY:** This is parallel sequence spread spectrum (PSSS) PHY, employing amplitude shift keying (ASK) and BPSK modulation. PSSS is an advanced encoding scheme that offers increased range, throughput, data rates, and signal integrity compared to DSSS.



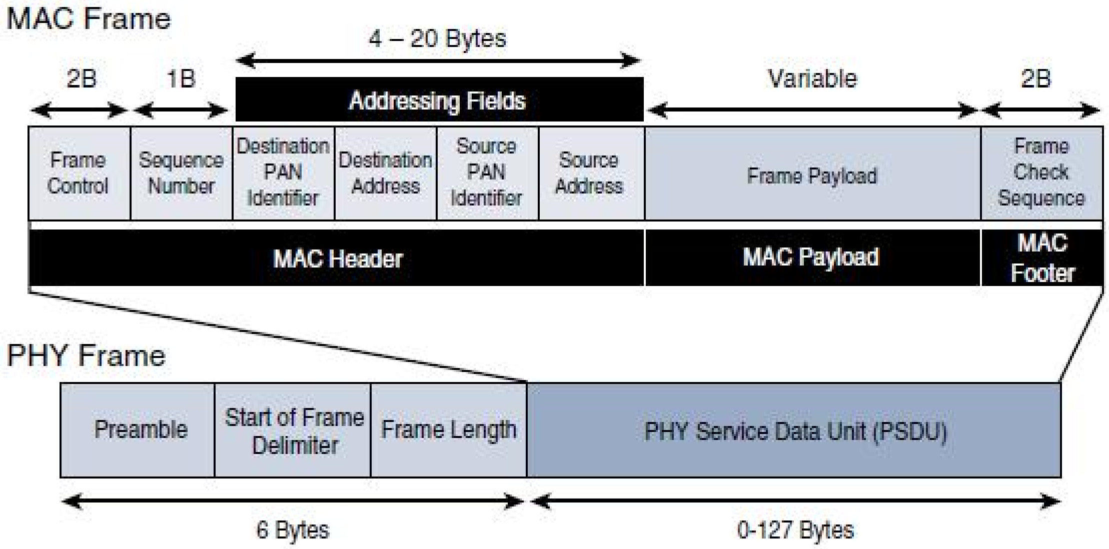
IEEE 802.15.4 PHY Format

The PHY Header portion of the PHY frames a frame length value. It lets the receiver know how much total data to expect in the PHY service data unit (PSDU) portion of the 802.4.15 PHY. The PSDU is the data field or payload.

- **MAC Layer:** The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated. At this layer, the scheduling and routing of data frames are also coordinated. The 802.15.4 MAC layer performs the following tasks:
  - Network beaconing for devices acting as coordinators
  - PAN association and disassociation by a device
  - Device security
  - Reliable link communications between two peer MAC entities

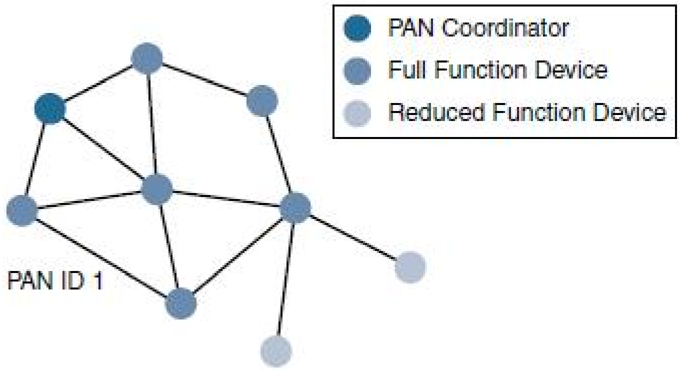
The MAC layer achieves these tasks by using various predefined frame types. They are:

- Data frame**:** Handles all transfers of data
- Beacon frame**:** Used in the transmission of beacons from a PAN coordinator
- Acknowledgement frame: Confirms the successful reception of a frame
- MAC command frame: Responsible for control communication between devices



IEEE 802.15.4 MAC Format

- **Topology:** IEEE 802.15.4–based networks can be built as star, peer-to-peer, or mesh topologies. Mesh networks tie together many nodes. This allows nodes that would be out of range if trying to communicate directly to leverage intermediary nodes to transfer communications.



802.15.4 Sample Mesh Network Topology

- **Security:** The IEEE 802.15.4 specification uses Advanced Encryption Standard (AES) with a 128-bit key length as the base encryption algorithm for securing its data.
- Competitive Technologies: A competitive radio technology that is different in its PHY and MAC layers is DASH7. They are commonly employed in active radio frequency identification (RFID) implementations. The current DASH7 technology offers low power consumption, a compact protocol stack, range up to 1 mile, and AES encryption.

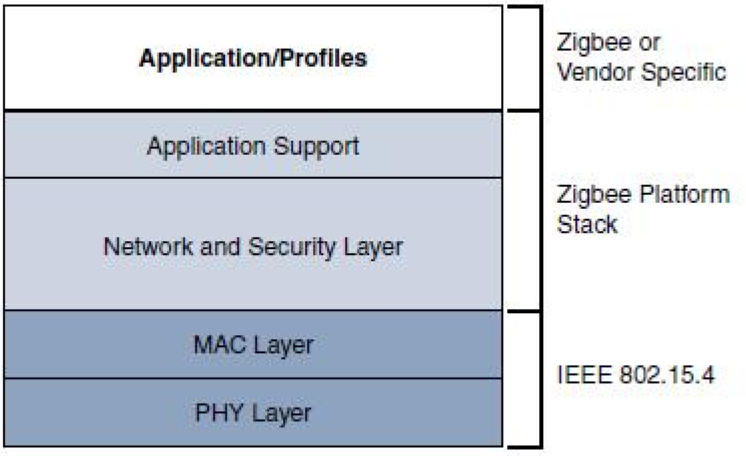
12. What is all the Protocol Stacks Utilizing IEEE 802.15.4?

Answer: See question 11 point 2: Standardization and Alliances

13. Write a short note on High-Level ZigBee and zigbee IP Protocol Stack.

Answer:

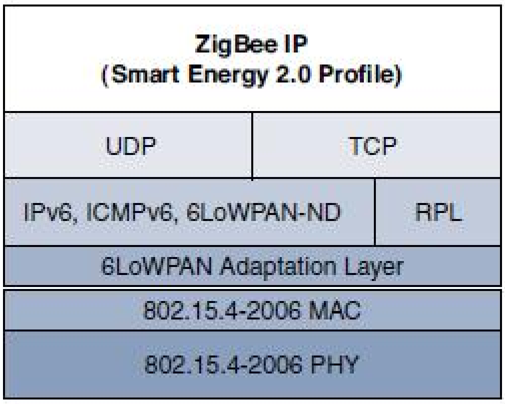
High-Level ZigBee:



High-Level ZigBee Protocol Stack

- The ZigBee network and security layer provides mechanisms for network start-up, configuration, routing, and securing communications.
- This includes calculating routing paths in what is often a changing topology, discovering 12eighbours, and managing the routing tables as devices join for the first time.
- The network layer is also responsible for forming the appropriate topology, which is often a mesh but could be a star or tree as well.
- ZigBee utilizes 802.15.4 for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.
- ZigBee uses Ad hoc On-Demand Distance Vector (AODV) routing across a mesh network. This routing algorithm does not send a message until a route is needed.

ZigBee IP:



ZigBee IP Protocol Stack

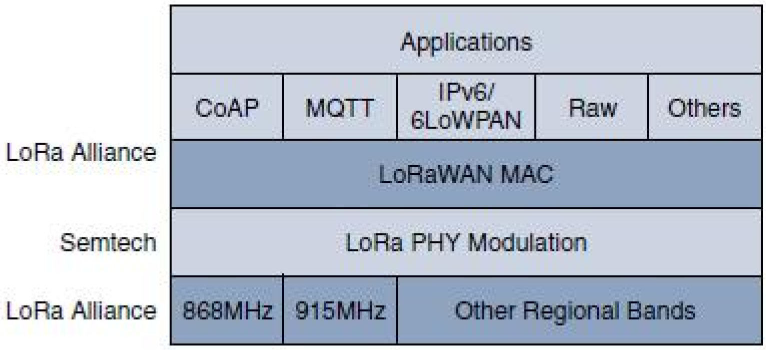
- ZigBee IP was created to embrace the open standards coming from the IETF’s work on LLNs, such as Ipv6, 6LoWPAN, and RPL.
- They provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.
- ZigBee IP utilizes the mesh over or route-over method for forwarding packets. ZigBee IP requires the support of 6LoWPAN’s fragmentation and header compression schemes.

14. Explain LoRaWAN.

Answer:

Low-Power Wide-Area is adapted for long-range and battery-powered endpoints,

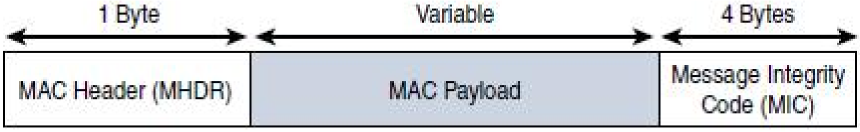
- **Standardization and Alliances**: Semtech LoRa as a Layer 1 PHY modulation technology is available through multiple chipset vendors. To differentiate from the physical layer modulation known as LoRa, the LoRa Alliance uses the term LoRaWAN to refer to its architecture and its specifications that describe end-to-end LoRaWAN communications and protocols.



LoRaWAN Layers

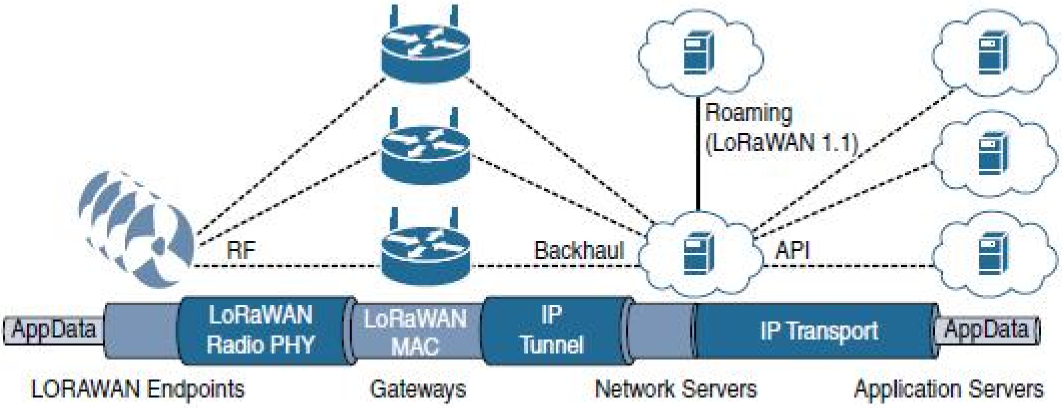
- **Physical Layer:** LoRaWAN 1.0.2 regional specifications describe the use of the main unlicensed sub-GHz frequency bands of 433 MHz, 779–787 MHz, 863–870 MHz, and 902–928 MHz, as well as regional profiles for a subset of the 902–928 MHz bandwidth.A LoRa gateway is deployed as the center hub of a star network architecture. It uses multiple transceivers and channels and can demodulate multiple channels at once or even demodulate multiple signals on the same channel simultaneously. LoRa gateways serve as a transparent bridge relaying data between endpoints, and the endpoints use a single-hop wireless connection to communicate with one or many gateways.

- **MAC Layer**: The LoRaWAN specification documents three classes of LoRaWAN devices:
  - **Class A:** Optimized for battery-powered nodes, it allows bidirectional communications, where a given node is able to receive downstream traffic after transmitting.
  - **Class B:** A Class B node or endpoint should get additional receive windows compared to Class A, but gateways must be synchronized through a beaconing process.
  - **Class C:** This class is particularly adapted for powered nodes. This classification enables a node to be continuously listening by keeping its receive window open when not transmitting.



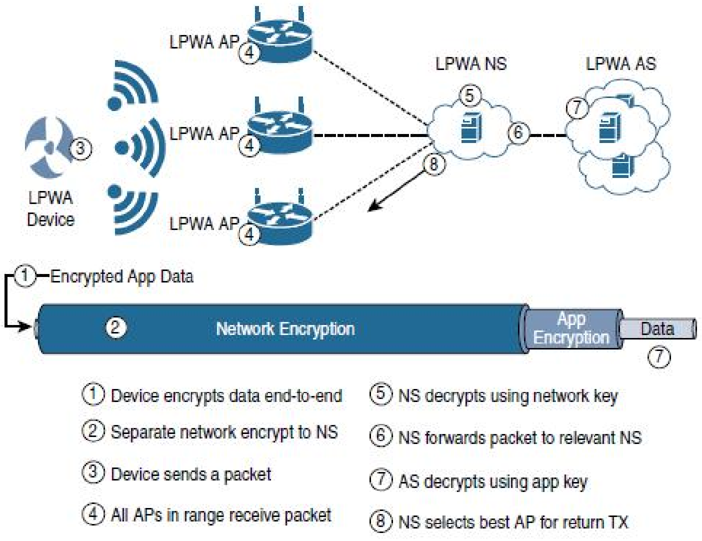
High-Level LoRaWAN MAC Frame Format

- **Topology:** LoRaWAN topology is often described as a “star of stars” topology. Infrastructure consists of endpoints exchanging packets through gateways acting as bridges, with a central LoRaWAN network server. Gateways connect to the backend network using standard IP connections, and endpoints communicate directly with one or more gateways.



LoRaWAN Architecture

- **Security:**
  - Each endpoint implements a network session key (NwkSKey), used by both itself and the LoRaWAN network server. The NwkSKey ensures data integrity through computing and checking the MIC of every data message as well as encrypting and decrypting MAC-onlydata message payloads.
  - The second layer is an application session key (AppSKey), which performs encryption and decryption functions between the endpoint and its application server. Endpoints receive their AES-128 application key (AppKey) from the application owner.
  - LoRaWAN endpoints attached to a LoRaWAN network must get registered and authenticated. This can be achieved through one of the two join mechanisms:
    - **Activation by personalization (ABP):** Endpoints don’t need to run a join procedure as their individual details, including DevAddr and the NwkSKey and AppSKey session keys, are preconfigured and stored in the end device.
    - **Over-the-air activation (OTAA):** Endpoints are allowed to dynamically join a particular LoRaWAN network after successfully going through a join procedure. The join procedure must be done every time a session context is renewed.


LPWA AP
LPWA AP
LPWA AP
LPWA NS
LPWA AS
LPWA Device
1 Encrypted App Data
2 Network Encryption
App Encryption
Data
1 Device encrypts data end-to-end
2 Separate network encrypt to NS
3 Device sends a packet
4 All APs in range receive packet
5 NS decrypts using network key
6 NS forwards packet to relevant NS
7 AS decrypts using app key
8 NS selects best AP for return TX

LoRaWAN Security

- **Competitive Technologies:** LPWA solutions and technologies are split between unlicensed and licensed bands. The licensed-band technologies are dedicated to mobile service providers that have acquired spectrum licenses.