MODULE 2

Imagine the IoT-enabled connected vehicle and roadway working system composed of many sensors that collected data that can be intelligently consumed by a variety of systems and services.
The car is filled with sensors of all types (for example, temperature, location [GPS], pressure, velocity) that are meant to provide a wealth of rich and relevant data to, among many other things, improve safety, simplify vehicle maintenance, and enhance the driver experience. sensors are fundamental building blocks of IoT networks

Such sensors are fundamental building blocks of IoT networks.

In fact, they are the foundational elements found in smart objects—the “things” in the Internet of Things. Smart objects are any physical objects that contain embedded technology to sense and/or interact with their environment in a meaningful way by being interconnected and enabling communication among themselves or an external agent.

the following sections are included:

- **Sensors, Actuators, and Smart Objects:**
- **Sensor Networks:**

Sensors, Actuators, and Smart Objects

The following sections describe the capabilities, characteristics, and functionality of sensors and actuators you will see how to bring these foundational elements together to form smart objects, which are connected to form the sensor and actuator networks that make most IoT use cases possible.

Sensors, Actuators, and Smart Objects

Sensors

A sensor does exactly as its name indicates: It senses. More specifically, a sensor measures some physical quantity and converts that measurement reading into a digital representation. That digital representation is typically passed to another device for transformation into useful data that can be consumed by intelligent devices or humans.

. They can measure anything worth measuring. This additional dimension of data makes the physical world an incredibly valuable source of information.

- Sensors can be readily embedded in any physical objects that are easily connected to the Internet by wired or wireless networks. Because these connected host physical objects with multidimensional sensing capabilities communicate with each other and external systems, they can interpret their environment and make intelligent decisions. Connecting sensing devices in this way has ushered in the world of IoT and a whole new paradigm of business intelligence.

Different categories of sensor including the following:

- **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).

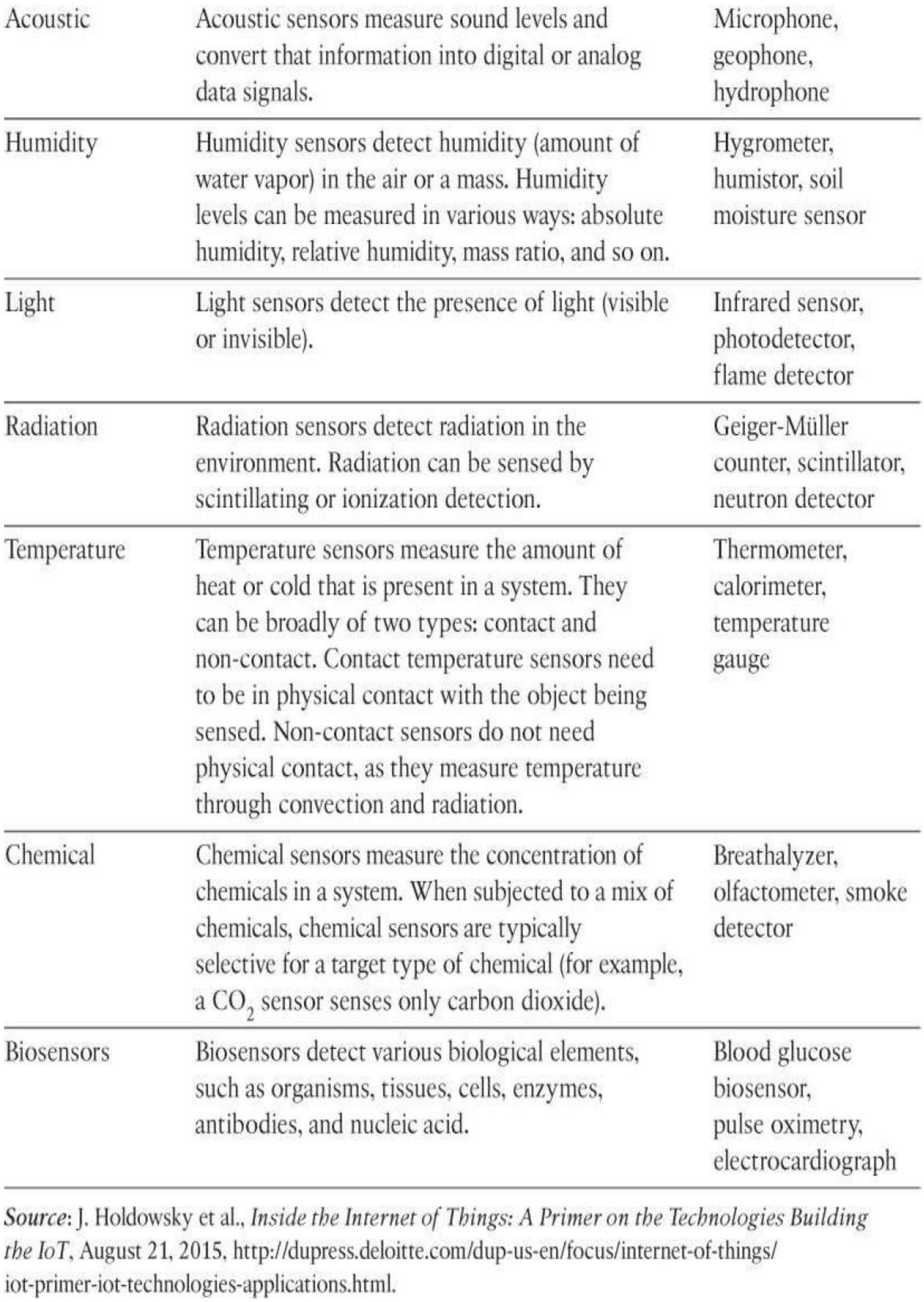
- **Area of application:** Sensors can be categorized based on the specific industry or vertical where they are being used.

- **How sensors measure:** Sensors can be categorized based on the physical mechanism used to measure sensory input (for example, thermoelectric, electrochemical, piezoresistive, optic, electric, fluid mechanic, photoelastic).

- **What sensors measure:** Sensors can be categorized based on their applications or what physical variables they measure

classify based on what physical phenomenon a sensor is measuring.

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

Source: J. Holdowsky et al., *Inside the Internet of Things: A Primer on the Technologies Building the IoT*, August 21, 2015, http://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-primer-iot-technologies-applications.html.

Table 3-1 *Sensor Types*

Sensors come in all shapes and sizes can measure all types of physical conditions. example precision agriculture to improve the efficiency, sustainability, and profitability of traditional farming practices. This includes the use of GPS and satellite aerial imagery for determining field viability; robots for high-precision planting, harvesting, irrigation, and so on; and real-time analytics and artificial intelligence to predict optimal crop yield, weather impacts, and soil quality. sensor measurement of a variety of soil characteristics

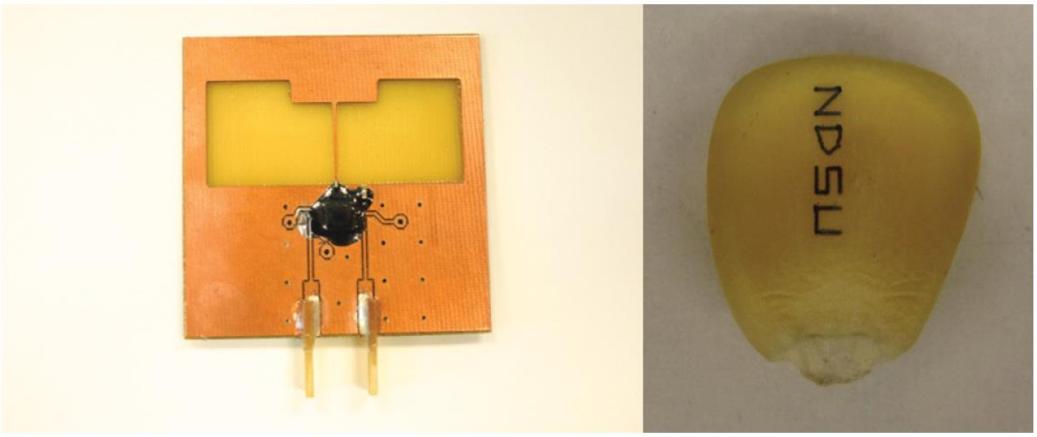


Figure 3-1 *Biodegradable Sensors Developed by NDSU for Smart Farming (Reprinted with permission from NDSU.)*

IoT and, by extension, networked sensors have been repeatedly named among a small number of emerging revolutionary technologies that will change the global economy and shape the future

Imagine the exponential effect of extending sensors to practically every technology, industry, and vertical. For example, there are smart homes with potentially hundreds of sensors, intelligent vehicles with 100+ sensors each, connected cities with thousands upon thousands of connected sensors,

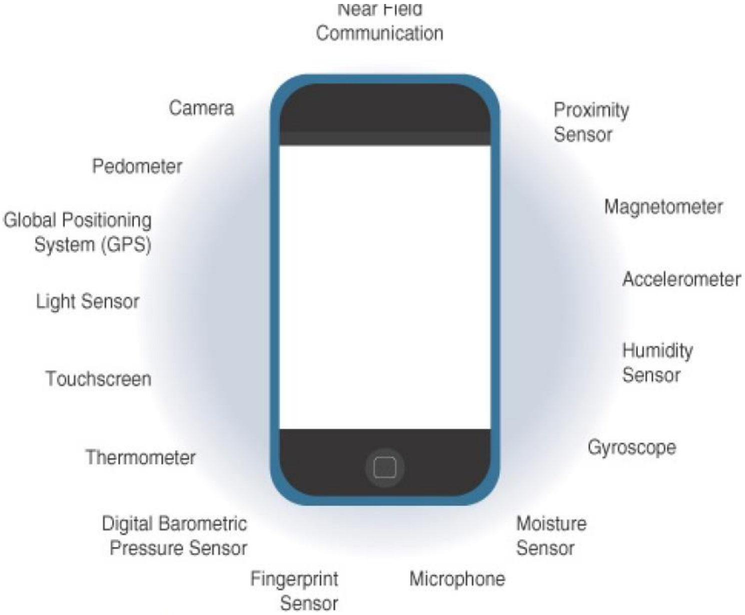


Figure 3-2 *Sensors in a Smart Phone*

Actuators

Actuators are natural complements to sensors. Figure 3-4 demonstrates the symmetry and complementary nature of these two types of devices.

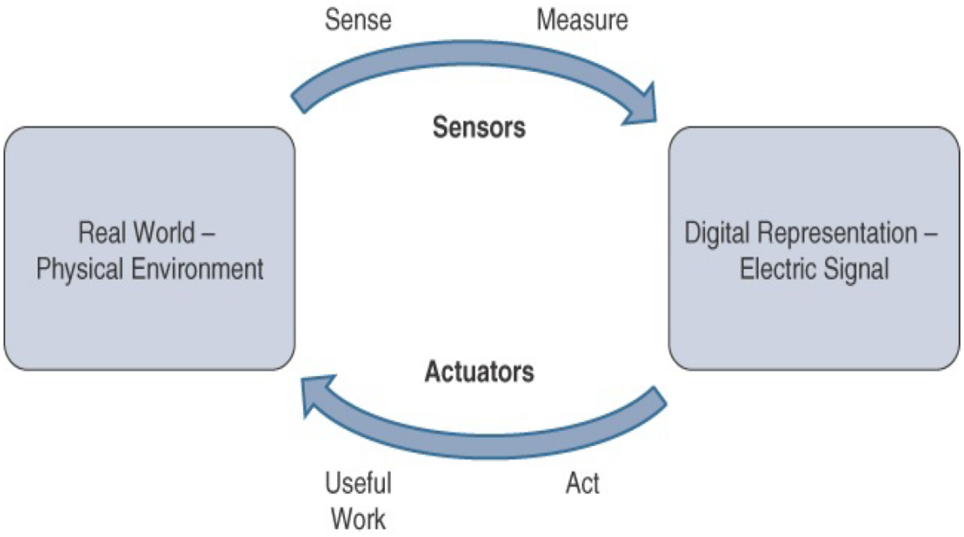


Figure 3-4 *How Sensors and Actuators Interact with the Physical World*

- sensors are designed to sense and measure practically any measurable variable in the physical world. They convert their measurements (typically analog) into electric signals or digital representations that can be consumed by an intelligent agent (a device or a human). Actuators, on the others hand, receive some type of control signal (commonly an electric signal or digital command) that triggers a physical effect, usually some type of motion, force, and so on.
- This interaction between sensors, actuators, and processors and the similar functionality in biological systems is the basis for various technical fields, including robotics and biometrics.
- The human brain signals motor function and movement, and the nervous system carries that information to the appropriate part of the muscular system.

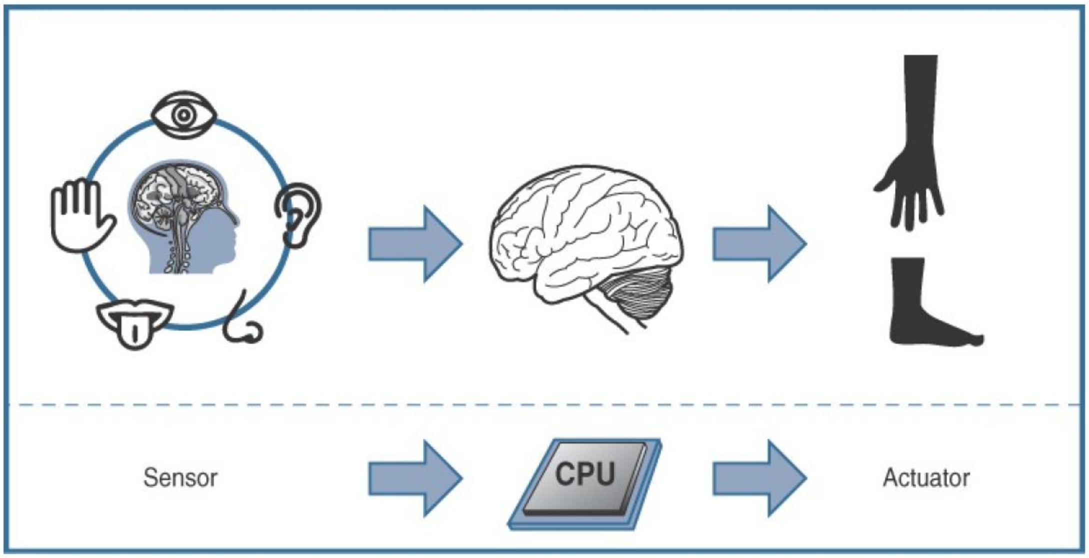


Figure 3-5 *Comparison of Sensor and Actuator Functionality with Humans*

Some common classification actuators

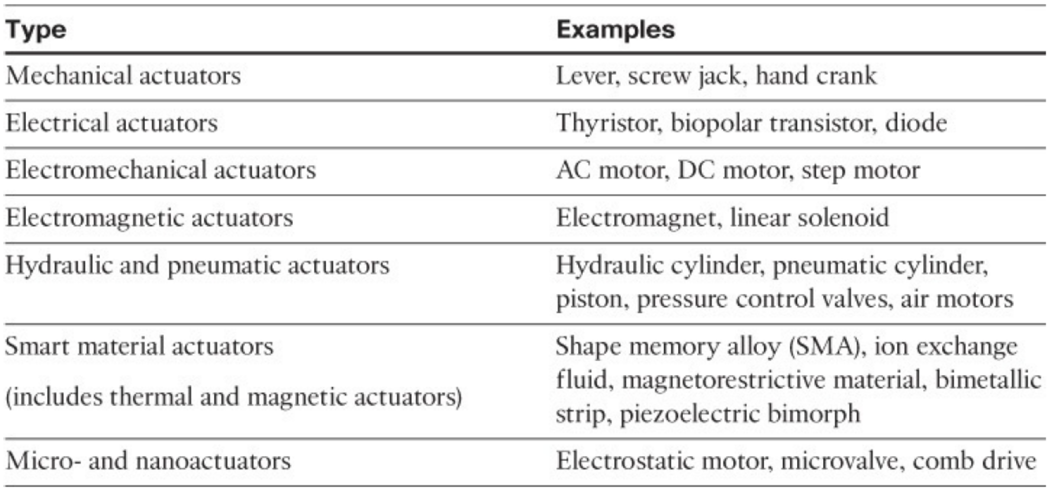
- **Type of motion:** Actuators can be classified based on the type of motion they produce (for example, linear, rotary, one/two/three-axes).

- **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.



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

Table 3-2 *Actuator Classification by Energy Type*

Whereas sensors provide the information, actuators provide the action. the smart sensors used to evaluate soil quality (by measuring a variety of soil, temperature, and plant characteristics) can be connected with electrically or pneumatically controlled valve actuators that control water, pesticides, fertilizers, herbicides, and so on. Intelligently triggering a high-precision actuator based on well-defined sensor readings of temperature, pH, soil/air humidity, nutrient levels, and so on to deliver a highly optimized and custom environment-specific solution is truly smart farming.

Micro-Electro-Mechanical Systems (MEMS)

One of the most interesting advances in sensor and actuator technologies is in how they are packaged and deployed. Micro-electro-mechanical systems (MEMS), referred to as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimeter or less) scale. One of the keys to this technology is a microfabrication technique that is similar to what is used for microelectron integrated circuits. MEMS an attractive option for a huge number of IoT applications.

MEMS devices have already been widely used in a variety of different applications and can be found in very familiar everyday devices. For example, inkjet printers use micropump MEMS. Smart phones also use MEMS technologies for things like accelerometers and gyroscopes. In fact, automobiles were among the first to commercially introduce MEMS into the mass market, with airbag accelerometers

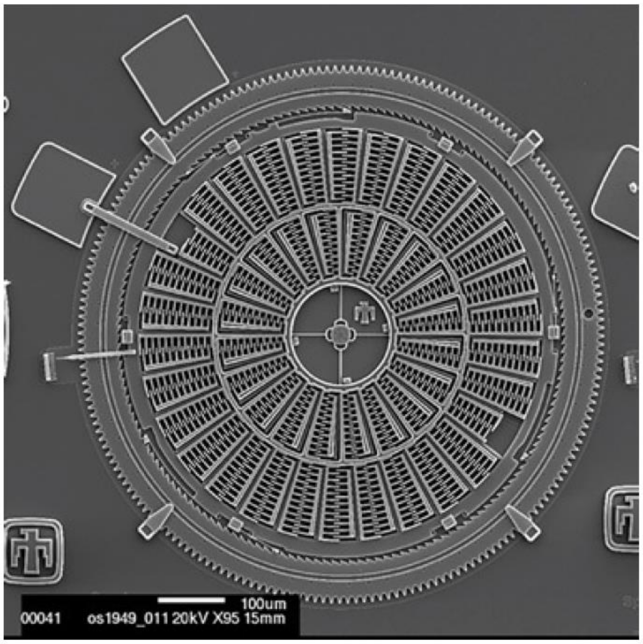


Figure 3-6 *Torsional Ratcheting Actuator (TRA) MEMS (Courtesy Sandia National Laboratories, SUMMiT™ Technologies, www.sandia.gov/mstc.)*

Smart Objects

Smart objects are, quite simply, the building blocks of IoT. They are what transform everyday objects into a network of intelligent objects that are able to learn from and interact with their environment in a meaningful way.
the definition of a smart object has been a bit nebulous because of the different interpretations of the term by varying sources. To add to the overall confusion, the term *smart object*, despite some semantic differences, is often used interchangeably with terms such as *smart sensor*, *smart device*, *IoT device*,*intelligent device*, *thing*, *smart thing*, *intelligent node*, *intelligent thing*, *ubiquitous thing*, and *intelligent product*. the following four defining characteristics.

- **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. 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. 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. There are myriad different communication protocols for smart objects.
- **Power source:** Smart objects have components that need to be powered. Interestingly, 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. This combination, especially when the smart object relies on battery power, implies that power efficiency, judicious power management, sleep modes, ultra-low power consumption hardware, and so on are critical design elements.

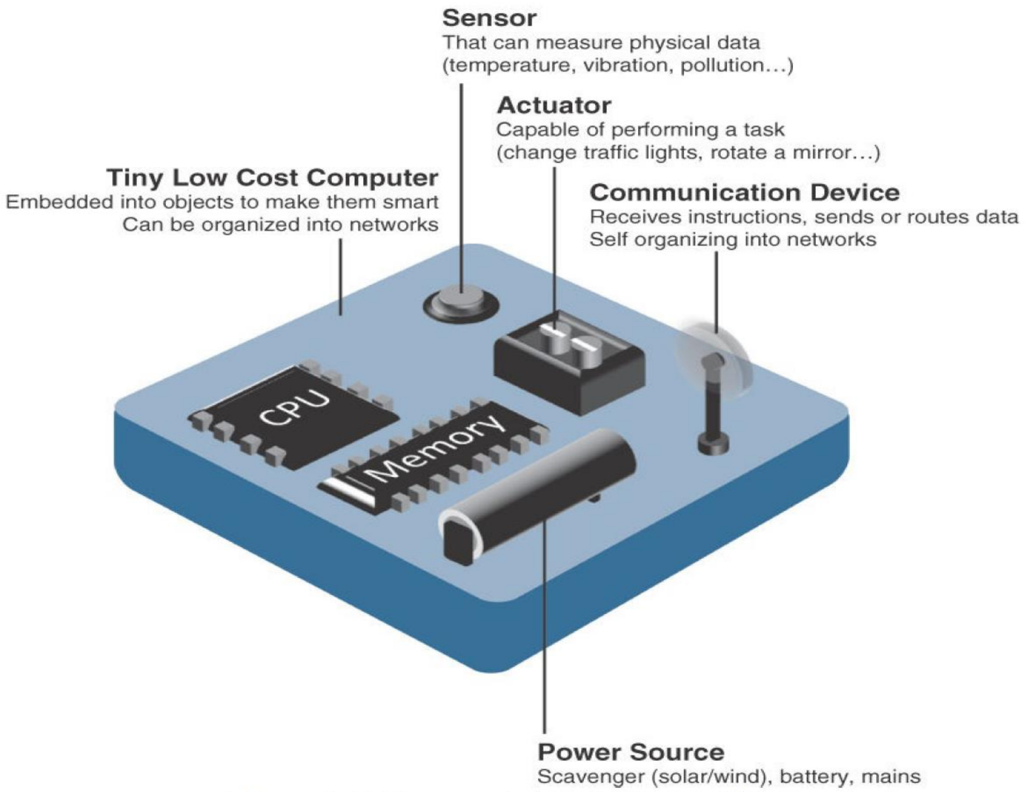

Sensor
That can measure physical data
(temperature, vibration, pollution...)
Actuator
Capable of performing a task
(change traffic lights, rotate a mirror...)
Tiny Low Cost Computer
Embedded into objects to make them smart
Can be organized into networks
Communication Device
Receives instructions, sends or routes data
Self organizing into networks
CPU
Memory
Power Source
Scavenger (solar/wind), battery, mains

Figure 3-7 *Characteristics of a Smart Object*

Trends in Smart Objects

broad generalizations and trends impacting IoT:

- **Size is decreasing:** As discussed earlier, in reference to MEMS, there is a clear trend of ever-decreasing size. 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. Some battery-powered sensors last 10 or more years without battery replacement.

- **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:** It’s no big surprise that wireless speeds are continually increasing, but they are also increasing in range. 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. In addition, there are more and more open source efforts to advance IoT.

Sensor Networks

A sensor/actuator network (SANET), , is a network of sensors that sense and measure their environment and/or actuators that act on their environment. capable of communicating and cooperating in a productive manner. Effective and well-coordinated communication and cooperation is a prominent challenge, primarily because the sensors and actuators in SANETs are diverse, heterogeneous, and resource-constrained.

. Smart homes are a type of SANET that display this coordination between distributed sensors and actuators. For example, smart homes can have temperature sensors that are strategically networked with heating, ventilation, and air-conditioning (HVAC) actuators. When a sensor detects a specified temperature, this can trigger an actuator to take action and heat or cool the home as needed.

While such networks can theoretically be connected in a wired or wireless fashion, the fact that SANETs are typically found in the “real world” means that they need an extreme level of deployment flexibility. For example, smart home temperature sensors need to be expertly located in strategic locations throughout the home, including at HVAC entry and exit points.

The following are some advantages and disadvantages that a wireless-based solution offers:

- 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

Wireless Sensor Networks (WSNs)

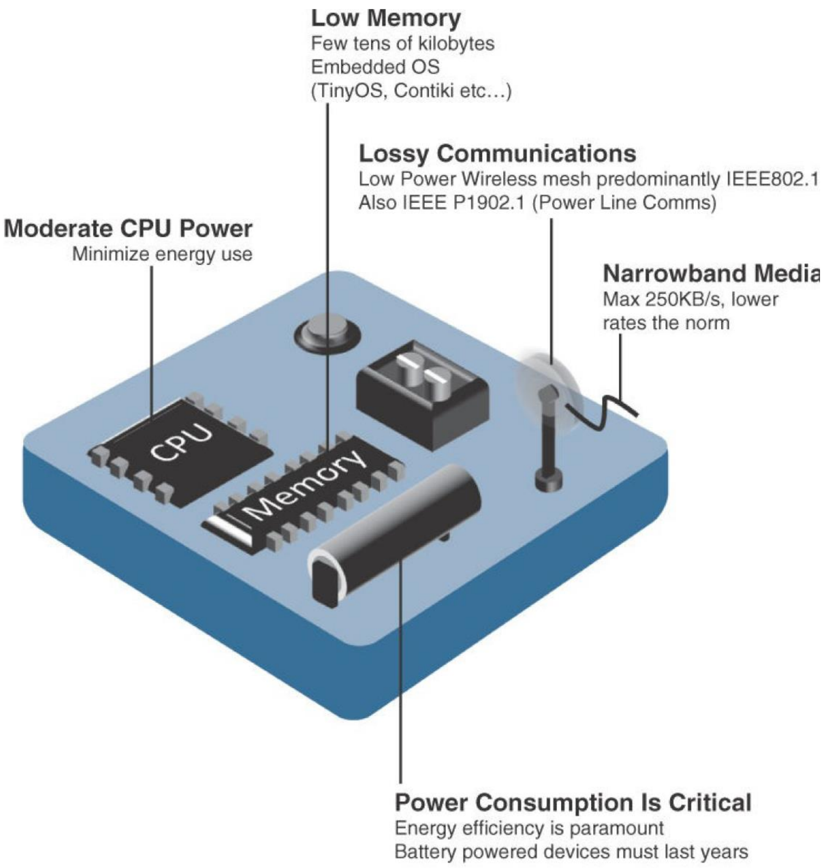
Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as *motes*. The fact that there is no infrastructure to consider with WSNs is surely a powerful advantage for flexible deployments, but there are a variety of design constraints to consider with these wirelessly connected smart objects. Figure 3-8 illustrates some of these assumptions and constraints usually involved in WSNs.

The following are some of the most significant limitations of the smart objects in

\WSNs:

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

- Limited power


Low Memory
Few tens of kilobytes
Embedded OS
(TinyOS, Contiki etc…)
Lossy Communications
Low Power Wireless mesh predominantly IEEE802.1
Also IEEE P1902.1 (Power Line Comms)
Moderate CPU Power
Minimize energy use
Narrowband Media
Max 250KB/s, lower
rates the norm
CPU
Memory
Power Consumption Is Critical
Energy efficiency is paramount
Battery powered devices must last years

- Smart objects with limited processing, memory, power, and so on are often referred to as **constrained nodes.**
- Large numbers of sensors permit the introduction of hierarchies of smart objects.
- Such a 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 (and energy)** in WSNs with very large numbers of deployed smart objects.
    - 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.
- The decision of which of these communication schemes is used depends greatly on the specific application.
- For example, in some medical use cases sensors
- Sends **periodically**, such as temperature or blood pressure readings

- blood pressure or temperature readings are triggered to be sent only when **certain critically low or high readings** are measured
-

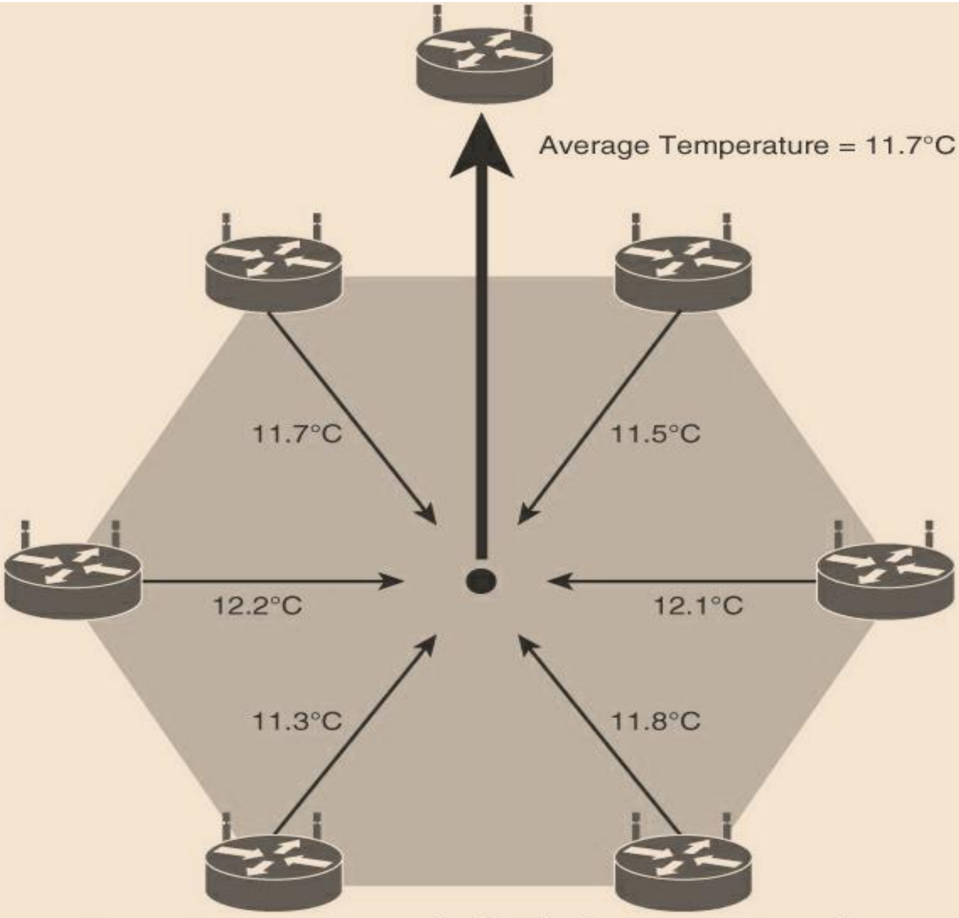


Figure 3-9 Data Aggregation in Wireless Sensor Networks

- As WSNs grow to very large numbers of smart objects, there is a trend toward ever increasing levels of autonomy.
    - For example, manual configuration of thousands of smart objects is impractical and unwieldy, so smart objects in a WSN are typically self-configuring or automated by an IoT management platform in the background.
        - For example, “smart dust” applications,
            - in which very small sensor nodes (that is, MEMS) are scattered over a geographic area to detect vibrations, temperature, humidity, and so on.
- Self organization is required for networking the scads of wireless smart objects such that these nodes autonomously come together to form a true network with a common purpose.
- This capability to self-organize is able to adapt and evolve the logical topology of a WSN to optimize communication
- Autonomous techniques, such as **self-healing, self-protection, and self-optimization,** are often employed to perform these functions on behalf of an overall WSN system.
- IoT applications are often mission critical, and in large-scale WSNs, the **overall system can’t fail if** the environment suddenly changes, wireless communication is temporarily lost, or a limited number of nodes run out of battery power or function improperly.

Communication Protocols for Wireless Sensor Networks

- WSNs are becoming increasingly heterogeneous, with more sophisticated interactions.
- WSNs are seeing transitions from homogenous wireless networks made up of mostly a single type of sensor to networks made up of multiple types of sensors that can even be a hybridized mix of many cheap sensors with a few expensive ones used for very specific high-precision functions.
  - For Example: WSN that has multiple types of sensors, and one of those types is a temperature sensor that can be flexibly used concurrently for environmental applications, weather applications, and smart farming applications.
- Coordinated communication with sophisticated interactions by constrained devices within such a heterogeneous environment is quite a challenge.
- For example:
- Any communication protocol must be able to scale to a large number of nodes.
- When selecting a communication protocol, must care about the requirements of the specific application and consider the communication protocol offers low power consumption, maximum transmission speed, range, tolerance for packet loss, topology optimization, security, and so on.
- The fact that WSNs are often deployed outdoors in harsh and unpredictable environments adds yet another variable to consider because obviously not all communication protocols are designed to be equally rugged.
- Sensors produce large amounts of sensing and measurement data.
- Communication protocols need to facilitate routing and message handling for this data flow between sensor nodes as well as from sensor nodes to optional gateways, edge compute, or centralized cloud compute.
- Data transmission over various networking application like multivendor environments, these communication protocols must be standardized.
- Standardization means, communication protocols is a complicated task, requiring protocol definition across multiple layers of the stack, as well as a great deal of coordination across multiple standards development organizations.

Connecting Smart Objects

A number of different protocols used to connect sensors, actuators, and smart objects with considering the Communication Criteria and IoT Access Technologies

Communication Criteria

- **Range: signal propagation and distance.**
- **Frequency Bands: licensed and unlicensed spectrum**
- **Power Consumption: stable power source or battery powered.**
- **Topology: various layouts that may be supported for connecting multiple smart objects.**
- **Constrained Devices: limitations of certain smart objects from a connectivity perspective.**
- **Constrained-Node Networks: challenges that are often encountered with networks connecting smart objects.**

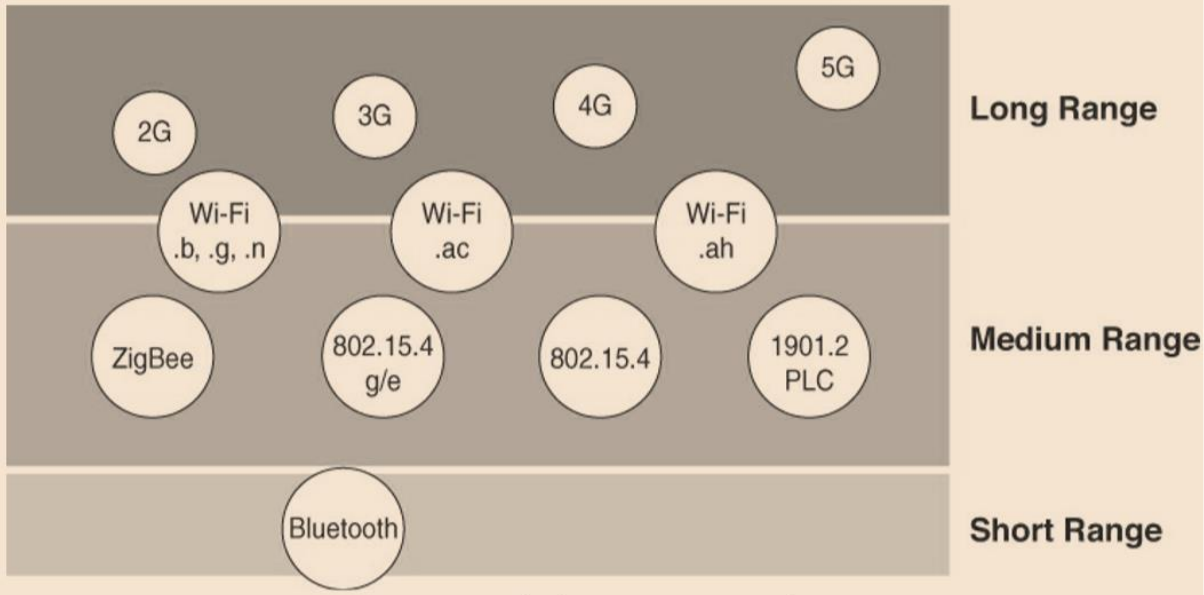


Figure 4-1 Wireless Access Landscape

Range

- Short range:
  - 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:
  - the range of tens to hundreds of meters (generally less than 1 mile between two devices)
    - Examples of medium-range wireless technologies include IEEE 802.11 Wi-Fi, IEEE 802.15.4, and 802.15.4g WPAN.
    - Wired technologies such as IEEE 802.3 Ethernet and IEEE 1901.2 Narrowband Power Line Communications (PLC)
- Long range:
  - Distances greater than 1 mile between two devices

        - Wireless examples are cellular (2G, 3G, 4G) IEEE 802.11 Wi-Fi
        - Low-Power Wide-Area (LPWA) technologies have the ability to communicate over a large area without consuming much power. These technologies are therefore ideal for battery-powered IoT sensors.
        - Industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications.

Frequency Bands

- Radio spectrum is regulated the **International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).**
    - For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.
- **The spectrum for various communications uses is often viewed as a critical resource.**
    - For example, mobile operators pay for licenses in the cellular spectrum.
- **Frequency bands leveraged by wireless communications are split between licensed and unlicensed bands.**
    - **ITU Licensed spectrum**
    - is generally applicable to IoT long-range access technologies and allocated to communications infrastructures deployed by services providers, public services (for example, first responders, military), broadcasters, and utilities.
    - Examples of licensed spectrum commonly used for IoT access are cellular, WiMAX, and Narrowband IoT (NB-IoT) technologies.
- **ITU Unlicensed spectrum**
    - Unlicensed means that no guarantees or protections are offered for device communications.
    - The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands. These frequencies are used for short-range devices (SRDs).
    - **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
        - Unlicensed spectrum it can suffer from more interference because other devices may be competing for the same frequency in a specific area.
- Licensed spectrum are more reliable
- ISM bands operate in the sub-GHz range.
    - Sub-GHz bands are used by protocols such as IEEE 802.15.4, 802.15.4g, and 802.11ah, and LPWA technologies such as LoRa and Sigfox.
    - Sub-GHz ranges are 169 MHz, 433 MHz, 868 MHz, and 915 MHz.
    - For example, European countries, the 169 MHz band is best suited for wireless water and gas metering applications.
- The European Conference of Postal and Telecommunications Administrations (CEPT), in the European Radiocommunications Committee (ERC) Recommendation 70-03, defines the 868 MHz frequency band for telecommunications and postal organizations.
- The 868 MHz band is applicable to IoT access technologies such as IEEE 802.15.4 and 802.15.4g, 802.11ah, and LoRaWAN.
- Frequencies and corresponding regulations of a country when implementing or deploying IoT smart objects.

Smart objects running over unlicensed bands can be easily optimized in terms of hardware supporting the two main worldwide sub-GHz frequencies, 868 MHz and 915 MHz

Power Consumption

- Powered nodes and Battery-powered nodes
- **A powered node**
  - has a direct connection to a power source, and communications are usually not limited by power consumption criteria.
  - deployment of powered nodes is limited by the availability of a power source
- **Battery-powered nodes**
  - Often classified by the required lifetimes of their batteries.
    - A node need 10 to 15 years of battery life, such as on water or gas meters
- IoT wireless access technologies
  - wireless environment known as **Low-Power Wide-Area (LPWA)**
- Wired IoT access technologies
  - consisting of powered nodes are not exempt from power optimization
  - For example, deployment of smart meters over PLC, the radio interface on meters can’t consume 5 to 10 watts of power

Topology

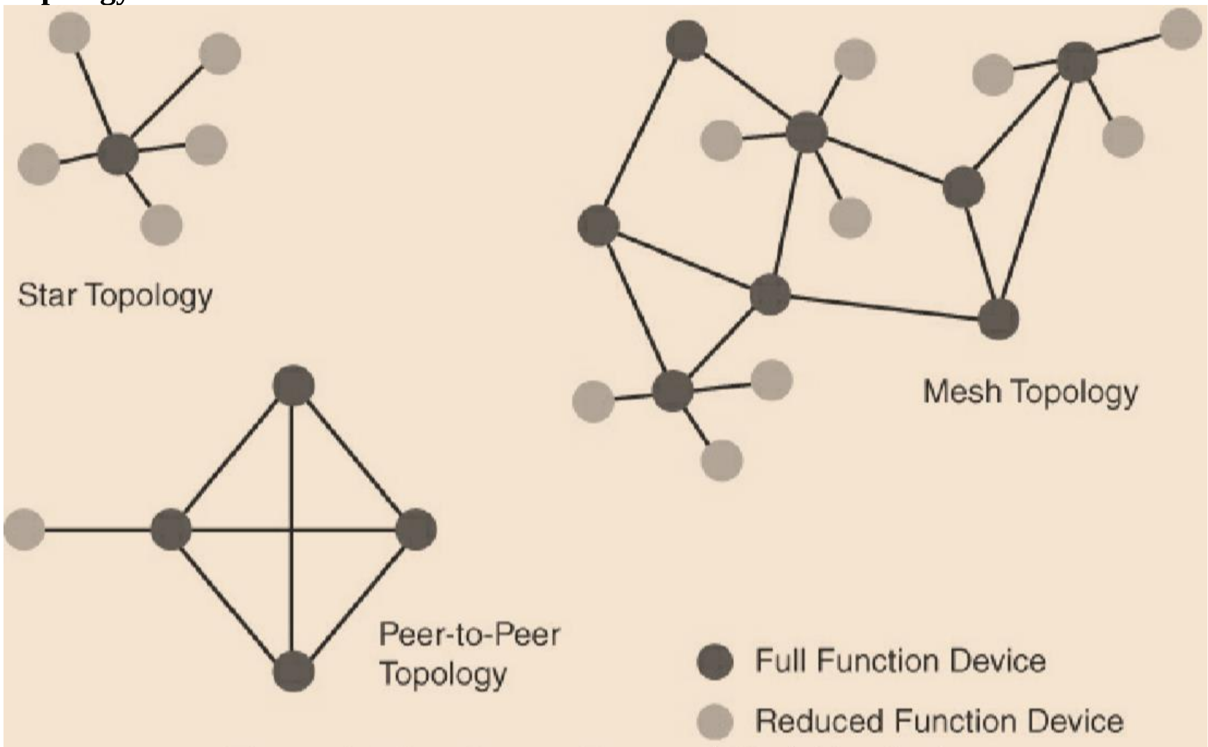


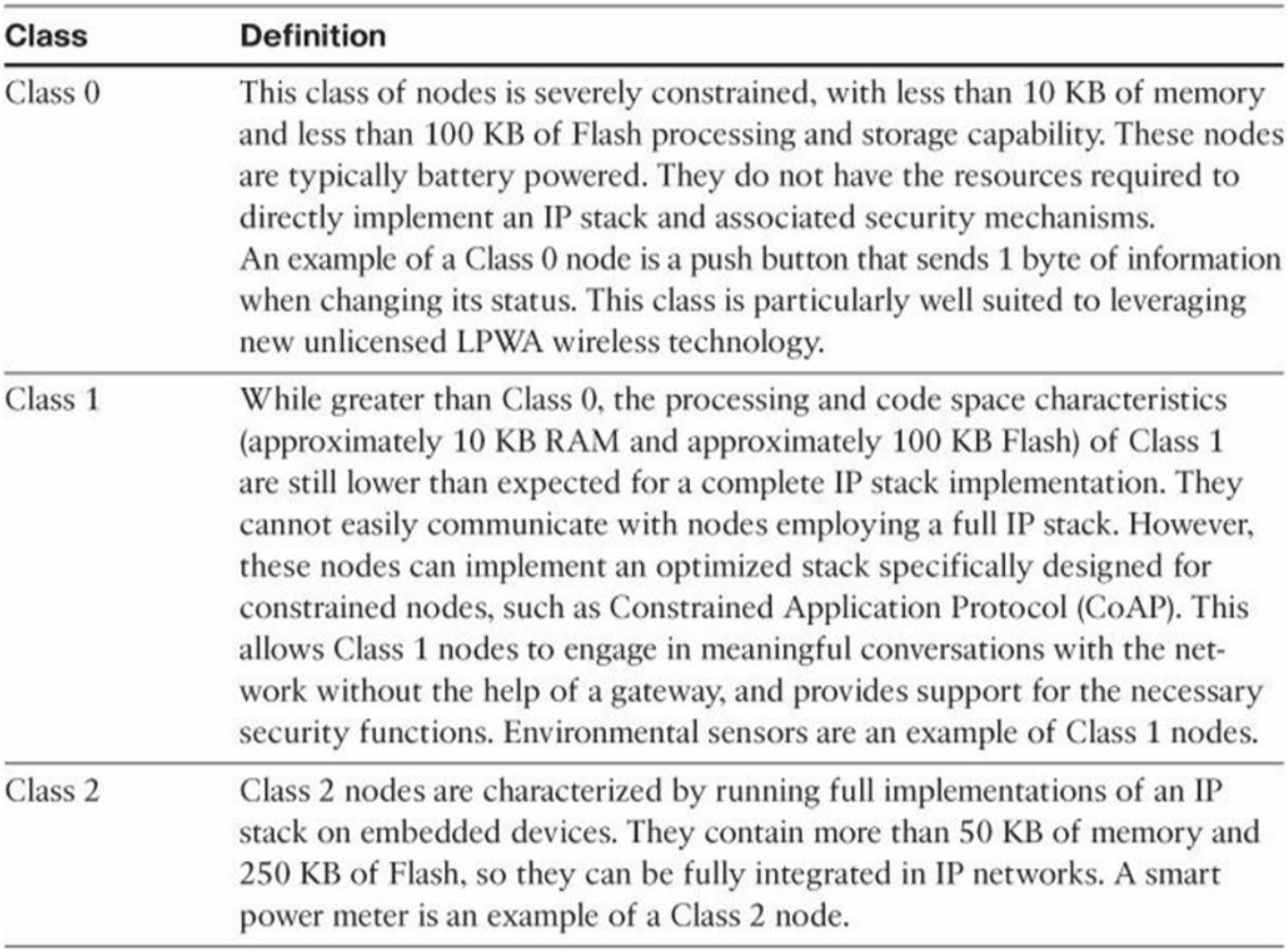
Figure 4-2 Star, Peer-to-Peer, and Mesh Topologies

- IoT devices uses, three main topology schemes are dominant: star, mesh, and peer-to-peer.
  - Star Topology
    - Star topologies utilize a single central base station or controller to allow communications with endpoints.
    - Long-range, medium-range technologies and Shortrange technologies,

        - For Example: Cellular, LPWA, indoor Wi-Fi deployments and Bluetooth networks.
    - Peer-to-peer Topology
        - Allow any device to communicate with any other device as long as they are in range of each other
        - medium-range technologies
        - rely on multiple full-function devices
    - Mesh topology
        - helps cope with low transmit power, searching to reach a greater overall distance, and coverage by having intermediate nodes relaying traffic for other nodes.
        - medium-range technologies, Long-range
        - For example: outdoor Wi-Fi, IEEE 802.15.4 and 802.15.4g and even wired IEEE 1901.2a PLC
- Mesh topology requires the implementation of a Layer 2 forwarding protocol known as mesh-under or a Layer 3 forwarding protocol referred to as mesh-over on each intermediate node.
- Powered nodes, mesh topology requires a properly optimized implementation for battery-powered nodes.
- Battery-powered nodes, in the case of mesh topology, either the battery-powered nodes act as leaf nodes (or reduced-function device RFD) or as a “last resource path” to relay traffic when used as intermediate nodes.
- For battery-powered nodes, the topology type and the role of the node in the topology (for example, being an intermediate or leaf node) are significant factors for a successful implementation.

Constrained Devices

- Constrained nodes have limited resources that impact their networking feature set and capabilities.
- The Internet Engineering Task Force (IETF) acknowledges in RFC (Request for Comments) 7228 that different categories of IoT devices are deployed.



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. An example of a Class 0 node is a push button that sends 1 byte of information when changing its status. This class is particularly well suited to leveraging new unlicensed LPWA wireless technology.
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). This allows Class 1 nodes to engage in meaningful conversations with the network without the help of a gateway, and provides support for the necessary security functions. Environmental sensors are an example of Class 1 nodes.
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. A smart power meter is an example of a Class 2 node.

Table 4-1 Classes of Constrained Nodes, as Defined by RFC 7228

Constrained-Node Networks

  - Data Rate and Throughput
  - Latency and Determinism
  - Overhead and Payload
- Constrained-node networks are often referred to as **low-power and lossy networks (LLNs).**
  - **Low-power** indicate powered and battery powered constrained nodes
  - **Lossy networks** indicates 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

- **Data Rate and Throughput:**
- The data rates available from IoT access technologies like Sigfox, LTE, and IEEE 802.11ac.
- Throughput is less than the data rate.
- Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints.
  - For example, Bluetooth sensors

- Constrained nodes are limited in terms of data rate, which depends on the selected frequency band, and throughput.
- LPWA networks,
  - which are designed with a certain number of messages per day or per endpoint rather than just having a pure bandwidth usage limit in place.
- LLN constrained nodes
  - that send only one message a day, real throughput is often very important for constrained devices implementing an IP stack.
  - throughput is a lower percentage of the data rate
  - Two-way communication handling, and the variable data payload size, which reduces the throughput.
- **Latency and Determinism**
- Latency depends on IoT access technology.
    - For wireless networks, where packet loss and retransmissions due to interference, collisions, and noise are normal behaviors.
- 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**
- For constrained access network technologies, the MAC payload size decides the requirement for applications and IP.
  - For example, minimum IPv6 MTU size is expected to be 1280 bytes.
  - Fragmentation of the IPv6 payload has to be taken into account by link layer access protocols.
- LLNs are able to transport IP,
  - such as IEEE 802.15.4 and 802.15.4g, IEEE 1901.2, and IEEE 802.11ah, Layer 1 or Layer 2 fragmentation capabilities and/or IP optimization.
  - For example,
    - IEEE 802.15.4 payload size is 127 bytes
    - IPv6 payload size is 1280 bytes
    - IEEE 802.15.4g payload size is 2048 bytes
- LPWA technologies offer small payload sizes
  - LoRaWAN technology payload size is 19 bytes

IoT Access Technologies

- IoT Access Technologies
  - IEEE 802.15.4: an older but foundational wireless protocol for connecting smart objects.
  - IEEE 802.15.4g and IEEE 802.15.4e: are targeted to utilities and smart cities deployments.
  - IEEE 1901.2a: which is a technology for connecting smart objects over power lines.
  - IEEE 802.11ah: a technology built on the well-known 802.11 Wi-Fi standards that is specifically for smart objects.
  - LoRaWAN: a scalable technology designed for longer distances with low power requirements in the unlicensed spectrum.

        - NB-IoT and Other LTE Variations: which are often the choice of mobile service providers looking to connect smart objects over longer distances in the licensed spectrum.
- Following topics are addressed for each IoT access technology:
    - Standardization and alliances: The standards bodies that maintain the protocols for a technology
    - Physical layer: The wired or wireless methods and relevant frequencies
    - MAC layer: Considerations at the Media Access Control (MAC) layer, which bridges the physical layer with data link control
    - Topology: The topologies supported by the technology
    - Security: Security aspects of the technology
    - Competitive technologies: Other technologies that are similar and may be suitable alternatives to the given technology

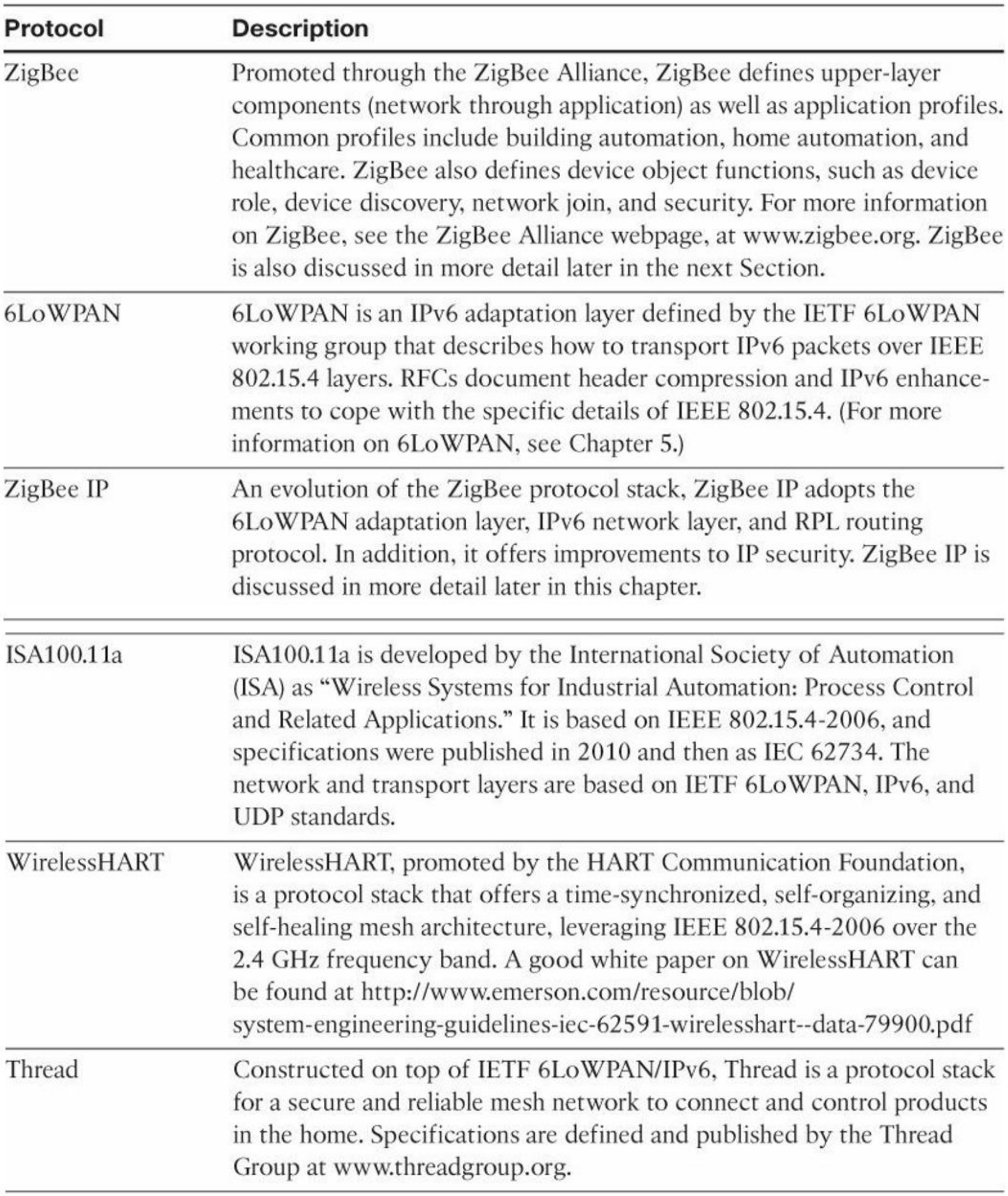
IEEE 802.15.4

- IEEE 802.15.4
    - is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries.
- 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
- IEEE 802.15.4 focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading.
    - The reliability and latency degraded because of Collision Sense Multiple Access/Collision Avoidance (CSMA/CA) algorithm.
        - CSMA/CA is an access method in which a device "listens" to make sure no other devices are transmitting before starting its own transmission.
        - If another device is transmitting, a wait time (which is usually random) occurs before "listening" occurs again.

Interference and multipath fading occur with IEEE 802.15.4 because it lacks a frequency-hopping technique

Standardization and Alliances

- Low-data-rate PHY and MAC layer in wireless personal area networks (WPAN).
    - This standard have low-complexity wireless devices with low data rates with good battery life.
- IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks
    - ZigBee
    - 6LoWPAN
    - ZigBeeIP
    - ISA100.11a
    - WirelessHART
    - Thread



Protocol	Description
ZigBee	Promoted through the ZigBee Alliance, ZigBee defines upper-layer components (network through application) as well as application profiles. Common profiles include building automation, home automation, and healthcare. ZigBee also defines device object functions, such as device role, device discovery, network join, and security. For more information on ZigBee, see the ZigBee Alliance webpage, at www.zigbee.org. ZigBee is also discussed in more detail later in the next Section.
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. RFCs document header compression and IPv6 enhancements to cope with the specific details of IEEE 802.15.4. (For more information on 6LoWPAN, see Chapter 5.)
ZigBee IP	An evolution of the ZigBee protocol stack, ZigBee IP adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol. In addition, it offers improvements to IP security. ZigBee IP is discussed in more detail later in this chapter.
ISA100.11a	ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications." It is based on IEEE 802.15.4-2006, and specifications were published in 2010 and then as IEC 62734. The network and transport layers are based on IETF 6LoWPAN, IPv6, and UDP standards.
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 over the 2.4 GHz frequency band. A good white paper on WirelessHART can be found at http://www.emerson.com/resource/blob/system-engineering-guidelines-iec-62591-wirelesshart--data-79900.pdf
Thread	Constructed on top of IETF 6LoWPAN/IPv6, Thread is a protocol stack for a secure and reliable mesh network to connect and control products in the home. Specifications are defined and published by the Thread Group at www.threadgroup.org.

Table 4-2 Protocol Stacks Utilizing IEEE 802.15.4

ZigBee

- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth, interoperate and low power needs.
- Sets of Commands and Message
  - Sets of commands and message types are called clusters.
  - ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy

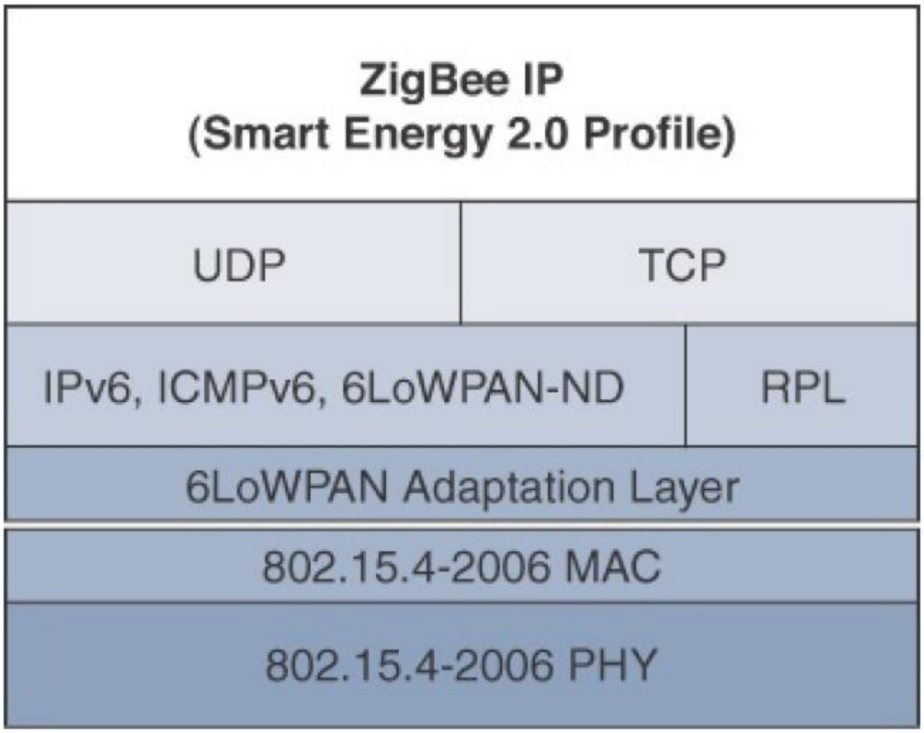


Figure 4-4 *ZigBee IP Protocol Stack*

- ZigBee utilizes the IEEE 802.15.4 standard at the lower PHY and MAC layers
- Network and security layer and application support layer that sit on top of the lower layers.
- The ZigBee network and security layer provides mechanisms for network startup, configuration, routing, and securing communications.
    - This includes calculating routing paths in what is often a changing topology, discovering neighbors, and managing the routing tables as devices join for the first time.
- **Network layer**
    - For forming the appropriate topology, which is a mesh, star or tree.
- **Security layer**,
    - 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.
- **Application Layer**
    - Interfaces the lower portion of the stack dealing with the network of ZigBee devices and with the higher-layer applications.

ZigBee IP

- IEEE 802.15.4 , IP and TCP/UDP protocols and various other open standards are supported at the network and transport layers.
- Open standards like LLNs, IPv6, 6LoWPAN, and RPL. These provides for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.

- ZigBee IP Applications like
    - Smart Energy (SE) Profile 2.0 or SE 2.0
    - smart metering and residential energy management systems

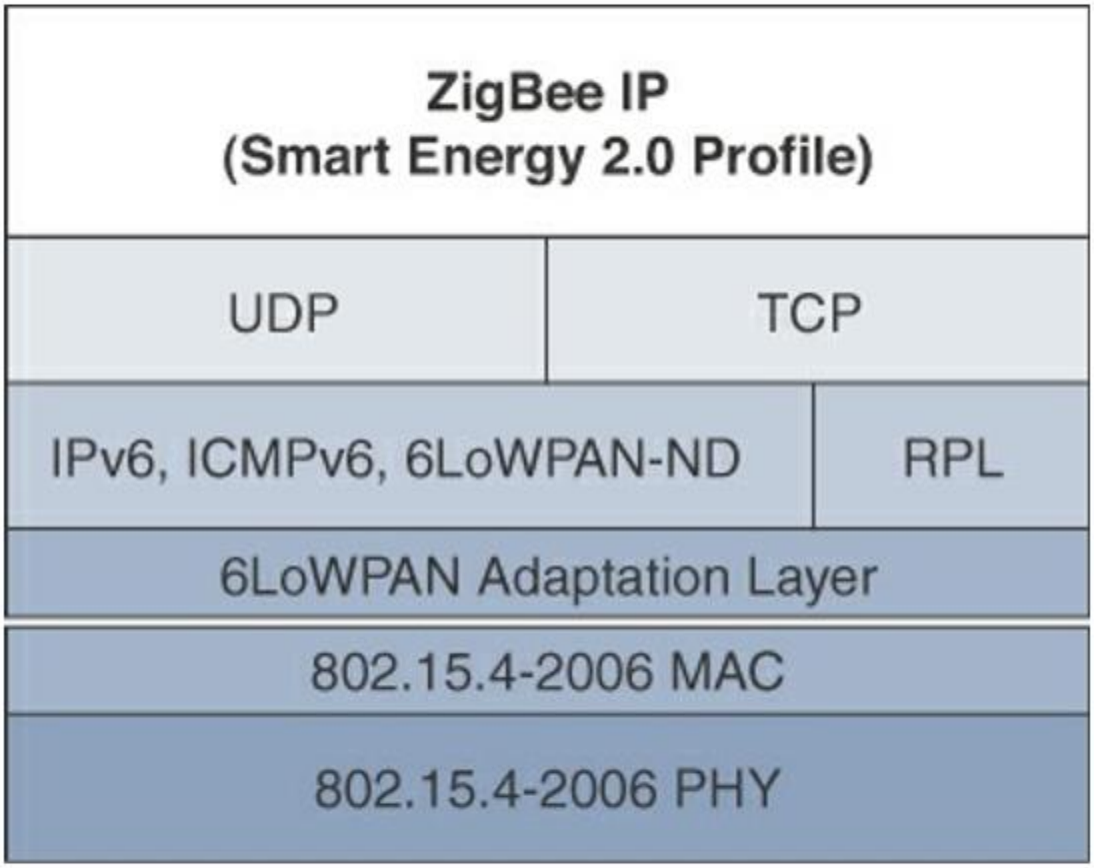


Figure 4-4 ZigBee IP Protocol Stack

- **6LoWPAN as an adaptation layer**
    - ZigBee IP utilizes the mesh-over or route-over method for forwarding packets.
    - It support of 6LoWPAN’s fragmentation and header compression schemes.
- **Network layer**,
    - Support IPv6, ICMPv6, and 6LoWPAN Neighbor Discovery (ND), and utilize RPL for the routing of packets across the mesh network.

Both TCP and UDP are also supported, to provide both connection-oriented and connectionless service.

IEEE 802.15.4 - 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.
    - These standards is based on DSSS (direct sequence spread spectrum), is a modulation technique in which a signal is intentionally spread in the frequency domain, resulting in greater bandwidth.
- The original physical layer transmission options were as follows:
    - 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
  - Note - only the 2.4 GHz band operates worldwide
- Additional PHY communication options 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 signaled by phase changes. An offset function that is present during phase shifts allows data to be transmitted more reliably.
  - **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. ASK uses amplitude shifts instead of phase shifts to signal different bit values.
    - These improvements increase the maximum data rate

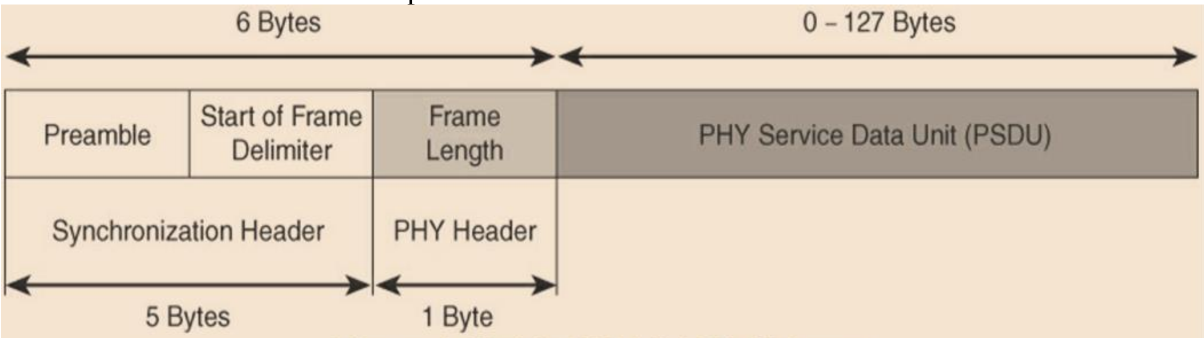


Figure 4-5 IEEE 802.15.4 PHY Format

- **The synchronization header**
  - **Preamble:** is a 32-bit or 4-byte (for parallel construction) pattern that identifies the start of the frame and is used to synchronize the data transmission.
  - **Start of Frame Delimiter fields:** informs the receiver that frame contents start immediately after this byte.
- **The PHY Header**
  - **Frame length value:** It lets the receiver know how much total data to expect in the PSDU.
- **PSDU (PHY service data unit)** is the data field or payload.
  - Maximum size of the PSDU is 127 bytes

MAC Layer

- MAC layer performs the following tasks:
  - Manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated.
  - The scheduling and routing of data frames are coordinated

    - Network beaconing for devices acting as coordinators (New devices use beacons to join an 802.15.4 network)
    - PAN association and disassociation by a device
    - Device security
    - Reliable link communications between two peer MAC entities
- MAC frames are specified in 802.15.4:
    - 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
- The 802.15.4 MAC frame broken down into the
    - MAC Header,
    - MAC Payload,
    - MAC Footer fields.

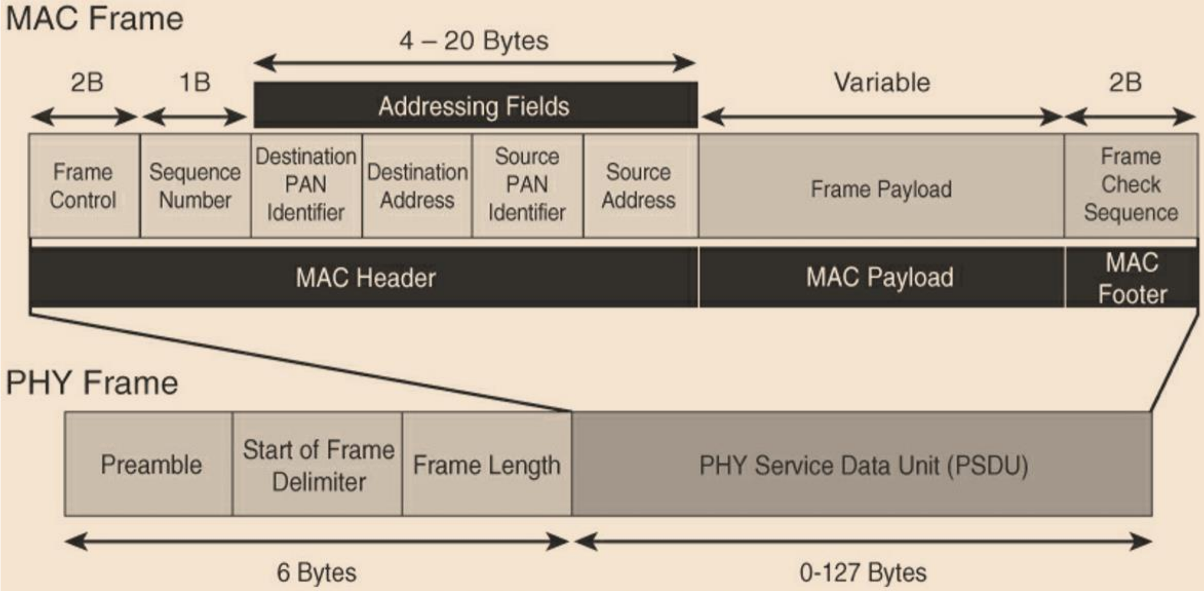


Figure 4-6 IEEE 802.15.4 MAC Format

- The MAC Header field
    - Frame Control : defines attributes such as frame type, addressing modes, and other control flags
    - Sequence Number : indicates the sequence identifier for the frame
    - Addressing fields : specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields.
- The MAC Payload field varies by individual frame type. maximum payload is 127 bytes, and also defines how a 16-bit “short address” is assigned to devices)
    - For example,
        - Beacon frames have specific fields and payloads related to beacons,
        - MAC command frames have different fields present.
- The MAC Footer
    - field is nothing more than a frame check sequence (FCS).
    - An FCS is a calculation based on the data in the frame that is used by the receiving side to confirm the integrity of the data in the frame.

Topology

- 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 PAN should be set up with a unique ID.
    - All the nodes in the same 802.15.4 network should use the same PAN ID

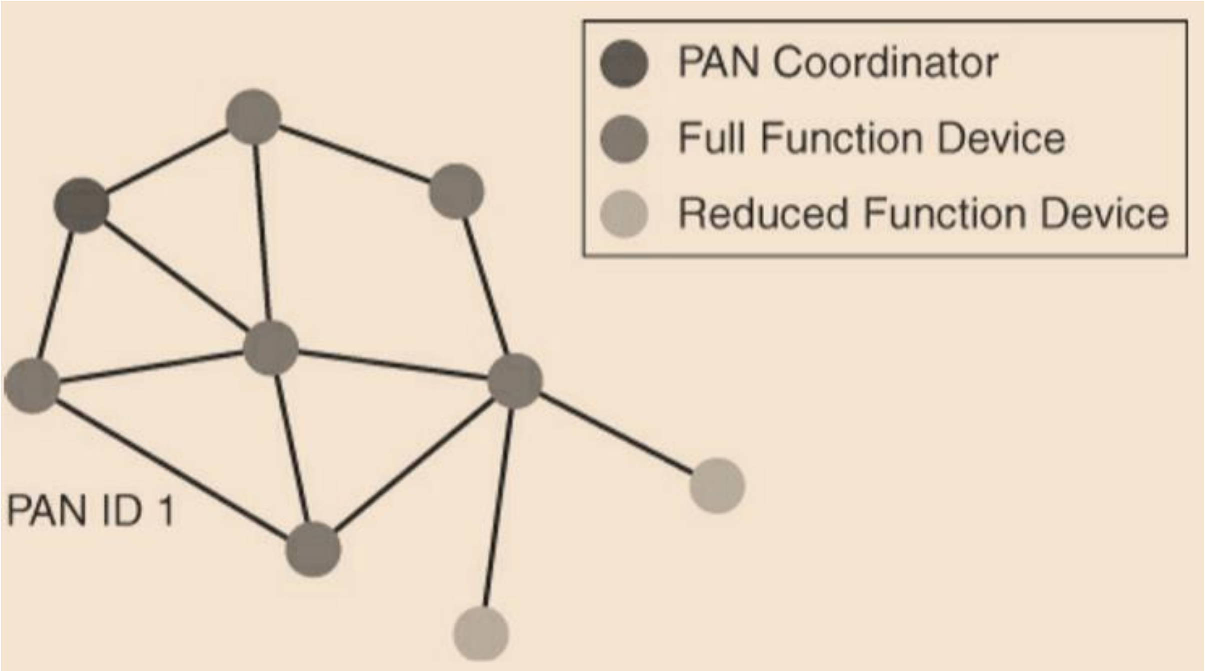


Figure 4-7 802.15.4 Sample Mesh Network Topology

- A minimum of one FFD acting as a PAN coordinator is required to deliver services that allow other devices to associate and form a cell or PAN.
- A single PAN coordinator is identified with PAN ID E.g. PAN ID1.
    - FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

Security

- IEEE 802.15.4 uses **Advanced Encryption Standard (AES)** with a 128-bit key length as the base encryption algorithm for securing its data and also validates the data that is sent
    - Validation is accomplished by a message integrity code (MIC), which is calculated for the entire frame using the same AES key that is used for encryption.
    - AES is a block cipher, which means it operates on fixed-size blocks of data.

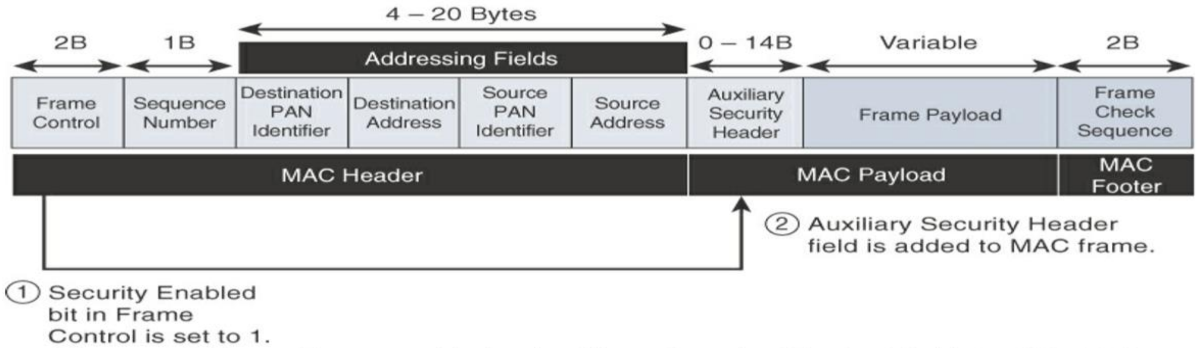


Figure 4-8 Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions

- Security features of 802.15.4 slightly and consumes some of the payload.
- Using the Security Enabled field in the Frame Control portion of the 802.15.4 header is the first step to enabling AES encryption.
  - This field is a single bit that is set to 1 for security.
  - Once this bit is set, a field called the Auxiliary Security Header is created after the Source Address field, by stealing some bytes from the Payload field.

Competitive Technologies

- A competitive radio technology that is different in its PHY and MAC layers is DASH7.
  - DASH7 was originally based on the ISO18000-7 standard and positioned for industrial communications, whereas IEEE 802.15.4 is more generic.
- Commonly employed in active radio frequency identification (RFID) implementations, DASH7 was used by US military forces for many years.
- Active RFID utilizes radio waves generated by a battery-powered tag on an object to enable continuous tracking.
- The current DASH7 technology offers low power consumption, a compact protocol stack, range up to 1 mile, and AES encryption.

IEEE 802.15.4g and 802.15.4e

- **IEEE 802.15.4e** enhanced the IEEE 802.15.4 MAC layer capabilities in the areas of
  - frame format, security, determinism mechanism, frequency hopping, reliability, unbounded latency, and multipath fading

improvements to better cope with certain application domains, such as factory and process automation and smart grid

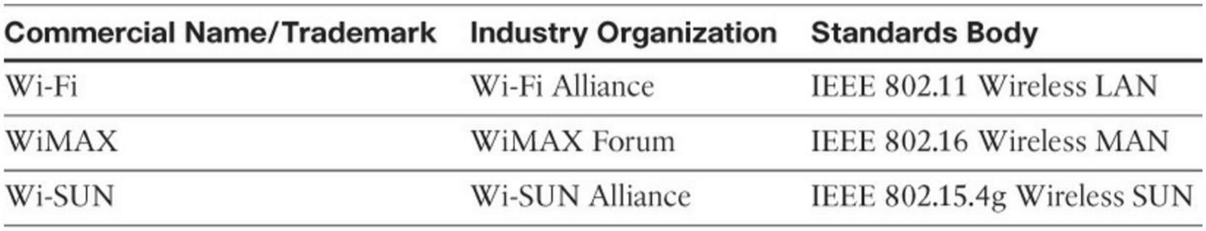
- **802.15.4g seeks** to optimize large outdoor wireless mesh networks for field area networks (FANs).
  - New PHY definitions are introduced, as well as some MAC modifications needed to support their implementation.
  - This focus of mainly on smart grid, smart utility network communication
  - Also used in IoT Applications like:
    - Distribution automation and industrial supervisory control and data acquisition (SCADA) environments for remote monitoring and control
    - Public lighting
    - Environmental wireless sensors in smart cities

- Electrical vehicle charging stations
- Smart parking meters
- Microgrids
- Renewable energy

IEEE 802.15.4u defines the PHY layer characteristics for India (865–867 MHz).

Standardization and Alliances

- 802.15.4g-2012 and 802.15.4e-2012 led to additional difficulty in achieving the interoperability between devices and mixed vendors that users requested.
- To guarantee interoperability, the Wi-SUN Alliance was formed. (SUN stands for smart utility network.)



Commercial Name/Trademark	Industry Organization	Standards Body
Wi-Fi	Wi-Fi Alliance	IEEE 802.11 Wireless LAN
WiMAX	WiMAX Forum	IEEE 802.16 Wireless MAN
Wi-SUN	Wi-SUN Alliance	IEEE 802.15.4g Wireless SUN

Table 4-3 Industry Alliances for Some Common IEEE Standards

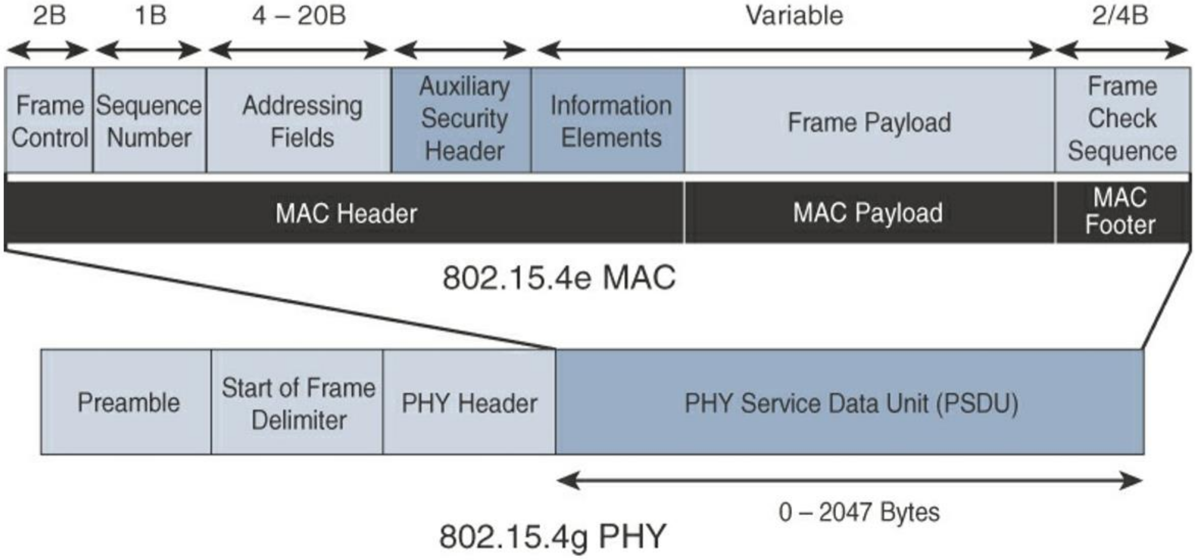
Physical Layer

- In IEEE 802.15.4g
    - payload size of 127 bytes was increased for the SUN PHY to 2047 bytes.
        - This provides a better match for the greater packet sizes found in many upper-layer protocols
    - the error protection was improved by evolving the CRC from 16 to 32 bits.
- Data must be modulated onto the frequency using at least one of the following PHY mechanisms:
    - Multi-Rate and Multi-Regional Frequency Shift Keying (MR-FSK): Offers good transmit power efficiency due to the constant envelope of the transmit signal
    - Multi-Rate and Multi-Regional Orthogonal Frequency Division Multiplexing (MR-OFDM): Provides higher data rates but may be too complex for low-cost and low-power devices
    - Multi-Rate and Multi-Regional Offset Quadrature Phase-Shift Keying (MRO-QPSK): Shares the same characteristics of the IEEE 802.15.4-2006 O-QPSK PHY , making multi-mode systems more cost-effective and easier to design
- Enhanced data rates and a greater number of channels for channel hopping are available, depending on the frequency bands and modulation.

MAC Layer

- The following are some of the main enhancements to the MAC layer:
    - **Time-Slotted Channel Hopping (TSCH):**
        - Channel hopping, also known as frequency hopping, utilizes different channels for transmission at different times.
        - TSCH divides time into fixed time periods, or “time slots,” which offer guaranteed bandwidth and predictable latency.
            - In a time slot, one packet and its acknowledgement can be transmitted, increasing network capacity because multiple nodes can communicate in the same time slot, using different channels.

        - A number of time slots are defined as a “slot frame,” which is regularly repeated to provide “guaranteed access.”
    - The transmitter and receiver agree on the channels and the timing for switching between channels through the combination of a global time slot counter and a global channel hopping sequence list, as computed on each node to determine the channel of each time slot.
    - TSCH adds robustness in noisy environments and smoother coexistence with other wireless technologies,
- **Information elements (IEs):**
- Allow for the exchange of information at the MAC layer in an extensible manner, either as header IEs (standardized) and/or payload IEs (private).
- Specified in a tag, length, value (TLV) format, the IE field allows frames to carry additional metadata to support MAC layer services.
- These services may include IEEE 802.15.9 key management, Wi-SUN 1.0 IEs to broadcast and unicast schedule timing information, and frequency hopping synchronization information.
- **Enhanced beacons (EBs):**
- Beacons to allow the construction of application-specific beacon content. This is accomplished by including relevant IEs in EB frames.
- Some IEs that may be found in EBs include network metrics, frequency hopping broadcast schedule, and PAN information version.
- **Enhanced beacon requests (EBRs):**
- Enhanced beacon request (EBRs) also leverages IEs.
- The IEs in EBRs allow the sender to selectively specify the request of information. Beacon responses are then limited to what was requested in the EBR.
- For example, a device can query for a PAN that is allowing new devices to join or a PAN that supports a certain set of MAC/PHY capabilities
- **Enhanced Acknowledgement:**
- Allows for the integration of a frame counter for the frame being acknowledged.
- This feature helps protect against certain attacks that occur when Acknowledgement frames are spoofed.



- **Figure 4-9** IEEE 802.15.4g/e MAC Frame Format

- 802.15.4g supporting payload up to 2047 bytes and 802.15.4 supporting payload only 127 bytes.
- The **Auxiliary Security header** provides for the encryption of the data frame.
- This field is optionally supported in both 802.15.4e-2012 and 802.15.4.
- **IE field** contains one or more information elements that allow for additional information to be exchanged at the MAC layer.

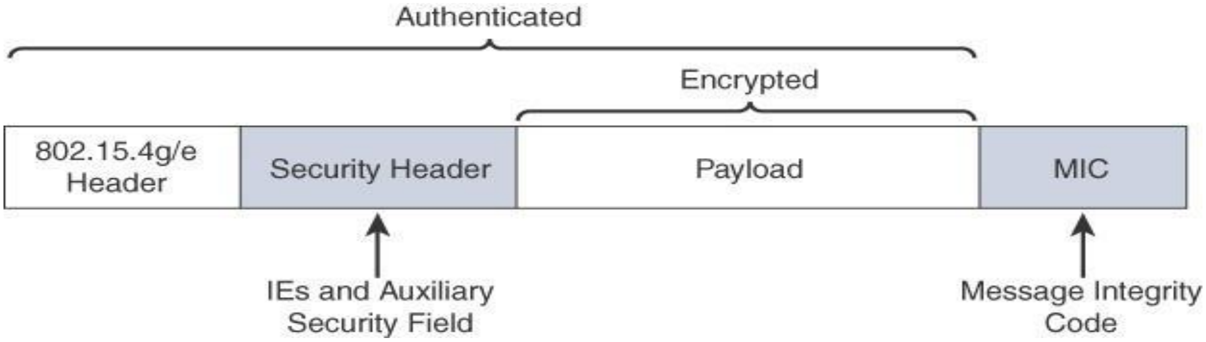
Topology

Deployments of IEEE 802.15.4g-2012 are mostly based on a mesh topology
A mesh topology allows deployments to be done in urban or rural areas, expanding the distance between nodes that can relay the traffic of other nodes
Support for battery-powered nodes with a long lifecycle requires optimized Layer 2 forwarding or Layer 3 routing protocol implementations. This provides an extra level of complexity but is necessary in order to cope with sleeping battery-powered nodes

Security

encryption is provided by AES, with a 128-bit key. In addition to the Auxiliary Security Header field initially defined in 802.15.4-2006, a secure acknowledgement and a secure Enhanced Beacon field complete the MAC layer security

Figure 4-10 *IEEE 802.15.4g/e MAC Layer Security*



The full frame in gets authenticated through the MIC at the end of frame. The MIC is a unique value that is calculated based on the frame contents. The Security Header field denoted in _is composed of the Auxiliary Security field and one or more Information Elements fields. Integration of the Information Elements fields allows for the adoption of additional security capabilities,

Key Management Protocol (KMP) specification. KMP provides a means for establishing keys for robust datagram security

IEEE 1901.2a
This is a standard for Narrowband Power Line Communication (NB-PLC). NB-PLC leverages a narrowband spectrum for low power, long range, and resistance to interference over the same wires that carry electric power.

Smart metering: NB-PLC can be used to automate the reading of utility meters, such as electric, gas, and water meters. This is true particularly in Europe, where PLC is the preferred technology for utilities deploying smart meter solutions.
Distribution automation: NB-PLC can be used for distribution automation, which involves monitoring and controlling all the devices in the power grid.
Public lighting: A common use for NB-PLC is with public lighting—the lights found in cities and along streets, highways, and public areas such as parks.
Electric vehicle charging stations: NB-PLC can be used for electric vehicle charging stations, where the batteries of electric vehicles can be recharged.
Microgrids: NB-PLC can be used for microgrids, local energy grids that can disconnect from the traditional grid and operate independently.
Renewable energy: NB-PLC can be used in renewable energy applications, such as solar, wind power, hydroelectric, and geothermal heat.

Standardization and Alliances
The first generations of NB-PLC implementations suffered from poor reliability, low throughput (in the range of a few hundred bits per second to a maximum of 2kbps), lack of manageability, and poor interoperability.
based on orthogonal frequency-divisionmultiplexing (OFDM)

OFDM encodes digital data on multiple carrier frequencies. This provides several parallel streams that suffer less from high frequency attenuation in copper wire and narrowband interference.
IEEE 1901.2 working group, G3-PLC (now ITU G.9903) and PRIME (now ITU G.9904) working groups,

The HomePlug Alliance was one of the main industry organizations that drove the promotion and certification of PLC technologies, with IEEE 1901.2a being part of its HomePlug Netricity program

alliance's broadband power line networking technology

- has also partnered with other alliances on continuing ongoing work. The HomePlug Alliance has struck a liaison agreement with the Wi-SUN Alliance with the goal of enabling hybrid smart grid networks that support both wireless and power line–wired connectivity.

Physical Layer
NB-PLC is defined for frequency bands from 3 to 500 kHz
Specifications include support for CENELEC A and B bands, US FCC-Low and FCC-above-CENELEC, and Japan ARIB bands.
The CENELEC A and B bands refer to 9–95 kHz and 95–125 kHz, respectively
The FCC-Low band encompasses 37.5–117.1875 kHz, and the FCC-above-CENELEC band is

154.6875–487.5 kHz

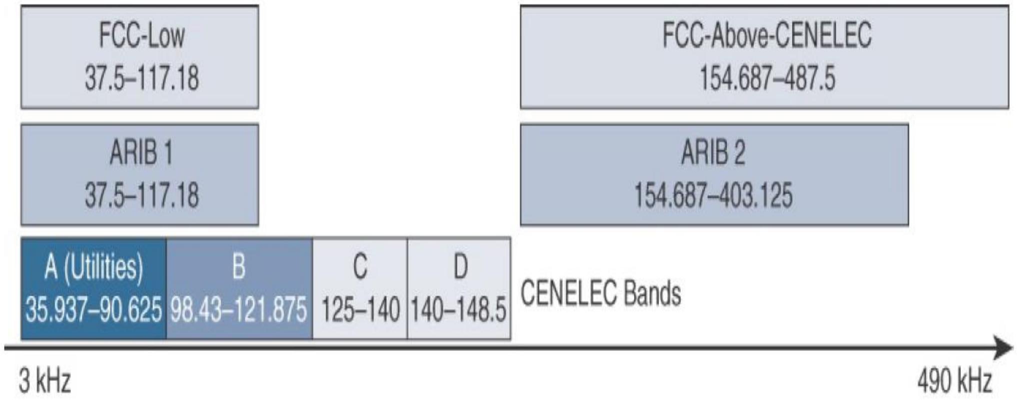


Figure 4-11 *NB-PLC Frequency Bands*

supports the largest set of coding and enables both robustness and
throughput.
The standard includes tone maps and modulations, such as
Robust modulation (ROBO), :transmits redundant information on multiple carriers,
differential binary phase shift keying (DBPSK),
differential quadrature phase shift keying (DQPSK),
differential 8-point phase shift keying (D8PSK) for all bands, and optionally
16 quadrature amplitude modulation (16QAM) for some bands
the phase of a signal is changed to signal a binary data transmission

- With IEEE 1901.2a, the data throughput rate has the ability to dynamically change, depending on the modulation type and tone map.

- For CENELEC Aband, the data rate ranges from 4.5 kbps in ROBO mode to 46 kbps with D8PSK modulation

- FCC-above-CENELEC frequencies, throughput varies from 21 kbps in ROBO mode to a maximum of 234 kbps using D8PSK.

- IEEE 1901.2a is the full integration of different types of modulation and tone maps by a single PHY layer in the IEEE 1901.2a specification.

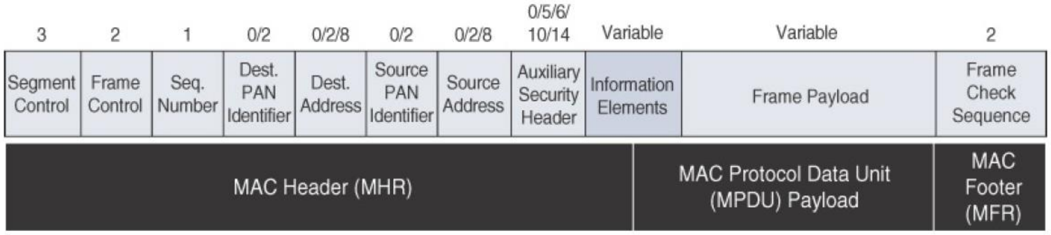
- The PHY payload size can change dynamically, based on channel conditions in IEEE 1901.2a.

- If the size of the MAC payload is too large to fit within one PHY service data unit (PSDU), the MAC payload is partitioned into smaller segments. MAC payload segmentation is done by dividing the MAC payload into multiple smaller amounts of data (segments), based on PSDU size. The segmentation may require the addition of padding bytes to the last payload segment so that the final MPDU fills the PSDU

MAC Layer

- The MAC frame format of IEEE 1901.2a is based on the IEEE 802.15.4 MAC frame but integrates the latest IEEE 802.15.4e-2012 amendment,

- Additional features information elements. With IE support, additional capabilities, such as IEEE 802.15.9 Key Management Protocol and SSID



3	2	1	0/2	0/2/8	0/2	0/2/8	0/5/6/ 10/14	Variable	Variable	2
Segment Control	Frame Control	Seq. Number	Dest. PAN Identifier	Dest. Address	Source PAN Identifier	Source Address	Auxiliary Security Header	Information Elements	Frame Payload	Frame Check Sequence
MAC Header (MHR)									MAC Protocol Data Unit (MPDU) Payload	MAC Footer (MFR)

Figure 4-12 *General MAC Frame Format for IEEE 1901.2*

- Segment Control field handles the segmentation or fragmentation of upper-layer packets with sizes larger than what can be carried in the MAC protocol data unit (MPDU).

Topology

NB-PLC deployments use some sort of mesh topology. Mesh networks offer the advantage of devices relaying the traffic of other devices so longer distances can be segmented. Highlights a network scenario in which a PLC mesh network is applied to a neighborhood.

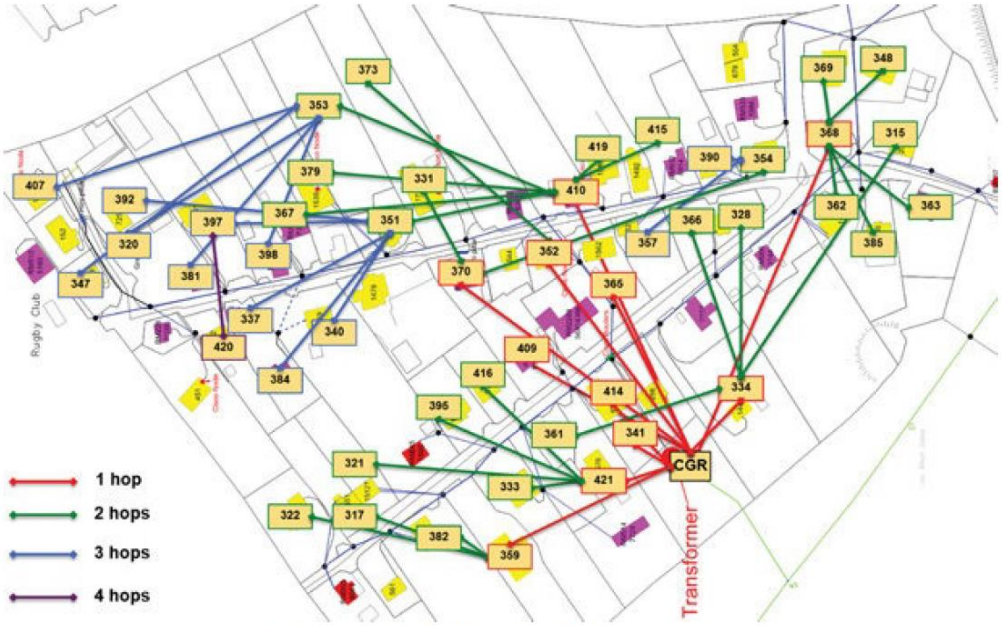


Figure 4-13 *IPv6 Mesh in NB-PLC*

Security

IEEE 1901.2a security offers similar features to IEEE 802.15.4g. Encryption and authentication are performed using AES.

IEEE 1901.2a aligns with 802.15.4g in its ability to support the IEEE 802.15.9 Key Management Protocol

- The Security Enabled bit in the Frame Control field should be set in all MAC frames carrying segments of an encrypted frame.
- If data encryption is required, it should be done before packet

segmentation. During packet encryption, the Segment Control field should not be included in the input to the encryption algorithm.

- On the receiver side, the data decryption is done after packet reassembly.
- When security is enabled, the MAC payload is composed of the cipheredpayload and the message integrity code (MIC) authentication tag for nonsegmented payloads. If the payload is segmented, the MIC is part of the last packet (segment) only. The MIC authentication is computed using only information from the MHR of the frame carrying the first segment.

IEEE 802.11ah

- IEEE 802.11ah to specify a sub-GHz version of Wi-Fi. Three main use cases are identified for IEEE 802.11ah
- Wi-Fi lacks sub-GHz support for better signal penetration, low power for battery-powered nodes, and the ability to support a large number of devices.
- Three main use cases are identified for IEEE 802.11ah:
- ■ **Sensors and meters covering a smart grid:** Meter to pole, environmental/agricultural monitoring, industrial process sensors, indoor healthcare system and fitness sensors, home and building automation sensors
- ■ **Backhaul aggregation of industrial sensors and meter data:** Potentially connecting IEEE 802.15.4g subnetworks
- ■ **Extended range Wi-Fi:** For outdoor extended-range hotspot or cellular traffic offloading when distances already covered by IEEE 802.11a/b/g/n/ac are not good enough

Standardization and Alliances

IEEE 802.11 working group operate in unlicensed sub-GHz frequency bands
The industry organization that promotes Wi-Fi certifications and interoperability
for 2.4 GHz and 5 GHz products is the Wi-Fi Alliance

the Wi-Fi Alliance defined a new brand called Wi-Fi HaLow.
“11ah” inreverse and “low power.” It is similar to the word “hello” but it is pronounced “hay-low.”

MAC Layer

providing low power consumption and the ability to support a larger number of endpoints.
MAC layer include the following:
Number of devices: Has been scaled up to 8192 per access point. MAC header: Has been shortened to allow more efficient communication.
Null data packet (NDP) support: Is extended to cover several control and management frames. Relevant information is concentrated in the PHY header and the additional overhead associated with decoding the MAC header and data payload is avoided. Grouping and **sectorization:** Enables an AP to use sector antennas and also group stations (distributing a group ID).
Restricted access window (RAW): Is a control algorithm that avoids simultaneous transmissions when many devices are present and provides fair access to the wireless network
Target wake time (TWT): Reduces energy consumption by permitting anaccess point to define times when a device can access the network. This allows devices to enter a low-power state until their TWT time arrives.

Speed frame exchange: Enables an AP and endpoint to exchange frames during a reserved transmit opportunity (TXOP). This reduces contention on the medium, minimizes the number of frame exchanges to improve channel efficiency, and extends battery life by keeping awake times short.

Topology
IEEE 802.11ah is deployed as a star topology, it includes a simple hops
relay operation to extend its range.

task group worked on the assumption of two hops. It allows one 802.11ah device to act as an intermediary and relay data to another This relay operation can be combined with a higher transmission rate or modulation and coding scheme (MCS)

The transmit rate reduces as you move further from the access point via relay clients. This ensures an efficient system that limits transmission speeds at the edge of the relays so that communications close to the AP are not negatively affected.

Sectorization is a technique that involves partitioning the coverage area into several sectors to get reduced contention within a certain sector.

- Limiting collisions in cells that have many clients.

- The coverage area of 802.11ah access points is large, and interference from neighbouring access points is problematic.
  Sectorization uses an antenna array and beam-forming techniques to partition the cell

coverage area.

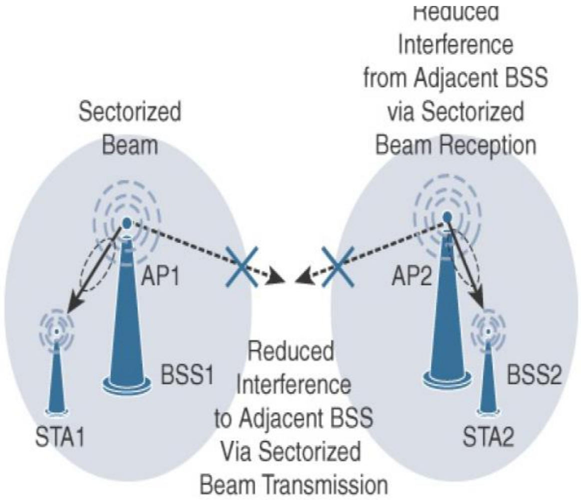


Figure 4-14 *IEEE 802.11ah Sectorization*

Security

No additional security has been identified for IEEE 802.11ah compared to other IEEE 802.11 specifications.

Competitive Technologies

Competitive technologies to IEEE 802.11ah are IEEE 802.15.4 and IEEE 802.15.4e, along with the competitive technologies highlighted in each of their sections.

LoRaWAN

LPWA technologies open new business opportunities to both services providers and enterprises considering IoT solutions.

unlicensed-band LPWA technology

Standardization and Alliances

LoRa was a physical layer, or Layer 1, modulation that was developed by a French company named Cycleo

Optimized for long-range, two-way communications and low power consumption, the technology evolved from Layer 1 to a broader scope through the creation of the LoRa Alliance 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.

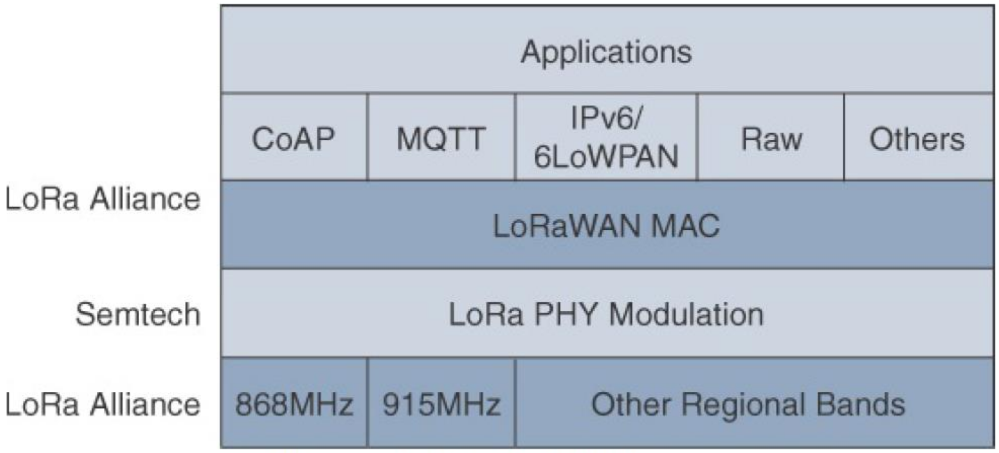


Figure 4-15 *LoRaWAN Layers*

Physical Layer

Semtech LoRa modulation is based on chirp spread spectrum modulation,

trades a lower data rate for receiver sensitivity to significantly increase the communication distance.
it allows demodulation below the noise floor, offers robustness to noise and interference, and manages a single channel occupation by different spreading factors.

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.
The data rate in LoRaWAN varies depending on the frequency bands and adaptive data rate (ADR)

ADR is an algorithm that manages the data rate and radio signal for each endpoint.

delivered at the best data rate possible and that network performance is both optimal and scalable.

Endpoints close to the gateways with good signal values transmit with the highest data rate, which enables a shorter transmission time over the wireless network, and the lowest transmit power

LoRaWAN data rates can vary depending on the associated spreading factor for the two main frequency bands, 863–870 MHz and 902–928 MHz.

MAC Layer

This layer takes advantage of the LoRa physical layer and classifies LoRaWAN endpoints to optimize their battery life and ensure downstream communications to the LoRaWAN endpoints.

The LoRaWAN specification documents three classes of LoRaWAN devices:
Class A: This class is the default implementation. Optimized for battery powered nodes, it allows bidirectional communications, where a given node is able to receive downstream traffic after transmitting. Two receive windows are available after each transmission.
Class B: This class was designated "experimental" in LoRaWAN 1.0.1 until it can be better defined. 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.

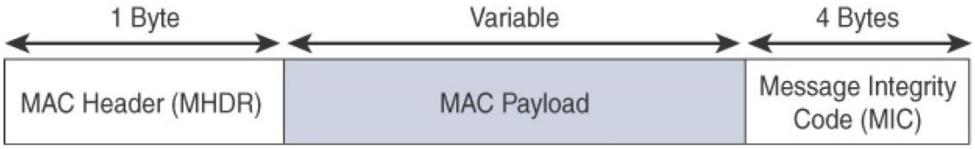


Figure 4-16 *High-Level LoRaWAN MAC Frame Format*

LoRaWAN messages, either uplink or downlink, have a PHY payload composedof a 1-byte MAC header, a variable-byte MAC payload, and a MIC that is 4 bytes in length. The MAC payload size depends on the frequency band and the data rate, ranging from 59 to 230 bytes for the 863–870 MHz band and 19 to 250 bytes for the 902–928 MHz band.

LoRaWAN utilizes six MAC message types.

- LoRaWAN devices use join request and join accept messages for over-the-air (OTA) activation and joining the network.
- The other message types are unconfirmed data up/down and confirmed data up/down. A "confirmed" message is one that must be acknowledged, and "unconfirmed" signifies that the end device does not need to acknowledge.
- "up/down" is simply a directional notation identifying whether the message flows in the uplink or downlink path.
- Uplink messages are sent from endpoints to the network server and are relayed by one or more LoRaWAN gateways.
- Downlink messages flow from the network server to a single endpoint and are relayed by only a single gateway. Multicast over LoRaWAN is being considered for future versions.

LoRaWAN endpoints are uniquely addressable through a variety of methods, including the following:

- An endpoint can have a global end device ID or DevEUI represented as an IEEE EUI-64 address.

- An endpoint can have a global application ID or AppEUI represented as an IEEE EUI-64 address that uniquely identifies the application provider, such as the owner, of the end device.

- In a LoRaWAN network, endpoints are also known by their end device address, known as a DevAddr, a 32-bit address. The 7 most significant bits are the network identifier (NwkID), which identifies the LoRaWAN network. The 25 least significant bits are used as the network address (NwkAddr) to identify the endpoint in the network.

Topology

LoRaWAN topology is often described as a “star of stars” topology. the infrastructure consists of endpoints exchanging packets through gateways acting as bridges, with a central LoRaWAN network server.

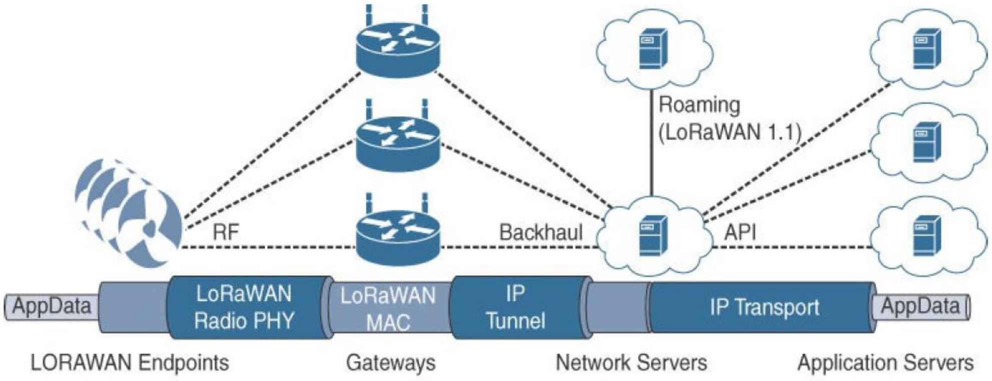


Figure 4-17 *LoRaWAN Architecture*

- LoRaWAN endpoints transport their selected application data over the LoRaWAN MAC layer on top of one of the supported PHY layer frequency bands. The application data is contained in upper protocol layers. These upper layers are not the responsibility of the LoRa Alliance, but best practices may be developed and recommended upper-layer protocols, such as ZigBee Control Layer (ZCL)
- The LoRaWAN network server manages the data rate and radio frequency (RF) of each endpoint through the adaptive data rate (ADR) algorithm. ADR is a key component of the network scalability, performance, and battery life of the endpoints

Security

Figure 4-18 LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.

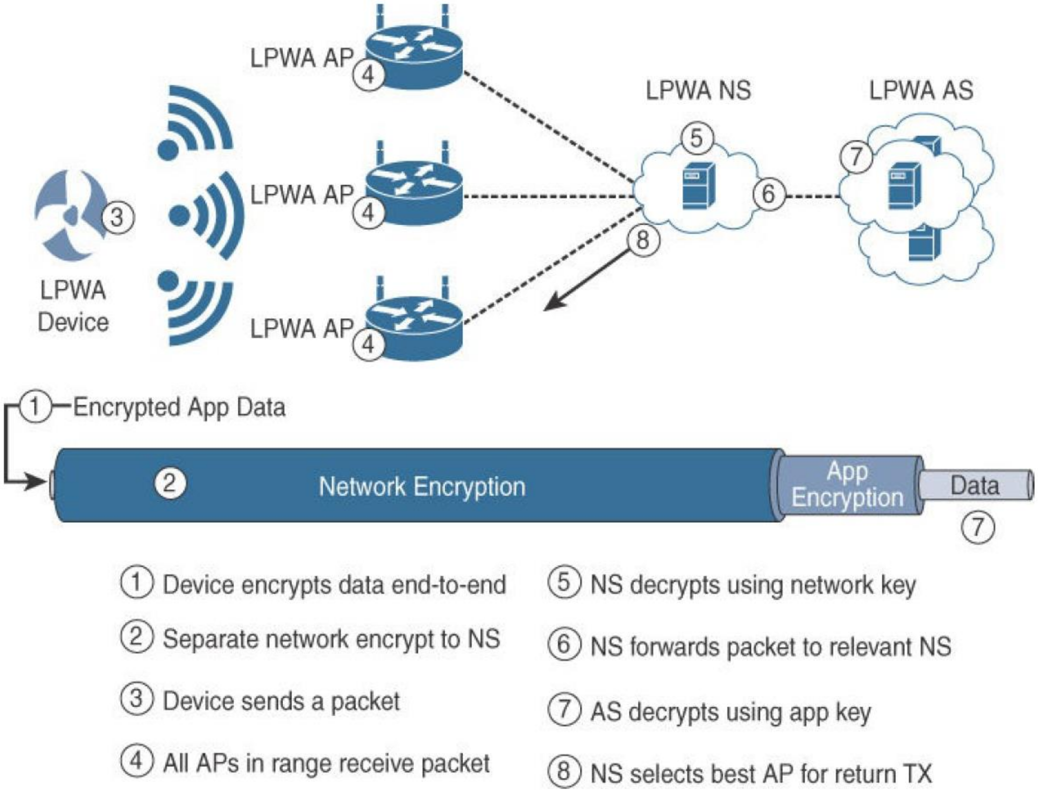

LPWA AP
4
LPWA AP
4
LPWA AP
4
LPWA NS
5
6
LPWA AS
7
8
3
LPWA Device
1 Encrypted App Data
2
Network Encryption
App Encryption
Data
7
1 Device encrypts data end-to-end
2 Separate network encrypt to NS
3 Device sends a packet
4 All APs in range receive packet
5 NS decrypts using network key
6 NS forwards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

Figure 4-18 *LoRaWAN Security*

The first layer, called "network security" but applied at the MAC layer, guarantees the authentication of the endpoints by the LoRaWAN network server. Also, it protects LoRaWAN packets by performing encryption based on AES.

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-only data message payloads.

The second layer is an application session key (AppSKey), which performs encryption and decryption functions between the endpoint and its application server. Furthermore, it computes and checks the application-level MIC, if included. This ensures that the LoRaWAN service provider does not have access to the application payload if it is not allowed that access.

Endpoints receive their AES-128 application key (AppKey) from the application owner. This key is most likely derived from an application-specific root key exclusively known to and under the control of the application provider.

For production deployments, it is expected that the LoRaWAN gateways are protected as well, for both the LoRaWAN traffic and the network management and operations over their backhaul link(s). This can be done using traditional VPN and IPsec technologies that demonstrate scaling in traditional IT deployments. Additional security add-ons are under evaluation by the LoRaWAN Alliance for future revisions of the specification.

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. This same information is registered in the LoRaWAN network server.

- **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. During the join process, which involves the sending and receiving of MAC layer join request and join accept messages, the node establishes its credentials with a LoRaWAN network server, exchanging its globally unique DevEUI, AppEUI, and AppKey. The AppKey is then used to derive the session NwkSKey and AppSKey keys.

NB-IoT and Other LTE Variations

Existing cellular technologies, such as GPRS, Edge, 3G, and 4G/LTE, are not particularly well adapted to battery-powered devices and small objects specifically developed for the Internet of Things. The aim was to both align with specific IoT requirements, such as low throughput and low power consumption, and decrease the complexity and cost of the LTE devices. This resulted in the definition of the LTE-M work item.

Standardization and Alliances

The 3GPP organization includes multiple working groups focused on many different aspects of telecommunications (for example, radio, core, terminal, and so on). The workflow within 3GPP involves receiving contributions related to licensed LPWA work from the involved vendors. Then, depending on the access technology that is most closely aligned, such as 3G, LTE, or GSM, the IoT-related contribution is handled by either 3GPP or the GSM EDGE Radio Access Networks (GERAN) group.

LTE Cat 0

The first enhancements to better support IoT devices in 3GPP occurred in LTE Release 12. A new user equipment (UE) category, Category 0, was added, with devices running at a maximum data rate of 1 Mbps. Generally, LTE enhancements target higher bandwidth improvements. Category 0 includes important characteristics to be supported by both the network and end devices. Meanwhile, the UE still can operate in existing LTE systems with bandwidths up to 20 MHz. These Cat 0 characteristics include the following:

- **Power saving mode (PSM):** This new device status minimizes energy consumption. Energy consumption is expected to be lower with PSM than with existing idle mode. PSM is defined as being similar to “powered off” mode, but the device stays registered with the network. By staying registered, the device avoids having to reattach or reestablish its network connection. The device negotiates with the network the idle time after which it will wake up. When it wakes up, it initiates a tracking area update (TAU), after which it stays available for a configured time and then switches back to sleep mode or PSM. A TAU is a procedure that an LTE device uses to let the network know its current tracking area, or the group of towers in the network from which it can be reached. Basically, with PSM, a device can be practically powered off but not lose its place in the network.

- **Half-duplex mode:** This mode reduces the cost and complexity of a device's implementation because a duplex filter is not needed. Most IoT endpoints are sensors that send low amounts of data that do not have a full-duplex communication requirement.

LTE-M

Following LTE Cat 0, the next step in making the licensed spectrum more supportive of IoT devices was the introduction of the LTE-M category for 3GPP LTE Release 13. These are the main characteristics of the LTE-M category in Release 13:

- **Lower receiver bandwidth:** Bandwidth has been lowered to 1.4 MHz versus the usual 20 MHz. This further simplifies the LTE endpoint.
- **Lower data rate:** Data is around 200 kbps for LTE-M, compared to 1 Mbps for Cat 0.
- **Half-duplex mode:** Just as with Cat 0, LTE-M offers a half-duplex mode that decreases node complexity and cost.
- **Enhanced discontinuous reception (eDRX):** This capability increases from seconds to minutes the amount of time an endpoint can "sleep" between paging cycles. A paging cycle is a periodic check-in with the network. This extended "sleep" time between paging cycles extends the battery lifetime for an endpoint significantly

NB-IoT

Recognizing that the definition of new LTE device categories was not sufficient to support LPWA IoT requirement, 3GPP specified Narrowband IoT (NB-IoT). The work on NB-IoT started with multiple proposals pushed by the involved vendors, including the following:

- Extended Coverage GSM (EC-GSM), Ericsson proposal
- Narrowband GSM (N-GSM), Nokia proposal
- Narrowband M2M (NB-M2M), Huawei/Neul proposal
- Narrowband OFDMA (orthogonal frequency-division multiple access), Qualcomm proposal
- Narrowband Cellular IoT (NB-CIoT), combined proposal of NB-M2M and NBOFDMA
- Narrowband LTE (NB-LTE), Alcatel-Lucent, Ericsson, and Nokia proposal
- Cooperative Ultra Narrowband (C-UNB), Sigfox proposal

Consolidation occurred with the agreement to specify a single NB-IoT version based on orthogonal frequency-division multiple access (OFDMA) in the downlink and a couple options for the uplink. OFDMA is a modulation scheme in which individual users are assigned subsets of subcarrier frequencies. This enables multiple users to transmit low-speed data simultaneously. For more information on the uplink options, refer to the 3GPP specification TR 36.802.

Three modes of operation are applicable to NB-IoT:

- **Standalone:** A GSM carrier is used as an NB-IoT carrier, enabling reuse of 900 MHz or 1800 MHz.
- **In-band:** Part of an LTE carrier frequency band is allocated for use as an NB-IoT frequency. The service provider typically makes this allocation, and IoT devices are configured accordingly. You should be aware that if these devices must be deployed across different countries or regions using a different service provider, problems may occur unless there is some coordination between the service providers, and the NB-IoT frequency band allocations are the same.
- **Guard band:** An NB-IoT carrier is between the LTE or WCDMA bands.

This requires coexistence between LTE and NB-IoT bands.

Mobile service providers consider NB-IoT the target technology as it allows them to leverage their licensed spectrum to support LPWA use cases. For instance, NB-IoT is defined for a 200-kHz-wide channel in both uplink and downlink, allowing mobile service providers to optimize their spectrum, with a number of deployment options for GSM, WCDMA, and LTE spectrum, as shown in Figure 4-19.

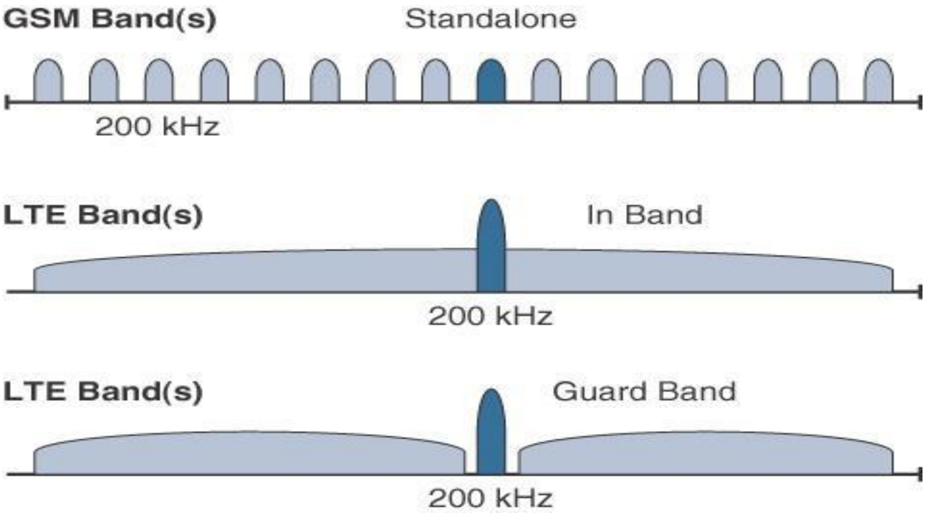


Figure 4-19 *NB-IoT Deployment Options*

In an LTE network, resource blocks are defined with an effective bandwidth of 180 kHz, while on NB-IoT, tone or subcarriers replace the LTE resource blocks. The uplink channel can be 15 kHz or 3.75 kHz or multi-tone (n*15 kHz, n up to 12). At Layer 1, the maximum transport block size (TBS) for downlink is 680 bits, while uplink is 1000 bits. At Layer 2, the maximum Packet Data Convergence Protocol (PDCP) service data unit (SDU) size is 1600 bytes.

NB-IoT operates in half-duplex frequency-division duplexing (FDD) mode with a maximum data rate uplink of 60 kbps and downlink of 30 kbps.

Topology

NB-IoT is defined with a link budget of 164 dB; compare this with the GPRS link budget of 144 dB, used by many machine-to-machine services. The additional 20 dB link budget increase should guarantee better signal penetration in buildings and basements while achieving battery life requirements.

Competitive Technologies

In licensed bands, it is expected that 3GPP NB-IoT will be the adopted LPWA technology when it is fully available. Competitive technologies are mostly the unlicensed-band LPWA technologies such as LoRaWAN. The main challenge faced by providers of the licensed bands is the opportunity for non-mobile service providers to grab market share by offering IoT infrastructure without buying expensive spectrum.