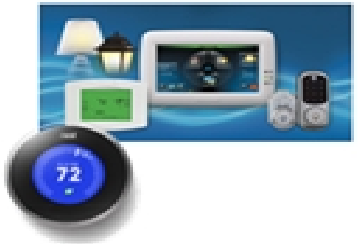
Chapter 4 Connecting Smart Objects

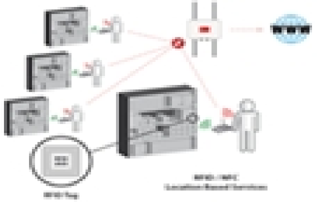
Data Collection Devices

Smart Machinery

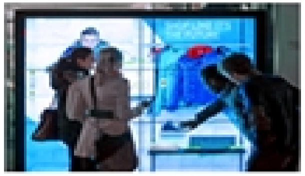
Phones and Tablets



Home Automation



RFID Systems



Digital Signage

Security Systems

Medical Devices

For IoT to produce data that is to be visualized, the sensors and actuators have to be connected using various protocols.

To achieve this connectivity, **characteristics and communications criteria** as well as **The various technologies used** need to be studied

The communication criteria that needs to be expounded include;

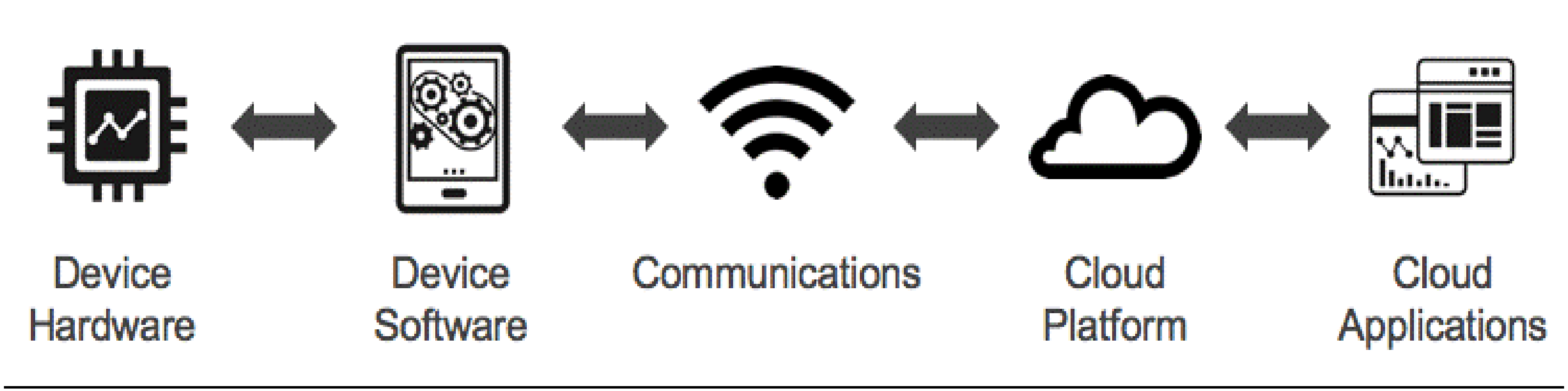
- Range, Frequency Bands, Power Consumption, Topology, Constrained Devices, Constrained-Node Networks.

Technologies for connecting smart objects include;

- IEEE 802.15.4, IEEE 802.15.4g and IEEE 802.15.4e, IEEE 1901.2a, IEEE 802.11ah, LoRaWAN, NB-IoT and Other LTE Variations.

1. Communications Criteria

In connecting things both wired and wireless connections are available or under development.



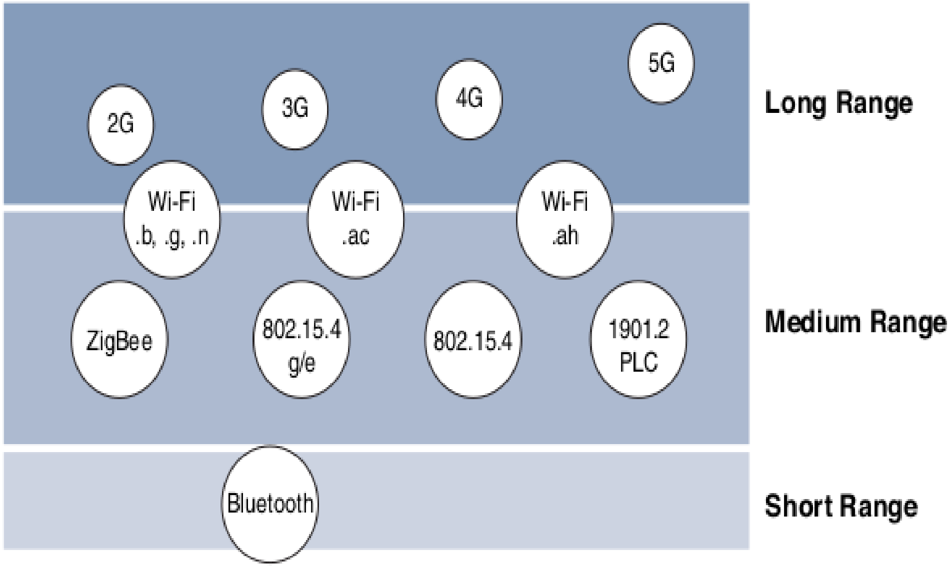
[Image from Senseware blog on iot-implementations-wireless-vs-wired]

Wireless Connections is more prevalent over wired because it eases deployment and allows smart objects to be mobile, changing location without losing connectivity. But nevertheless, wired connections are used where necessary.

1. Range

Range as one of the communication criteria helps us to answer the following questions while evaluating options of wired and wireless access technologies.

- How far does the signal need to be propagated?
- That is, what will be the area of coverage for a selected wireless technology?
- Should indoor versus outdoor deployments be differentiated?



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. Signals are transmitted as low as 10 kbit/s making it not suitable for deployment in most cases.

Examples include Bluetooth and Visible Light Communications

Medium Range

- This connection spans from 10 to 100 of meters, the maximum distance is generally 1 mile (1600 meters) between two devices.

RF technologies do not have real maximum distances defined, as long as the radio signal is transmitted and received in the scope of the applicable specification.

Medium Range Wireless Technologies	Wired Technologies
-IEEE 802.11 Wi-Fi,	-IEEE 802.3 Ethernet
-IEEE 802.15.4,	-IEEE 1901.2 Narrowband Power Line Communications (PLC)
-802.15.4g WPAN	

- **Long range**

  Two devices with distance of 1 mile between themselves require long – range technologies.

  Examples include cellular(2G, 3G and 4G and 5G) and outdoor IEEE 802.11 Wi-Fi and Low-Power Wide-Area (LPWA) technologies.

  Long range connections are found mainly in Industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications.

  For wireless deployment, consider;

  - Specifications or product descriptions
  - A proper radio planning using appropriate tools
  - Field radio survey to better understand the actual conditions in a given area such as noise and interference
  - Landscape and topology changes in the field such as buildings that may interfere with signal transmission

2. Frequency Bands

Frequency bands are ranges of radio wave frequencies used to transmit data in the wireless spectrum, and can further be broken down into WiFi channels. The higher the frequency, the faster the data transmission and shorter the signal range.

- Focusing on 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 (for example, first responders, military), broadcasters, and utilities.

When deploying large numbers of devices in licensed spectrum, there are platforms such as CISCO Jasper Control Center which make automating the provisioning, deployment, and management of large numbers of devices has become much easier.

Licensed vs Unlicensed bands

Licensed Spectrum is that in which users must subscribe to services when connecting their IoT devices. Licensed spectrum include

Cellular, WiMAX and NarrowBand IoT(NB-IoT) Technologies.

Unlicensed means that no guarantees or protections are offered in the ISM(Industrial, Scientific and Medical) bands for device communications. These bands are not regulated

Examples include; 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi, IEEE 802.15.1 Bluetooth, IEEE 802.15.4 WPAN

Regulation of bands mandates device compliance on parameters such as transmit power, duty cycle and dwell time, channel bandwidth, and channel hopping.

Unlicensed spectrum is usually simpler to deploy as it does not require service provider but suffer reliability and performance issues frequently than those implementing licensed spectrum

- See … https://www.iotacommunications.com/blog/licensed-vs-unlicensed-spectrum/

Sub-GHz range

- Some communications within the 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

  Advantage of Sub-Ghz bands;

  - Sub-GHz bands allow greater distances between devices better than the 2.4 GHz ISM band.
  - Low power consumption

  Disadvantage of Sub-GHz bands;

  - Lower rate of data delivery compared to higher frequencies(not a concern for IoT Sensors)

  Several sub-GHz ranges have been defined in the ISM band. The most well-known ranges are centered on 169 MHz, 433 MHz, 868 MHz, and 915 MHz. However, most IoT access technologies tend to focus on the two sub-GHz frequency regions around 868 MHz and 915 MHz.

Band Regulation parameters

- Several bands in different countries are not licensed but they are just regulated.

  The regulators document parameters such as;

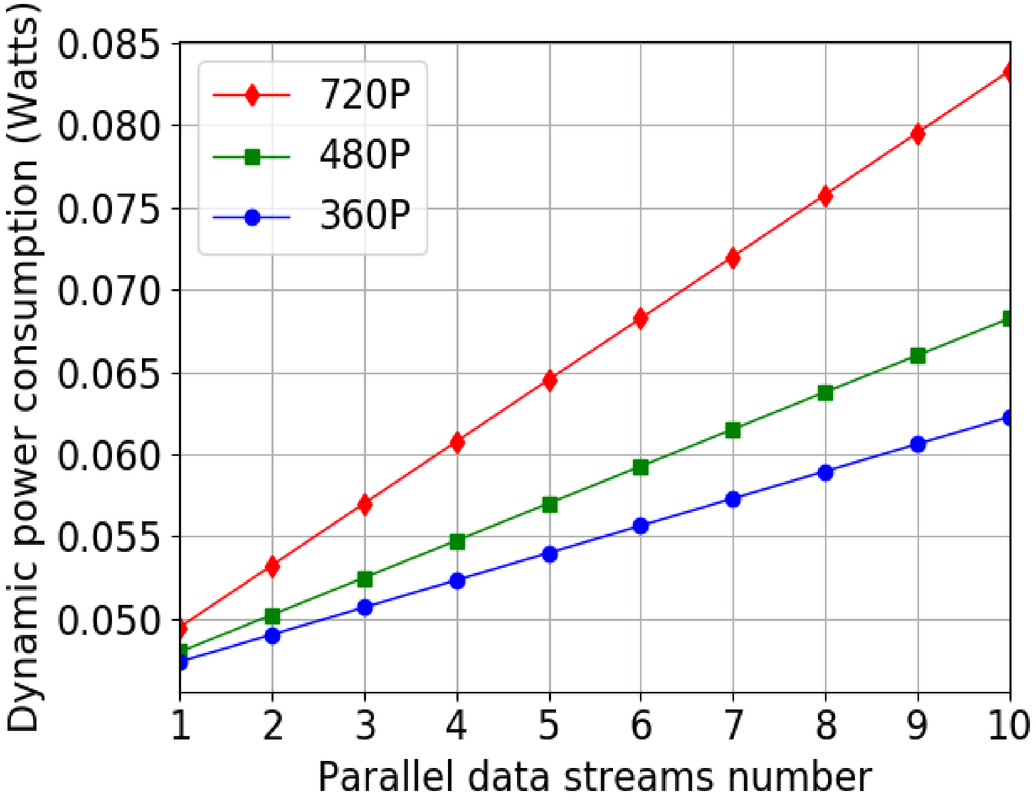
  - Channel bandwidth; effective bandwidth multiplied by frequency reuse factor
  - Channel Hopping; works by synchronizing the nodes in the network along a sequence of channels. All nodes must know the sequence and all nodes must know where in the sequence they should be.
  - Transmit Power; The proportionality of effective range to the access point Higher Transmitting power, the farther the signal travel
  - Dwell Time; (or transmit time) is the amount of time needed to transmit on a frequency.

- The UCC in Uganda notes that, the use of wireless devices in the bands 5150-5350 MHz, 5470-5725 MHz and 5725-5825 MHz for Wireless Access Systems including Radio Local Area Networks (WAS/RLAN′s) would be used to enhance wireless connection in the country. For more details https://www.ucc.co.ug/files/downloads/Guidelines-for-use-of-5.8-GHz-ISM-band.pdf

3.Power Consumption

A powered node has a direct connection to a power source, and communications are usually not limited by power consumption criteria

- IoT wireless access technologies must address the needs of low power consumption and connectivity for battery-powered nodes.
- This need for reduced power consumption has led to Low-Power Wide-Area (LPWA) wireless environment.
- Wired IoT technologies are not exempted from power consumption



4. Topology

A topology defines the way various components communicate with each other within an IoT network.

- Star topology-
- Peer-to-peer-
- Mesh topology-

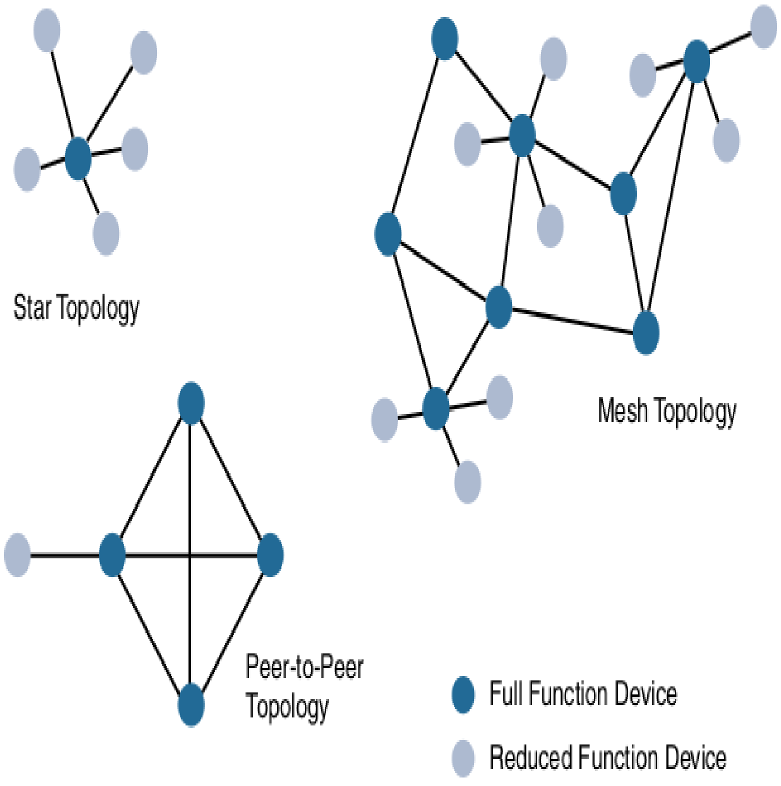


Figure 4-2 *Star, Peer-to-Peer, and Mesh Topologies*

4. Constrained Devices

- While categorizing the class of IoT nodes, constrained devices can be defined in terms of perilous exercise, with computing, memory, storage, power, and networking continuously evolving and improving.

- Constrained nodes have limited resources that impact their networking feature set and capabilities.

  Classes of Constrained Nodes, as Defined by RFC 7228

  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 forexample a push button.

  Class 1; These nodes can implement an optimized stack specifically designed for constrained nodes, such as Constrained Application Protocol (CoAP) example are environmental sensors.

  Class 2; These nodes are characterized by running full implementations of an IP stack on embedded devices. Example power meter

Constrained-Node Networks

These are often referred to as low-power and lossy networks (LLNs).

- Low Power refers to the fact that nodes must cope with the requirements from powered and battery-powered constrained nodes
- Lossy networks indicates that network performance may suffer from interference and variability due to harsh radio environments

Characteristics of protocols used in constrained-Node Network.

- Latency and Determinism
- Data Rate and Throughput
- Overhead and Payload

IoT Access Technologies

- This criteria highlights technologies that are seen as having market and/or mind share.

  The following topics address the 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

Access Technologies

- IEEE 802.15.4
- IEEE 802.15.4g and 802.15.4e
- IEEE 1901.2a
- IEEE 802.11ah
- LoRaWAN
- NB-IoT and Other LTE Variations

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. It enables easy installation.
- It can be found in the following deployments

  Home and building automation

  Automotive networks

  Industrial wireless sensor networks

  Interactive toys and remote controls
- Criticism of IEEE 802.15.4

  MAC reliability; Other devices are transmitting so there is back-off(waiting and listening time before transmission)

  Unbound Latency
- Multi-path fading; Multipath fading refers to multiple copies of the signal hitting the receiver at different points in time because of different signal paths and reflections, IEEE.802.15.2 lacks a frequency-hopping technique

Protocols based on IEEE 802.15.4

1. ZigBee;

   – It defines upper-layer components (network through application) as well as application profiles. These include building automation, home automation, and healthcare

2. 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

3. ZigBee IP;

   – It adopts the 6LoWPAN adaptation layer, IPv6 network layer, and RPL routing protocol

4. ISA100.11a;

   – ISA100.11a is developed by the International Society of Automation (ISA) as "Wireless Systems for Industrial Automation: Process Control and Related Applications."

   other protocols include; WirelessHART and Thread.

ZigBee

- ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs. Furthermore, products that are ZigBee compliant and certified by the ZigBee Alliance should interoperate even though different vendors may manufacture them.

The application support layer in Figure 4-3 interfaces the lower portion of the stack dealing with the networking of ZigBee devices with the higher-layer applications.

Network and security layer provides mechanisms for network startup, configuration, routing, and securing communications. and topology.

MAC Layer; defines how devices in the same area will share the frequencies allocated.

PHY Layer; this defines how frequencies are modulated

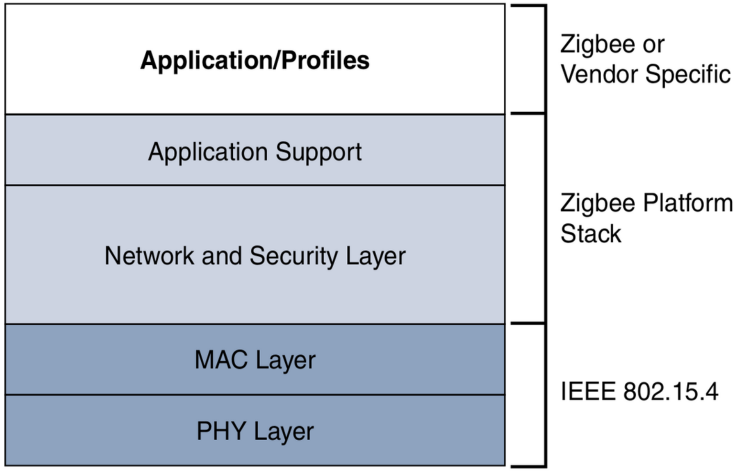


Figure 4-3 *High-Level ZigBee Protocol Stack*

ZigBee has not provided interoperability with other IoT solutions that is why ZigBee was developed

ZigBee IP

- In this IEEE 802.15.4 continues with support of IP and TCP/UDP protocols and various other open standards

  ZigBee IP was designed specifically for Smart Energies SE 2.0 but it is not limited to this use case

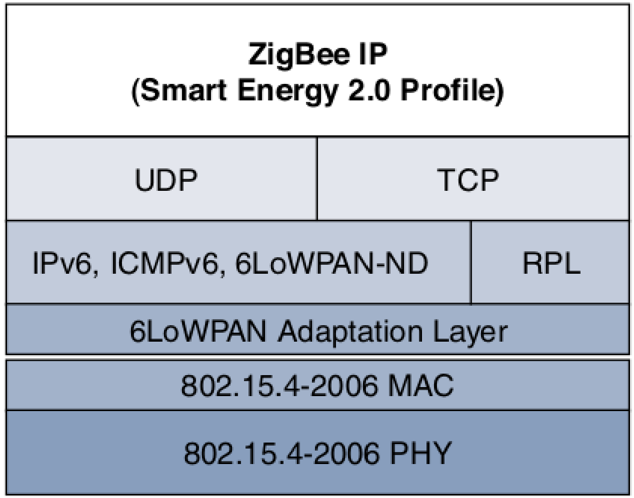


Figure 4-4 *ZigBee IP Protocol Stack*

-ZigBee IP supports 6LoWPAN as an adaptation layer unlike ZigBee.

-At Network layer ZigBee IP nodes support IPv6, ICMPv6, and 6LoWPAN Neighbor Discovery (ND)

The compelling protocol stack of ZigBee opens up opportunities for ZigBee IP to integrate and interoperate on just about any 802.15.4 network with other solutions built on these open IoT standards

PHY and MAC layers of 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.

  The original IEEE 802.15.4-2003 standard specified only three PHY options based on direct sequence spread spectrum (DSSS) modulation, Originally, the transmission layer was 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

- The following were introduced to support the above three in communication

  - OQPSK PHY: employs offset quadrature phase-shift keying (OQPSK) modulation
  - BPSK PHY: employs binary phase-shift keying (BPSK) modulation
  - ASK PHY: employs amplitude shift keying (ASK) and BPSK modulation

  These improvements increase the maximum data rate for both 868 MHz and 915 MHz to 100 kbps and 250 kbps, respectively.

IEEE 802.15.4 PHY Format

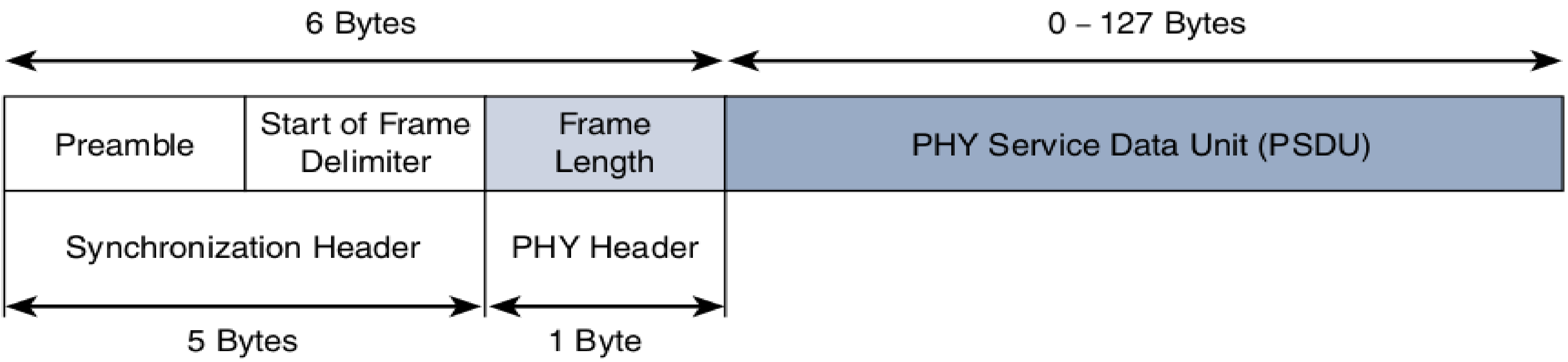


Figure 4-5 *IEEE 802.15.4 PHY Format*

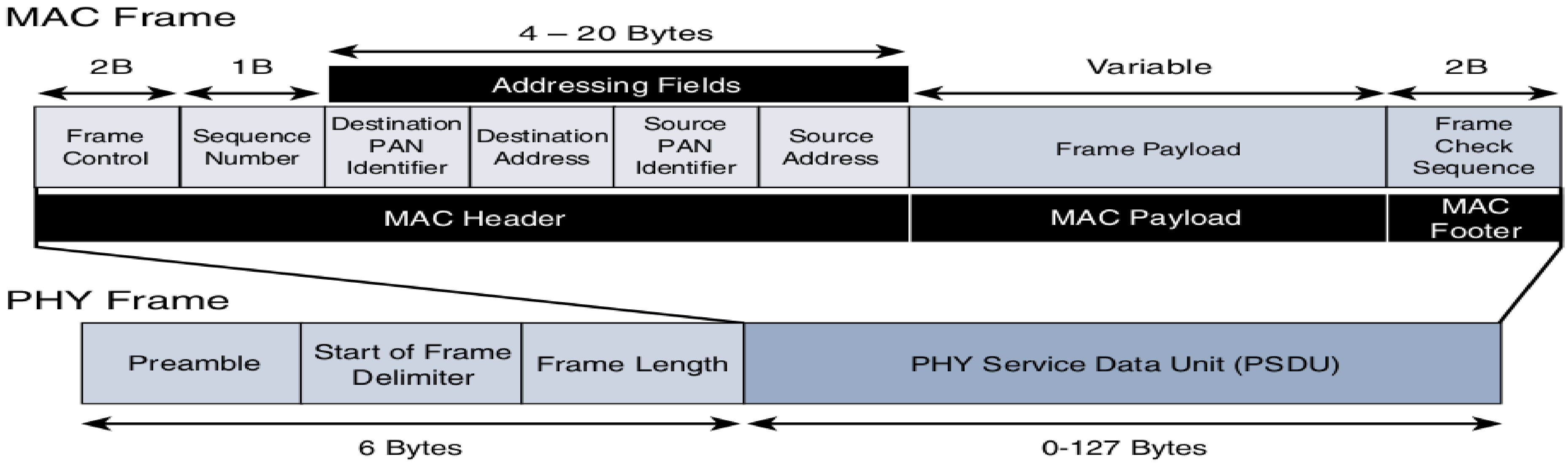
The **PHY Header** portion of the PHY frame shown in Figure 4-5 is simply a frame length value. It lets the receiver know how much total data to expect in the PHY service data

Products and solutions implementing PHY must refer to the proper IEEE 802.15.4 specification, frequency band, modulation, and data rate

MAC Layer of IEEE 802.15.4

- 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.
- **Tasks** performed at Mac Layer
  - 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
- These tasks can be achieved using predefined data **frame types**;
  - 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 802.15.2 MAC Layer Format



Frame Control field: defines attributes such as frame type, addressing modes, and other control flags.

Sequence Number field indicates the sequence identifier for the frame

Addressing field specifies the Source and Destination PAN Identifier fields as well as the Source and Destination Address fields

MAC Payload field defines payloads related to beacons and MAC commands

MAC Footer field defines a frame check sequence, calculation of data in the frame

IEEE 802.15.4 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.

- This allows nodes that would be out of range if trying to communicate directly to leverage intermediary nodes to transfer communications.

IEEE 802.15.4 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.

In addition to encrypting the data, AES in 802.15.4 also validates the data that is sent. This 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

IEEE 802.15.4 Competitive Technologies

The main competitor to IEEE 802.15.4 is DASH7, another wireless technology that compares favorably. However, IEEE 802.15.4 has an edge in the marketplace through all the different vendors and organizations that utilize its PHY and MAC layers. As 802.15.4 continues to evolve, you will likely see broader adoption of the IPv6 standard at the network layer.

For IoT sensor deployments requiring low power, low data rate, and low complexity, the IEEE 802.15.4 standard deserves strong consideration.

IEEE 802.15.4g and 802.15.4e

It is important to remember that IEEE 802.15.4g and 802.15.4e are simply amendments to the IEEE 802.15.4 standard.

They are mature specifications that are integrated into IEEE 802.15.4-2015.

They have been successfully deployed in real-world scenarios, and already support millions of endpoints.

IEEE 802.15.4g focuses mainly on improvements to the PHY layer, while IEEE 802.15.4e targets the MAC layer.

These improvements overcome many of the disadvantages of IEEE 802.15.4, such as latency and vulnerability to multipath fading. In addition, provisions in these amendments make them better suited to handle the unique deployment models in the areas of smart grid/utilities and smart cities.

There is an expectation to increasing use of both 802.15.4g and 802.15.4e, especially in the smart grid and smart cities verticals of IoT, where they have already seen strong adoption.

IEEE 1901.2a

IEEE 1901.2a is an open PHY and MAC standard approach to enable the use of Narrowband Power Line Communication. The set of use cases for this standard depends on and also benefits from the physical power lines that interconnect the devices.

The IEEE 1901.2a standard leverages the earlier standards G3-PLC (now ITU G.9903) and PRIME (now ITU G.9904). Supporting a wide range of frequencies at the PHY layer,

IEEE 1901.2a also has a feature-rich MAC layer, based on 802.15.4. This flexibility in the MAC layer lends readily to the support of mesh topologies.

The HomePlug Alliance´s Netricity program and the liaison agreement with the Wi-SUN Alliance provide industry support for IEEE 1901.2a by means of a profile definition and a certification program.

However, IEEE 1901.2a faces competition from G3-PLC and PRIME as they are more established standards that continue to evolve.

-

IEEE 802.11ah

The IEEE 802.11ah access technology is an ongoing effort of the IEEE 802.11 working group to define an "industrial Wi-Fi." Currently, this standard is just at the beginning of its evolution, and it is not clear how the market will react to this new Wi-Fi standard.

- This specification offers a longer range than traditional Wi-Fi technologies and provides good support for low-power devices that need to send smaller bursts of data at lower speeds. At the same time, it has the ability to scale to higher speeds as well.

- IEEE 802.11ah is quite different in terms of current products and the existing Wi-Fi technologies in the 2.4 GHz and 5 GHz frequency bands. To gain broad adoption and compete against similar technologies in this space, it will need an ecosystem of products and solutions that can be configured and deployed at a low cost.

LoRaWAN

The LoRaWAN wireless technology was developed for LPWANs that are critical for implementing many new devices on IoT networks. The term LoRa refers to the PHY layer, and LoRaWAN focuses on the architecture, the MAC layer, and a unified, single standard for seamless interoperability.

LoRaWAN is managed by the LoRa Alliance, an industry organization.

The PHY and MAC layers allow LoRaWAN to cover longer distances with a data rate that can change depending on various factors.

The LoRaWAN architecture depends on gateways to bridge endpoints to network servers.

From a security perspective, LoRaWAN offers AES authentication and encryption at two separate layers.

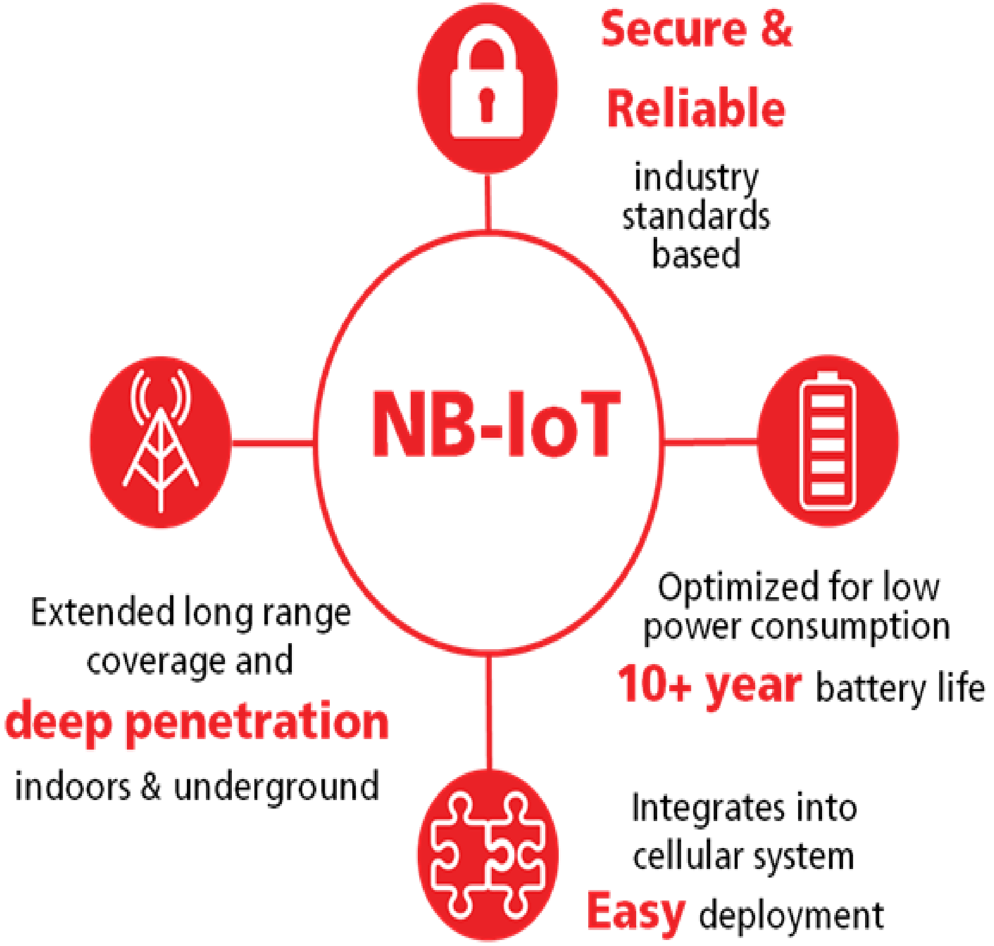
Unlicensed LPWA technologies represent new opportunities for implementing IoT infrastructures, solutions, and use cases for private enterprise networks, broadcasters, and mobile and non-mobile service providers.

The ecosystem of endpoints is rapidly growing and will certainly be the tie-breaker between the various LPWA technologies andsolutions, including LoRaWAN.

NB-IoT and Other LTE Variations

NarrowBand-Internet of Things (NB-IoT) is a standards-based low power wide area (LPWA) technology developed to enable a wide range of new IoT devices and services.

- NB-IoT specifically addresses the requirements of a massive number of low-throughput devices, low device power consumption, improved indoor coverage, and optimized network architecture.
- 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



Evolution of Cellular Technologies to support IoT

1. 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).
- Many service providers and vendors make up 3GPP, and the results of their collaborative work inthese areas are the 3GPP specifications and studies.
- The GSM Association (GSMA), has proposed the Mobile IoT Initiative, which is designed to accelerate the commercial availability of LPWA solutions in licensed spectrum.

2. LTE Cat 0.

- In Category 0 devices are running at a maximum data rate of 1 Mbps. Cat 0 includes important characteristics;

    a) Power saving mode (PSM).

    b) Half-duplex mode

- **3. LTE-M.**

It was introduced with a bid of making licensed spectrum more supportive of IoT devices

It has the following characteristics;

- Lower receiver bandwidth
- Lower data rate
- Half-duplex mode
- Enhanced discontinuous reception (eDRX)

4. NB-IoT

This was triggered after recognizing that the LTE categories were not sufficient to support LPWA IoT requirements

Modes of operation of NB-IoT;

- Standalone:
- In-band:
- Guard band:

Mobile service providers consider NB-IoT the target technology as it allows them to leverage their licensed spectrum to support LPWA use cases.

Topology of IoT

- 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**

  - 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.

NB-IoT and Other LTE Variations Conclusions

- IoT-related specifications must be completed and published by 3GPP to enable vendors, mobile service providers, and applications to successfully and widely endorse the technology.

- Evolution to eSIMs, which are still not widely supported, should be tied to NB-IoT as managing millions of SIM cards may not be an acceptable path for the market

- Widespread adoption of IEEE 1901.2a depends on implementation from vendors. Most chipsets offer support for IEEE 1901.2a, G3-PLC, and PRIME because they are the three competitive OFDM-based PLC technologies. If end-to-end IP communication or dual-PHY integration with IEEE 802.15.4g/e is expected, IEEE 1901.2a becomes the protocol of choice.
-

Table 4-6 *Main Characteristics of Access Technologies Discussed in This Chapter*

Characteristic	IEEE 802.15.4	IEEE 802.15.4g and IEEE 802.15.4e	IEEE 1901.2a	IEEE 802.11ah	LoRaWAN	NB-IoT
Wired or wireless	Wireless	Wireless	Wired	Wireless	Wireless	Wireless
Frequency bands	Unlicensed 2.4 GHz and sub-GHz	Unlicensed 2.4 GHz and sub-GHz	Unlicensed CENELEC A and B, FCC, ARIB	Unlicensed sub-GHz	Unlicensed sub-GHz	Licensed
Topology	Star, mesh	Star, mesh	Mesh	Star	Star	Star
Range	Medium	Medium	Medium	Medium	Long	Long
Data rate	Low	Low	Low	Low–high	Low	Low