Unit 1
Fundamentals of IOT

Contents

- Fundamentals of IOT
- Challenges of IOT
- Functional blocks of an IoT ecosystem
- Sensors and Actuators
- Evolution of Internet of Things
- Enabling Technologies
- Simplified IoT Architecture
- IoT Architectures: oneM2M
- IoT World Forum (IoTWF)
- Alternative IoT models- Core IoT Functional Stack
- Fog Computing and Edge Computing

Definitions of Internet of Things

- We are entering an era of the “Internet of Things” (abbreviated as IoT).There are 2 definitions: First one is defined by *Vermesan* and second by *Pe’na-L´opez*

  1. The Internet of Things as simply an interaction between the physical and digital worlds. The digital world interacts with the physical world using a plethora of sensors and actuators.

  2. Another is the Internet of Things is defined as a paradigm in which computing and networking capabilities are embedded in any kind of conceivable object.

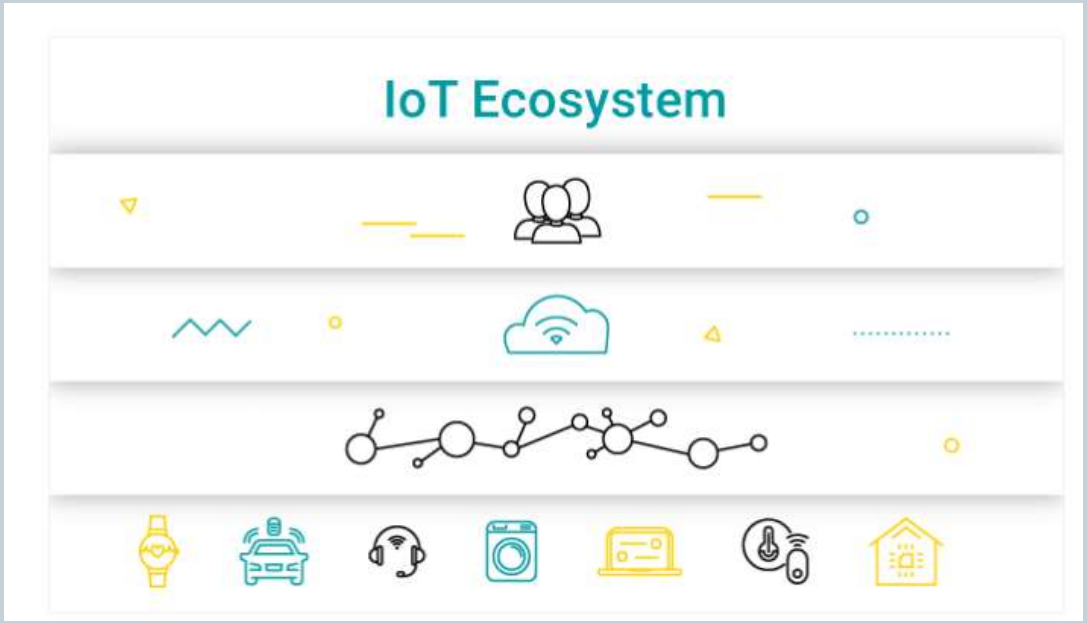
Fundamentals of IOT

- Today the Internet has become ubiquitous, has touched almost every corner of the globe, and is affecting human life in unimaginable ways.
- We are now entering an era of even more pervasive connectivity where a very wide variety of appliances will be connected to the web.
- One year after the past edition of the Cluster book 2012 it can be clearly stated that the Internet of Things (IoT) has reached many different players and gained further recognition. Out of the potential Internet of Things application areas, Smart Cities (and regions), Smart Car and mobility, Smart Home and assisted living, Smart Industries, Public safety, Energy & environmental protection, Agriculture and Tourism as part of a future IoT Ecosystem (Figure 1.1) have acquired high attention.
- IoT Ecosystem.

IOT NETWORKING CONSIDERATIONS AND CHALLENGES

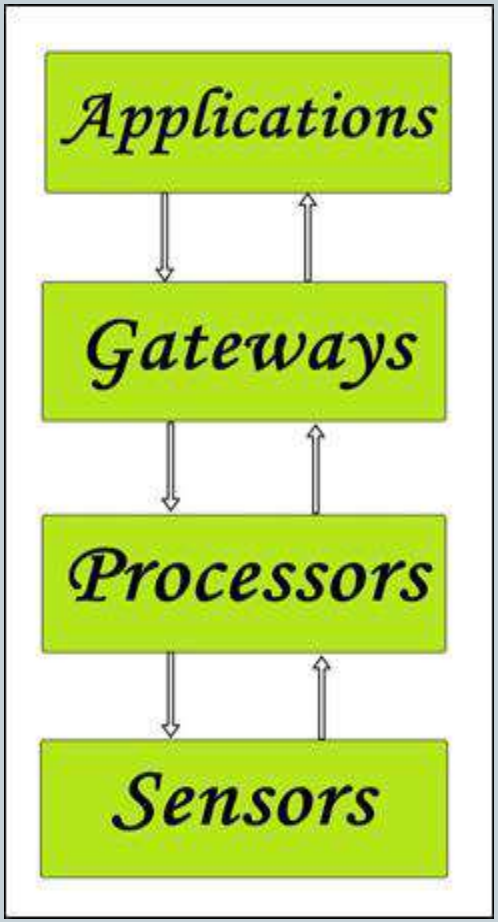
- When you consider which networking technologies to adopt within your IoT application, be mindful of the following constraints:
  - Range
  - Bandwidth
  - Power usage
  - Intermittent connectivity
  - Interoperability
  - Security

Functional block of IOT Ecosystem



Functional block of IOT Ecosystem

- We use these capabilities to query the state of the object and to change its state if possible.
- In common parlance, the Internet of Things refers to a new kind of world where almost all the devices and appliances that we use are connected to a network.
- We can use them collaboratively to achieve complex tasks that require a high degree of intelligence.
- For this intelligence and interconnection, IoT devices are equipped with embedded sensors, actuators, processors, and transceivers.
- IoT is not a single technology; rather it is an agglomeration of various technologies that work together in tandem.



Functional block of IOT Ecosystem

- **Sensors:**
  - These form the front end of the IoT devices. These are the so-called "Things" of the system. Their main purpose is to collect data from its surroundings (sensors) or give out data to its surrounding (actuators).
  - These have to be uniquely identifiable devices with a unique IP address so that they can be easily identifiable over a large network.
  - These have to be active in nature which means that they should be able to collect real-time data. These can either work on their own (autonomous in nature) or can be made to work by the user depending on their needs (user-controlled).
  - Examples of sensors are gas sensor, water quality sensor, moisture sensor, etc.

Functional block of IOT Ecosystem

- **Processors:**
  - Processors are the brain of the IoT system. Their main function is to process the data captured by the sensors and process them so as to extract the valuable data from the enormous amount of raw data collected. In a word, we can say that it gives intelligence to the data.
  - Processors mostly work on real-time basis and can be easily controlled by applications. These are also responsible for securing the data – that is performing encryption and decryption of data.
  - Embedded hardware devices, microcontroller, etc are the ones that process the data because they have processors attached to it.

Functional block of IOT Ecosystem

- **Gateways:**
  - Gateways are responsible for routing the processed data and send it to proper locations for its (data) proper utilization.
  - In other words, we can say that gateway helps in to and fro communication of the data. It provides network connectivity to the data. Network connectivity is essential for any IoT system to communicate.
  - LAN, WAN, PAN, etc are examples of network gateways.

- **Applications:**
  - Applications form another end of an IoT system. Applications are essential for proper utilization of all the data collected.
  - These cloud-based applications which are responsible for rendering the effective meaning to the data collected. Applications are controlled by users and are a delivery point of particular services.
  - Examples of applications are home automation apps, security systems, industrial control hub, etc.

Sensors and Actuators

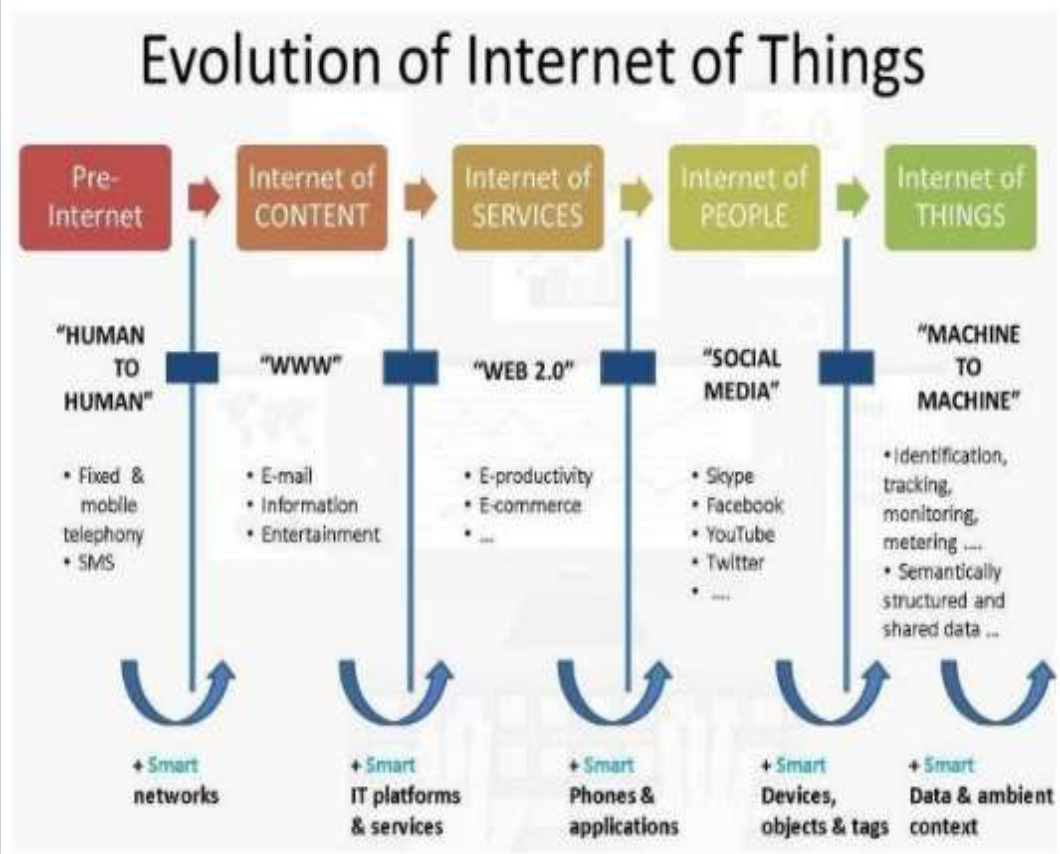
- Sensors and actuators are devices, which help in interacting with the physical environment.
- The data collected by the sensors has to be stored and processed intelligently in order to derive useful inferences from it.
- Note that we broadly define the term *sensor; a mobile phone or even a microwave oven can count as a sensor as long as it provides inputs about its current state (internal state + environment).*
- An *actuator is advice that is used to effect a change in the environment such as the temperature controller of an air conditioner.*
- The storage and processing of data can be done on the edge of the network itself or in a remote server.
- If any pre-processing of data is possible, then it is typically done at either the sensor or some other proximate device.
- The processed data is then typically sent to a remote server.

Sensors and Actuators

- The storage and processing capabilities of an IoT object are also restricted by the resources available, which are often very constrained due to limitations of size, energy, power, and computational capability.
- As a result the main research challenge is to ensure that we get the right kind of data at the desired level of accuracy.
- Along with the challenges of data collection, and handling, there are challenges in communication as well.
- The communication between IoT devices is mainly wireless because they are generally installed at geographically dispersed locations.
- The wireless channels often have high rates of distortion and are unreliable.
- this scenario reliably communicating data without too many retransmissions is an important problem and thus communication technologies are integral to the study of IoT devices.
- We can directly modify the physical world through actuators or we may do something virtually. For example, we can send some information to other smart things.

Evolution of Internet of Things

- The evolution of IoT **started with the first connected network ARPANET**.
- A coke vending machine at Carnegie Mellon University connected to the university ARPANET in 1982 WAS the first connected device.
- When Tim Berners-Lee proposed the framework of world wide web in 1989, the way for internet of things was paved.

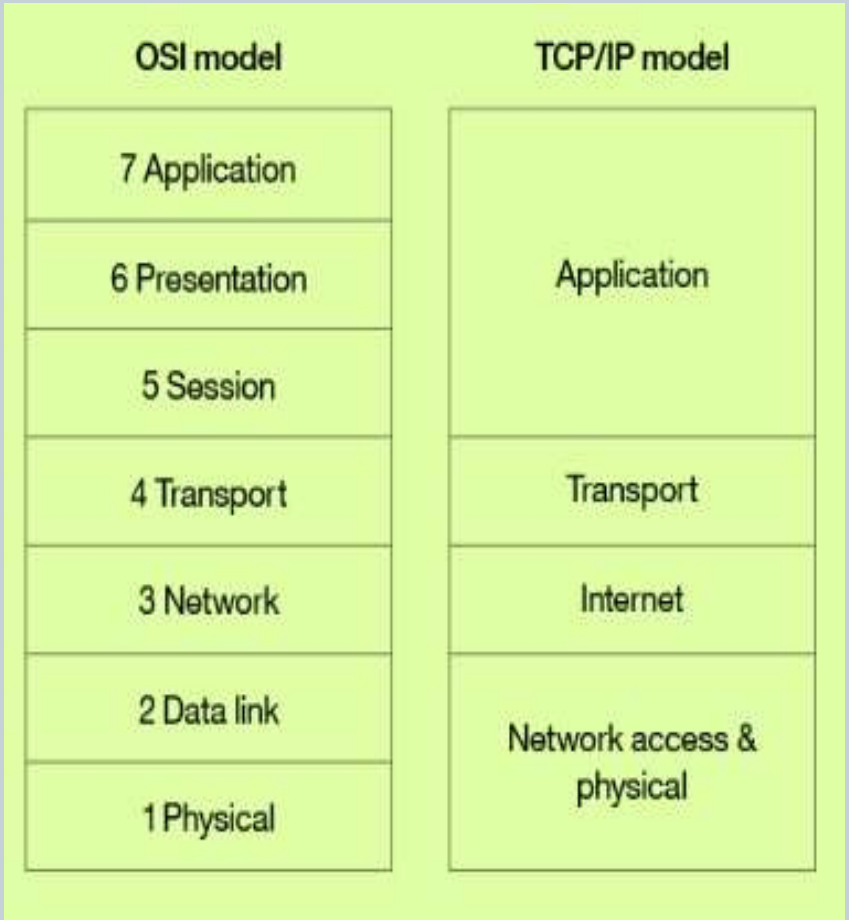


Enabling Technologies

- **TECHNOLOGIES INVOLVED IN IOT DEVELOPMENT: INTERNET/WEB AND NETWORKING BASICS OSI MODEL**
  - Networking technologies enable IoT devices to communicate with other devices, applications, and services running in the cloud.
  - The internet relies on standardized protocols to ensure communication between heterogeneous devices is secure and reliable.
  - Standard protocols specify rules and formats that devices use to establish and manage networks and transmit data across those networks.
  - Networks are built as a “stack” of technologies. A technology such as Bluetooth LE is at the bottom of the stack.
  - While others such as such as IPv6 technologies (which is responsible for the logical device addressing and routing of network traffic) are further up the stack. Technologies at the top of the stack are used by the applications that are running on top of those layers, such as message queuing technologies.
  - This article describes widely adopted technologies and standards for IoT networking. It also provides guidance for choosing one network protocol over another. It then discusses key considerations and challenges related to networking within IoT: range, bandwidth, power usage, intermittent connectivity, interoperability, and security.

Enabling Technologies

- **NETWORKING STANDARDS AND TECHNOLOGIES**
  - The Open Systems Interconnection (OSI) model is an ISO-standard abstract model is a stack of seven protocol layers.
  - From the top down, they are: application, presentation, session, transport, network, data link and physical. TCP/IP, or the Internet Protocol suite, underpins the internet, and it provides a simplified concrete implementation of these layers in the OSI model.



NETWORKING STANDARDS AND TECHNOLOGIES

- The TCP/IP model includes only four layers, merging some of the OSI model layers:
  - **Network Access & Physical Layer**
    - This TCP/IP Layer subsumes both OSI layers 1 and 2. The physical (PHY) layer (Layer 1 of OSI) governs how each device is physically connected to the network with hardware, for example with an optic cable, wires, or radio in the case of wireless network like wifi IEEE 802.11 a/b/g/n). At the link layer (Layer 2 of OSI), devices are identified by a MAC address, and protocols at this level are concerned with physical addressing, such as how switches deliver frames to devices on the network.
  - **Internet Layer**
    - This layer maps to the OSI Layer 3 (network layer). OSI Layer 3 relates to logical addressing. Protocols at this layer define how routers deliver packets of data
    - between source and destination hosts identified by IP addresses. IPv6 is commonly adopted for IoT device addressing.

NETWORKING STANDARDS AND TECHNOLOGIES

- **Transport Layer**
  - The transport layer (Layer 4 in OSI) focuses on end-to-end communication and provides features such as reliability, congestion avoidance, and guaranteeing that packets will be delivered in the same order that they were sent. UDP (User Datagram protocol) is often adopted for IoT transport for performance reasons.
- **Application Layer**
  - The application layer (Layers 5, 6, and 7 in OSI) covers application-level messaging. HTTP/S is an example of an application layer protocol that is widely adopted across the internet.
- Although the TCP/IP and OSI models provide you with useful abstractions for discussing networking protocols and specific technologies that implement each protocol, some protocols don't fit neatly into these layered models and are impractical. For example, the Transport Layer Security (TLS) protocol that implements encryption to ensure privacy and data integrity of network traffic can be considered to operate across OSI layers 4, 5, and 6.

NETWORK ACCESS AND PHYSICAL LAYER IOT NETWORK TECHNOLOGIES

- IoT network technologies to be aware of toward the bottom of the protocol stack include cellular, Wifi, and Ethernet, as well as more specialized solutions such as LPWAN, Bluetooth Low Energy (BLE), ZigBee, NFC, and RFID.
- NB-IoT is becoming the standard for LPWAN networks, according to Gartner. This IoT for All article tells more about NB-IoT.
- The following are network technologies with brief descriptions of each:
- LPWAN
  - (Low Power Wide Area Network) is a category of technologies designed for low-power, long-range wireless communication. They are ideal for large-scale deployments of low-power IoT devices such as wireless sensors. LPWAN technologies include LoRa (LongRange physical layer protocol), Haystack, SigFox, LTE-M, and NB-IoT (Narrow-Band IoT).

NETWORK ACCESS AND PHYSICAL LAYER IOT NETWORK TECHNOLOGIES

- Cellular
  - The LPWAN NB-IoT and LTE-M standards address low-power, low-cost IoT communication options using existing cellular networks. NB-IoT is the newest of these standards and is focused on long-range communication between large numbers of primarily indoor devices.

- Bluetooth Low Energy (BLE)
  - BLE is a low-power version of the popular Bluetooth 2.4 GHz wireless communication protocol. It is designed for short-range (no more than 100 meters) communication, typically in a star configuration, with a single primary device that controls several secondary devices. Bluetooth operates across both layers 1 (PHY) and 2 (MAC) of the OSI model. BLE is best suited to devices that transmit low volumes of data in bursts. Devices are designed to sleep and save power when they are not transmitting data. Personal IoT devices such as wearable health and fitness trackers, often use BLE.

NETWORK ACCESS AND PHYSICAL LAYER IOT NETWORK TECHNOLOGIES

- ZigBee
  - ZigBee operates on 2.4GHz wireless communication spectrum. It has a longer range than BLE by up to 100 meters. It also has a slightly lower data rate (250 kbps maximum compared to 270 kbps for BLE) than BLE. ZigBee is a mesh network protocol. Unlike BLE, not all devices can sleep between bursts. Much depends on their position in the mesh and whether they need to act as routers or controllers within the mesh. ZigBee was designed for building and home automation applications.
- NFC
  - The near field communication (NFC) protocol is used for very small range communication (up to 4 cm), such as holding an NFC card or tag next to a reader. NFC is often used for payment systems, but also useful for check-in systems and smart labels in asset tracking.

NETWORK ACCESS AND PHYSICAL LAYER IOT NETWORK TECHNOLOGIES

- RFID
  - RFID stands for Radio Frequency Identification. RFID tags store identifiers and data. The tags are attached to devices and read by an RFID reader. The typical range of RFID is less than a meter. RFID tags can be active, passive, or assisted passive. Passive tags are ideal for devices without batteries, as the ID is passively read by the reader. Active tags periodically broadcast their ID, while assisted passive tags become active when RFID reader is present. Dash7 is a communication protocol that uses active RFID that is designed to be used within Industrial IoT applications for secure long-range communication. Similar to NFC, a typical use case for RFID is tracking inventory items within retail and industrial IoT applications.
- Wifi
  - Wifi is standard wireless networking based on IEEE 802.11a/b/g/n specifications. 802.11n offers the highest data throughput, but at the cost of high-power consumption, so IoT devices might only use 802.11b or g for power conservation reasons. Although wifi is adopted within many prototype and current generation IoT devices, as longer-range and lower-power solutions become more widely available, it is likely that wifi will be superseded by lower-power alternatives.
- Ethernet
  - Widely deployed for wired connectivity within local area networks, Ethernet implements the IEEE 802.3 standard. Not all IoT devices need to be stationery wireless . For example, sensor units installed within a building automation system can use wired networking technologies like Ethernet. Power line communication (PLC), an alternative hard-wired solution, uses existing electrical wiring instead of dedicated network cables.

INTERNET LAYER IOT NETWORK TECHNOLOGIES

Internet layer technologies (OSI Layer 3) identify and route packets of data. Technologies commonly adopted for IoT are related to this layer, and include IPv6, 6LoWPAN, and RPL.

- IPv6
  - At the Internet layer, devices are identified by IP addresses. IPv6 is typically used for IoT applications over legacy IPv4 addressing. IPv4 is limited to 32-bit addresses, which only provide around 4.3 billion addresses in total, which is less than the current number of IoT devices that are connected, while IPv6 uses 128 bits, and so provides 2 128 addresses (around 3.4 × 10 38 or 340 billion billion billion billion) addresses. In practice, not all IoT devices need public addresses. Of the tens of billions of devices expected to connect via the IoT over the next few years, many will be deployed in private networks that use private address ranges and only communicate out to other devices or services on external networks by using gateways.
- 6LoWPAN
  - The IPv6 Low Power Wireless Personal Area Network (6LoWPAN) standard allows IPv6 to be used over 802.15.4 wireless networks. 6LoWPAN is often used for wireless sensor networks, and the Thread protocol for home automation devices also runs over 6LoWPAN.
- RPL
  - The Internet Layer also covers routing. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is designed for routing IPv6 traffic over low-power networks like those networks implemented over 6LoWPAN. RPL (pronounced “ripple”) is designed for routing packets within constrained networks such as wireless sensor networks, where not all devices are reachable at all times and there are high or unpredictable amounts of packet loss. RPL can compute the optimal path by building up a graph of the nodes in the network based on dynamic metrics and

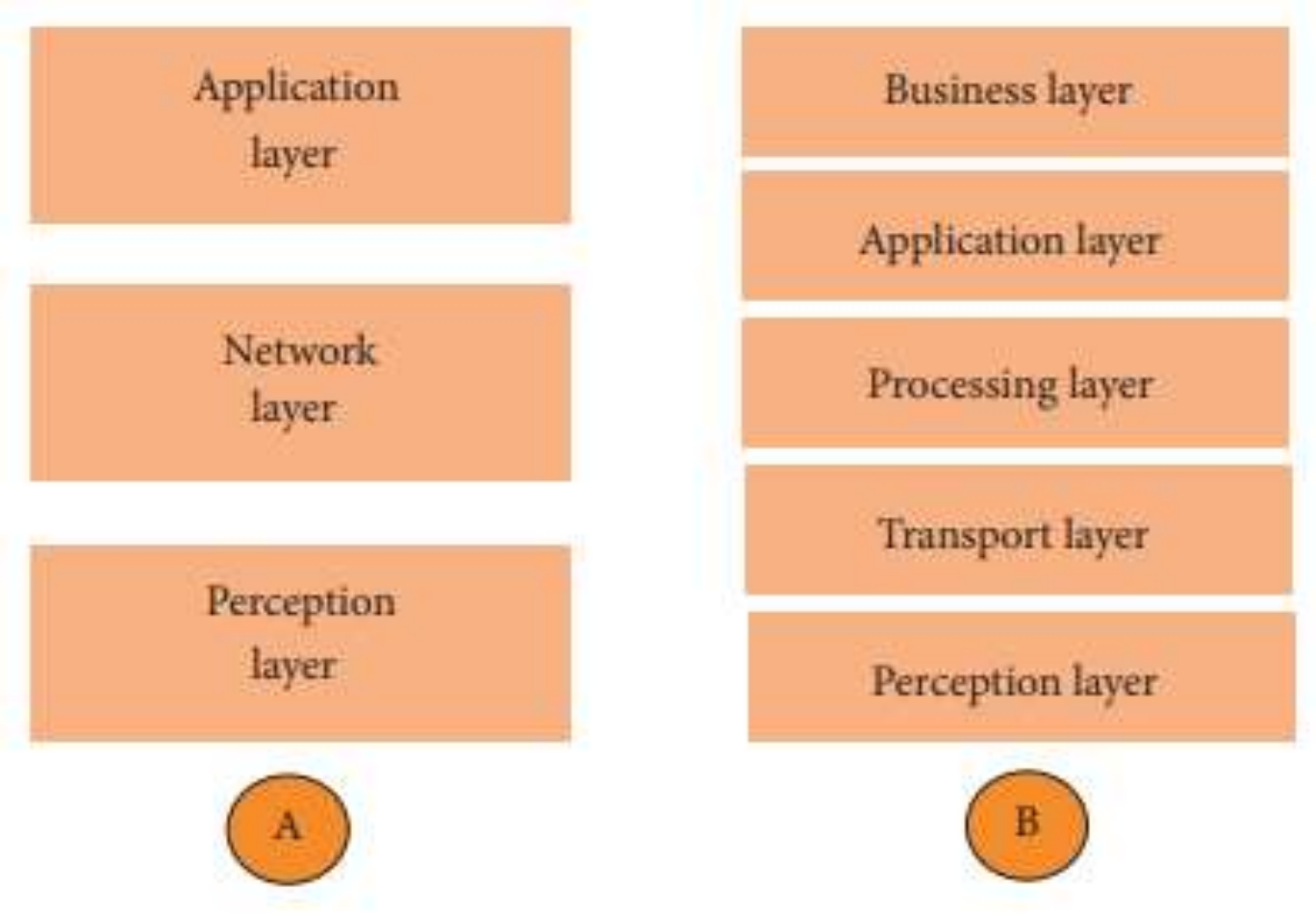
APPLICATION LAYER IOT NETWORK TECHNOLOGIES

- HTTP and HTTPS are ubiquitous across internet applications, which is true also within IoT, with RESTful HTTP and HTTPS interfaces widely deployed. CoAP (Constrained Application Protocol) is like a lightweight HTTP that is often used in combination with 6LoWPAN over UDP. Messaging protocols like MQTT, AMQP, and XMPP are also frequently used within IoT applications:
- MQTT
  - Message Queue Telemetry Transport (MQTT) is a publish/subscribe-based messaging protocol that was designed for use in low bandwidth situations, particularly for sensors and mobile devices on unreliable networks.
- AMQP
  - Advanced Message Queuing Protocol (AMQP) is an open standard messaging protocol that is used for message-oriented middleware. Most notably, AMQP is implemented by RabbitMQ.
- XMPP
  - The Extensible Messaging and Presence Protocol (XMPP) was originally designed for real-time human-to-human communication including instant messaging. This protocol has been adapted for machine-to-machine (M2M) communication to implement lightweight middleware and for routing XML data. XMPP is primarily used with smart appliances.

Architecture of IOT

- Figure below has three layers, namely, the perception, network, and application layers.
  - (i) The perception layer is the physical layer, which has sensors for sensing and gathering information about the environment. It senses some physical parameters or identifies other smart objects in the environment.
  - (ii) The network layer is responsible for connecting to other smart things, network devices, and servers. Its features are also used for transmitting and processing sensor data.
  - (iii) The application layer is responsible for delivering application specific services to the user. It defines various applications in which the Internet of Things can be deployed, for example, smart homes, smart cities, and smart health.

Simplified IOT Architecture



Simplified IOT Architecture

- The three-layer architecture defines the main idea of the Internet of Things, but it is not sufficient for research on IoT because research often focuses on finer aspects of the Internet of Things. That is why, we have many more layered architectures proposed in the literature. One is the five layer architecture, which additionally includes the processing and business layers [3–6]. The five layers are perception, transport, processing, application, and business layers (see Figure 1). The role of the perception and application layers is the same as the architecture with three layers. We outline the function of the remaining three layers.
  - (i) The transport layer transfers the sensor data from the perception layer to the processing layer and vice versa through networks such as wireless, 3G, LAN, Bluetooth, RFID, and NFC.

Simplified IOT Architecture

- (ii) The processing layer is also known as the middleware layer. It stores, analyzes, and processes huge amounts of data that comes from the transport layer. It can manage and provide a diverse set of services to the lower layers. It employs many technologies such as databases, cloud computing, and big data processing modules.
- (iii) The business layer manages the whole IoT system, including applications, business and profit models, and users' privacy. The business layer is out of the scope of this paper. Hence, we do not discuss it further.

IOT Architecture:M2M

- Machine-to-machine communication, or M2M, is exactly as it sounds: two machines "communicating," or exchanging data, without human interfacing or interaction. This includes serial connection, power line connection (PLC), or wireless communications in the industrial Internet of Things (IoT). Switching over to wireless has made M2M communication much easier and enabled more applications to be connected.
- In general, when someone says M2M communication, they often are referring to cellular communication for embedded devices. Examples of M2M communication in this case would be vending machines sending out inventory information or ATM machines getting authorization to despense cash.
- As businesses have realized the value of M2M, it has taken on a new name: the Internet of Things (IoT). IoT and M2M have similar promises: to fundamentally change the way the world operates. Just like IoT, M2M allows virtually any sensor to communicate, which opens up the possibility of systems monitoring themselves and automatically responding to changes in the environment, with a much reduced need for human involvement. M2M and IoT are almost synonymous—the exception is IoT (the newer term) typically refers to wireless communications, whereas M2M can refer to any two machines—wired or wireless—communicating with one another.
- Traditionally, M2M focused on "industrial telematics," which is a fancy way of explaining data transfer for some commercial benefit. But many original uses of M2M still stand today, like smart meters. Wireless M2M has been dominated by cellular since it came out in the mid-2000's with 2G cell networks. Because of this, the cellular market has tried to brand M2M as an inherently cellular thing by offering M2M data plans. But cellular M2M is only one subsection of the market, and it shouldn't be thought of as a cellular-only area.

IOT Architecture:M2M

- How M2M Works
  - As previously stated, machine-to-machine communication makes the Internet of Things possible. According to Forbes, M2M is among the fastest-growing types of connected device technologies in the market right now, largely because M2M technologies can connect millions of devices within a single network. The range of connected devices includes anything from vending machines to medical equipment to vehicles to buildings. Virtually anything that houses sensor or control technology can be connected to some sort of wireless network.
  - This sounds complex, but the driving thought behind the idea is quite simple. Essentially, M2M networks are very similar to LAN or WAN networks, but are exclusively used to allow machines, sensors, and controls, to communicate. These devices feed information they collect back to other devices in the network. This process allows a human (or an intelligent control unit) to assess what is going on across the whole network and issue appropriate instructions to member devices.

IoT World Forum (IoTWF)

- In 2014 the IoTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others)published a seven-layer IoT architectural reference model. While various IoT reference models exist, the one put forth by the IoT World Forum offers a clean, simplified perspective on IoT and includes edge computing, data storage, and access. It provides a succinct way of visualizing IoT from a technical perspective. Each of the seven layers is broken down into specific functions, and security encompasses the entire model. Figure below details the IoT Reference Model published by the IoTWF. As shown in Figure 2-2, the IoT Reference Model defines a set of levels with control flowing from the center (this could be either a cloud service or a dedicated data center), to the edge, which includes sensors, devices, machines, and other types of intelligent end nodes. In general, data travels up the stack, originating from the edge, and goes northbound to the center. Using this reference model, we are able to achieve the following:
- Decompose the IoT problem into smaller parts
- Identify different technologies at each layer and how they relate to one another
- Define a system in which different parts can be provided by different vendors

IoT World Forum (IoTWF)

Levels

7 **Collaboration & Processes**
(Involving People & Business Processes)

6 **Application**
(Reporting, Analytics, Control)

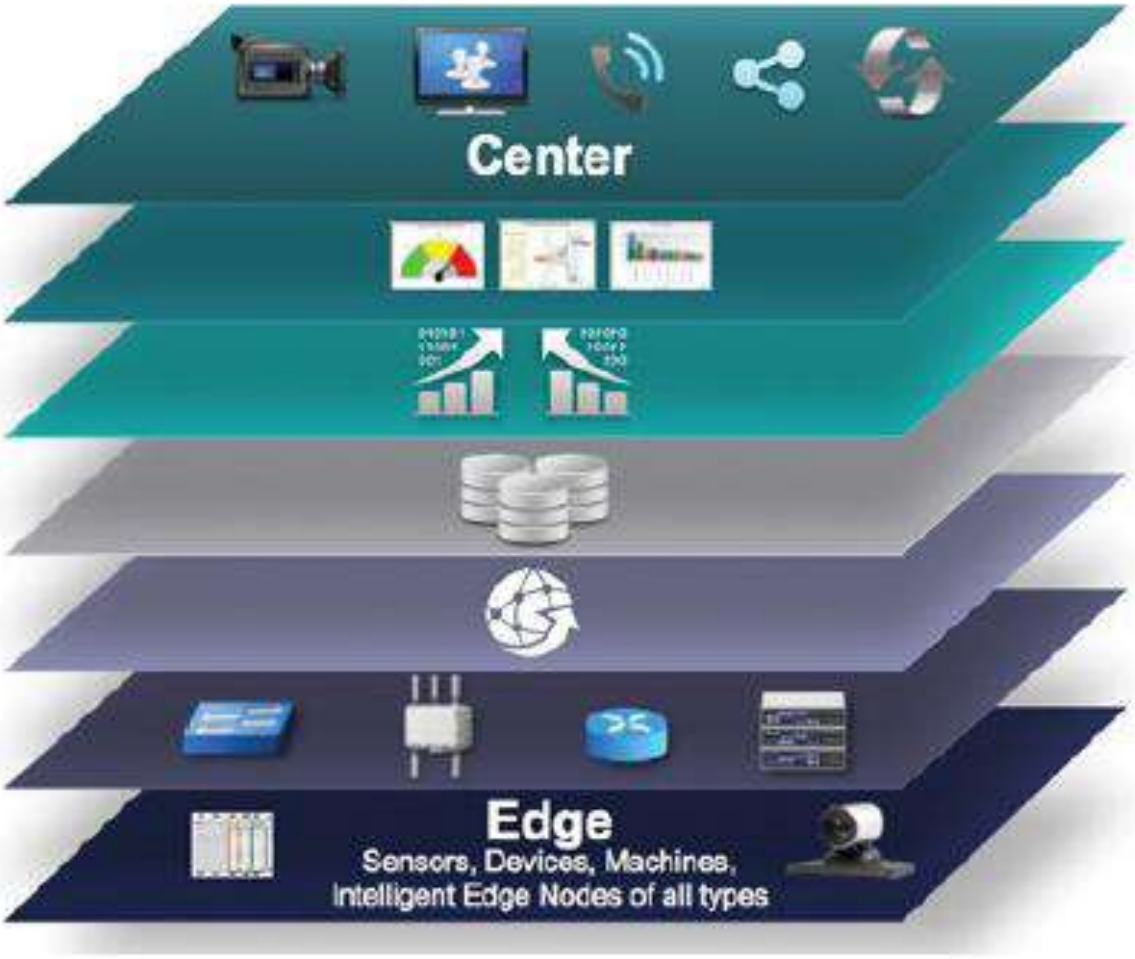
5 **Data Abstraction**
(Aggregation & Access)

4 **Data Accumulation**
(Storage)

3 **Edge Computing**
(Data Element Analysis & Transformation)

2 **Connectivity**
(Communication & Processing Units)

1 **Physical Devices & Controllers**
(The "Things" in IoT)



IoT World Forum (IoTWF)

- The following sections look more closely at each of the seven layers of the IoT Reference Model.
- **Layer 1: Physical Devices and Controllers Layer**
  - The first layer of the IoT Reference Model is the physical devices and controllers layer. This layer is home to the "things" in the Internet of Things, including the various endpoint devices and sensors that send and receive information. The size of these "things" can range from almost microscopic sensors to giant machines in a factory. Their primary function is generating data and being capable of being queried and/or controlled over a network.
- **Layer 2: Connectivity Layer**
  - In the second layer of the IoT Reference Model, the focus is on connectivity. The most important function of this IoT layer is the reliable and timely transmission of data. More specifically, this includes transmissions between Layer 1 devices and the network and between the network and information processing that occurs at Layer 3 (the edge computing layer).As you may notice, the connectivity layer encompasses all networking elements of IoT and doesn't really distinguish between the last-mile network (the network between the sensor/endpoint and the IoT gateway, discussed later in this chapter), gateway, and backhaul networks. Functions of the connectivity layer are detailed in Figure 2-3.

IoT World Forum (IoTWF)

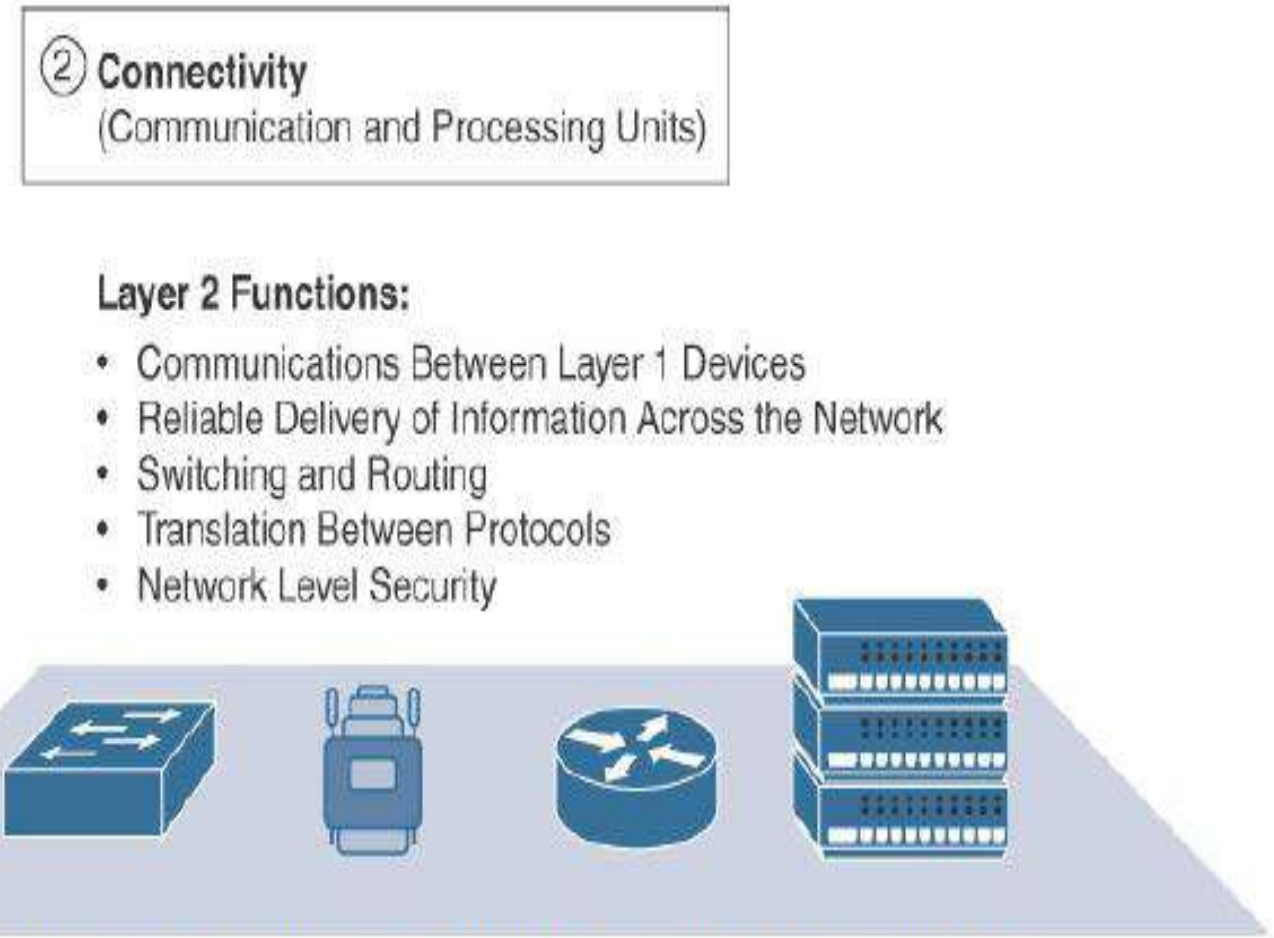


Figure 2-3 *IoT Reference Model Connectivity Layer Functions*

IoT World Forum (IoTWF)

- **Layer 3: Edge Computing Layer**
  - Edge computing is the role of Layer 3. Edge computing is often referred to as the "fog" layer and is discussed in the section "Fog Computing," later in this chapter. At this layer, the emphasis is on data reduction and converting network data flows into information that is ready for storage and processing by higher layers. One of the basic principles of this reference model is that information processing is initiated as early and as close to the edge of the network as possible. Figure 2-4 highlights the functions handled by Layer 3 of the IoT Reference Model. Another important function that occurs at Layer 3 is the evaluation of data to see if it can be filtered or aggregated before being sent to a higher layer. This also allows for data to be reformatted or decoded, making additional processing by other systems easier. Thus, a critical function is assessing the data to see if predefined thresholds are crossed and any action or alerts need to be sent.
- **Upper Layers: Layers 4–7**
  - The upper layers deal with handling and processing the IoT data generated by the bottom layer. For the sake of completeness, Layers 4–7 of the IoT Reference Model are summarized in Table 2-2.

IoT World Forum (IoTWF)

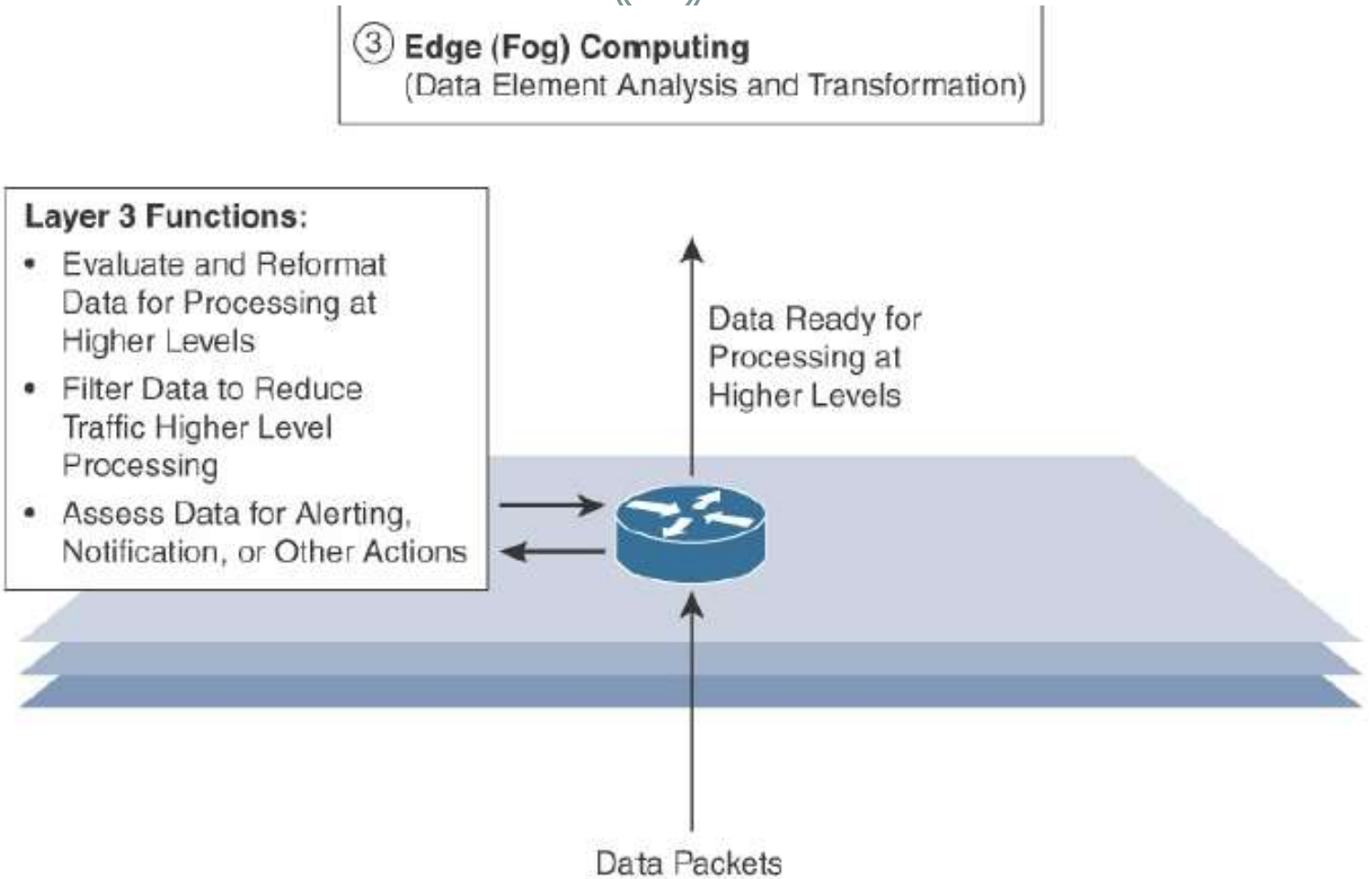


Figure 2-4 *IoT Reference Model Layer 3 Functions*

IoT World Forum (IoTWF)

IoT Reference Model Layer	Functions
Layer 4: Data accumulation layer	Captures data and stores it so it is usable by applications when necessary. Converts event-based data to query-based processing.
Layer 5: Data abstraction layer	Reconciles multiple data formats and ensures consistent semantics from various sources. Confirms that the data set is complete and consolidates data into one place or multiple data stores using virtualization.
Layer 6: Applications layer	Interprets data using software applications. Applications may monitor, control, and provide reports based on the analysis of the data.
Layer 7: Collaboration and processes layer	Consumes and shares the application information. Collaborating on and communicating IoT information often requires multiple steps, and it is what makes IoT useful. This layer can change business processes and delivers the benefits of IoT.

Table 2-2 *Summary of Layers 4–7 of the IoTWF Reference Model*

Core IoT Functional Stack

- The IoT network must be designed to support its unique requirements and constraints. This section provides an overview of the full networking stack, from sensors all the way to the applications layer.
- The Core IoT Functional Stack IoT networks are built around the concept of “things,” or smart objects performing functions and delivering new connected services. These objects are “smart” because they use a combination of contextual information and configured goals to perform actions. These actions can be self-contained (that is, the smart object does not rely on external systems for its actions); however, in most cases, the “thing” interacts with an external system to report information that the smart object collects, to exchange with other objects, or to interact with a management platform. In this case, the management platform can be used to process data collected from the smart object and also guide the behavior of the smart object.
- From an architectural standpoint, several components have to work together for an IoT network to be operational: “Things” layer: At this layer, the physical devices need to fit the constraints of the environment in which they are deployed while still being able to provide the information needed. Communications network layer: When smart objects are not self-contained, they need to communicate with an external system. In many cases, this communication uses a wireless technology. This layer has four sublayers: Access network sublayer: The last mile of the IoT network is the access network. This is typically made up of wireless technologies such as 802.11ah, 802.15.4g, and LoRa. The sensors connected to the access network may also be wired.

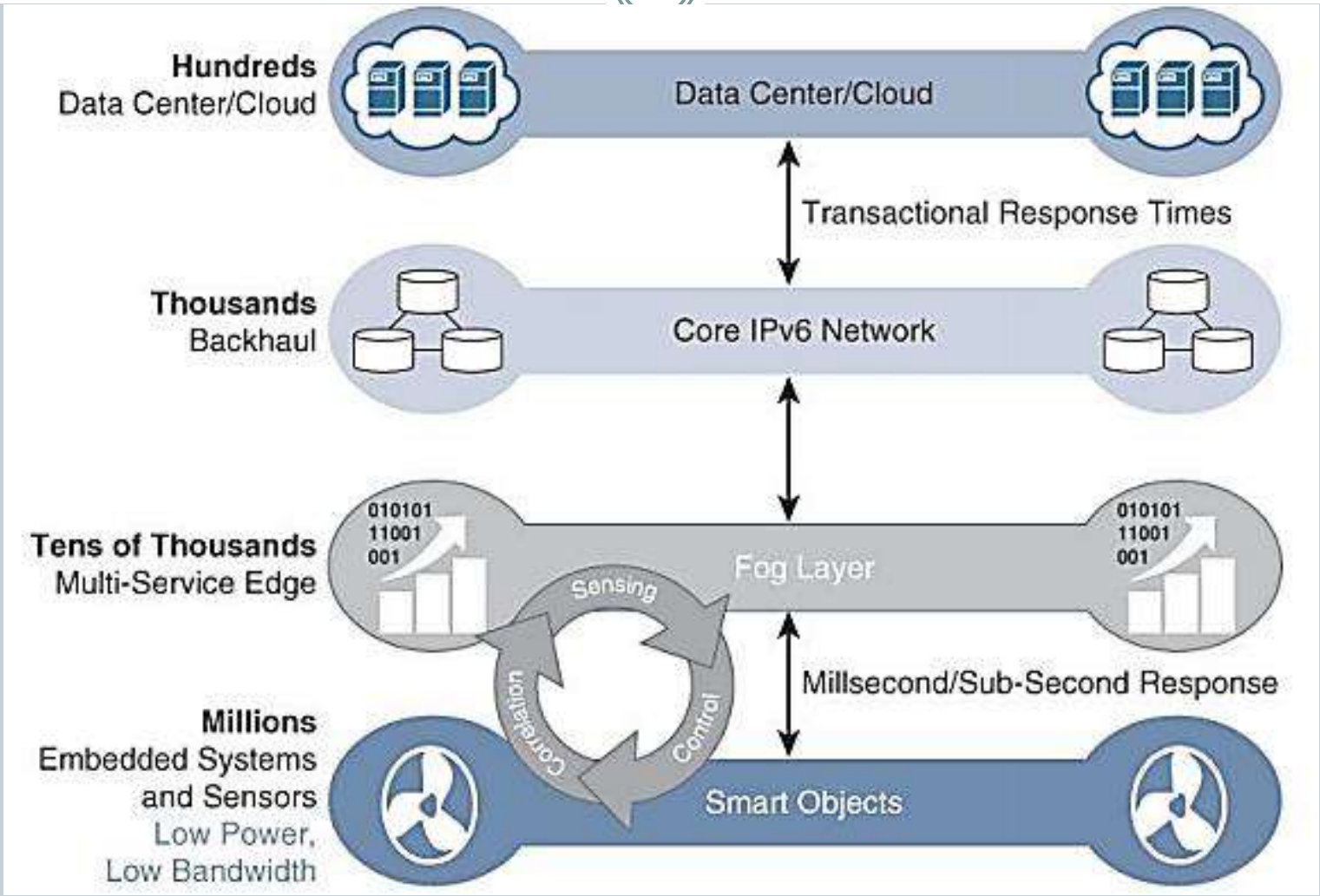
Core IoT Functional Stack

- Gateways and backhaul network sublayer: A common communication system organizes multiple smart objects in a given area around a common gateway.
- The gateway communicates directly with the smart objects. The role of the gateway is to forward the collected information through a longer-range medium (called the backhaul) to a headend central station where the information is processed. This information exchange is a Layer 7 (application) function, which is the reason this object is called a gateway. On IP networks, this gateway also forwards packets from one IP network to another, and it therefore acts as a router.
- Network transport sublayer: For communication to be successful, network and transport layer protocols such as IP and UDP must be implemented to support the variety of devices to connect and media to use. IoT network management sublayer: Additional protocols must be in place to allow the headend applications to exchange data with the sensors. Examples include CoAP and MQTT.
- Application and analytics layer: At the upper layer, an application needs to process the collected data, not only to control the smart objects when necessary, but to make intelligent decision based on the information collected and, in turn, instruct the “things” or other systems to adapt to the analyzed conditions and change their behaviors or parameters. The following sections examine these elements and help you architect your IoT communication network.

Fog Computing

- The solution to the challenges mentioned in the previous section is to distribute data management throughout the IoT system, as close to the edge of the IP network as possible. The best-known embodiment of edge services in IoT is fog computing. Any device with computing, storage, and network connectivity can be a fog node.
- Examples include industrial controllers, switches, routers, embedded servers, and IoT gateways. Analyzing IoT data close to where it is collected minimizes latency, offloads gigabytes of network traffic from the core network, and keeps sensitive data inside the local network.
- Fog services are typically accomplished very close to the edge device, sitting as close to the IoT endpoints as possible. One significant advantage of this is that the fog node has contextual awareness of the sensors it is managing because of its geographic proximity to those sensors. For example, there might be a fog router on an oil derrick that is monitoring all the sensor activity at that location.
- Because the fog node is able to analyze information from all the sensors on that derrick, it can provide contextual analysis of the messages it is receiving and may decide to send back only the relevant information over the backhaul network to the cloud.
- In this way, it is performing distributed analytics such that the volume of data sent upstream is greatly reduced and is much more useful to application and analytics servers residing in the cloud.

Fog Computing



Fog Computing

- The defining characteristic of fog computing are as follows:
  - Contextual location awareness and low latency: The fog node sits as close to the IoT endpoint as possible to deliver distributed computing.
  - Geographic distribution: In sharp contrast to the more centralized cloud, the services and applications targeted by the fog nodes demand widely distributed deployments.
  - Deployment near IoT endpoints: Fog nodes are typically deployed in the presence of a large number of IoT endpoints. For example, typical metering deployments often see 3000 to 4000 nodes per gateway router, which also functions as the fog computing node.
  - Wireless communication between the fog and the IoT endpoint: Although it is possible to connect wired nodes, the advantages of fog are greatest when dealing with a large number of endpoints, and wireless access is the easiest way to achieve such scale.
  - Use for real-time interactions: Important fog applications involve real-time interactions rather than batch processing. Preprocessing of data in the fog nodes allows upper-layer applications to perform batch processing on a subset of the data.

Edge Computing

- Fog computing solutions are being adopted by many industries, and efforts to develop distributed applications and analytics tools are being introduced at an accelerating pace.
- The natural place for a fog node is in the network device that sits closest to the IoT endpoints, and these nodes are typically spread throughout an IoT network.
- However, in recent years, the concept of IoT computing has been pushed even further to the edge, and in some cases it now resides directly in the sensors and IoT devices.

Unit 2
IoT Protocols & IoT Access Technologies

Contents

IoT Protocols

- IoT devices communicate using IoT protocols. Internet protocol (IP) is a set of rules that dictates how data gets sent to the internet. IoT protocols ensure that information from one device or sensor gets read and understood by another device, a gateway, a service. Different IoT protocols have been designed and optimized for different scenarios and usage. Given the diverse array of IoT devices available, using the right protocol in the right context is important.
- **What IoT protocol is right for me?**
  - The type of IoT protocol you'll need depends on the system architecture layer that the data will travel in. The Open Systems Interconnection (OSI) model provides a map of the various layers that send and receive data. Each IoT protocol in the IoT system architecture enables device-to-device, device-to-gateway, gateway-to-data center, or gateway-to-cloud communication, as well as communication between data centers.

Physical and MAC layer

Physical layer

- The physical layer is the communication channel between devices within a specific environment.
- 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. DSSS 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

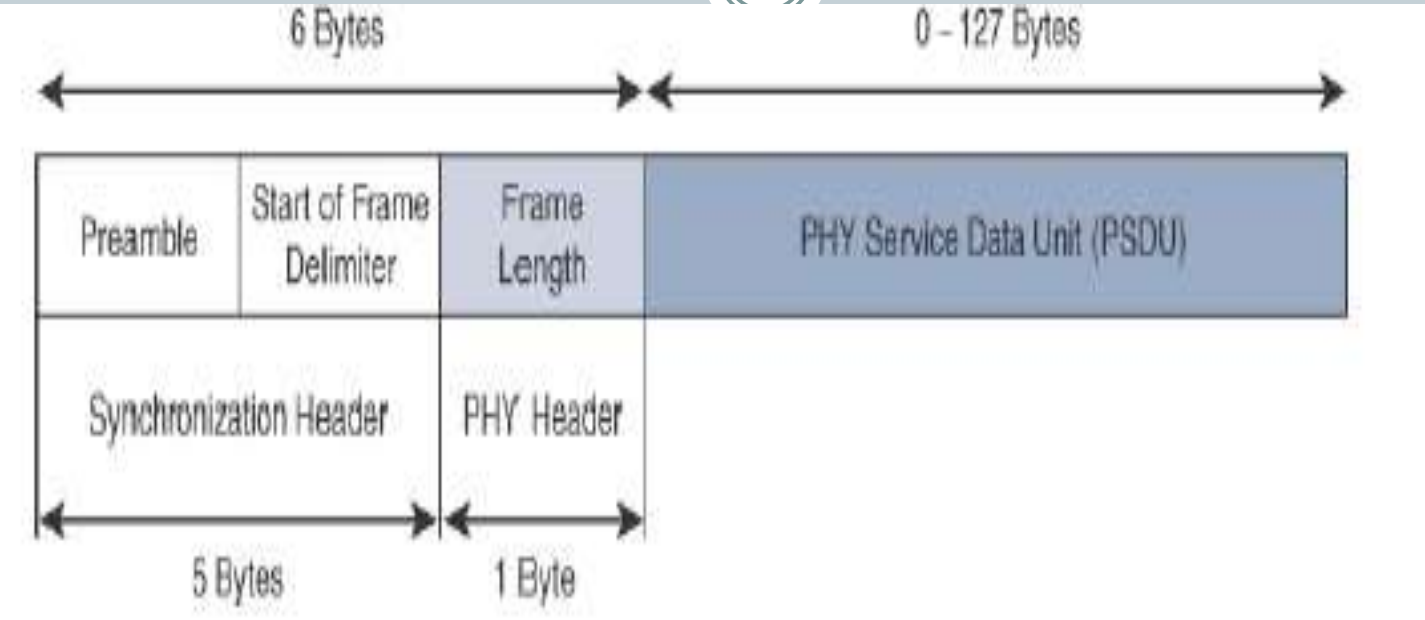
Physical and MAC layer

- The 2.4 GHz band operates worldwide. The 915 MHz band operates mainly in North and South America, and the 868 MHz frequencies are used in Europe, the Middle East, and Africa. IEEE 802.15.4-2006, 802.15.4-2011, and IEEE 802.15.4-2015 introduced additional PHY communication options, including the following:
- 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.

Physical and MAC layer

- 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.

IEEE 802.15.4 PHY Format



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

Physical and MAC layer

MAC Layer

- The IEEE 802.15.4 MAC layer manages access to the PHY channel by defining how devices in the same area will share the frequencies allocated. At this layer, the scheduling and routing of data frames are also coordinated. The 802.15.4 MAC layer performs the following tasks:
- Network beaconing for devices acting as coordinators (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

Physical and MAC layer

- The MAC layer achieves these tasks by using various predefined frame types. In fact, four types of 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

Physical and MAC layer

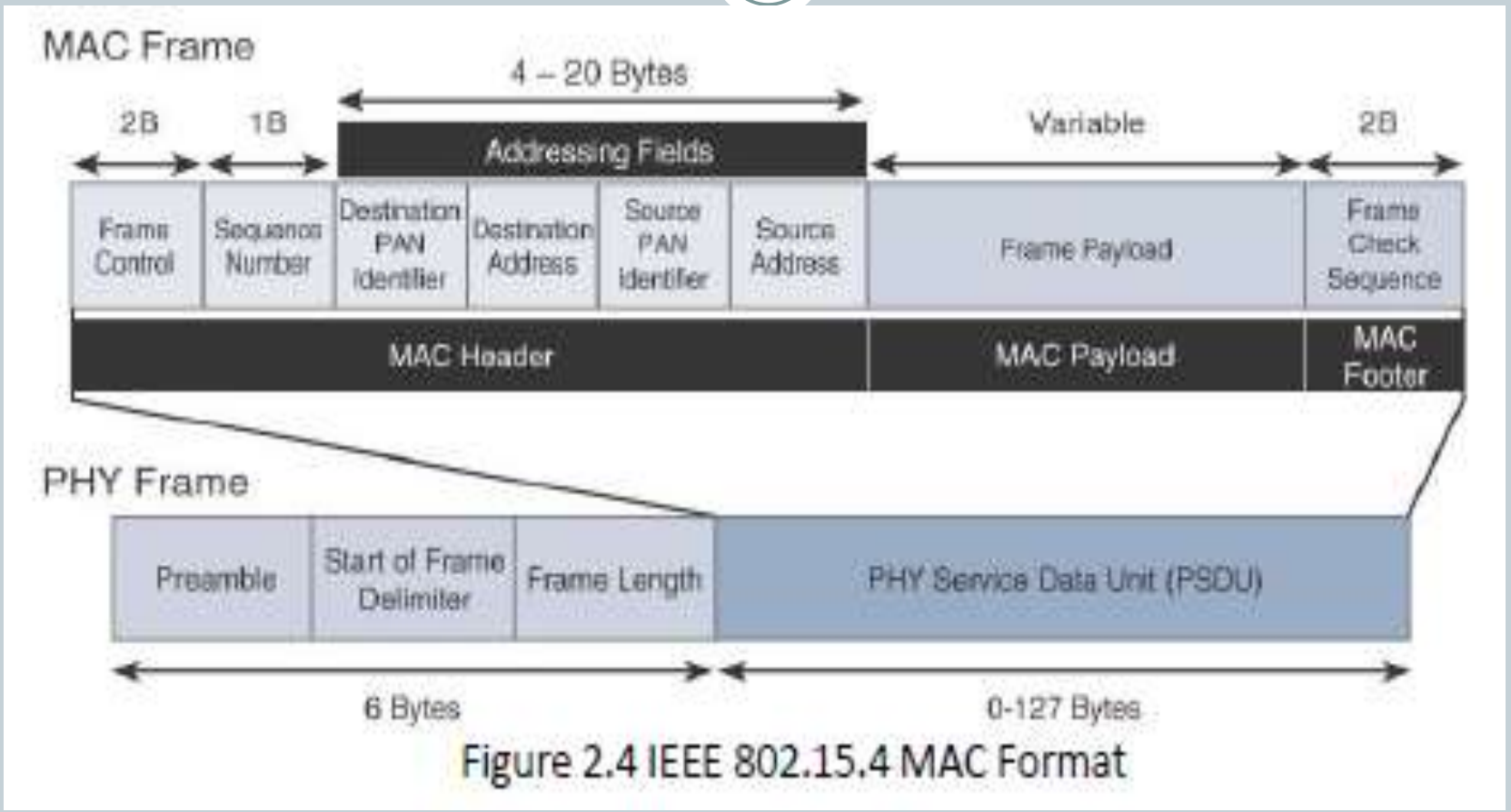


Figure 2.4 IEEE 802.15.4 MAC Format

Physical and MAC layer

- The MAC Header field is composed of the Frame Control, Sequence Number and the Addressing fields. The Frame Control field defines attributes such as frame type, addressing modes, and other control flags. The Sequence Number field indicates the sequence identifier for the frame. The Addressing field 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. For example, beacon frames have specific fields and payloads related to beacons, while 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.
- IEEE 802.15.4 requires all devices to support a unique 64-bit extended MAC address, based on EUI-64. However, because the maximum payload is 127 bytes, 802.15.4 also defines how a 16-bit “short address” is assigned to devices.
- This short address is local to the PAN and substantially reduces the frame overhead compared to a 64-bit extended MAC address. However, you should be aware that the use of this short address might be limited to specific upper-layer protocol stacks.

Physical and MAC layer

- **Bluetooth Low Energy (BLE)**
  - BLE dramatically reduces power consumption and cost and maintains a similar connectivity range as classic Bluetooth. BLE works natively across mobile operating systems and is fast becoming a favorite for consumer electronics due to its low cost and long battery life.
- **Ethernet**
  - This wired connection is a less expensive option that provides fast data connection and low latency.

Physical and MAC layer

- **Long-term evolution (LTE)**
  - A wireless broadband communication standard for mobile devices and data terminals. LTE increases the capacity and speed of wireless networks and supports multicast and broadcast streams.
- **Near field communication (NFC)**
  - A set of communication protocols using electromagnetic fields that allows two devices to communicate from within four centimeters of each other. NFC-enabled devices function as identity keycards and are commonly used for contactless mobile payments, ticketing, and smart cards.
- **Power Line Communication (PLC)**
  - A communication technology that enables the sending and receiving of data over existing power cables. This allows you to both power and control an IoT device through the same cable.

Physical and MAC layer

- **Radio frequency identification (RFID)**
  - RFID uses electromagnetic fields to track otherwise unpowered electronic tags. Compatible hardware supplies power and communicate with these tags, reading their information for identification and authentication.
- **Wi-Fi/802.11**
  - Wi-Fi/802.11 is a standard in homes and offices. Although it's an inexpensive option, it may not suit all scenarios due to its limited range and 24/7 energy consumption.
- **Z-Wave**
  - A mesh network using low-energy radio waves to communicate from appliance to appliance.
- **Zigbee**
  - An IEEE 802.15.4-based specification for a suite of high-level communication protocols used to create personal area networks with small, low-power digital radios.

Data link layer

- The data layer is the part of an IoT protocol that transfers data within the system architecture, identifying and correcting errors found in the physical layer.

Data link layer

- **IEEE 802.15.4**
  - A radio standard for low-powered wireless connection. It's used with Zigbee, 6LoWPAN, and other standards to build wireless embedded networks.
- **LPWAN**
  - Low-power wide-area networks (LPWAN) networks enable communication across distances of 500 meters to over 10km in some places. LoRaWAN is an example of LPWAN that's optimized for low power consumption.

Network layer

- The network layer of an IoT protocol helps individual devices communicate with the router.
- **IP**
  - Many IoT protocols utilize IPv4, while more recent executions use IPv6. This recent update to IP routes traffic across the internet and identifies and locates devices on the network.
- **6LoWPAN**
  - This IoT protocol works best with low-power devices that have limited processing capabilities.

Low-power, wide-area networks (LPWAN)

- LPWANs enable communication across a minimum of 500 meters, require minimal power, and are used for a majority of IoT devices. Common examples of LPWANs are:
  - **4G LTE IoT**
    - High capacity and low latency, these networks are a great choice for IoT scenarios that require real-time information or updates.
  - **5G IoT**
    - Although not yet available, 5G IoT networks are expected to enable further innovations in IoT by providing much faster download speeds and connectivity to many more devices in a given area.

LPWAN

- **Cat-0**
  - These LTE-based networks are the lowest cost option. They lay the groundwork for Cat-M, a technology that will replace 2G.
- **Cat-1**
  - This standard for cellular IoT will eventually replace 3G. Cat-1 networks are easy to set up and offer a great solution for applications requiring a voice or browser interface.
- **LoRaWAN**
  - Long-range wide-area networks (LoRaWANs) connect mobile, secure, bi-directional battery-operated devices.

LPWAN

- **LTE Cat-M1**
  - These networks are fully compatible with LTE networks. They optimize cost and power in a second generation of LTE chips designed specifically for IoT applications.
- **Narrowband or NB-IoT/Cat-M2**
  - NB-IoT/Cat-M2 uses direct-sequence spread spectrum (DSSS) modulation to send data directly to the server, eliminating the need for a gateway. Although NB-IoT networks cost more to set up, not requiring a gateway makes them less expensive to run.
- **Sigfox**
  - This global IoT network provider offers wireless networks to connect low-power objects that emit continuous data.

Topology and Security of IEEE

Topology

- The network formation of the IEEE 802.15.4 does not impose constraints on the topology and it contains two topologies: **the star topology, the peer-to-peer, and the tree 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.

Topology and Security of IEEE

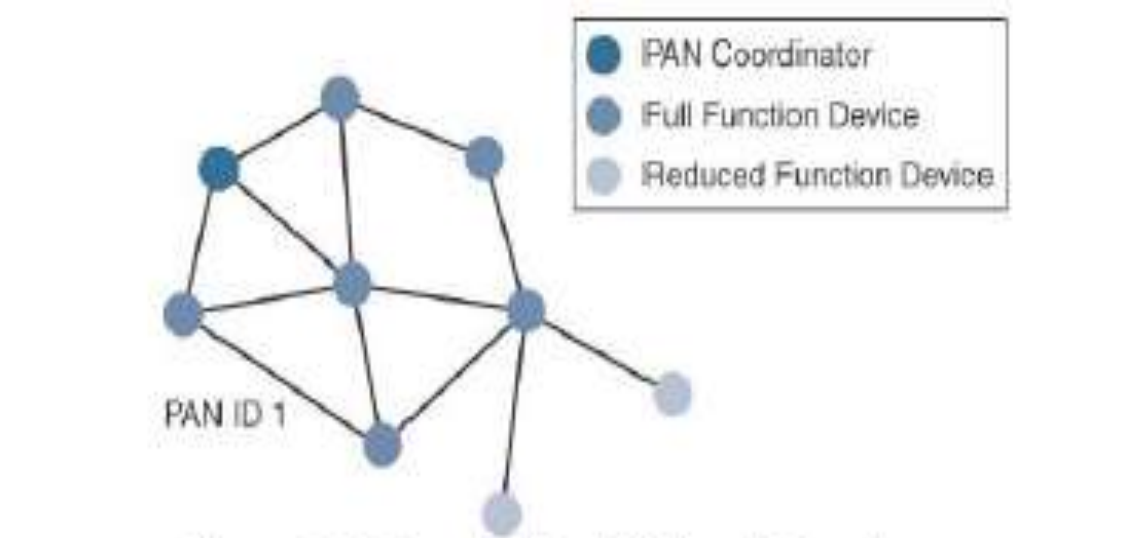


Figure 2.5: Sample Mesh Network Topology

Please note that every 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 2.5 shows an example of an 802.15.4 mesh network with a PAN ID of 1.

Topology and Security of IEEE

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. Established by the US National Institute of Standards and Technology in 2001, AES is a block cipher, which means it operates on fixed-size blocks of data. The use of AES by the US government and its widespread adoption in the private sector has helped it become one of the most popular algorithms used in symmetric key cryptography. (A *symmetric key means that the same key is used for both the encryption and decryption of the 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

- IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries. In addition to being low cost and offering a reasonable battery life, this access technology enables easy installation using a compact protocol stack while remaining both simple and flexible. Several network communication stacks, including deterministic ones, and profiles leverage this technology to address a wide range of IoT use cases in both the consumer and business markets.
- 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
- Criticisms of IEEE 802.15.4 often focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading.

IEEE 802.15.4

- IEEE 802.15.4 is a low-cost, low-data-rate wireless access technology for devices that are operated or work on batteries. This describes how low-rate wireless personal area networks (LR-WPANs) function.
- The IEEE 802.15.4 wireless PHY and MAC layers are mature specifications that are the foundation for various industry standards and products as listed in Table 2.1. The PHY layer offers a maximum speed of up to 250 kbps, but this varies based on modulation and frequency. The MAC layer for 802.15.4 is robust and handles how data is transmitted and received over the PHY layer. Specifically, the MAC layer handles the association and disassociation of devices to/from a PAN, reliable communications between devices, security, and the formation of various topologies.

IEEE 802.15.4

- The topologies used in 802.15.4 include star, peer-to-peer, and cluster trees that allow for the formation of mesh networks. From a security perspective, 802.15.4 utilizes AES encryption to allow secure communications and also provide data integrity.
- The main competitor to IEEE 802.15.4 is DASH7, another wireless technology that compares favourably. 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.

802.15.4g and 802.15.4e

- These are the result of improvements done to 802.15.4 and are mainly targeted to utilities and smart cities deployments.

1901.2a

- This is a technology for connecting smart objects over power lines.
- The IEEE Std 1901-2010 is a standard for high speed (up to 500 Mbit/s at the physical layer) communication devices via electric power lines, often called broadband over power lines (BPL). The standard uses transmission frequencies below 100 MHz. This standard is usable by all classes of BPL devices, including BPL devices used for the connection (<1500m to the premises) to Internet access services as well as BPL devices used within buildings for local area networks, smart energy applications, transportation platforms (vehicle), and other data distribution applications (<100m between devices).

802.11ah

- In unconstrained networks, IEEE 802.11 Wi-Fi is certainly the most successfully deployed wireless technology. This standard is a key IoT wireless access technology, either for connecting endpoints such as fog computing nodes, high-data-rate sensors, and audio or video analytics devices or for deploying Wi-Fi backhaul infrastructures, such as outdoor Wi-Fi mesh in smart cities, oil and mining, or other environments.
- However, 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. For these reasons, the IEEE 802.11 working group launched a task group named IEEE 802.11ah to specify a sub-GHz version of Wi-Fi. Three main use cases are identified for IEEE 802.11ah:

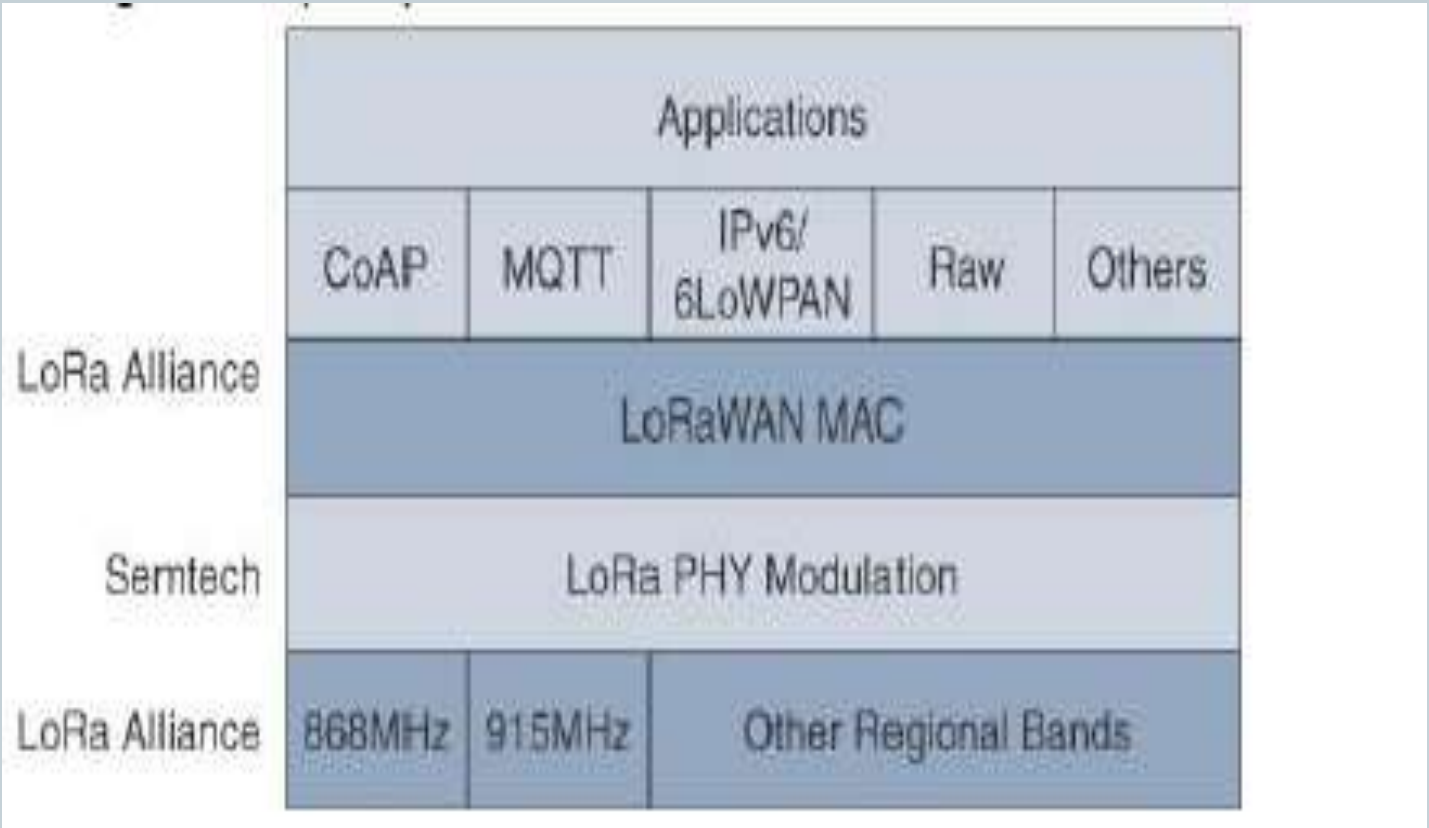
802.11ah

- 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 sub networks
- 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.

LoraWAN

- In recent years, a new set of wireless technologies known as Low-Power Wide-Area (LPWA) has received a lot of attention from the industry and press. Particularly well adapted for long-range and battery-powered endpoints, LPWA technologies open new business opportunities to both services providers and enterprises considering IoT solutions. LoRaWAN is an unlicensed-band LPWA technology.

LoraWAN layers



LoraWAN layers

- LoRaWAN 1.0.2 regional specifications describe the use of the main unlicensed sub-GHz frequency bands of 433 MHz, 779–787 MHz, 863–870 MHz, and 902–928 MHz, as well as regional profiles for a subset of the 902–928 MHz bandwidth. For example, Australia utilizes 915–928 MHz frequency bands, while South Korea uses 920–923 MHz and Japan uses 920–928 MHz
- Understanding LoRa gateways is critical to understanding a LoRaWAN system. A LoRa gateway is deployed as the center hub of 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.

Constrained Nodes and Constraints Networks

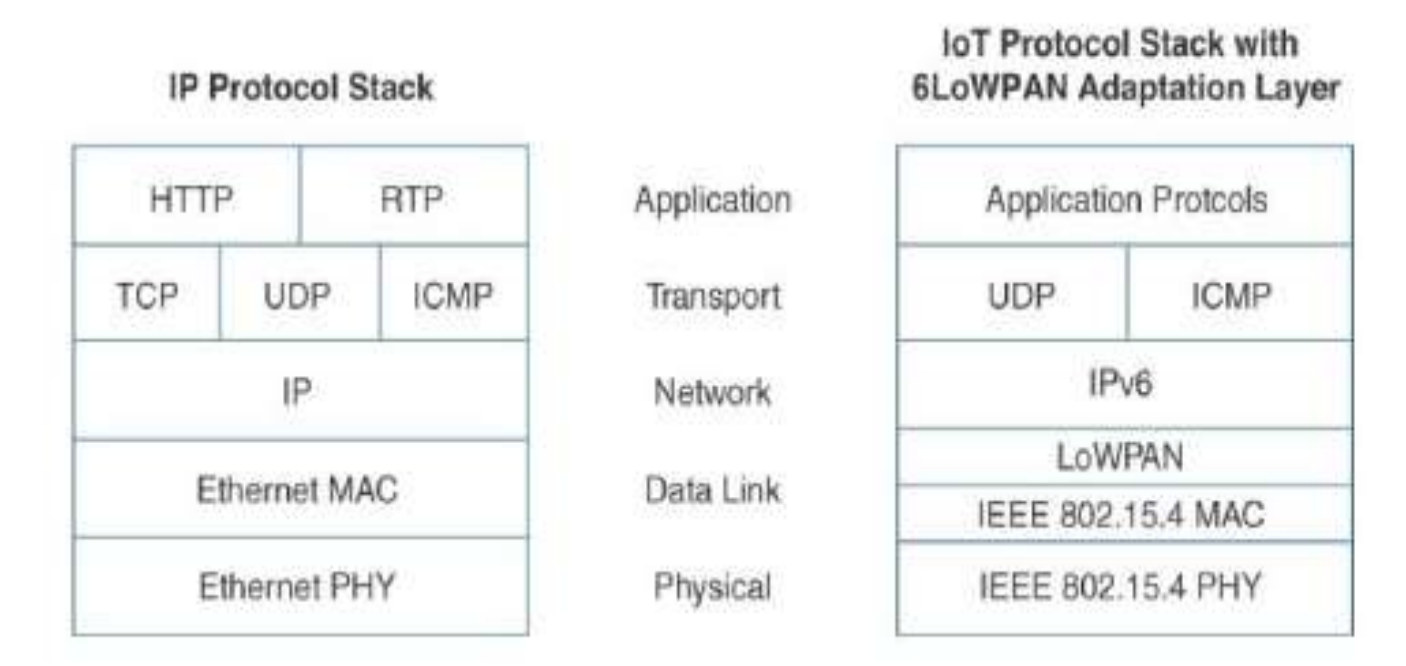
- A constrained network is composed of a significant portion of constrained nodes. Mostly, these constrained node networks are deployed in the edge network of an IoT system. Constrained node networks are deployed in the edge network of an IoT system.
- The majority devices that will constitute the IoT are Constrained Devices (also known as sensors, smart objects, or smart devices) with **limited CPU, memory, and power resources**. These devices have no idea about the security and they don't have enough resources to handle extra functionalities and protocols.

6LoWPAN

6LoWPAN

- While the Internet Protocol is key for a successful Internet of Things, constrained nodes and constrained networks mandate optimization at various layers and on multiple protocols of the IP architecture. Some optimizations are already available from the market or under development by the IETF.

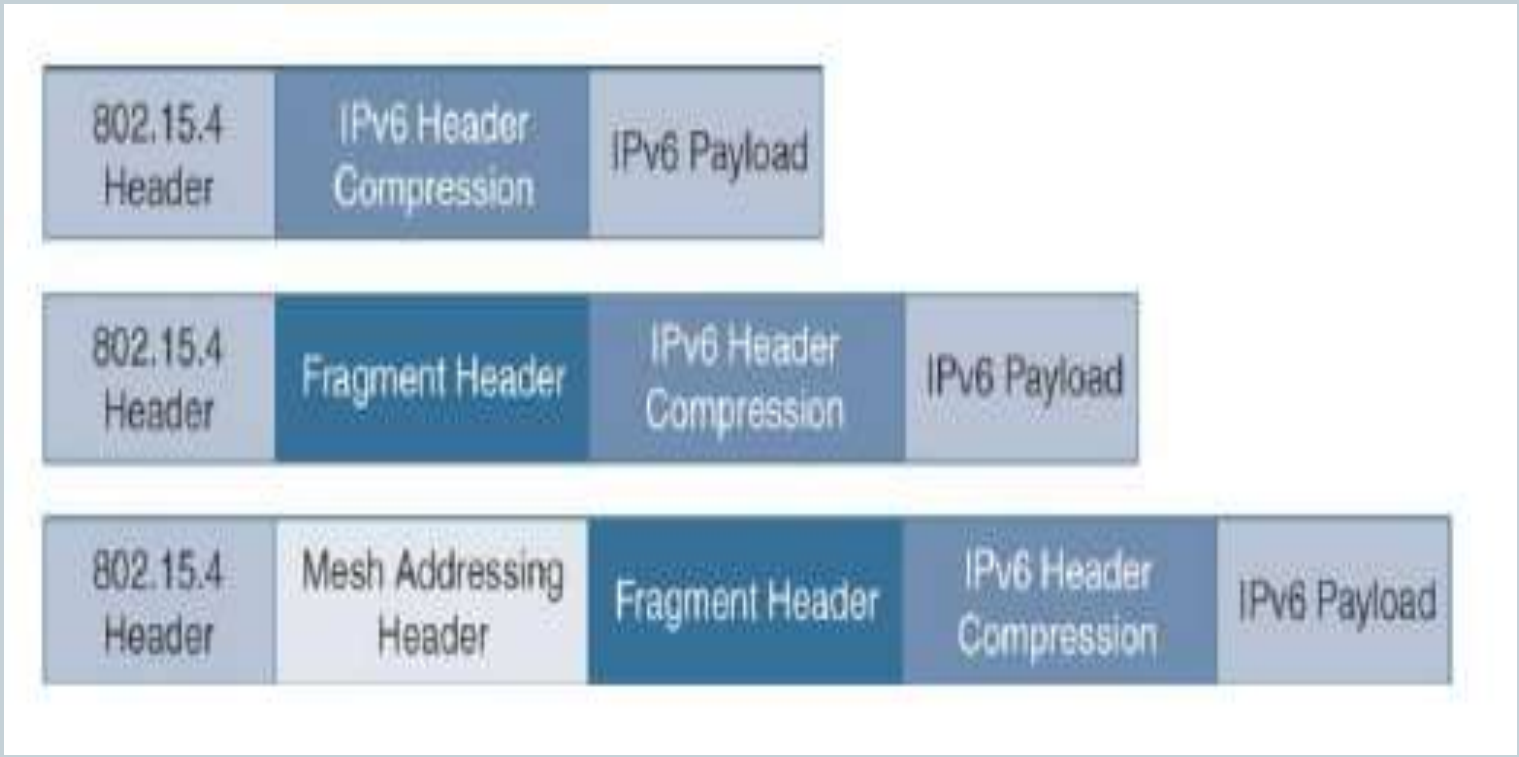
Comparison of an IoT Protocol Stack Utilizing 6LoWPAN and an IP Protocol Stack



6LoWPAN

- The 6LoWPAN working group published several RFCs, but RFC 4994 is foundational because it defines frame headers for the capabilities of header compression, fragmentation, and mesh addressing. These headers can be stacked in the adaptation layer to keep these concepts separate while enforcing a structured method for expressing each capability.
- Depending on the implementation, all, none, or any combination of these capabilities and their corresponding headers can be enabled. Figure shows some examples of typical 6LoWPAN header stacks.

6LoWPAN Header stack



Routing over Low Power and Lossy Networks

- The Internet Layer also covers routing. IPv6 Routing Protocol for Low-Power and Lossy Networks (RPL) is designed for routing IPv6 traffic over low-power networks like those networks implemented over 6LoWPAN. RPL (pronounced “ripple”) is designed for routing packets within constrained networks such as wireless sensor networks, where not all devices are reachable at all times and there are high or unpredictable amounts of packet loss. RPL can compute the optimal path by building up a graph of the nodes in the network based on dynamic metrics and constraints like minimizing energy consumption or latency.
- The IEEE 802.15.4 specification does not define a path selection within the MAC layer for a mesh topology. This function can be done at Layer 2 and is known as *mesh-under*. *Generally, this is based on a proprietary solution. Alternatively, the routing function can occur at Layer 3, using a routing protocol, such as the IPv6 Routing Protocol for Low Power and Lossy Networks (RPL). This is referred to as mesh-over*.

Routing over Low Power and Lossy Networks

- Edge computing is a type of computing that pushes the frontier of computing applications, data and services away from centralised nodes to IoT data generating nodes, that means at logical extremes of the network.2 IoT device nodes are pushed by events, triggers, alerts, messages and data is collected for enrichment, storage and computations from the remote centralised database nodes. Pushing the computations from centralised nodes enables the usage of resources at device nodes, which could be a requirement in case of low power lossy networks.
- The processing can also be classified as edge computing at local cloud, grid or mesh computing. The nodes may be mobile or of a wireless sensor network or cooperative distributed in peer-to-peer and ad-hoc networks.

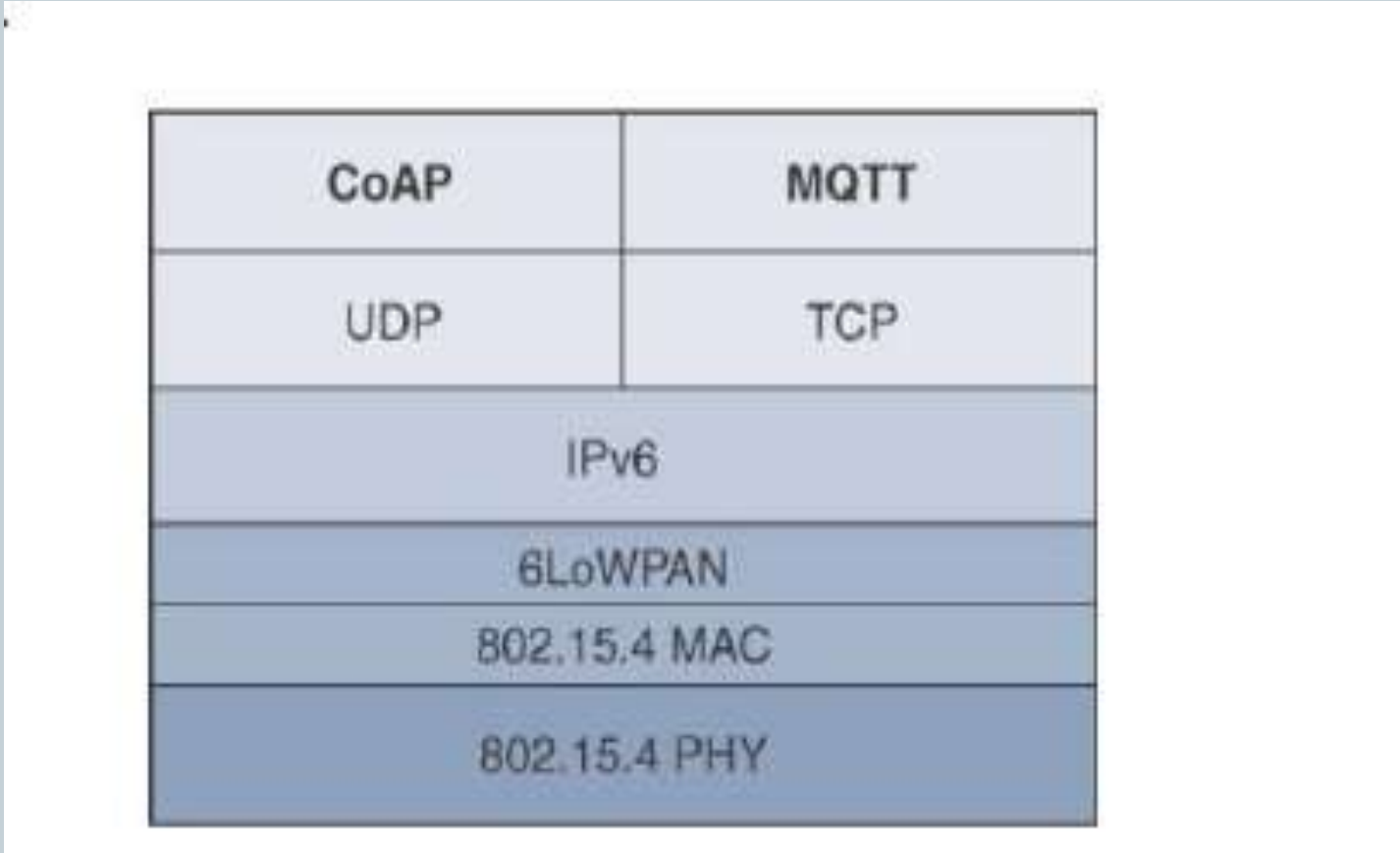
Application layer

- The application layer serves as the interface between the user and the device within a given IoT protocol.
- **Advanced Message Queuing Protocol (AMQP)**
  - A software layer that creates interoperability between messaging middleware. It helps a range of systems and applications work together, creating standardized messaging on an industrial scale.
- **Constrained Application Protocol (CoAP)**
  - A constrained-bandwidth and constrained-network protocol designed for devices with limited capacity to connect in machine-to-machine communication. CoAP is also a document-transfer protocol that runs over User Datagram Protocol (UDP).

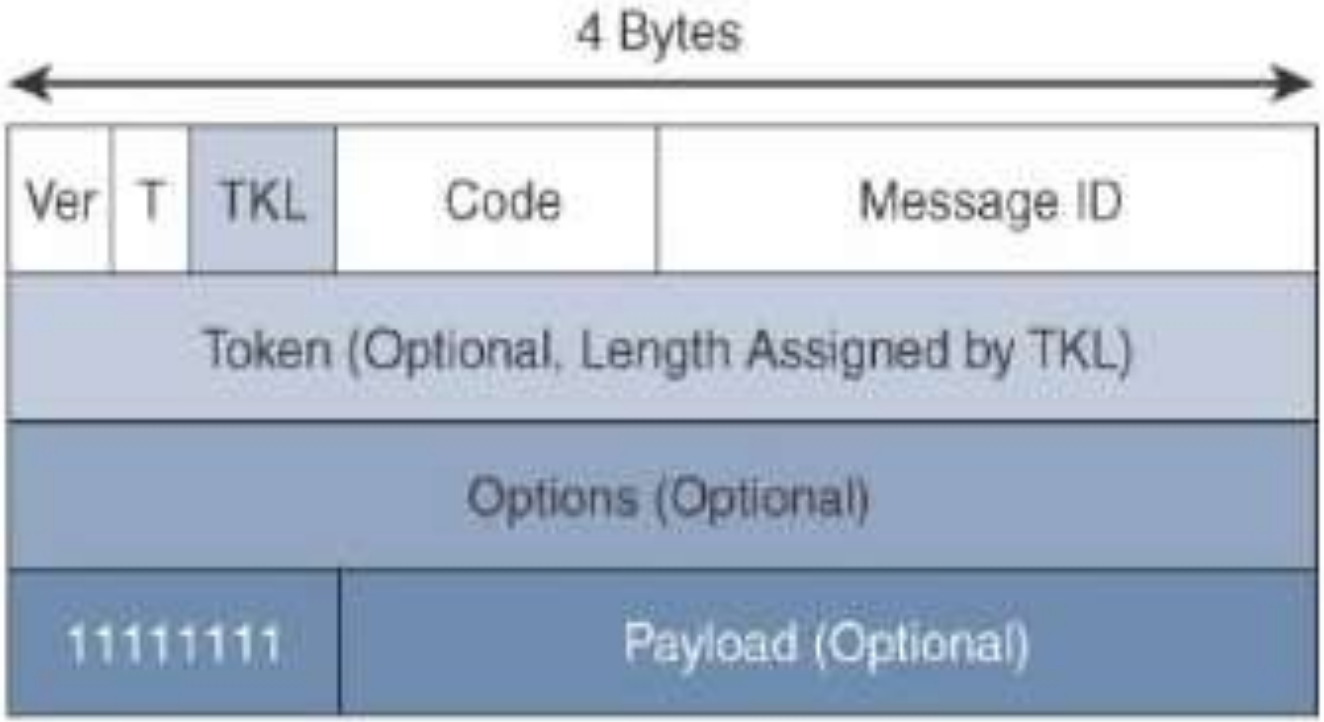
Application layer

- **Data Distribution Service (DDS)**
  - A versatile peer-to-peer communication protocol that does everything from running tiny devices to connecting high-performance networks. DDS streamlines deployment, increases reliability, and reduces complexity.
- **Message Queue Telemetry Transport (MQTT)**
  - A messaging protocol designed for lightweight machine-to-machine communication and primarily used for low-bandwidth connections to remote locations. MQTT uses a publisher-subscriber pattern and is ideal for small devices that require efficient bandwidth and battery use.

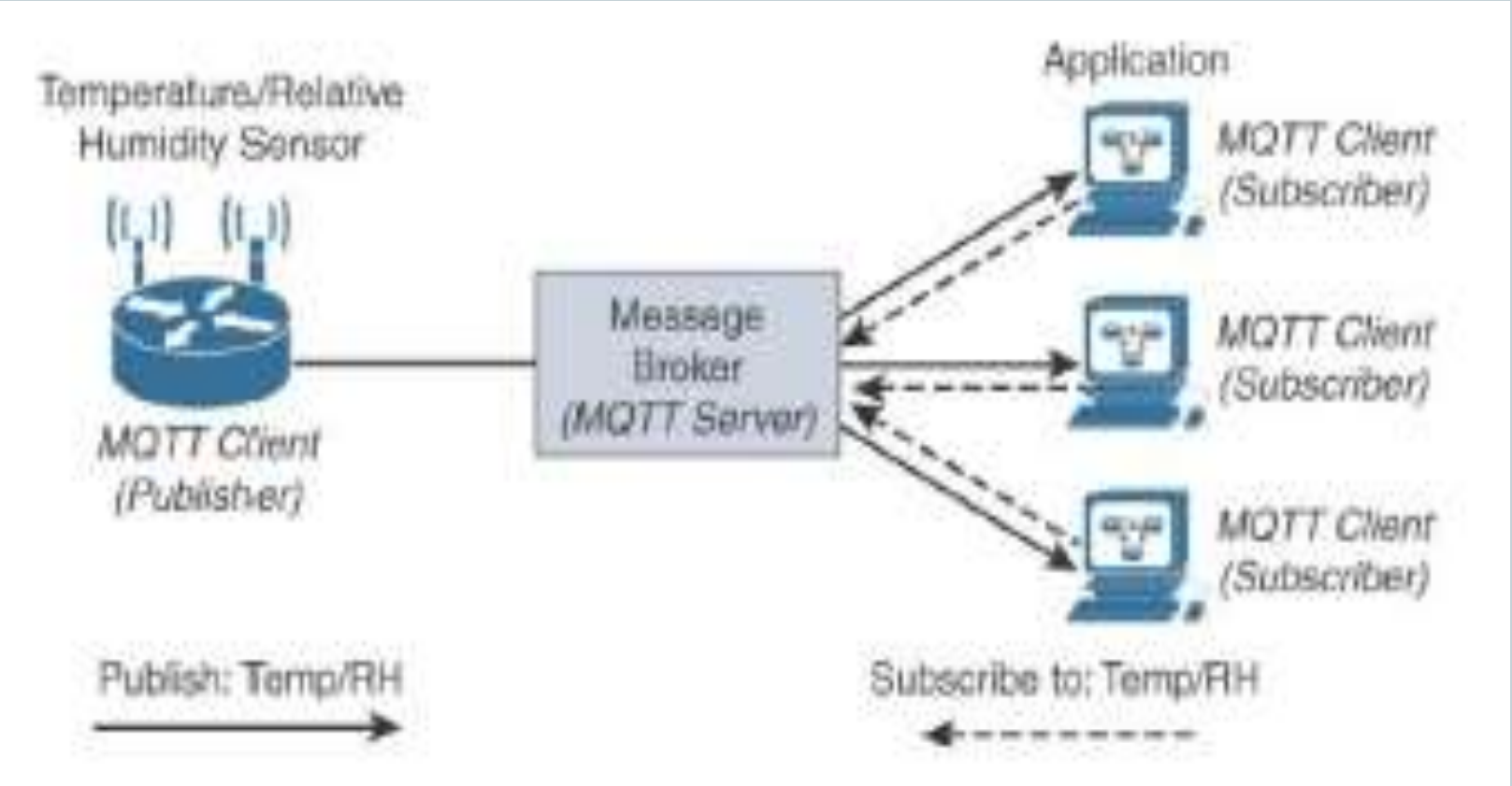
Protocol Stacks for CoAP and MQTT



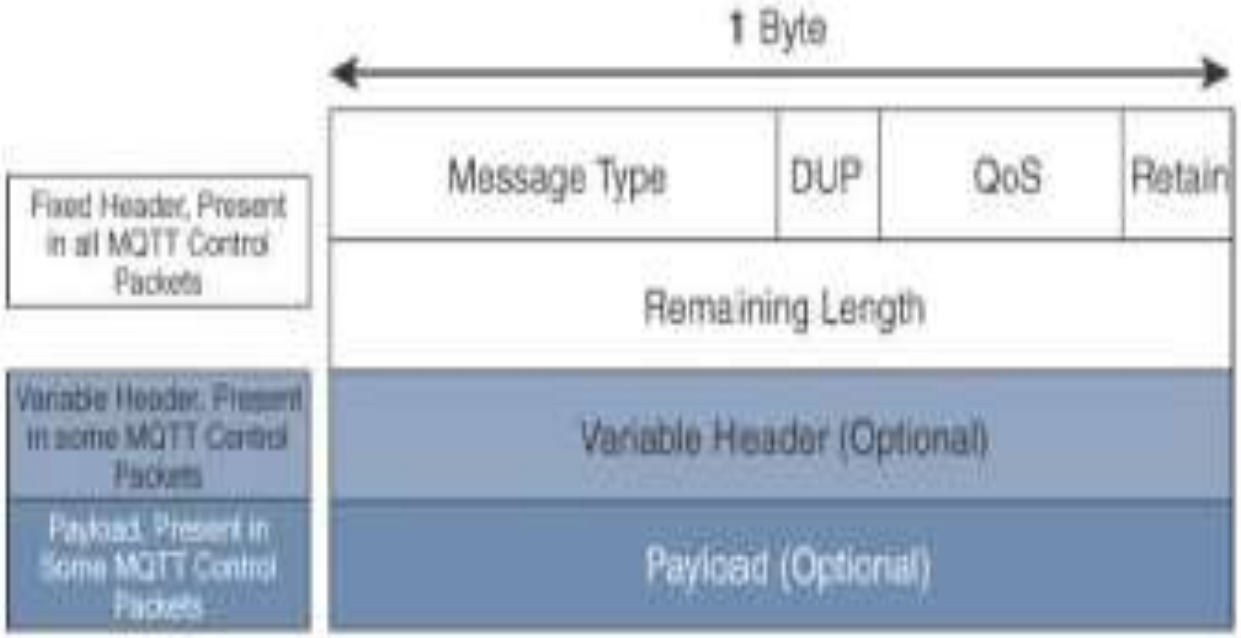
CoAP message format



MQTT Publish/Subscribe framework



MQTT message format



Application transport methods

Supervisory Control and Data Acquision(SCADA)

- In the world of networking technologies and protocols, IoT is relatively new. Combined with the fact that IP is the de facto standard for computer networking in general, older protocols that connected sensors and actuators have evolved and adapted themselves to utilize IP.
- A prime example of this evolution is supervisory control and data acquisition (SCADA). Designed decades ago, SCADA is an automation control system that was initially implemented without IP over serial links, before being adapted to Ethernet and IPv4.

SCADA

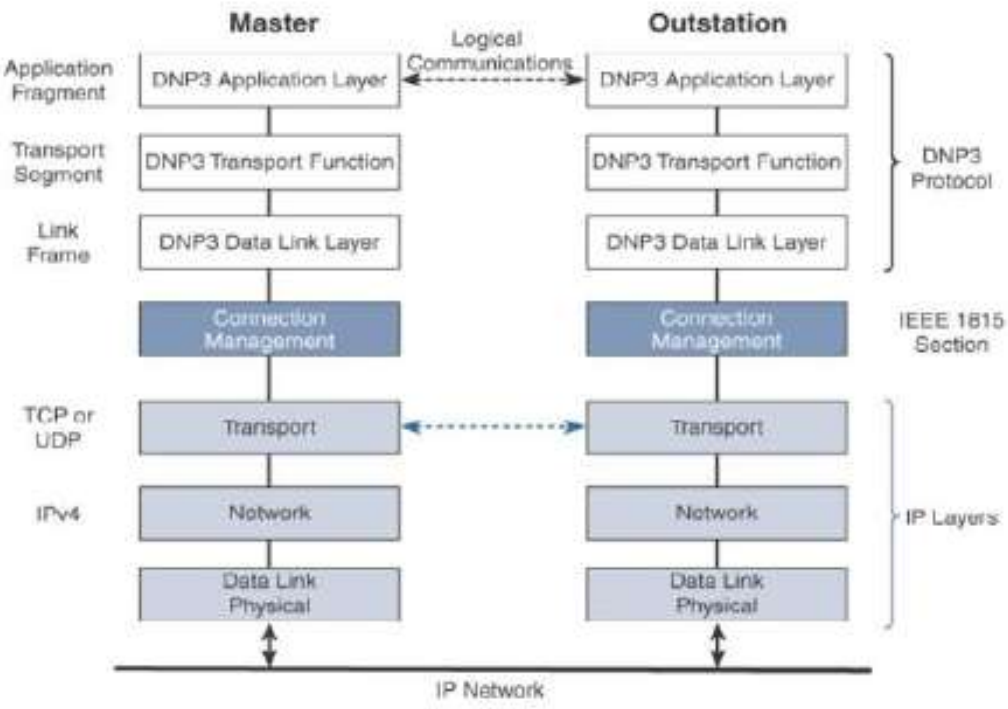


Figure 2.18: Protocol Stack for Transporting Serial DNP3 SCADA over IP