MODULE 1

What Is IoT?

IoT is a technology transition in which devices will allow us to sense and control the physical world by making objects smarter and connecting them through an intelligent network.

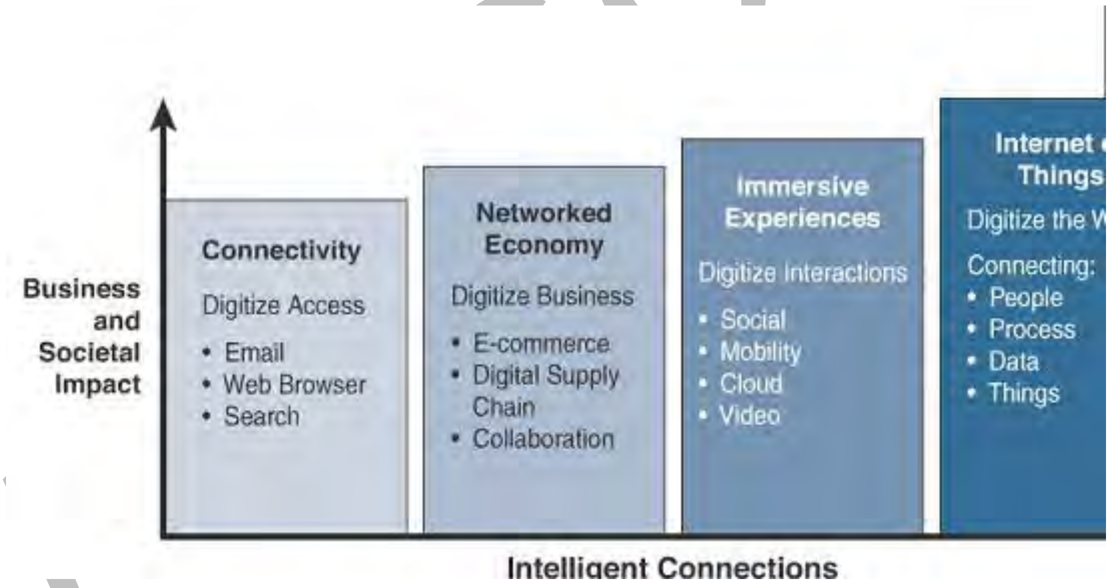
GOAL: The basic premise and goal of IoT is to "connect the unconnected." This means that objects that are not currently joined to a computer network, namely the Internet, will be conn ected so that they can communicate and interact with people and other objects.

When objects and machines can be sensed and controlled remotely across a network, a tighter integration between the physical world and computers is enabled.

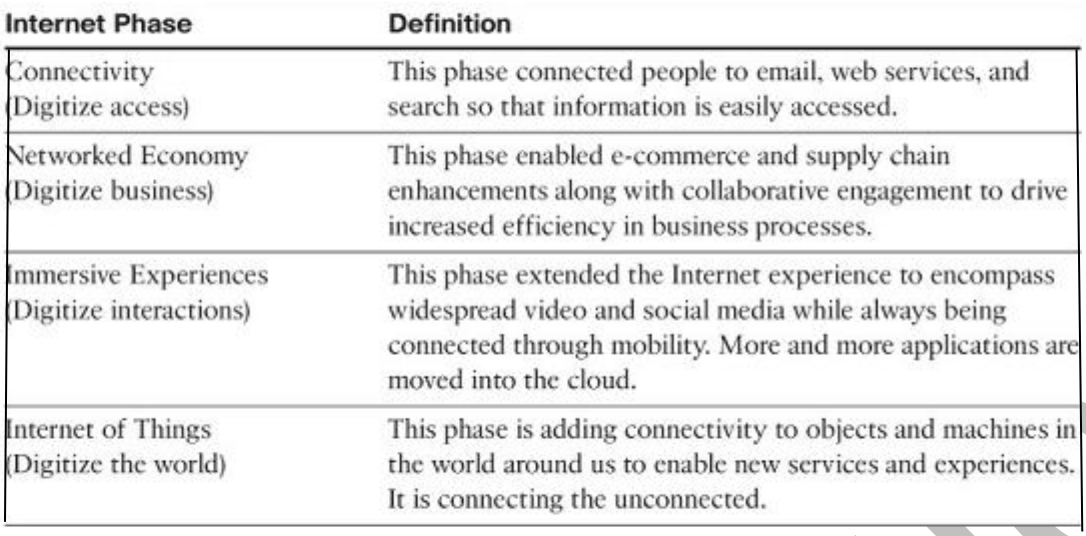
This allows for improvements in the areas of efficiency, accuracy, automation, and the enable ment of advanced applications.

GENESIS OF IOT

The person credited with the creation of the term "Internet of Things" is Kevin Ashton. While working for Procter & Gamble in 1999, Kevin used this phrase to explain a new idea related to linking the company's supply chain to the Internet.



the evolution of the Internet can be categorized into four phases. Each of these phases has had a profound impact on our society and our lives. These four phases are further defined in Table below.



Internet Phase	Definition
Connectivity (Digitize access)	This phase connected people to email, web services, and search so that information is easily accessed.
Networked Economy (Digitize business)	This phase enabled e-commerce and supply chain enhancements along with collaborative engagement to drive increased efficiency in business processes.
Immersive Experiences (Digitize interactions)	This phase extended the Internet experience to encompass widespread video and social media while always being connected through mobility. More and more applications are moved into the cloud.
Internet of Things (Digitize the world)	This phase is adding connectivity to objects and machines in the world around us to enable new services and experiences. It is connecting the unconnected.

IOT AND DIGITIZATION

IoT and *digitization* are terms that are often used interchangeably. In most contexts, this duality is fine, but there are key differences to be aware of.

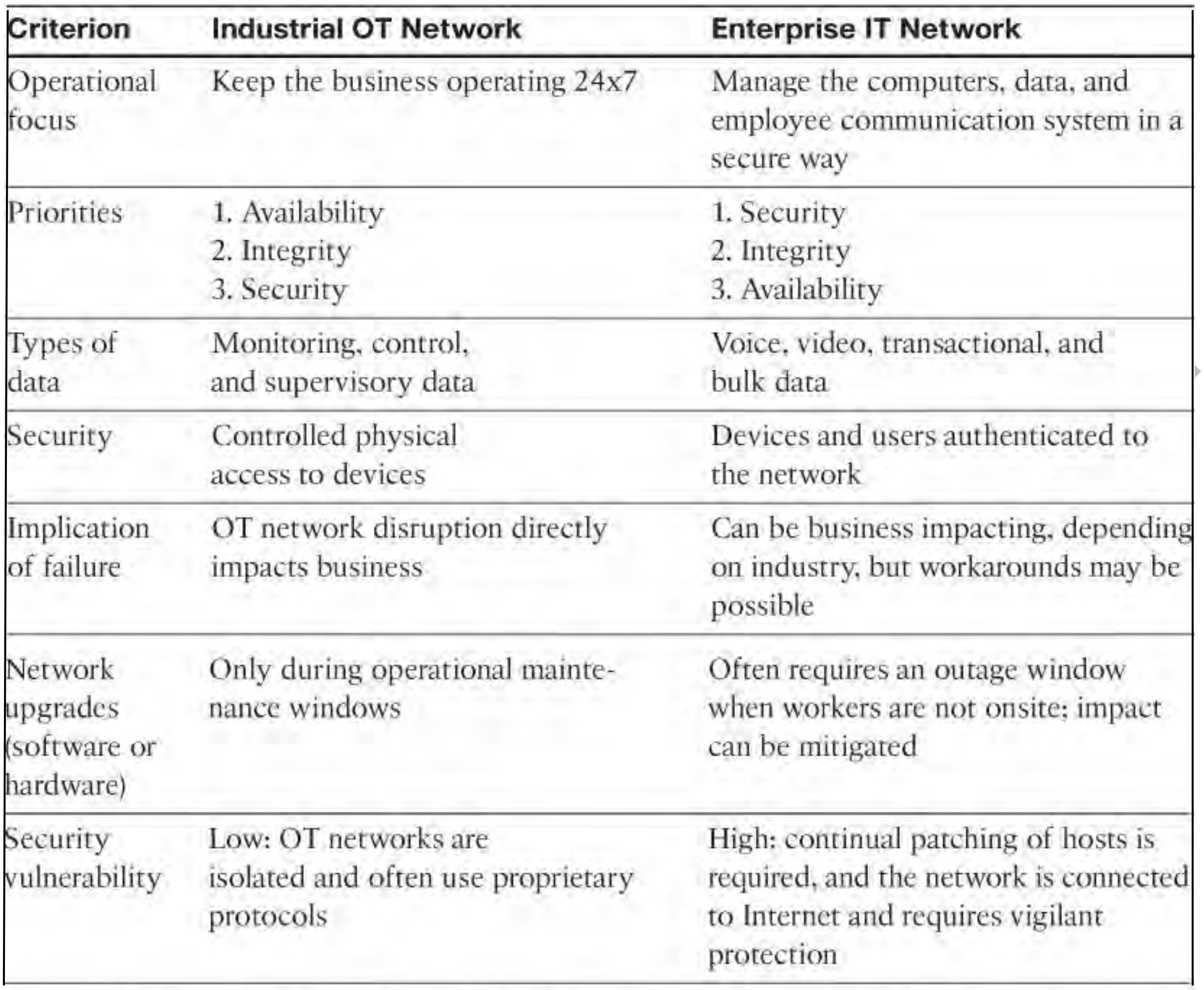
At a high level, IoT focuses on connecting "things," such as objects and machines, to a computer network, such as the Internet. IoT is a well-understood term used across the industry as a whole. On the other hand, digitization can mean different things to different people but generally encompasses the connection of "things" with the data they generate and the business insights that result.

Digitization, as defined in its simplest form, is the conversion of information into a digital format. Digitization has been happening in one form or another for several decades. For example, the whole photography industry has been digitized. Pretty much everyone has digital cameras these days, either standalone devices or built into their mobile phones. Almost no one buys film and takes it to a retailer to get it developed. The digitization of photography has completely changed our experience when it comes to capturing images.

CONVERGENCE OF IT AND OT

Until recently, information technology (IT) and operational technology (OT) have for the most part lived in separate worlds. IT supports connections to the Internet along with related data and technology systems and is focused on the secure flow of data across an organization. OT monitors and controls devices and processes on physical operational systems. These systems include assembly lines, utility distribution networks, production facilities, roadway systems, and many more. Typically, IT did not get involved with the production and logistics of OT environments.

Management of OT is tied to the lifeblood of a company. For example, if the network connecting the machines in a factory fails, the machines cannot function, and production may come to a standstill, negatively impacting business on the order of millions of dollars. On the other hand, if the email server (run by the IT department) fails for a few hours, it may irritate people, but it is unlikely to impact business at anywhere near the same level. **Table below highlights some of the differences between IT and OT networks and their various challenges**.

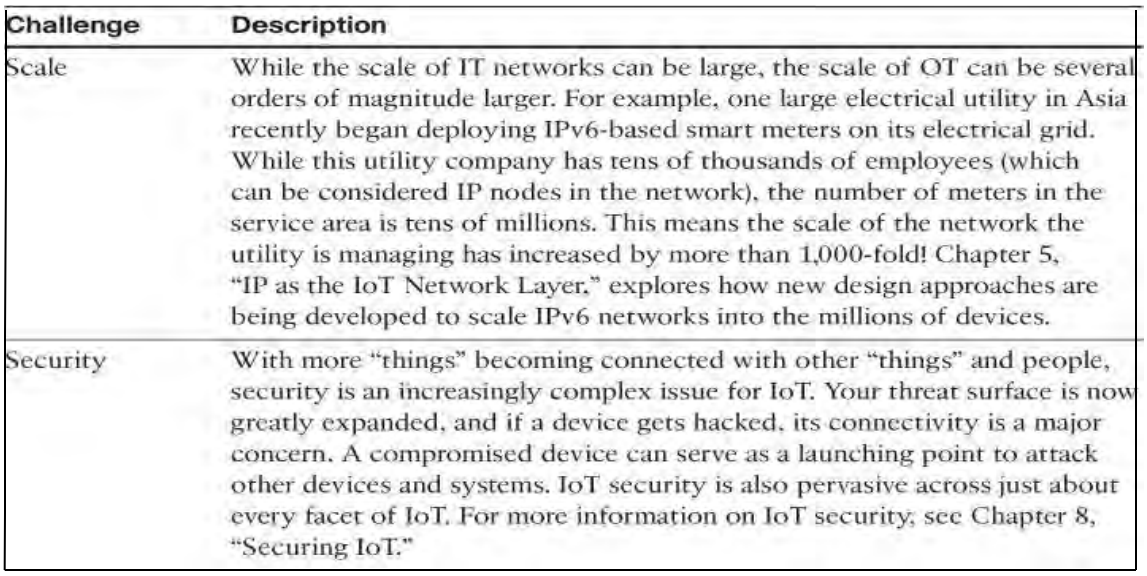


Criterion	Industrial OT Network	Enterprise IT Network
Operational focus	Keep the business operating 24x7	Manage the computers, data, and employee communication system in a secure way
Priorities	1. Availability 2. Integrity 3. Security	1. Security 2. Integrity 3. Availability
Types of data	Monitoring, control, and supervisory data	Voice, video, transactional, and bulk data
Security	Controlled physical access to devices	Devices and users authenticated to the network
Implication of failure	OT network disruption directly impacts business	Can be business impacting, depending on industry, but workarounds may be possible
Network upgrades (software or hardware)	Only during operational maintenance windows	Often requires an outage window when workers are not onsite; impact can be mitigated
Security vulnerability	Low: OT networks are isolated and often use proprietary protocols	High: continual patching of hosts is required, and the network is connected to Internet and requires vigilant protection

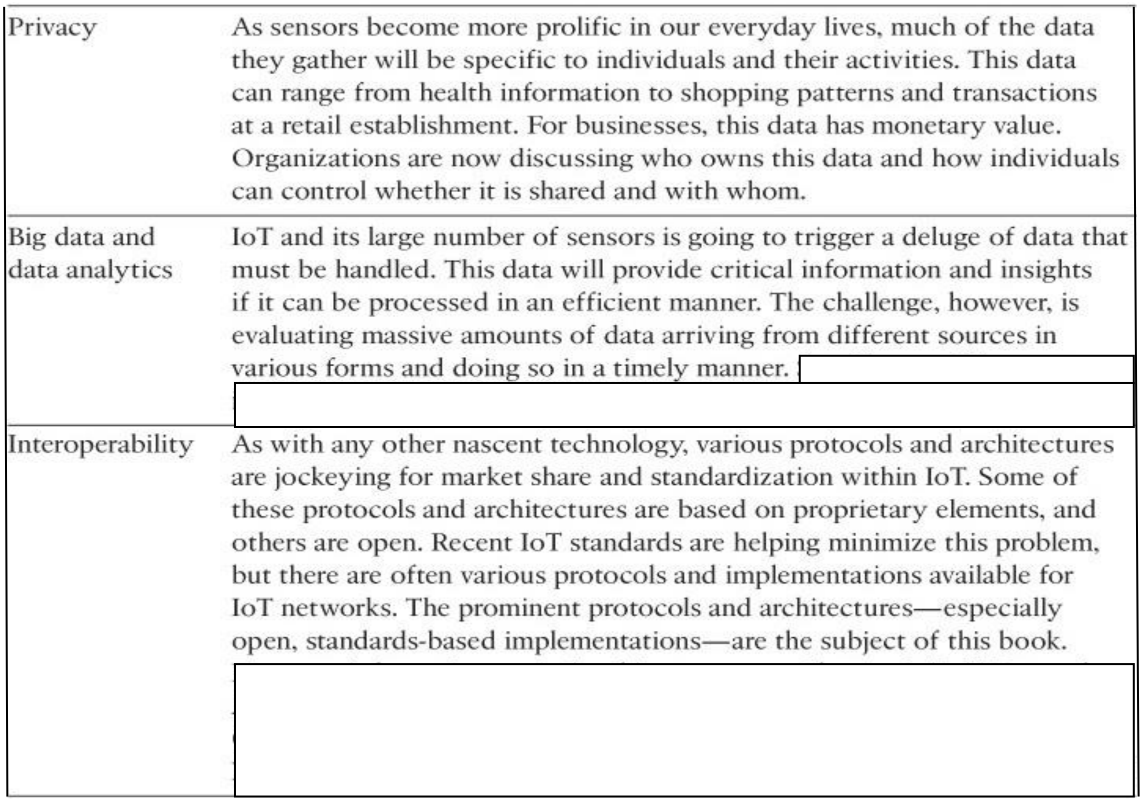
Source: Maciej Kranz, *IT Is from Venus, OT Is from Mars*, blogs.cisco.com/digital/it-is-from-venus-ot-is-from-mars, July 14, 2015.

IOT CHALLENGES

The most significant challenges and problems that IoT is currently facing are



Challenge	Description
Scale	While the scale of IT networks can be large, the scale of OT can be several orders of magnitude larger. For example, one large electrical utility in Asia recently began deploying IPv6-based smart meters on its electrical grid. While this utility company has tens of thousands of employees (which can be considered IP nodes in the network), the number of meters in the service area is tens of millions. This means the scale of the network the utility is managing has increased by more than 1,000-fold! Chapter 5, "IP as the IoT Network Layer," explores how new design approaches are being developed to scale IPv6 networks into the millions of devices.
Security	With more "things" becoming connected with other "things" and people, security is an increasingly complex issue for IoT. Your threat surface is now greatly expanded, and if a device gets hacked, its connectivity is a major concern. A compromised device can serve as a launching point to attack other devices and systems. IoT security is also pervasive across just about every facet of IoT. For more information on IoT security, see Chapter 8, "Securing IoT."



Privacy	As sensors become more prolific in our everyday lives, much of the data they gather will be specific to individuals and their activities. This data can range from health information to shopping patterns and transactions at a retail establishment. For businesses, this data has monetary value. Organizations are now discussing who owns this data and how individuals can control whether it is shared and with whom.
Big data and data analytics	IoT and its large number of sensors is going to trigger a deluge of data that must be handled. This data will provide critical information and insights if it can be processed in an efficient manner. The challenge, however, is evaluating massive amounts of data arriving from different sources in various forms and doing so in a timely manner.
Interoperability	As with any other nascent technology, various protocols and architectures are jockeying for market share and standardization within IoT. Some of these protocols and architectures are based on proprietary elements, and others are open. Recent IoT standards are helping minimize this problem, but there are often various protocols and implementations available for IoT networks. The prominent protocols and architectures—especially open, standards-based implementations—are the subject of this book.

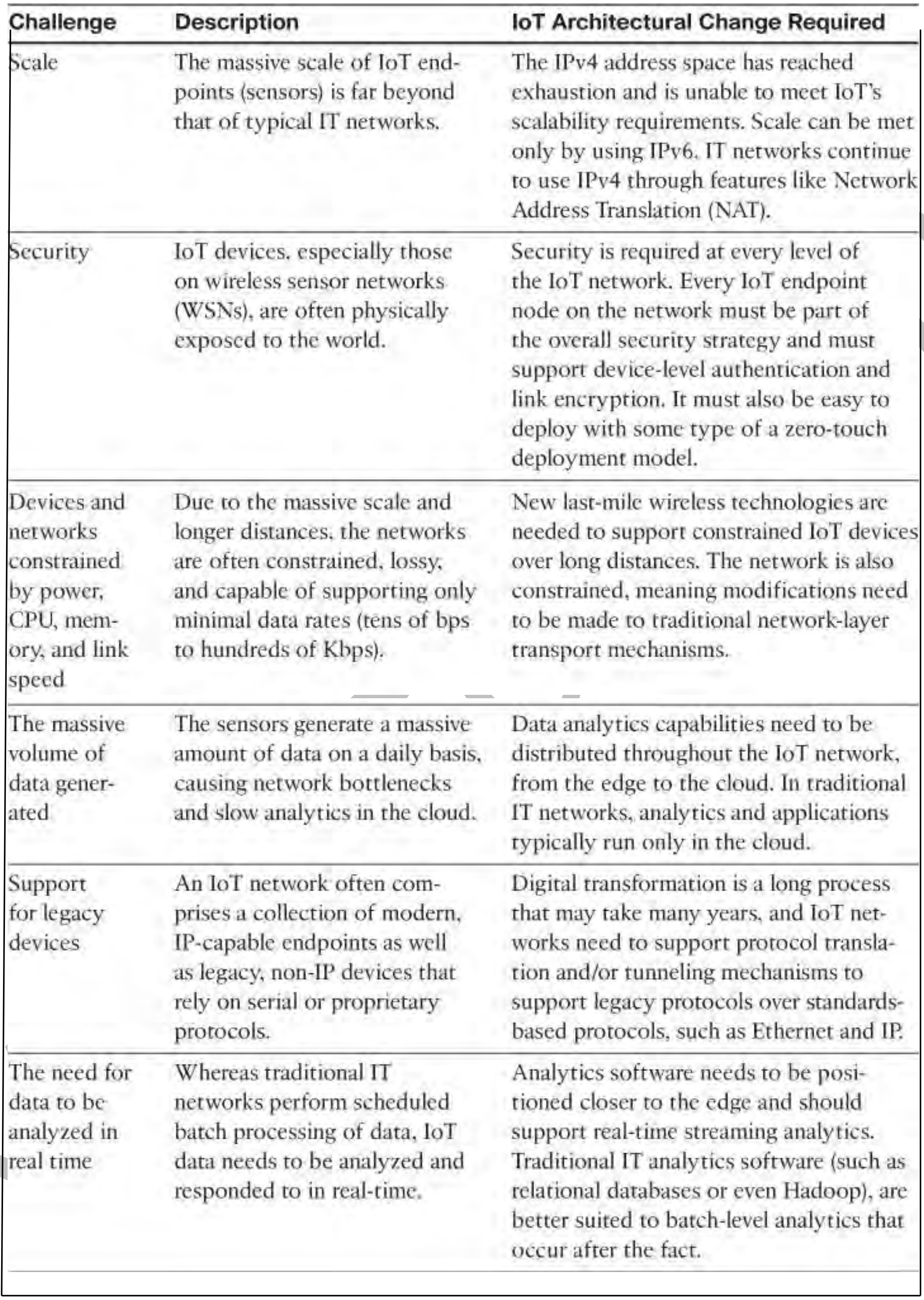
IoT Network Architecture and Design

The unique challenges posed by IoT networks and how these challenges have driven new architectural models.

- Drivers Behind New Network Architectures
- Comparing IoT Architectures.
- A Simplified IoT Architecture
- The Core IoT Functional Stack
- IoT Data Management and Compute Stack

DRIVERS BEHIND NEW NETWORK ARCHITECTURES

This begins by comparing how using an architectural blueprint to construct a house is similar to the approach we take when designing a network. Take a closer look at some of the differences between IT and IoT networks, with a focus on the IoT requirements that are driving new network architectures, and considers what adjustments are needed.



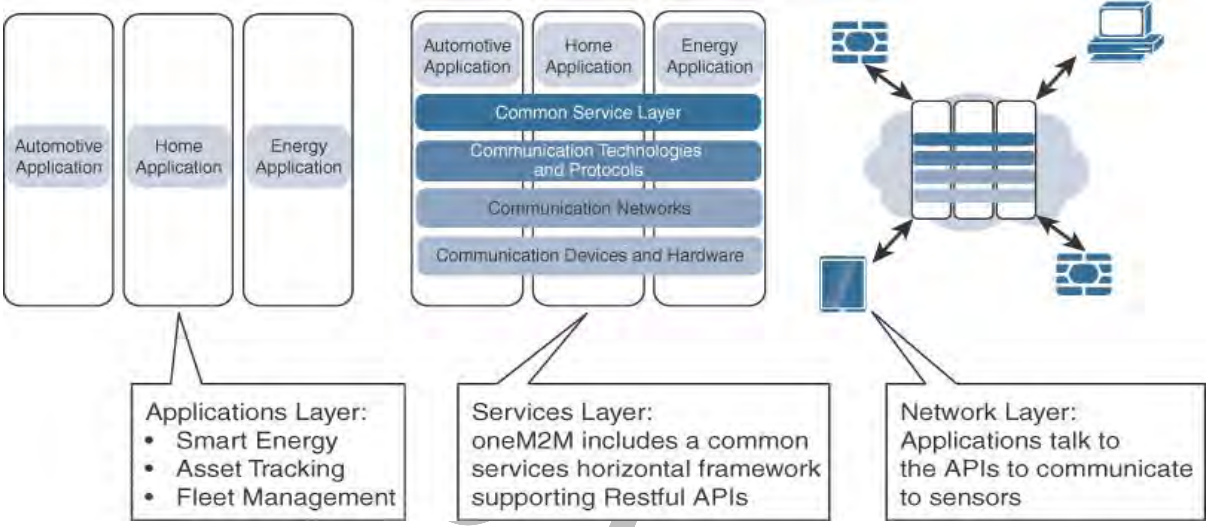
Challenge	Description	IoT Architectural Change Required
Scale	The massive scale of IoT endpoints (sensors) is far beyond that of typical IT networks.	The IPv4 address space has reached exhaustion and is unable to meet IoT's scalability requirements. Scale can be met only by using IPv6. IT networks continue to use IPv4 through features like Network Address Translation (NAT).
Security	IoT devices, especially those on wireless sensor networks (WSNs), are often physically exposed to the world.	Security is required at every level of the IoT network. Every IoT endpoint node on the network must be part of the overall security strategy and must support device-level authentication and link encryption. It must also be easy to deploy with some type of a zero-touch deployment model.
Devices and networks constrained by power, CPU, memory, and link speed	Due to the massive scale and longer distances, the networks are often constrained, lossy, and capable of supporting only minimal data rates (tens of bps to hundreds of Kbps).	New last-mile wireless technologies are needed to support constrained IoT devices over long distances. The network is also constrained, meaning modifications need to be made to traditional network-layer transport mechanisms.
The massive volume of data generated	The sensors generate a massive amount of data on a daily basis, causing network bottlenecks and slow analytics in the cloud.	Data analytics capabilities need to be distributed throughout the IoT network, from the edge to the cloud. In traditional IT networks, analytics and applications typically run only in the cloud.
Support for legacy devices	An IoT network often comprises a collection of modern, IP-capable endpoints as well as legacy, non-IP devices that rely on serial or proprietary protocols.	Digital transformation is a long process that may take many years, and IoT networks need to support protocol translation and/or tunneling mechanisms to support legacy protocols over standards-based protocols, such as Ethernet and IP.
The need for data to be analyzed in real time	Whereas traditional IT networks perform scheduled batch processing of data, IoT data needs to be analyzed and responded to in real-time.	Analytics software needs to be positioned closer to the edge and should support real-time streaming analytics. Traditional IT analytics software (such as relational databases or even Hadoop), are better suited to batch-level analytics that occur after the fact.

COMPARING IOT ARCHITECTURES

The oneM2M IoT Standardized Architecture

In an effort to standardize the rapidly growing field of machine-to-machine (M2M) communications, the European Telecommunications Standards Institute (ETSI) created the M2M Technical Committee in 2008. The goal of this committee was to create a common architecture that would help accelerate the adoption of M2M applications and devices. Over time, the scope has expanded to include the Internet of Things.

One of the greatest challenges in designing an IoT architecture is dealing with the heterogeneity of devices, software, and access methods. By developing a horizontal platform architecture, oneM2M is developing standards that allow interoperability at all levels of the IoT stack



The Main Elements of the oneM2M IoT Architecture

The oneM2M architecture divides IoT functions into three major domains: the application layer, the services layer, and the network layer

- **Applications layer:** The oneM2M architecture gives major attention to connectivity between devices and their applications. This domain includes the application-layer protocols and attempts to standardize northbound API definitions for interaction with business intelligence (BI) systems. Applications tend to be industry-specific and have their own sets of data models, and thus they are shown as vertical entities.

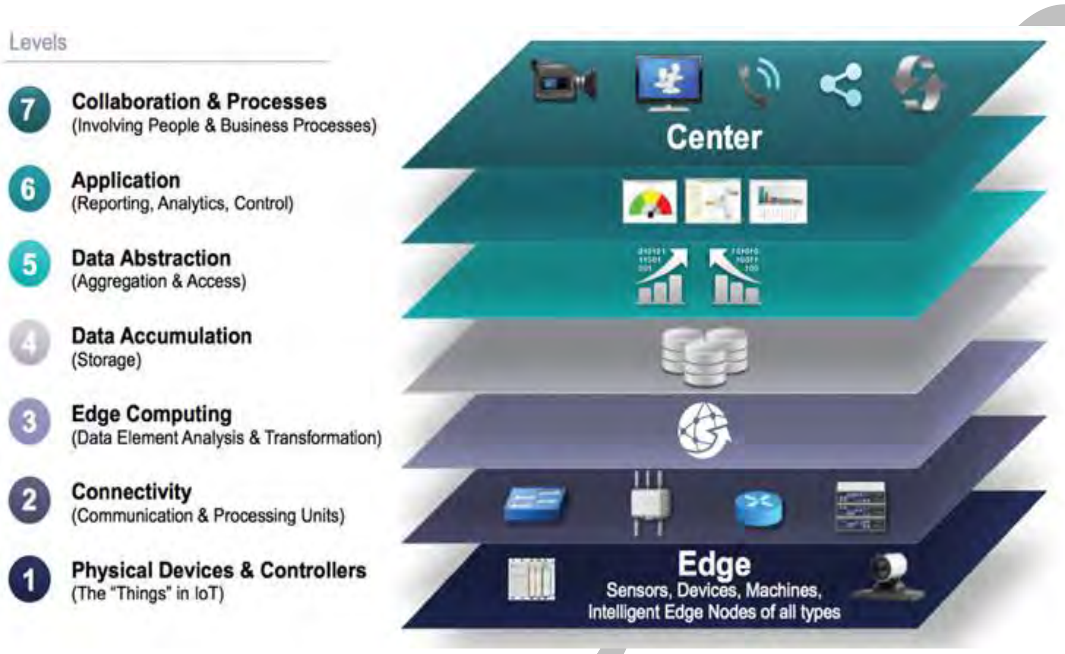
- **Services layer:** This layer is shown as a horizontal framework across the vertical industry applications. At this layer, horizontal modules include the physical network that the IoT applications run on, the underlying management protocols, and the hardware. Examples include backhaul communications via cellular, MPLS networks, VPNs, and so on. Riding on top is the common services layer.

- **Network layer:** This is the communication domain for the IoT devices and endpoints. It includes the devices themselves and the communications network that links them. Embodiments of this communications infrastructure include wireless mesh technologies, such as IEEE 802.15.4, and wireless point-to-multipoint systems, such as IEEE 801.11ah.

The IoT World Forum (IoTWF) Standardized Architecture

This publish 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.


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)
Center
Edge
Sensors, Devices, Machines,
Intelligent Edge Nodes of all types

Using this reference model, we are able to achieve the following:

1. Decompose the IoT problem into smaller parts
2. Identify different technologies at each layer and how they relate to one another
3. Define a system in which different parts can be provided by different vendors
4. Have a process of defining interfaces that leads to interoperability
5. Define a tiered security model that is enforced at the transition points between levels

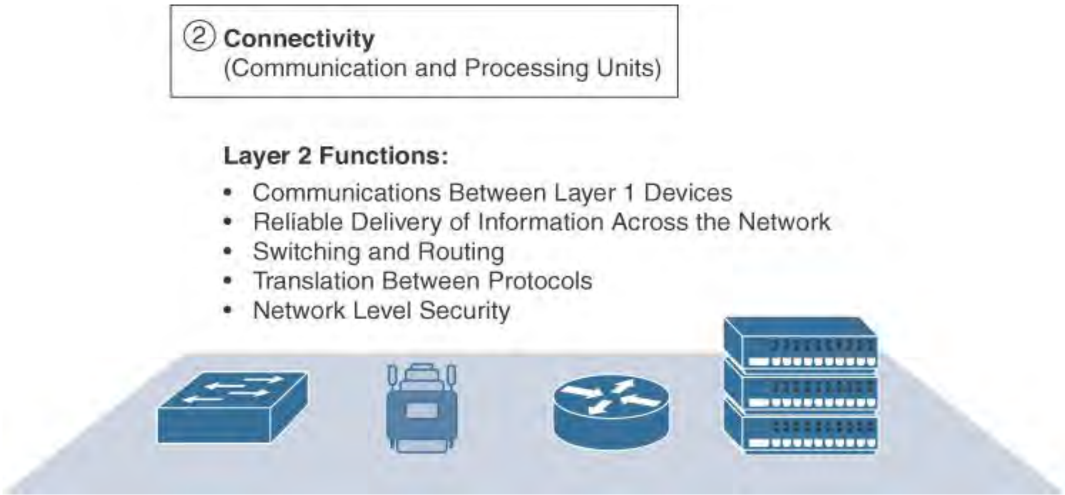
Layer 1: Physical Devices and Controllers Layer

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).

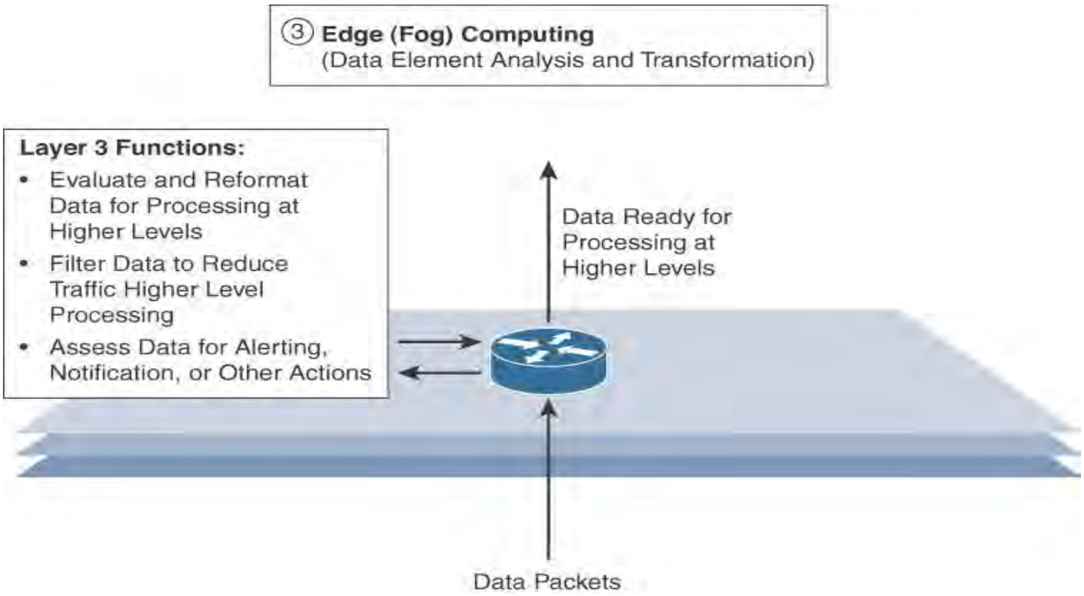
.


② Connectivity
(Communication and Processing Units)
Layer 2 Functions:
• Communications Between Layer 1 Devices
• Reliable Delivery of Information Across the Network
• Switching and Routing
• Translation Between Protocols
• Network Level Security

IoT Reference Model Connectivity Layer Functions

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

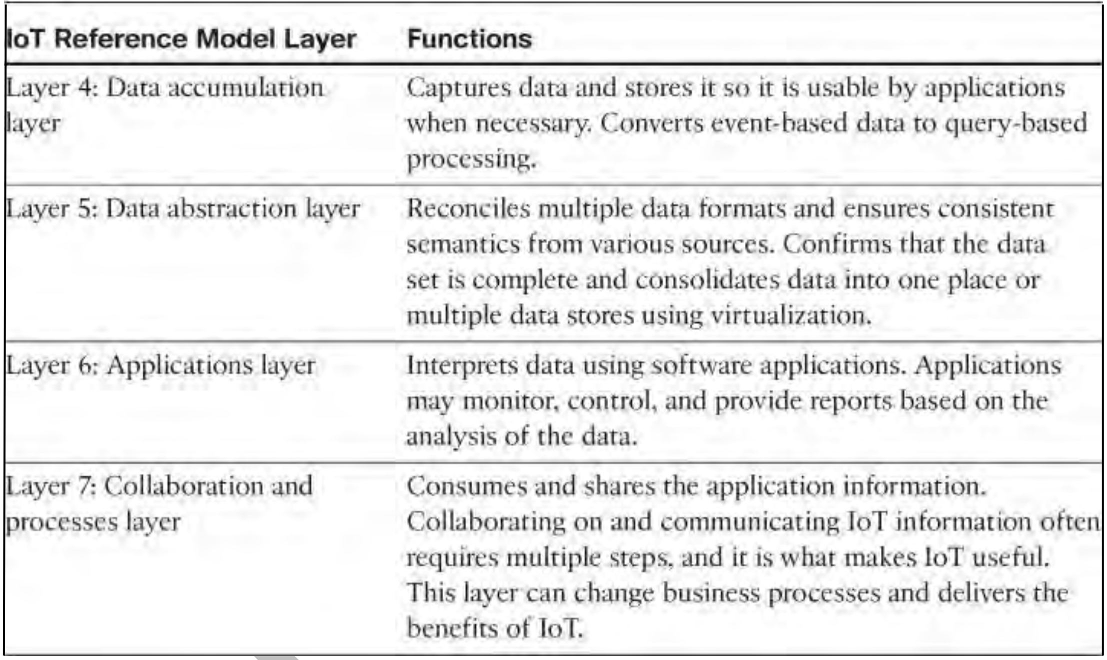

③ Edge (Fog) Computing
(Data Element Analysis and Transformation)
Layer 3 Functions:
• Evaluate and Reformat Data for Processing at Higher Levels
• Filter Data to Reduce Traffic Higher Level Processing
• Assess Data for Alerting, Notification, or Other Actions
Data Ready for Processing at Higher Levels
Data Packets

IoT Reference Model Layer 3 Functions

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.

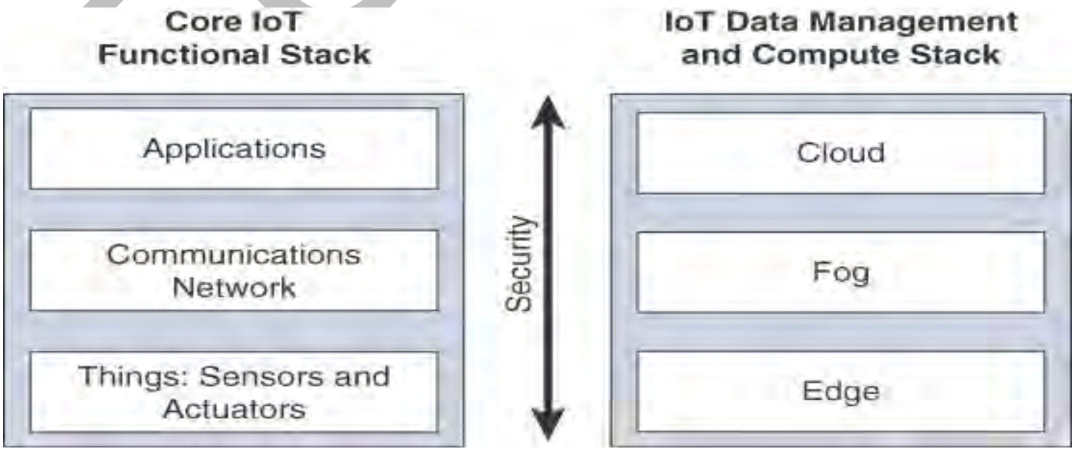
Upper Layers: Layers 4–7

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 .



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.

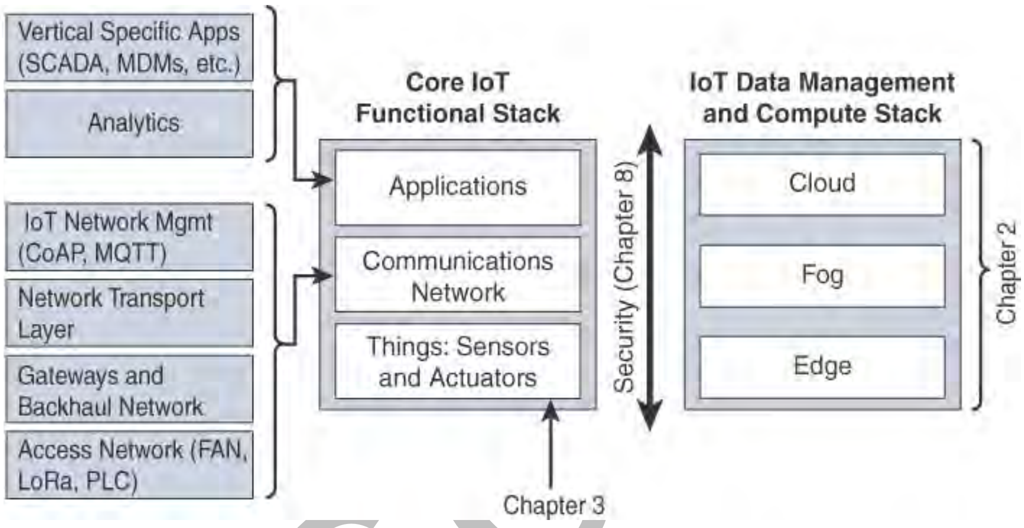
A SIMPLIFIED IOT ARCHITECTURE


Core IoT Functional Stack
Applications
Communications Network
Things: Sensors and Actuators
Security
IoT Data Management and Compute Stack
Cloud
Fog
Edge

Simplified IoT Architecture

The presentation of the Core IoT Functional Stack in three layers is meant to simplify your understanding of the IoT architecture into its most foundational building blocks. The network communications layer of the IoT stack itself involves a significant amount of detail and incorporates a vast array of technologies.

Data management is aligned with each of the three layers of the Core IoT Functional Stack. The three data management layers are the edge layer (data management within the sensors themselves), the fog layer (data management in the gateways and transit network), and the cloud layer (data management in the cloud or central data center). An expanded view of the IoT architecture presented as below:


Vertical Specific Apps (SCADA, MDMs, etc.)
Analytics
IoT Network Mgmt (CoAP, MQTT)
Network Transport Layer
Gateways and Backhaul Network
Access Network (FAN, LoRa, PLC)
Core IoT Functional Stack
Applications
Communications Network
Things: Sensors and Actuators
Chapter 3
Security (Chapter 8)
IoT Data Management and Compute Stack
Cloud
Fog
Edge
Chapter 2

Expanded View of the Simplified IoT Architecture

The Core IoT Functional Stack can be expanded into sublayers containing greater detail and specific network functions. For example, the communications layer is broken down into four separate sublayers: the access network, gateways and backhaul, IP transport, and operations and management sublayers.

The applications layer of IoT networks is quite different from the application layer of a typical enterprise network. Instead of simply using business applications, IoT often involves a strong big data analytics component. One message that is stressed throughout this book is that IoT is not just about the control of IoT devices but, rather, the useful insights gained from the data generated by those devices. Thus, the applications layer typically has both analytics and industry-specific IoT control system components.

presented in Part II, and it gives you the tools you need to understand how these technologies are applied in key industries in Part III.

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.

From an architectural standpoint, several components have to work together for an IoT network to be operational:

- "Things" layer:
- Communications network layer
- Access network sublayer
- Gateways and backhaul network sublayer
- Network transport sublayer
- IoT network management sublayer
- Application and analytics layer

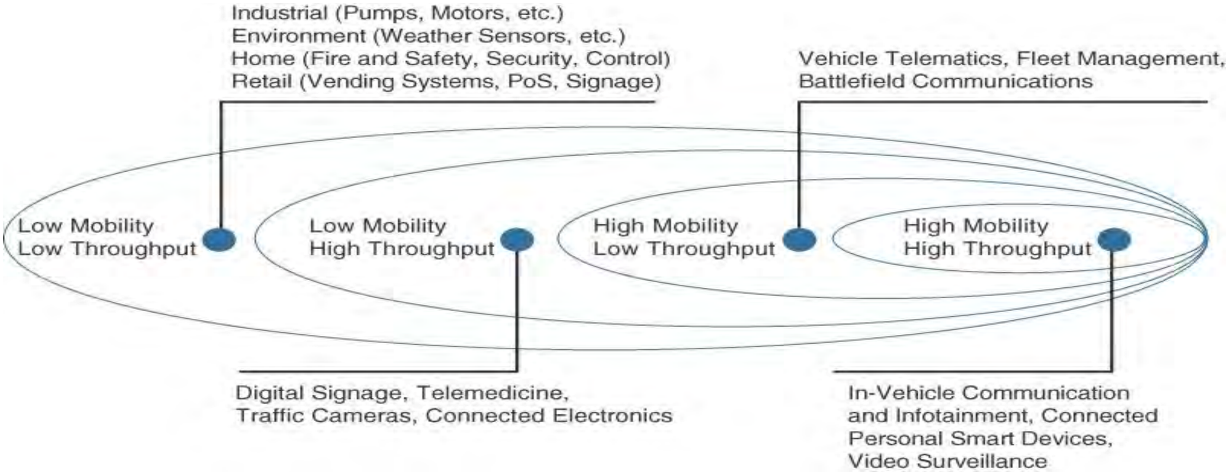
The following sections examine these elements and help you architect your IoT communication network.

Layer 1: Things: Sensors and Actuators Layer

"Smart Objects: The 'Things' in IoT," provides more in-depth information about smart objects. From an architectural standpoint, the variety of smart object types, shapes, and needs drive the variety of IoT protocols and architectures. One architectural classification could be:

- **Battery-powered or power-connected:** This classification is based on whether the object carries its own energy supply or receives continuous power from an external power source.
- **Mobile or static:** This classification is based on whether the "thing" should move or always stay at the same location. A sensor may be mobile because it is moved from one object to another or because it is attached to a movin
- **Low or high reporting frequency:** This classification is based on how often the object should report monitored parameters. A rust sensor may report values once a month. A motion sensor may report acceleration several hundred times per second.
- **Simple or rich data:** This classification is based on the quantity of data exchanged at each report cycle
- **Report range:** This classification is based on the distance at which the gateway is located. For example, for your fitness band to communicate with your phone, it needs to be located a few meters away at most.
- **Object density per cell:** This classification is based on the number of smart objects (with a similar need to communicate) over a given area, connected to the same gateway.

Below figure provides some examples of applications matching the combination of mobility and throughput requirements.


Industrial (Pumps, Motors, etc.)
Environment (Weather Sensors, etc.)
Home (Fire and Safety, Security, Control)
Retail (Vending Systems, PoS, Signage)
Vehicle Telematics, Fleet Management,
Battlefield Communications
Low Mobility
Low Throughput
Low Mobility
High Throughput
High Mobility
Low Throughput
High Mobility
High Throughput
Digital Signage, Telemedicine,
Traffic Cameras, Connected Electronics
In-Vehicle Communication
and Infotainment, Connected
Personal Smart Devices,
Video Surveillance

Example of Sensor Applications Based on Mobility and Throughput

Layer 2: Communications Network Layer

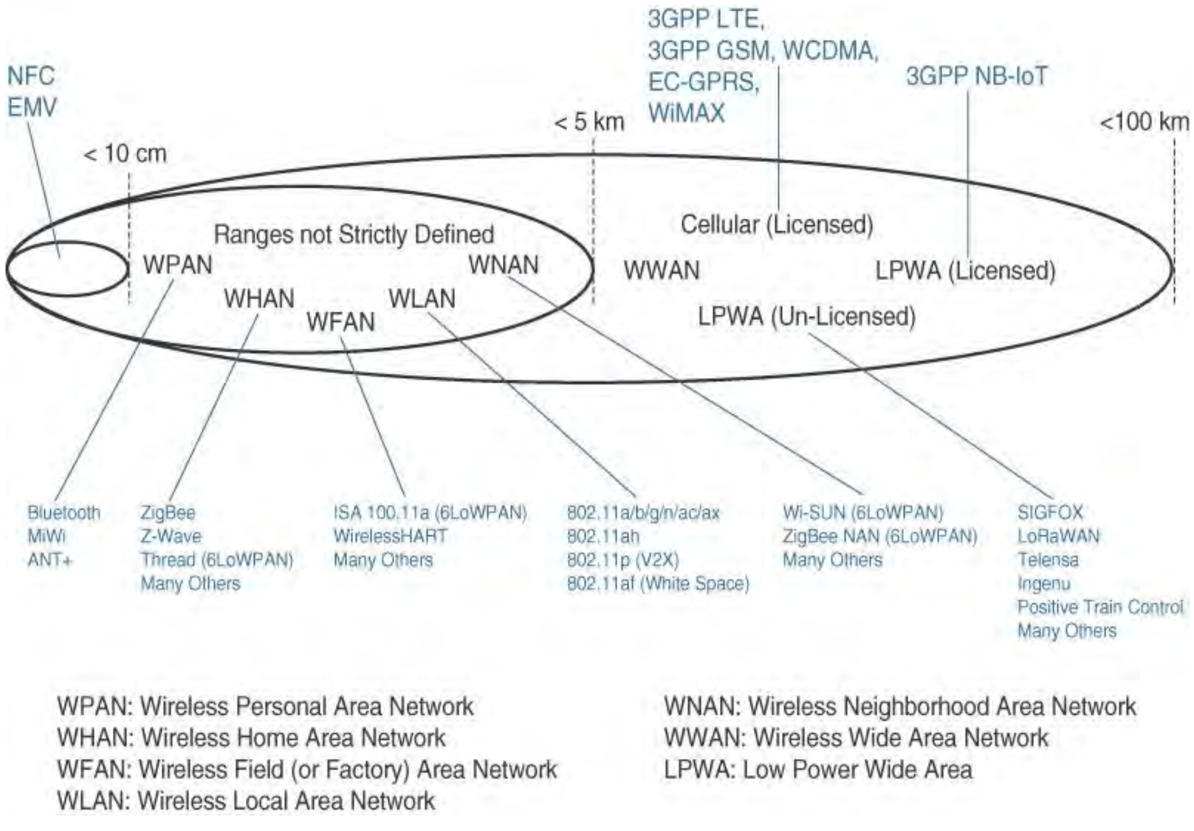
Once you have determined the influence of the smart object form factor over its transmission capabilities (transmission range, data volume and frequency, sensor density and mobility), you are ready to connect the object and communicate.

Compute and network assets used in IoT can be very different from those in IT environments. The difference in the physical form factors between devices used by IT and OT is obvious even to the most casual of observers. What typically drives this is the physical environment in which the devices are deployed. What may not be as inherently obvious, however, is their operational differences. The operational differences must be understood in order to apply the correct handling to secure the target assets.

Access Network Sublayer

There is a direct relationship between the IoT network technology you choose and the type of connectivity topology this technology allows. Each technology was designed with a certain number of use cases in mind (what to connect, where to connect, how much data to transport at what interval and over what distance). These use cases determined the frequency band that was expected to be most suitable, the frame structure matching the expected data pattern (packet size and communication intervals), and the possible topologies that these use cases illustrate.

One key parameter determining the choice of access technology is the range between the smart object and the information collector. Figure 2-9 lists some access technologies you may encounter in the IoT world and the expected transmission distances.

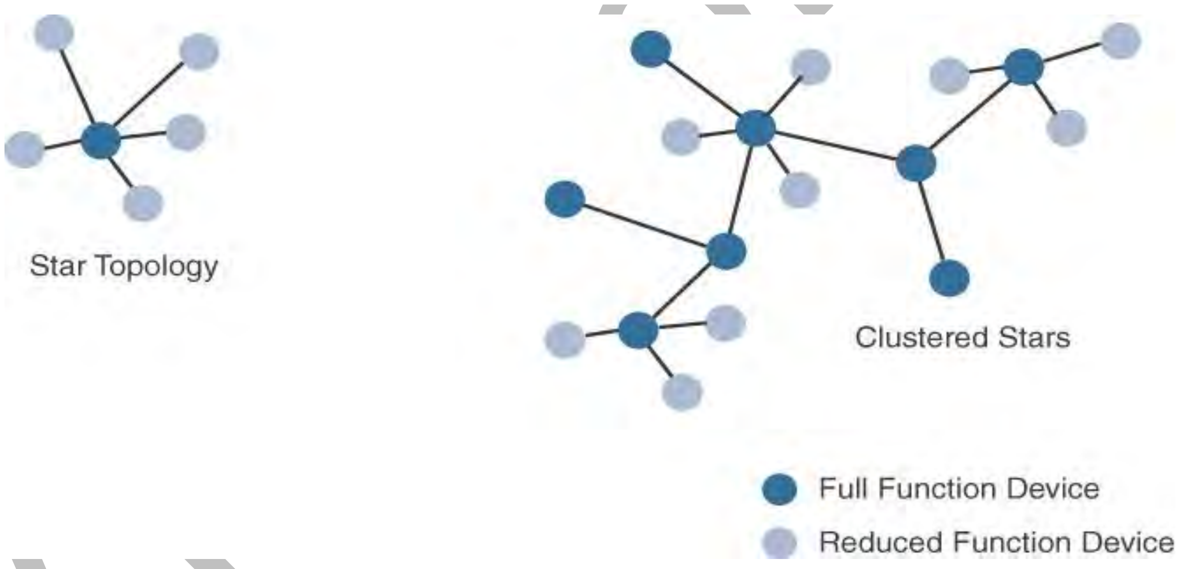


Access Technologies and Distances

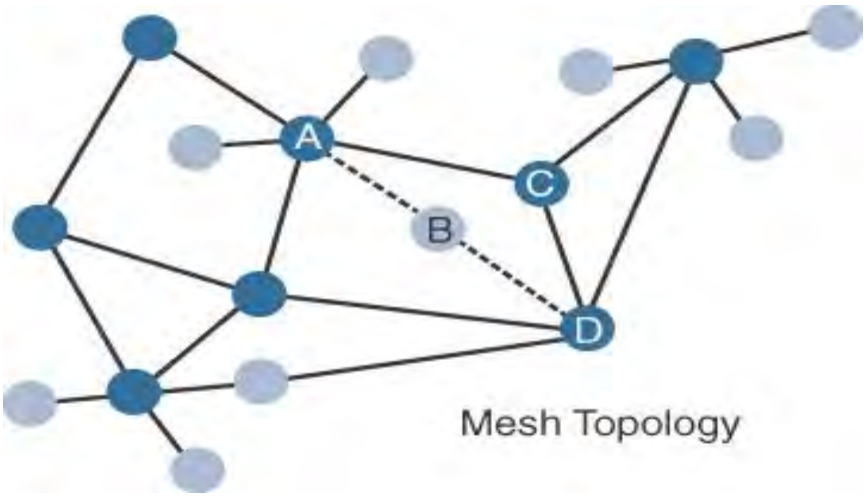
- ✓ Range estimates are grouped by category names that illustrate the environment or the vertical where data collection over that range is expected. Common groups are as follows:

- **PAN (personal area network):** Scale of a few meters. This is the personal space around a person. A common wireless technology for this scale is Bluetooth.
- **HAN (home area network):** Scale of a few tens of meters. At this scale, common wireless technologies for IoT include ZigBee and Bluetooth Low Energy (BLE).
- **NAN (neighborhood area network):** Scale of a few hundreds of meters. The term NAN is often used to refer to a group of house units from which data is collected.
- **FAN (field area network):** Scale of several tens of meters to several hundred meters. FAN typically refers to an outdoor area larger than a single group of house units. The FAN is often seen as "open space" (and therefore not secured and not controlled).
- **LAN (local area network):** Scale of up to 100 m. This term is very common in networking, and it is therefore also commonly used in the IoT space when standard networking technologies (such as Ethernet or IEEE 802.11) are used.

- ✓ Similar ranges also do not mean similar topologies. Some technologies offer flexible connectivity structure to extend communication possibilities:
  - **Point-to-point topologies**
  - **Point-to-multipoint**



Star and Clustered Star Topologies



Comparison of the main solutions from an architectural angle.

Technology	Type and Range	Architectural Characteristics
Ethernet	Wired, 100 m max	Requires a cable per sensor/sensor group; adapted to static sensor position in a stable environment; range is limited; link is very reliable
Wi-Fi (2.4 GHz, 5 GHz)	Wireless, 100 m (multipoint) to a few kilometers (P2P)	Can connect multiple clients (typically fewer than 200) to a single AP; range is limited; adapted to cases where client power is not an issue (continuous power or client battery recharged easily); large bandwidth available, but interference from other systems likely; AP needs a cable
802.11ah (HaloW, Wi-Fi in sub-1 GHz)	Wireless, 1.5 km (multipoint), 10 km (P2P)	Can connect a large number of clients (up to 6000 per AP); longer range than traditional Wi-Fi; power efficient; limited bandwidth; low adoption; and cost may be an issue
WiMAX (802.16)	Wireless, several kilometers (last mile), up to 50 km (backhaul)	Can connect a large number of clients; large bandwidth available in licensed spectrum (fee-based); reduced bandwidth in license-free spectrum (interferences from other systems likely); adoption varies on location
Cellular (for example, LTE)	Wireless, several kilometers	Can connect a large number of clients; large bandwidth available; licensed spectrum (interference-free; license-based)

Architectural Considerations for WiMAX and Cellular Technologies

Layer 3: Applications and Analytics Layer

Once connected to a network, your smart objects exchange information with other systems. As soon as your IoT network spans more than a few sensors, the power of the Internet of Things appears in the applications that make use of the information exchanged with the smart objects.

Analytics Versus Control Applications

Multiple applications can help increase the efficiency of an IoT network. Each application collects data and provides a range of functions based on analyzing the collected data. It can be difficult to compare the features offered. From an architectural standpoint, one basic classification can be as follows:

- **Analytics application:** This type of application collects data from multiple smart objects, processes the collected data, and displays information resulting from the data that was processed. The display can be about any aspect of the IoT network, from historical reports, statistics, or trends to individual system states. The important aspect is that the application processes the data to convey a view of the network that cannot be obtained from solely looking at the information displayed by a single smart object.

- **Control application:** This type of application controls the behavior of the smart object or the behavior of an object related to the smart object. For example, a pressure sensor may be connected to a pump. A control application increases the pump speed when the connected sensor detects a drop in pressure. Control applications are very useful for controlling complex aspects of an IoT network with a logic that cannot be programmed inside a single IoT object, either because the configured changes are too complex to fit into the local system or because the configured changes rely on parameters that include elements outside the IoT object.

Data Versus Network Analytics

Analytics is a general term that describes processing information to make sense of collected data. In the world of IoT, a possible classification of the analytics function is as follows:

- **Data analytics:** This type of analytics processes the data collected by smart objects and combines it to provide an intelligent view related to the IoT system. At a very basic level, a dashboard can display an alarm when a weight sensor detects that a shelf is empty in a store. In a more complex case, temperature, pressure, wind, humidity, and light levels collected from thousands of sensors may be combined and then processed to determine the likelihood of a storm and its possible path .

- **Network analytics:** Most IoT systems are built around smart objects connected to the network. A loss or degradation in connectivity is likely to affect the efficiency of the system. Such a loss can have dramatic effects. For example, open mines use wireless networks to automatically pilot dump trucks. A lasting loss of connectivity may result in an accident or degradation of operations efficiency (automated dump trucks typically stop upon connectivity loss). On a more minor scale, loss of connectivity means that data stops being fed to your data analytics platform, and the system stops making intelligent analyses of the IoT system.

Data Analytics Versus Business Benefits

Data analytics is undoubtedly a field where the value of IoT is booming. Almost any object can be connected, and multiple types of sensors can be installed on a given object. Collecting and interpreting the data generated by these devices is where the value of IoT is realized.

Smart Services

- The ability to use IoT to improve operations is often termed “smart services.” This term is generic, and in many cases the term is used but its meaning is often stretched to include one form of service or another where an additional level of intelligence is provided.

- Smart services can also be used to measure the efficiency of machines by detecting machine output, speed, or other forms of usage evaluation.

- Smart services can be integrated into an IoT system. For example, sensors can be integrated in a light bulb. A sensor can turn a light on or off based on the presence of a human in the room.

IOT DATA MANAGEMENT AND COMPUTE STACK

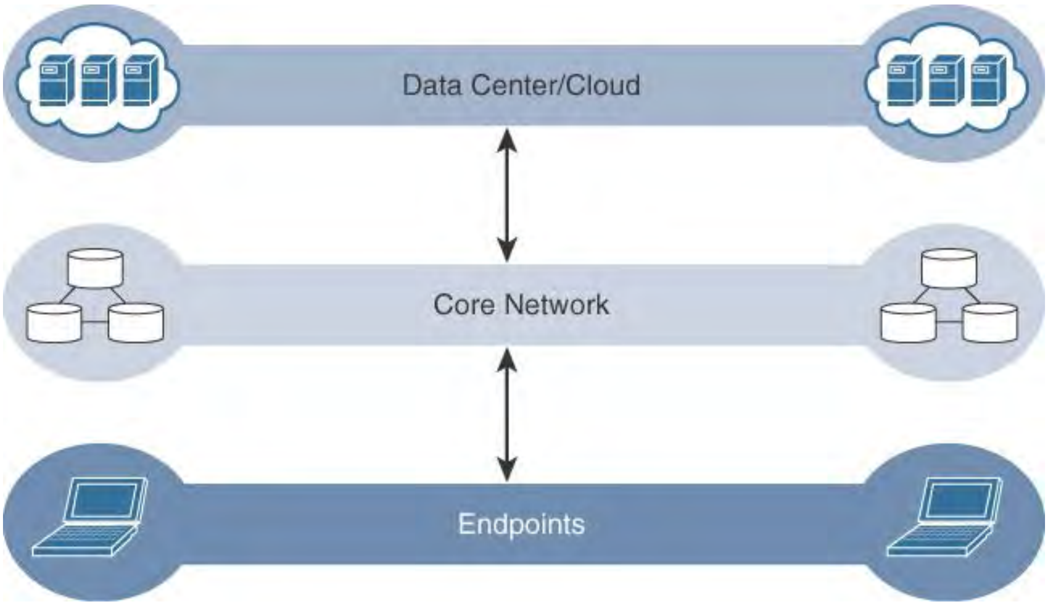
This model also has limitations. As data volume, the variety of objects connecting to the network, and the need for more efficiency increase, new requirements appear, and those requirements tend to bring the need for data analysis closer to the IoT system. These new requirements include the following:

■ **Minimizing latency:** Milliseconds matter for many types of industrial systems, such as when you are trying to prevent manufacturing line shutdowns or restore electrical service. Analyzing data close to the device that collected the data can make a difference between averting disaster and a cascading system failure.

■ **Conserving network bandwidth:** Offshore oil rigs generate 500 GB of data weekly. Commercial jets generate 10 TB for every 30 minutes of flight. It is not practical to transport vast amounts of data from thousands or hundreds of thousands of edge devices to the cloud. Nor is it necessary because many critical analyses do not require cloud-scale processing and storage.

■ **Increasing local efficiency:** Collecting and securing data across a wide geographic area with different environmental conditions may not be useful. The environmental conditions in one area will trigger a local response independent from the conditions of another site hundreds of miles away. Analyzing both areas in the same cloud system may not be necessary for immediate efficiency.

.



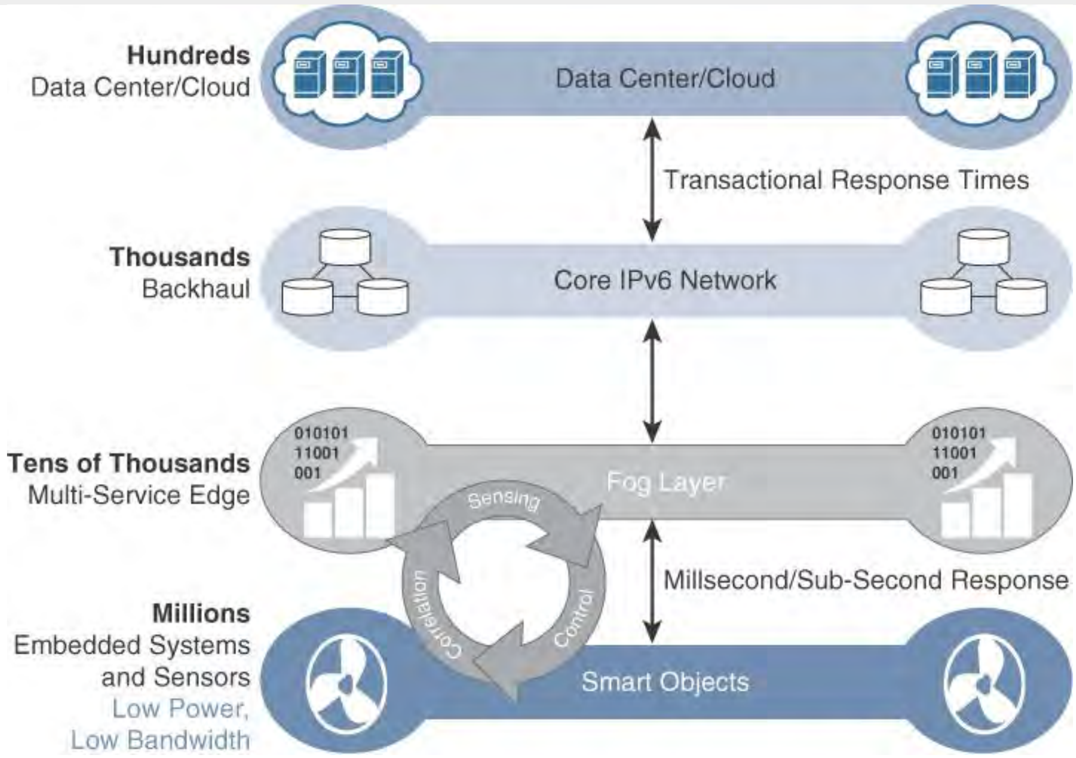
The Traditional IT Cloud Computing Model

IoT systems function differently. Several data-related problems need to be addressed:

- Bandwidth in last-mile IoT networks is very limited. When dealing with thousands/millions of devices, available bandwidth may be on order of tens of Kbps per device or even less.
- Latency can be very high. Instead of dealing with latency in the milliseconds range, large IoT networks often introduce latency of hundreds to thousands of milliseconds.
- Network backhaul from the gateway can be unreliable and often depends on 3G/LTE or even satellite links. Backhaul links can also be expensive if a per-byte data usage model is necessary.
- The volume of data transmitted over the backhaul can be high, and much of the data may not really be that interesting (such as simple polling messages).
- Big data is getting bigger. The concept of storing and analyzing all sensor data in the cloud is impractical. The sheer volume of data generated makes real-time analysis and response to the data almost impossible.

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.



The IoT Data Management and Compute Stack with Fog Computing

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 applications are as diverse as the Internet of Things itself. What they have in common is data reduction—monitoring or analyzing real-time data from network-connected things and then initiating an action, such as locking a door, changing equipment settings, applying the brakes on a train, zooming a video camera, opening a valve in response to a pressure reading, creating a bar chart, or sending an alert to a technician to make a preventive repair.

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

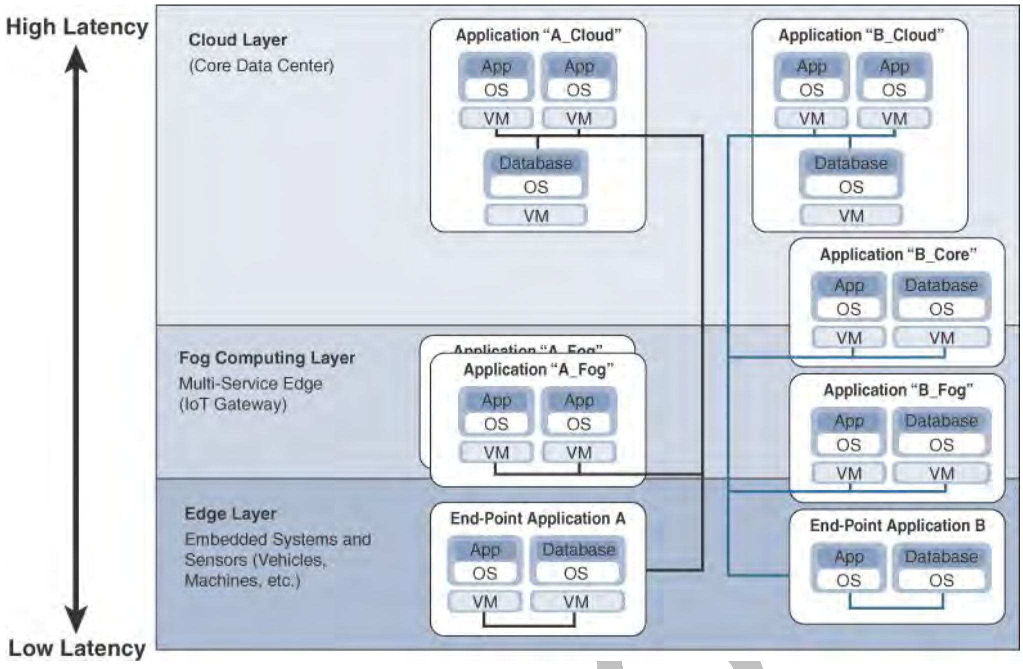
Fog computing solutions are being adopted by many industries, and efforts to develop distributed applications and analytics tools are being introduced at an accelerating pace. The natural place for a fog node is in the network device that sits closest to the IoT endpoints, and these nodes are typically spread throughout an IoT network

Note

Edge computing is also sometimes called “mist” computing. If clouds exist in the sky, and fog sits near the ground, then mist is what actually sits on the ground. Thus, the concept of mist is to extend fog to the furthest point possible, right into the IoT endpoint device itself.

The Hierarchy of Edge, Fog, and Cloud

It is important to stress that edge or fog computing in no way replaces the cloud. Rather, they complement each other, and many use cases actually require strong cooperation between layers. In the same way that lower courts do not replace the supreme court of a country, edge and fog computing layers simply act as a first line of defense for filtering, analyzing, and otherwise managing data endpoints. This saves the cloud from being queried by each and every node for each event.



Distributed Compute and Data Management Across an IoT System

From an architectural standpoint, fog nodes closest to the network edge receive the data from IoT devices. The fog IoT application then directs different types of data to the optimal place for analysis:

- The most time-sensitive data is analyzed on the edge or fog node closest to the things generating the data.
- Data that can wait seconds or minutes for action is passed along to an aggregation node for analysis and action.
- Data that is less time sensitive is sent to the cloud for historical analysis, big data analytics, and long-term storage. For example, each of thousands or hundreds of thousands of fog nodes might send periodic summaries of data to the cloud for historical analysis and storage.

In summary, when architecting an IoT network, you should consider the amount of data to be analyzed and the time sensitivity of this data. Understanding these factors will help you decide whether cloud computing is enough or whether edge or fog computing would improve your system efficiency. Fog computing accelerates awareness and response to events by eliminating a round trip to the cloud for analysis. It avoids the need for costly bandwidth additions by offloading gigabytes of network traffic from the core network. It also protects sensitive IoT data by analyzing it inside company walls.

MODULE-2

SMART OBJECTS

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.

Some of the fundamental building blocks of IoT networks are

- Sensors
- Actuators
- Smart Objects

Sensors:

- A sensor does exactly as its name indicates: It senses.
- 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.
- Sensors are not limited to human-like sensory data.
- They are able to provide an extremely wide spectrum of rich and diverse measurement data with far greater precision than human senses.
- Sensors provide superhuman sensory capabilities.
- Sensors can be readily embedded in any physical objects that are easily connected to the Internet by wired or wireless networks, they can interpret their environment and make intelligent decisions.

Sensors have been grouped into different categories

- **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).

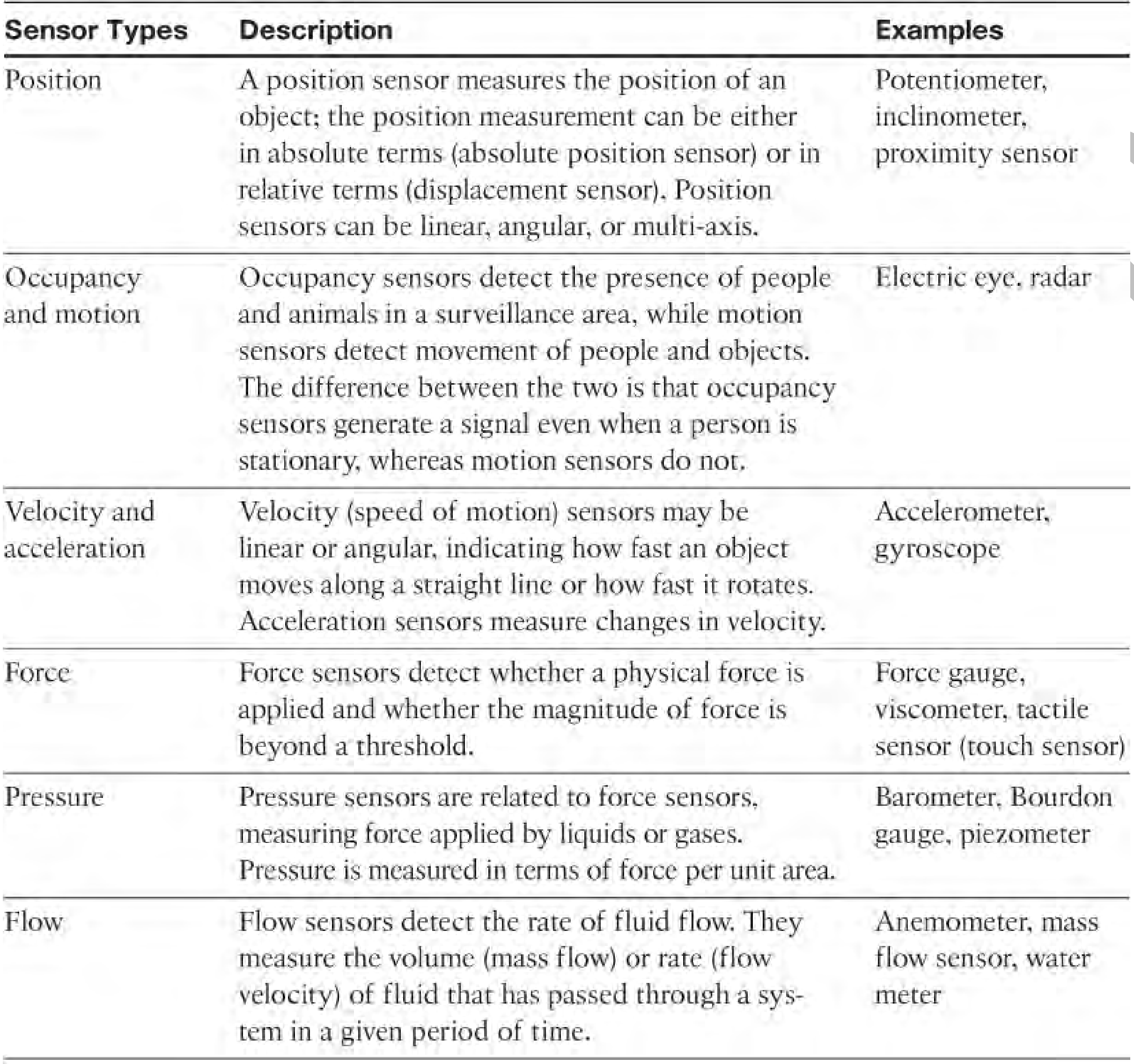
- **Absolute or relative:** Sensors can be categorized based on whether they measure on an absolute scale (absolute) or based on a difference with a fixed or variable reference value (relative).

- **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.

The physical phenomenon a sensor is measuring is shown in Table-2.1



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

- A fascinating use case to highlight the power of sensors and IoT is in the area of precision agriculture (sometimes referred to as smart farming), which uses a variety of technical advances 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.

Different types of sensors in a smart phone is shown in figure 2.1

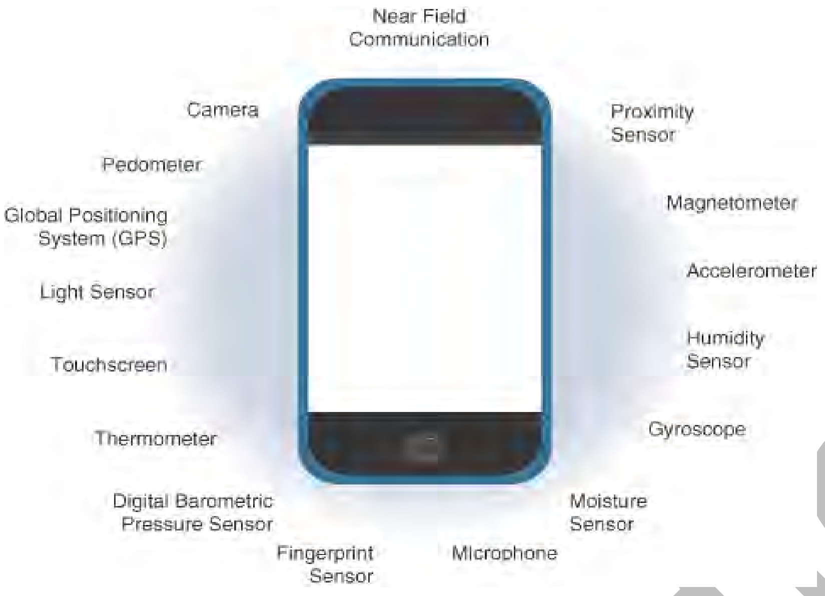


Figure 2.1: Sensors in a smart phone

Actuators:

- Actuators are natural complements to sensors.
- Figure 2.2 demonstrates the symmetry and complementary nature of these two types of devices.
- 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.

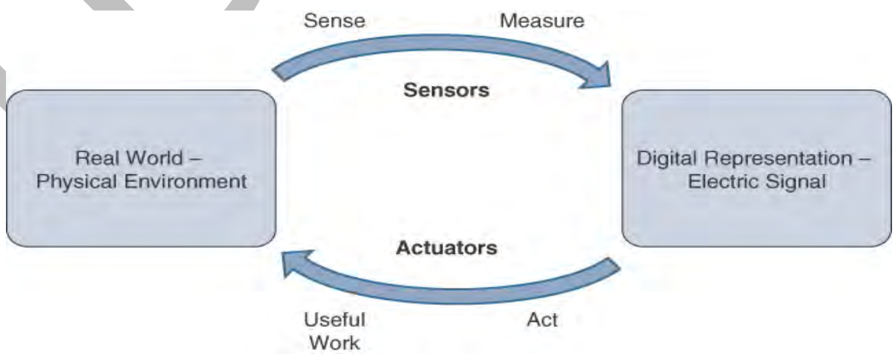
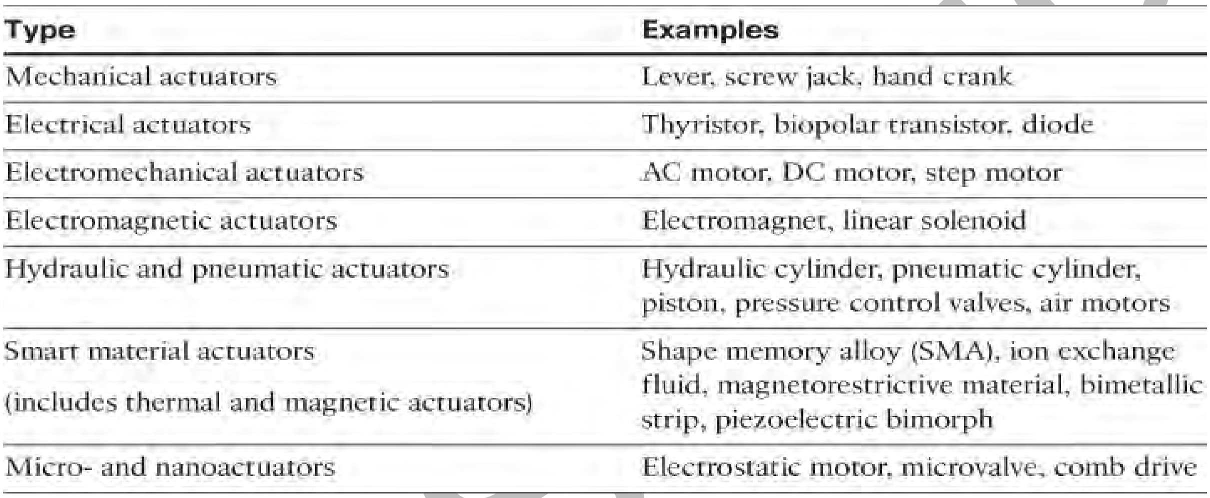

Sense
Measure
Sensors
Real World – Physical Environment
Digital Representation – Electric Signal
Actuators
Useful Work
Act

Figure 2.2 : How Sensors and Actuators Interact with the Physical World

Much like sensors, actuators also vary greatly in function, size, design, and so on. Some common ways that they can be classified include the following:

- **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.

Different types of Actuators are presented in Table -2.2



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 -2.2: Actuator Classification by Energy Type

Micro-Electro-Mechanical Systems (MEMS)

- 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.
- The combination of tiny size, low cost, and the ability to mass produce makes MEMS an attractive option for a huge number of IoT applications.

Ex: Inkjet printers use micropump MEMS. Smart phones also use MEMS technologies for things like accelerometers and gyroscopes

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. A *smart object*, is a device that has, at a minimum, 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.
- **Sensor(s) and /or actuator(s):** A smart object is capable of interacting with the physical world through sensors and actuators. A smart object does not need to contain

both sensors and actuators. In fact, a smart object can contain one or multiple sensors and/or actuators, depending upon the application.

- **Communication Device:** The communication unit is responsible for connecting a smart object with other smart objects and the outside world (via the network). Communication devices for smart objects can be either wired or wireless.
- **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.

Trends in Smart Objects:

The broad generalizations and trends impacting IoT are

- **Size is decreasing:** Some smart objects are so small they are not even visible to the naked eye. This reduced size makes smart objects easier to embed in everyday objects.
- **Power consumption is decreasing:** The different hardware components of a smart object continually consume less power. Some battery-powered sensors last 10 or more years without battery replacement.
- **Processing power is increasing:** Processors are continually getting more powerful and smaller.
- **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), as the name suggests, is a network of sensors that sense and measure their environment and/or actuators that act on their environment.
- The sensors and/or actuators in a SANET are capable of communicating and cooperating in a productive manner.
- SANETs offer highly coordinated sensing and actuation capabilities.
- 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.

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 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

These limitations greatly influence how WSNs are designed, deployed, and utilized. Figure 2.3 below shows an example of such a data aggregation function in a WSN where temperature readings from a logical grouping of temperature sensors are aggregated as an average temperature reading.

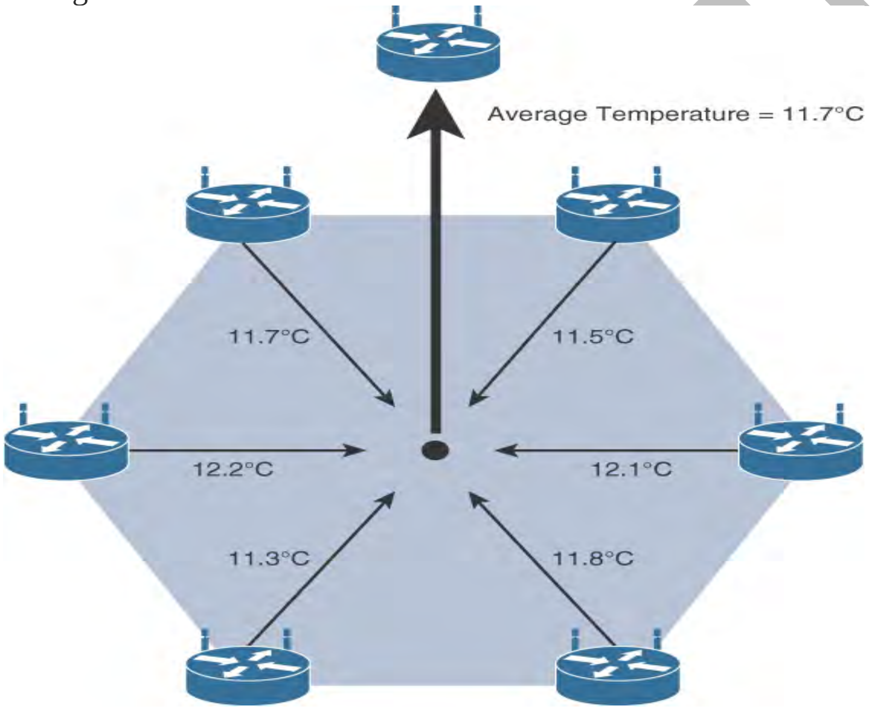


Figure 2.3 Data Aggregation in Wireless Sensor Networks

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. 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.

Communication Protocols for Wireless Sensor Networks:

- Any communication protocol must be able to scale to a large number of nodes.
- Likewise, when selecting a communication protocol, you must carefully take into account the requirements of the specific application.

- Also consider any trade-offs the communication protocol offers between power consumption, maximum transmission speed, range, tolerance for packet loss, topology optimization, security, and so on.
- Sensors often produce large amounts of sensing and measurement data that needs to be processed.
- This data can be processed locally by the nodes of a WSN or across zero or more hierarchical levels in IoT networks.
- IoT is one of those rare technologies that impacts all verticals and industries, which means standardization of 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

The characteristics and attributes considered when selecting and dealing with connecting smart objects are

1)Range: It defines how far does the signal need to be propagated? That is, what will be the area of coverage for a selected wireless technology? The below figure 2.4 shows the range considered

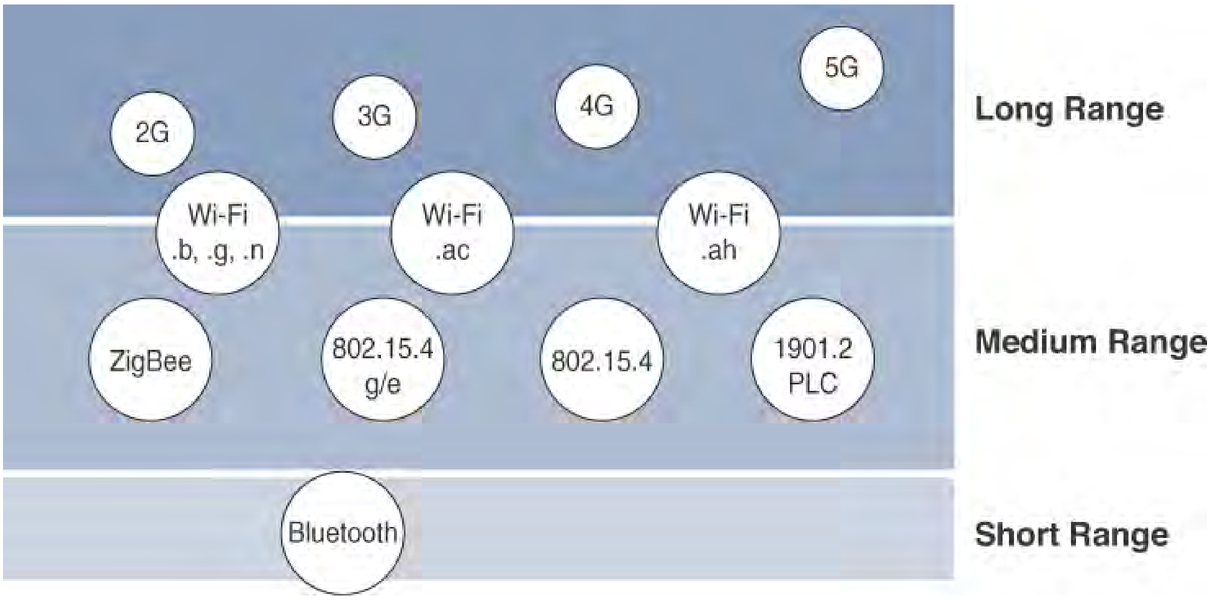


Figure 2.4 ***Wireless Access Landscape***

- **Short Range:**
  - The classical wired example is a serial cable.
  - Wireless short-range technologies are often considered as an alternative to a serial cable, supporting tens of meters of maximum distance between two devices.
  - Examples of short-range wireless technologies are IEEE 802.15.1 Bluetooth and IEEE 802.15.7 Visible Light Communications (VLC).
  - These short-range communication methods are found in only a minority of IoT installations.
- **Medium Range:**
  - In the range of tens to hundreds of meters, many specifications and implementations are available.
  - The maximum distance is 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) may also be classified as medium range, depending on their physical media characteristics.
- **Long Range**:
  - Distances greater than 1 mile between two devices require long-range technologies. Wireless examples are cellular (2G, 3G, 4G) and some applications of outdoor IEEE 802.11 Wi-Fi and Low-Power Wide-Area (LPWA) technologies.
  - LPWA communications have the ability to communicate over a large area without consuming much power.
  - These technologies are therefore ideal for battery-powered IoT sensors.
  - Found mainly in industrial networks, IEEE 802.3 over optical fiber and IEEE 1901 Broadband Power Line Communications are classified as long range but are not really considered IoT access technologies.

2)Frequency Bands:

- Radio spectrum is regulated by countries and/or organizations, such as the International Telecommunication Union (ITU) and the Federal Communications Commission (FCC).
- These groups define the regulations and transmission requirements for various frequency bands.
- For example, portions of the spectrum are allocated to types of telecommunications such as radio, television, military, and so on.
- 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.
- The ITU has also defined unlicensed spectrum for the industrial, scientific, and medical (ISM) portions of the radio bands.
- These frequencies are used in many communications technologies for short-range devices (SRDs).
- Unlicensed means that no guarantees or protections are offered in the ISM bands for device communications.
- For IoT access, these are the most well-known ISM bands:
  - 2.4 GHz band as used by IEEE 802.11b/g/n Wi-Fi
  - IEEE 802.15.1 Bluetooth
  - IEEE 802.15.4 WPAN
- Unlicensed spectrum is usually simpler to deploy than licensed because it does not require a service provider.
- 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.
- The most well-known ranges are centered on 169 MHz, 433 MHz, 868 MHz, and 915 MHz.
- The 868 MHz band is applicable to IoT access technologies such as IEEE 802.15.4 and 802.15.4g, 802.11ah, and LoRaWAN.

Power Consumption:

- Battery-powered nodes bring much more flexibility to IoT devices.
- These nodes are often classified by the required lifetimes of their batteries.
- 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 has led to the evolution of a new wireless environment known as Low-Power Wide-Area (LPWA).

Topology

- Among the access technologies available for connecting IoT devices, three main topology schemes are dominant: star, mesh, and peer-to-peer.
- For long-range and short-range technologies, a star topology is prevalent, as seen with cellular, LPWA, and Bluetooth networks.
- Star topologies utilize a single central base station or controller to allow communications with endpoints.
- For medium-range technologies, a star, peer-to-peer, or mesh topology is common.
- Peer-to-peer topologies allow any device to communicate with any other device as long as they are in range of each other.
- Peer-to-peer topologies enable more complex formations, such as a mesh networking topology.

The figure 2.5 below represents the various topology.

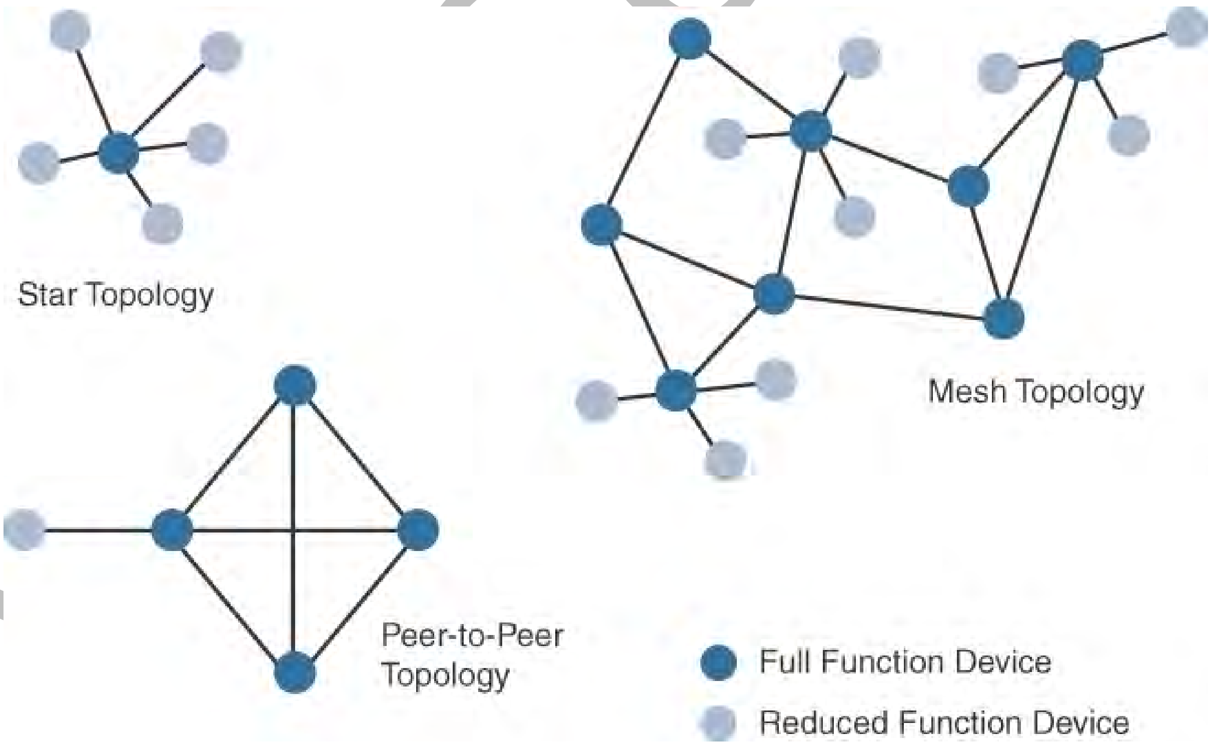


Figure 2.5 ***Star, Peer-to-Peer, and Mesh Topologies***

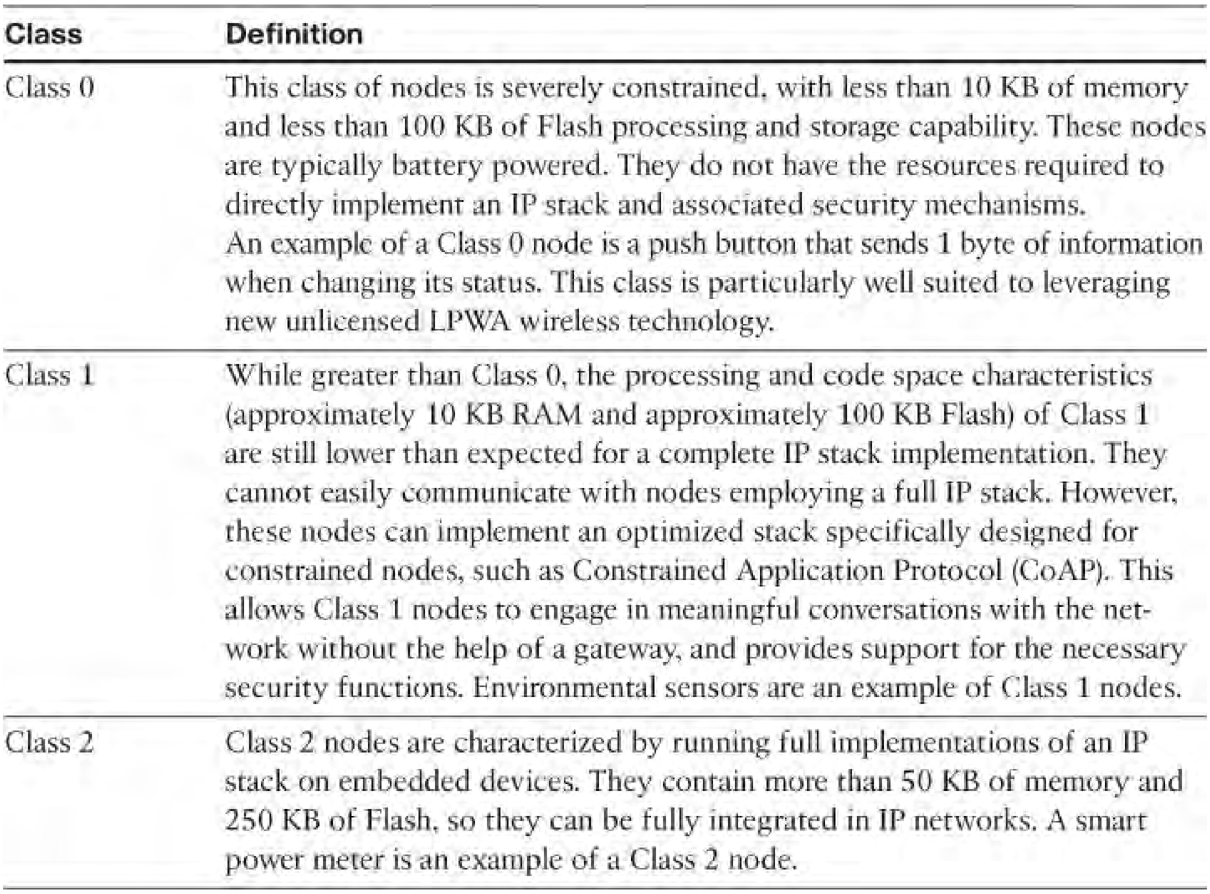
- The disadvantage of sub-GHz frequency bands is their lower rate of data delivery compared to higher frequencies.
- Example: Indoor Wi-Fi deployments are mostly a set of nodes forming a star topology around their access points (APs).

- Outdoor Wi-Fi may consist of a mesh topology for the backbone of APs, with nodes connecting to the APs in a star topology.
- IEEE 802.15.4 and 802.15.4g and even wired IEEE 1901.2a PLC are generally deployed as a mesh topology.

- 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.

Constrained Devices:

Constrained nodes have limited resources that impact their networking feature set and capabilities. Constrained nodes can broken down into different classes such as shown in Table 2.3:



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 2.3 Classes of Constrained Nodes, as Defined by RFC 7228

- Constrained-node networks are often referred to as low-power and lossy networks (LLNs).
- 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 must be evaluated in the context of the following characteristics for use-case applicability: data rate and throughput, latency and determinism, and overhead and payload.
- The IoT access technologies developed for constrained nodes are optimized for low power consumption, but they are also limited in terms of data rate, which depends on the selected frequency band, and throughput.

- The data rates available from IoT access technologies range from 100 bps with protocols such as Sigfox to tens of megabits per second with technologies such as LTE and IEEE 802.11ac.
- Short-range technologies can also provide medium to high data rates that have enough throughput to connect a few endpoints.
- On constrained networks, latency may range from a few milliseconds to seconds, and applications and protocol stacks must cope with these wide-ranging values.
- For example, UDP at the transport layer is strongly recommended for IP endpoints communicating over LLNs
- When considering constrained access network technologies, it is important to review the MAC payload size characteristics required by applications.
- In addition, you should be aware of any requirements for IP.
- The minimum IPv6 MTU size is expected to be 1280 bytes. Therefore, the fragmentation of the IPv6 payload has to be considered by link layer access protocols with smaller MTUs.
- Example: The payload size for IEEE 802.15.4 is 127 bytes and requires an IPv6 payload with a minimum MTU of 1280 bytes to be fragmented.
- On the other hand, IEEE 802.15.4g enables payloads up to 2048 bytes, easing the support of the IPv6 minimum MTU of 1280 bytes.

IoT Access Technologies

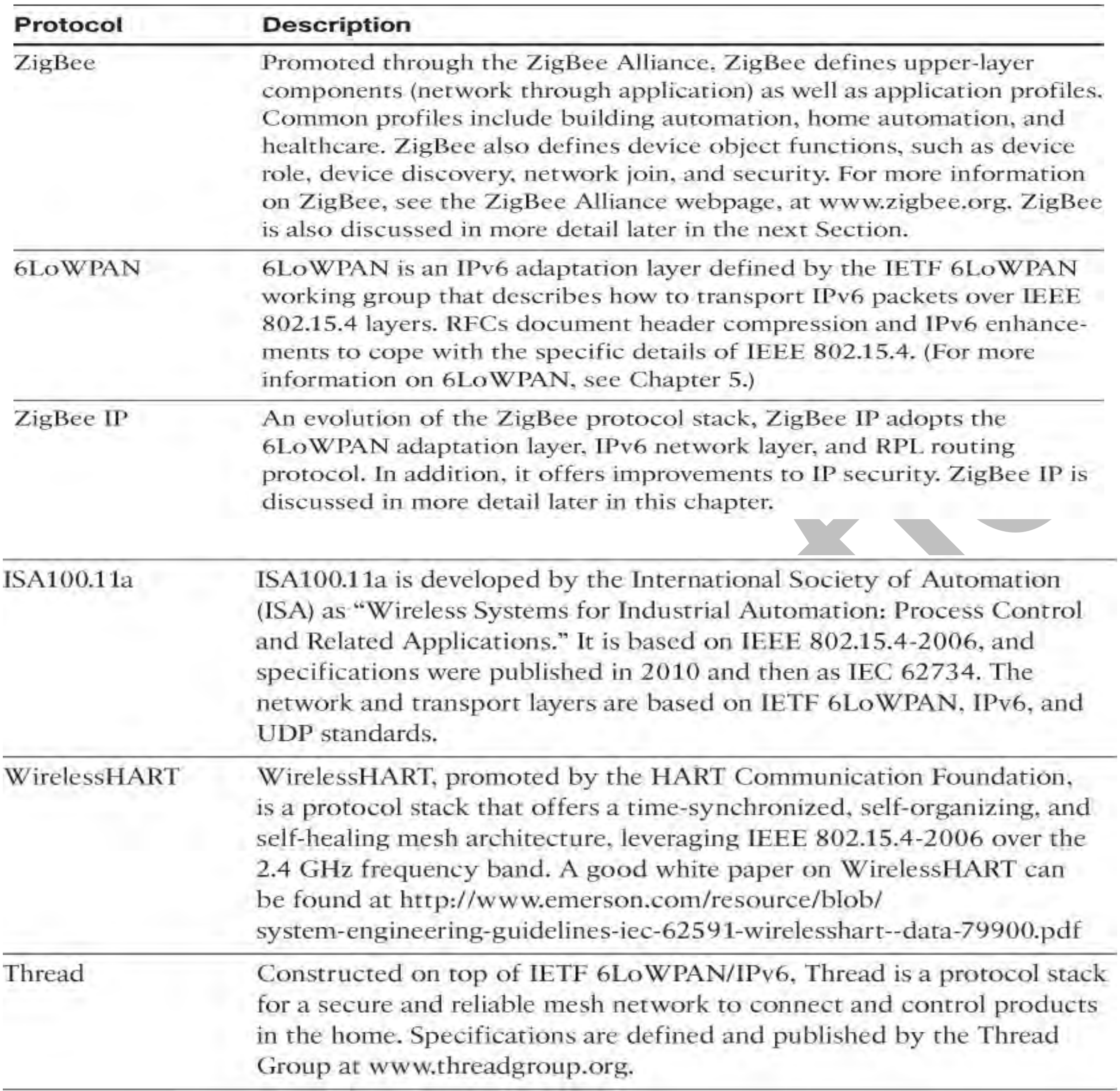
IEEE 802.15.4:

- IEEE 802.15.4 is a wireless access technology for low-cost and low-data-rate devices that are powered or run on batteries.
- This access technology enables easy installation using a compact protocol stack while remaining both simple and flexible.
- IEEE 802.15.4 is commonly found in the following types of deployments:
  - Home and building automation
  - Automotive networks
  - Industrial wireless sensor networks
  - Interactive toys and remote controls
- Criticisms of IEEE 802.15.4 often focus on its MAC reliability, unbounded latency, and susceptibility to interference and multipath fading.
- Interference and multipath fading occur with IEEE 802.15.4 because it lacks a frequency-hopping technique.

❖ Standardization and Alliances

- IEEE 802.15.4 or IEEE 802.15 Task Group 4 defines low-data-rate PHY and MAC layer specifications for wireless personal area networks (WPAN).
- The IEEE 802.15.4 PHY and MAC layers are the foundations for several networking protocol stacks.
- These protocol stacks make use of 802.15.4 at the physical and link layer levels, but the upper layers are different.

Some of the most well-known protocol stacks based on 802.15.4 are as shown in Table 2.4



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 2.4 Protocol Stacks Utilizing IEEE 802.15.4

- **ZigBee:**
  - It is an IoT solution for interconnecting smart objects.
  - ZigBee solutions are aimed at smart objects and sensors that have low bandwidth and low power needs.
  - The Zigbee specification has undergone several revisions.
  - In the 2006 revision, sets of commands and message types were introduced, and increased in number in the 2007 (called Zigbee pro) iteration, to achieve different functions for a device, such as metering, temperature, or lighting control.
  - These sets of commands and message types are called clusters.
  - Ultimately, these clusters from different functional domains or libraries form the building blocks of Zigbee application profiles.
  - Vendors implementing pre-defined Zigbee application profiles like Home Automation or Smart Energy can ensure interoperability between their products.
  - The main areas where ZigBee is the most well-known include automation for commercial, retail, and home applications and smart energy.
  - In the industrial and commercial automation space, ZigBee-based devices can handle various functions, from measuring temperature and humidity to tracking assets.

- For home automation, ZigBee can control lighting, thermostats, and security functions.
- ZigBee Smart Energy brings together a variety of interoperable products, such as smart meters, that can monitor and control the use and delivery of utilities, such as electricity and water.
- The traditional ZigBee stack is illustrated in the below figure 2.6.

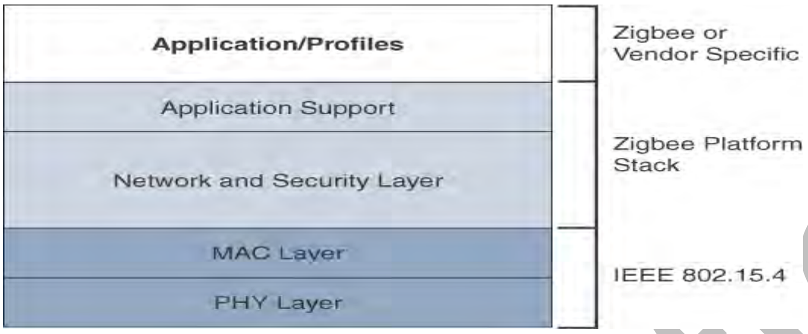


Figure 2.6 High-Level ZigBee Protocol Stack

- 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. The network layer is also responsible for forming the appropriate topology, which is often a mesh but could be a star or tree as well. From a security perspective, ZigBee utilizes 802.15.4 for security at the MAC layer, using the Advanced Encryption Standard (AES) with a 128-bit key and also provides security at the network and application layers.
- ZigBee is one of the most well-known protocols built on an IEEE 802.15.4 foundation. On top of the 802.15.4 PHY and MAC layers, ZigBee specifies its own network and security layer and application profiles.

➢ **ZigBee IP**

- ZigBee IP was created to embrace the open standards coming from the IETF's work on LLNs, such as IPv6, 6LoWPAN, and RPL They provide for low-bandwidth, low-power, and cost-effective communications when connecting smart objects.
- ZigBee IP is a critical part of the Smart Energy (SE) Profile 2.0 specification from the ZigBee Alliance. SE 2.0 is aimed at smart metering and residential energy management systems. Any other applications that need a standards-based IoT stack can utilize Zigbee IP. The ZigBee IP stack is shown in below figure 2.7.

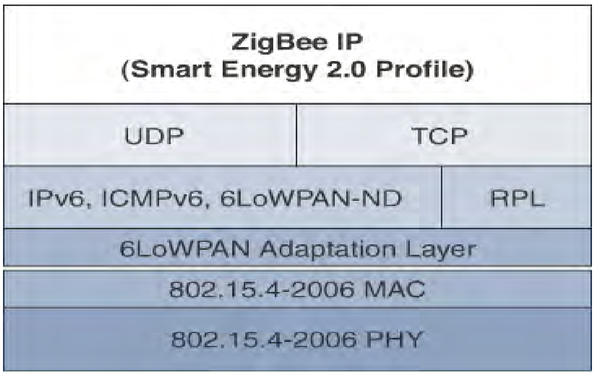


Figure 2.7 ZigBee IP Protocol Stack

- ZigBee IP supports 6LoWPAN as an adaptation layer.
- ZigBee IP requires the support of 6LoWPAN's fragmentation and header compression schemes
- At the network layer, all ZigBee IP nodes support IPv6, ICMPv6, and 6LoWPAN Neighbor Discovery (ND), and utilize RPL for the routing of packets across the mesh network.

❖ 802.15.4 Physical and MAC 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.
- 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
- 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.
  - **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.

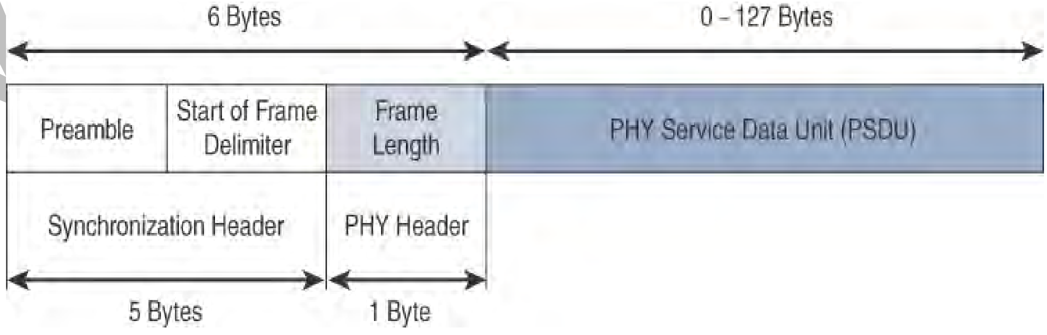


Figure 2.8 IEEE 802.15.4 PHY Format

- The PHY Header portion of the PHY frame is shown in Figure 2.8 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.
- 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
    - 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
- Each of these four 802.15.4 MAC frame types follows the frame format shown in Figure 2.9. In Figure 2.9, notice that the MAC frame is carried as the PHY payload.
- The 802.15.4 MAC frame can be broken down into the MAC Header, MAC Payload, and MAC Footer fields.

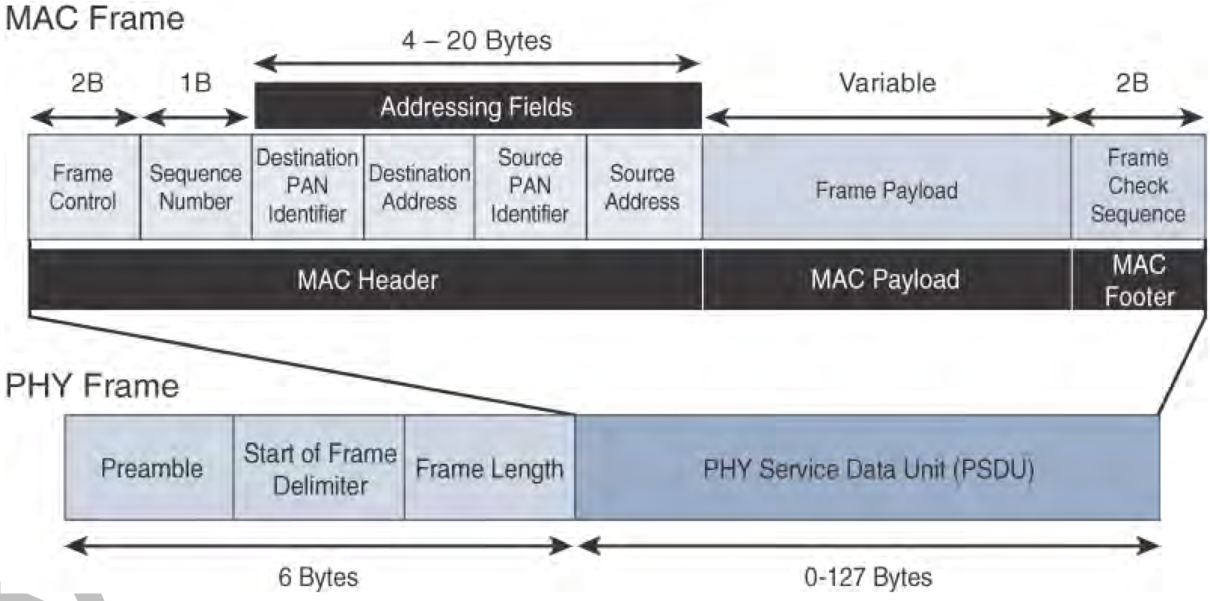


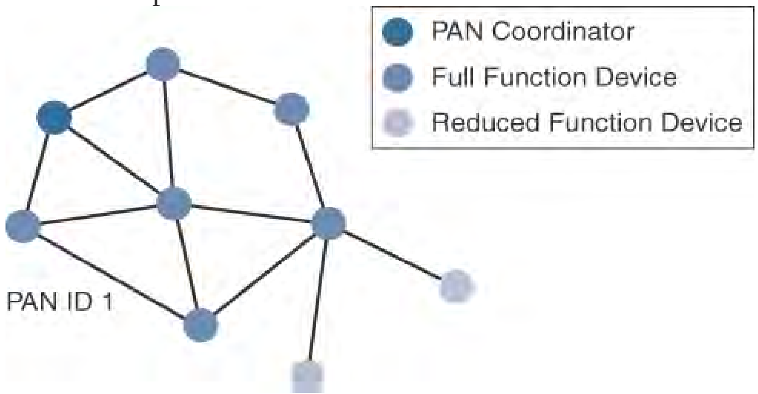
Figure 2.9 IEEE 802.15.4 MAC Format

- 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.
- 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

- 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.
- 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 2.10 shows an example of an 802.15.4 mesh network with a PAN ID of 1.



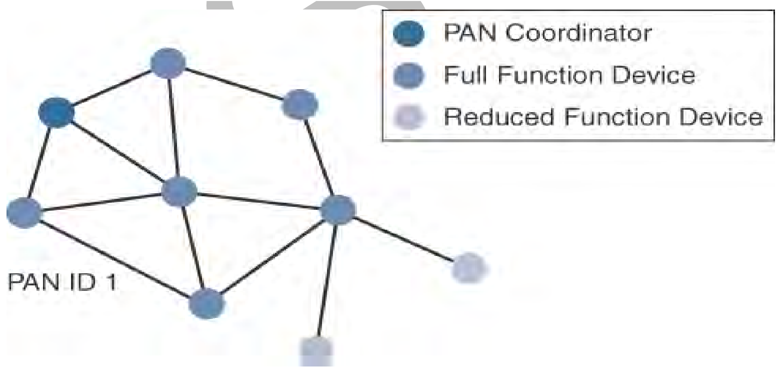


Figure 2.10: 802.15.4 Sample Mesh Network Topology

- FFD (full-function devices) acts as a PAN coordinator to deliver services that allow other devices to associate and form a cell or PAN.
- FFD devices can communicate with any other devices, whereas RFD devices can communicate only with FFD devices.

❖ 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.

- The figure 2.11 below shows the IEEE 802.15.4 frame format at a high level, with the Security Enabled bit set and the Auxiliary Security Header field present.

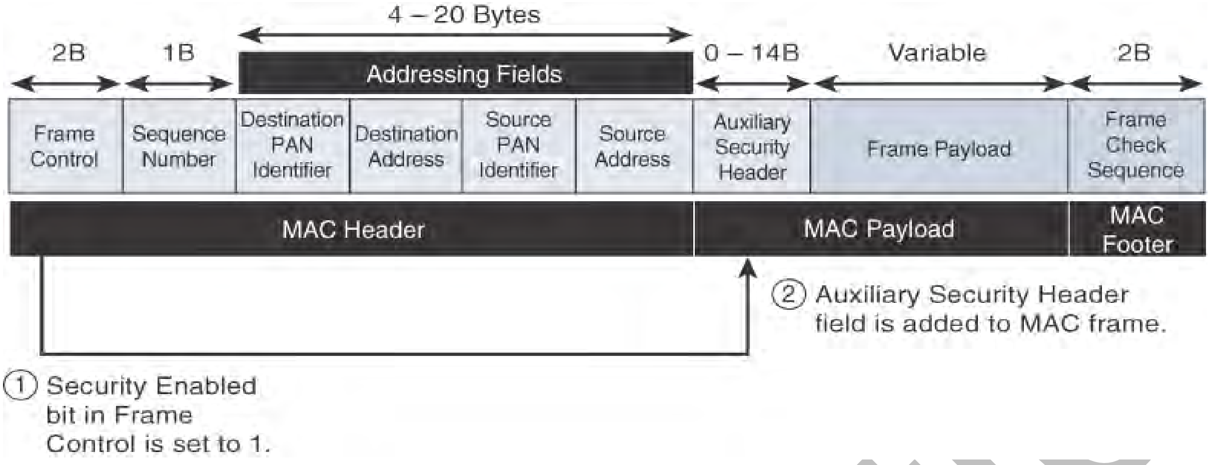


Figure 2.11:Frame Format with the Auxiliary Security Header Field for 802.15.4-2006 and Later Versions

IEEE 802.15.4g and 802.15.4e

- IEEE 802.15.4g-2012 is also an amendment to the IEEE 802.15.4-2011 standard, and just like 802.15.4e-2012, it has been fully integrated into the core IEEE 802.15.4-2015 specification.
- 802.15.4g seeks to optimize large outdoor wireless mesh networks for field area networks (FANs)
- This technology applies to IoT use cases such as the following:
  - 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.

❖ Standardization and Alliances:

- 802.15.4g-2012 and 802.15.4e-2012 are simply amendments to IEEE 802.15.4-2011.
- Same IEEE 802.15 Task Group 4 standards body authors, maintains, and integrates them into the next release of the core specification.
- To guarantee interoperability, the Wi-SUN Alliance was formed.
- It defines communication profiles for smart utility and related networks.
- These profiles are based on open standards, such as 802.15.4g-2012, 802.15.4e-2012, IPv6, 6LoWPAN, and UDP for the FAN profile.
- The Wi-SUN Alliance performs the same function as the Wi-Fi Alliance and WiMAX Forum

❖ Physical Layer:

- In IEEE 802.15.4g-2012, the original IEEE 802.15.4 maximum PSDU or 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.
- For example, the default IPv6 MTU setting is 1280 bytes. Fragmentation is no longer necessary at Layer 2 when IPv6 packets are transmitted over IEEE 802.15.4g MAC frames. Also, the error protection was improved in IEEE 802.15.4g by evolving the CRC from 16 to 32 bits.
- The SUN PHY, as described in IEEE 802.15.4g-2012, supports multiple data rates in bands ranging from 169 MHz to 2.4 GHz.\
- Within these bands, data must be modulated onto the frequency using at least one of the following PHY mechanisms to be IEEE 802.15.4g compliant:
  - **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 (MR-O-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.

❖ **MAC Layer:**

The following are some of the main enhancements to the MAC layer proposed by IEEE 802.15.4e-2012:

- **Time-Slotted Channel Hopping (TSCH):**
  - TSCH is an IEEE 802.15.4e-2012 MAC operation mode that works to guarantee media access and channel diversity.
  - 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, especially for industrial use cases.
- **Information elements:**
  - 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 for the 6TiSCH architecture.
- **Enhanced beacons (EBs):**
  - EBs extend the flexibility of IEEE 802.15.4 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):**
  - Like enhanced beacons, an 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:**
  - The Enhanced Acknowledgement frame 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.
- The 802.15.4e-2012 MAC amendment is quite often paired with the 802.15.4g-2012 PHY. Figure 2.11 details this format

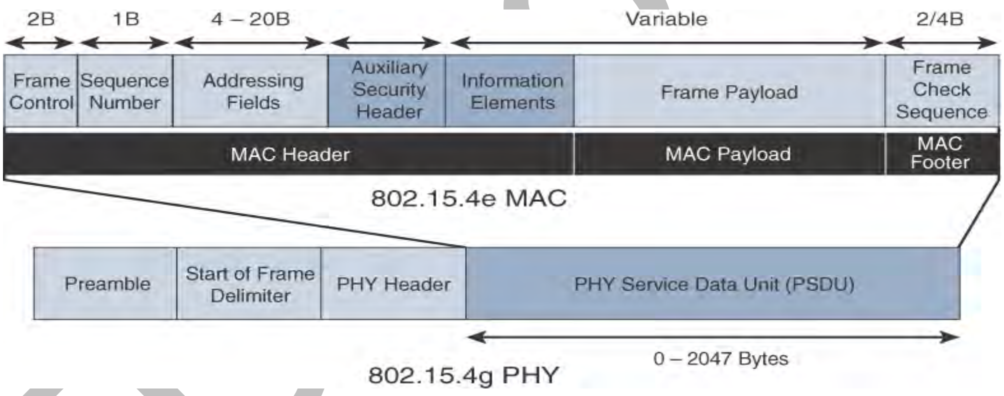


Figure 2.11: IEEE 802.15.4g/e MAC Frame Format

❖ **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:**

- Both IEEE 802.15.4g and 802.15.4e inherit their security attributes from the IEEE 802.15.4-2006 specification.
- Therefore, 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 2.12 shows a high-level overview of the security associated with an IEEE 802.15.4e MAC frame.

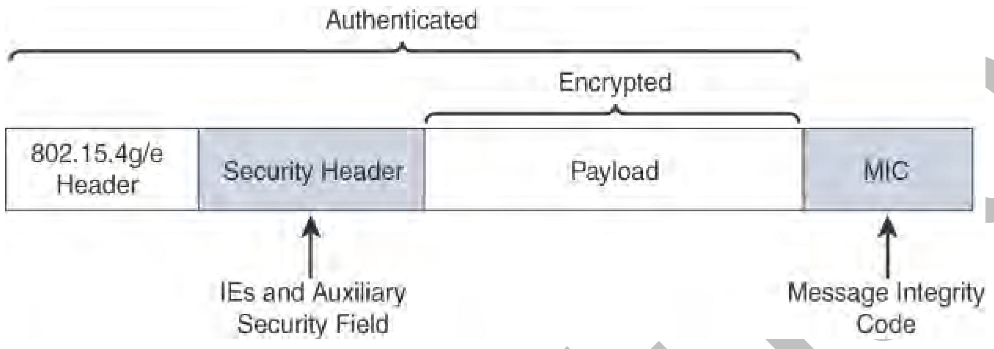


Figure 2.12: IEEE 802.15.4g/e MAC Layer Security

- The MIC is a unique value that is calculated based on the frame contents.
- The Security Header field denoted in Figure 2.12 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, such as the IEEE 802.15.9 Key Management Protocol (KMP) specification.
- KMP provides a means for establishing keys for robust datagram security. Without key management support, weak keys are often the result, leaving the security system open to attack.

IEEE 1901.2a

- IEEE 1901.2a-2013 is a wired technology that is an update to the original IEEE 1901.2 specification
- 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.
- NB-PLC is often found in use cases such as the following:
- 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 IEEE 1901.2 working group published the IEEE 1901.2a specification in November 2013.
- IEEE 1901.2 working group only looked at standardizing the NB-PLC PHY and MAC layers independently of the upper layers.
- Using the 802.15.4e Information Element fields eases support for IEEE 802.15.9 key management.
- 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.

❖ Physical Layer

- NB-PLC is defined for frequency bands from 3 to 500 kHz.
- Figure 2.13 shows the various frequency bands for NB-PLC. The most well-known bands are regulated by CENELEC (Comité Européen de Normalisation Électro technique) and the FCC (Federal Communications Commission).
- The two ARIB frequency bands are ARIB 1, 37.5–117.1875 kHz, and ARIB 2, 154.6875–403.125 kHz.

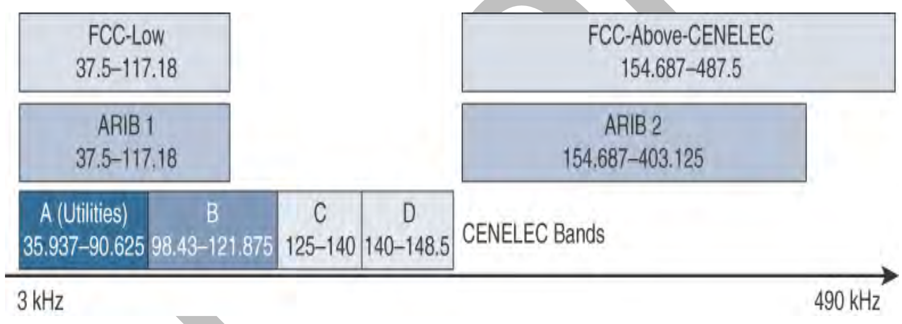


Figure 2.13 NB-PLC Frequency Bands

- With IEEE 1901.2a, the data throughput rate has the ability to dynamically change, depending on the modulation type and tone map.
- One major difference between IEEE 802.15.4g/e and 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.
- IEEE 802.15.4g/e doesn’t really define a multi-PHY management algorithm.
- The PHY payload size can change dynamically, based on channel conditions in IEEE 1901.2a.
- Therefore, MAC sublayer segmentation is implemented. 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, which enables key features to be supported.
- One of the key components brought from 802.15.4e to IEEE 1901.2a is information elements.
- Figure 2.14 provides a overview of the general MAC frame format for IEEE 1901.2.

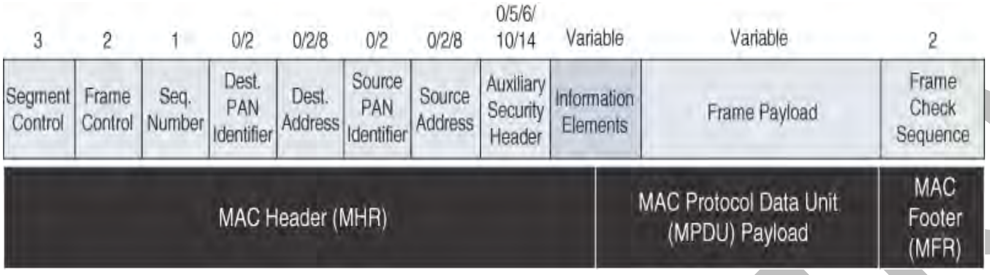


Figure 2.14: General MAC Frame Format for IEEE 1901.2

- IEEE 1901.2 has a Segment Control field.
- This 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:**

- Use cases and deployment topologies for IEEE 1901.2a are tied to the physical power lines.
- As with wireless technologies, signal propagation is limited by factors such as noise, interference, distortion, and attenuation.
- These factors become more prevalent with distance, so most 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.

❖ **Security:**

- IEEE 1901.2a security offers similar features to IEEE 802.15.4g. Encryption and authentication are performed using AES. I
- In addition, 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 ciphered payload and the message integrity code (MIC) authentication tag for non-segmented 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.

❖ **Competitive Technologies:**

- G3-PLC (now ITU G.9903)
- PRIME (now ITU G.9904).

  Both of these technologies were initially developed to address a single use case: smart metering deployment in Europe over the CENELEC A band.

IEEE 802.11ah

- In unconstrained networks, IEEE 802.11 Wi-Fi is certainly the most successfully deployed wireless technology.
- 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.
- Hence 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:

- **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**

- In July 2010, the IEEE 802.11 working group decided to work on an “industrial Wi-Fi” and created the IEEE 802.11ah group.
- The 802.11ah specification would operate in unlicensed sub-GHz frequency bands, similar to IEEE 802.15.4 and other LPWA technologies.
- For the 802.11ah standard, the Wi-Fi Alliance defined a new brand called Wi-Fi HaLow.
- It is similar to the word “hello” but it is pronounced “hay-low.”

❖ **Physical Layer**

- IEEE 802.11ah essentially provides an additional 802.11 physical layer operating in unlicensed sub-GHz bands.
- Various countries and regions use the following bands for IEEE 802.11ah: 868–868.6 MHz for EMEAR, 902–928 MHz and associated subsets for North America and Asia-Pacific regions, and 314–316 MHz, 430–434 MHz, 470–510 MHz, and 779–787 MHz for China.
- Based on OFDM modulation, IEEE 802.11ah uses channels of 2, 4, 8, or 16 MHz.
- Ex: At a data rate of 100 kbps, the outdoor transmission range for IEEE 802.11ah is expected to be 0.62 mile.

❖ **MAC Layer**

- The IEEE 802.11ah MAC layer is optimized to support the new sub-GHz Wi-Fi PHY while providing low power consumption and the ability to support a larger number of endpoints.
- Enhancements and features specified by IEEE 802.11ah for the 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).
        - In combination with RAW and TWT, this mechanism reduces contention in large cells with many clients by restricting which group, in which sector, can contend during which time window.
    - **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.
        - By providing more efficient access to the medium, additional power savings for battery-powered devices can be achieved, and collisions are reduced.
    - **Target wake time (TWT):**
        - Reduces energy consumption by permitting an access 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.
        - It also reduces the probability of collisions in large cells with many clients.
    - **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**

- While IEEE 802.11ah is deployed as a star topology, it includes a simple hops relay operation to extend its range.
- This relay operation can be combined with a higher transmission rate or modulation and coding scheme (MCS).
- This means that a higher transmit rate is used by relay devices talking directly to the access point.
- The transmit rate reduces as you move further from the access point via relay clients.
- Sectorization is a technique that involves partitioning the coverage area into several sectors to get reduced contention within a certain sector.
- This technique is useful for limiting collisions in cells that have many clients.

- This technique is also often necessary when the coverage area of 802.11ah access points is large, and interference from neighbouring access points is problematic.
- Figure 2.15 shows an example of 802.11ah sectorization.

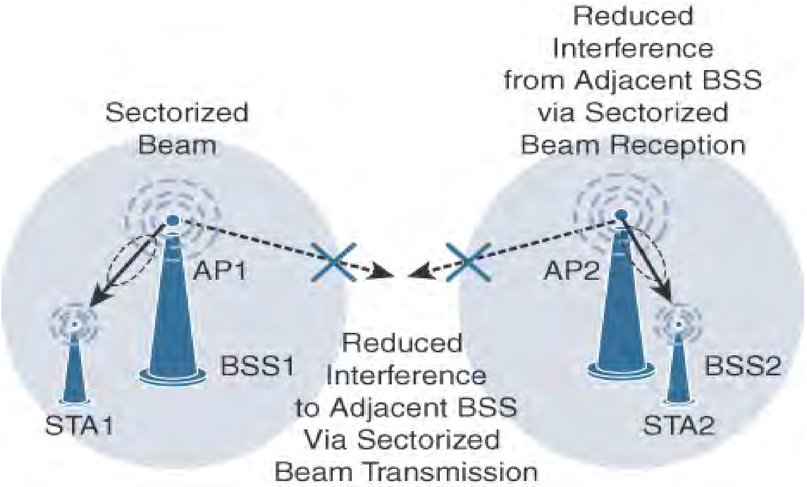

Sectorized Beam
Reduced Interference from Adjacent BSS via Sectorized Beam Reception
AP1
AP2
BSS1
BSS2
STA1
STA2
Reduced Interference to Adjacent BSS Via Sectorized Beam Transmission

Figure 2.15 :IEEE 802.11ah Sectorization

❖ **Security**

- Similar to IEEE 802.11 specifications

❖ **Competitive Technologies**

- Competitive technologies to IEEE 802.11ah are IEEE 802.15.4 and IEEE 802.15.4e

LoRaWAN:

- It is an unlicensed-band LPWA(Low-Power Wide-Area) technology.

❖ **Standardization and Alliances**

- 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.
- The LoRa Alliance quickly achieved industry support and currently has hundreds of members.
- LoRa Alliance uses the term LoRaWAN to refer to its architecture and its specifications that describe end-to-end LoRaWAN communications and protocols.
- Figure 2.16 provides a high-level overview of the LoRaWAN layers.

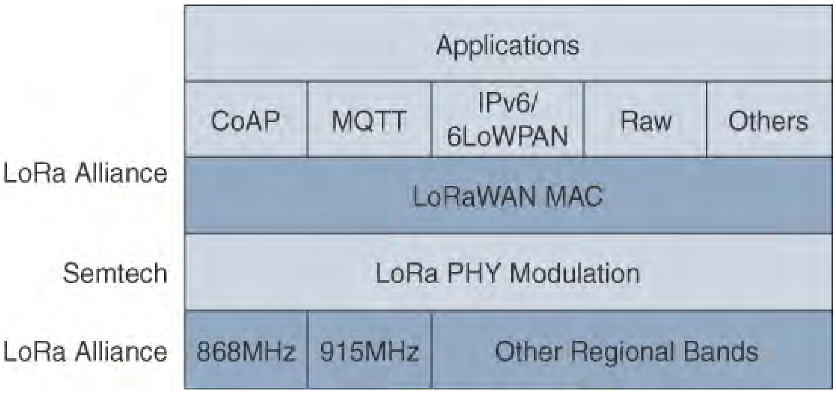


Figure 2.16 LoRaWAN Layers

❖ **Physical Layer**

- LoRaWAN 1.0.2 regional specifications describe the use of the main unlicensed sub-GHz frequency bands of 433 MHz, 779–787 MHz, 863–870 MHz, and 902–928 MHz, as well as regional profiles for a subset of the 902–928 MHz bandwidth.
- For example, Australia utilizes 915–928 MHz frequency bands, while South Korea uses 920–923 MHz and Japan uses 920–928 MHz.
- 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.
- The ADR algorithm ensures that packets are 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.
- An important feature of LoRa is its ability to handle various data rates via the spreading factor.
- Devices with a low spreading factor (SF) achieve less distance in their communications but transmit at faster speeds, resulting in less airtime. A higher SF provides slower transmission rates but achieves a higher reliability at longer distances.

❖ **MAC Layer**

- 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.
- LoRaWAN messages, either uplink or downlink, have a PHY payload composed of 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.
- Figure 2.17 shows a high-level LoRaWAN MAC frame format.

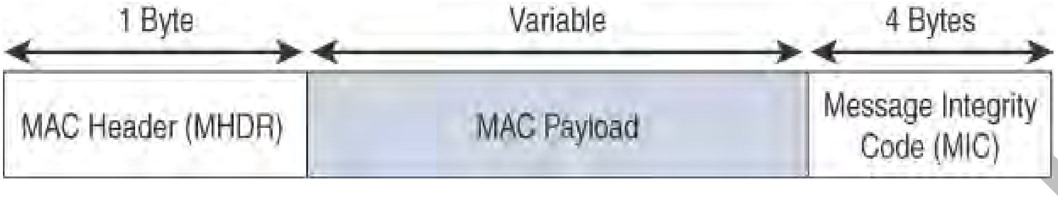


Figure 2.17: High-Level LoRaWAN MAC Frame Format

- In version 1.0.x, LoRaWAN utilizes six MAC message types
  - **Join request :** over-the-air (OTA) activation and joining the network.
  - **Join accept messages**: over-the-air (OTA) activation and joining the network.
  - **Unconfirmed data up/down message** : End device does not need to acknowledge
  - **Confirmed data up/down message** : A message that must be acknowledged
  - **Uplink messages:** These messages are sent from endpoints to the network server and are relayed by one or more LoRaWAN gateways
  - **Downlink messages:** These messages flow from the network server to a single endpoint and are relayed by only a single gateway.
- LoRaWAN endpoints are uniquely addressable through a variety of methods.
- 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.
- Gateways connect to the backend network using standard IP connections, and endpoints communicate directly with one or more gateways.

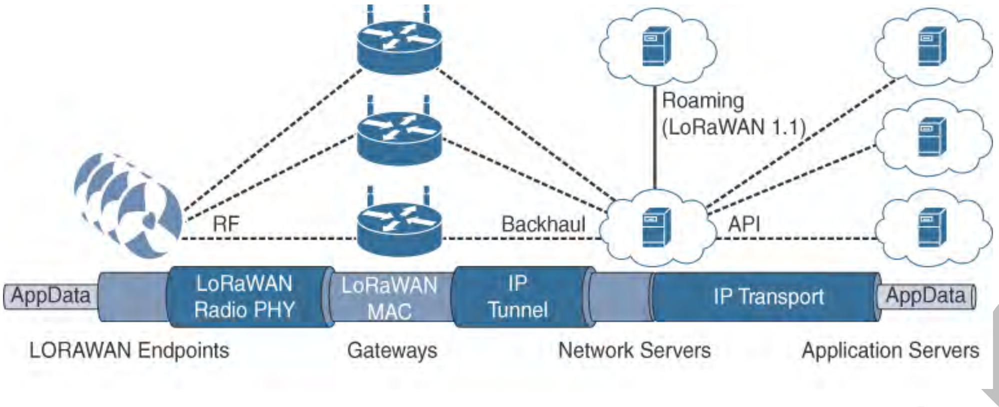


Figure 2.18: LoRaWAN Architecture

- In the figure 2.18 LoRaWAN endpoints transport their selected application data over the LoRaWAN MAC layer on top of one of the supported PHY layer frequency bands.
- LoRaWAN gateways act as bridges that relay between endpoints and the network servers.
- Multiple gateways can receive and transport the same packets. When duplicate packets are received, de-duplication is a function of the network server.
- 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:**

- LoRaWAN endpoints must implement two layers of security, protecting communications and data privacy across the network.
- Security in a LoRaWAN deployment applies to different components of the architecture as shown in figure 2.19

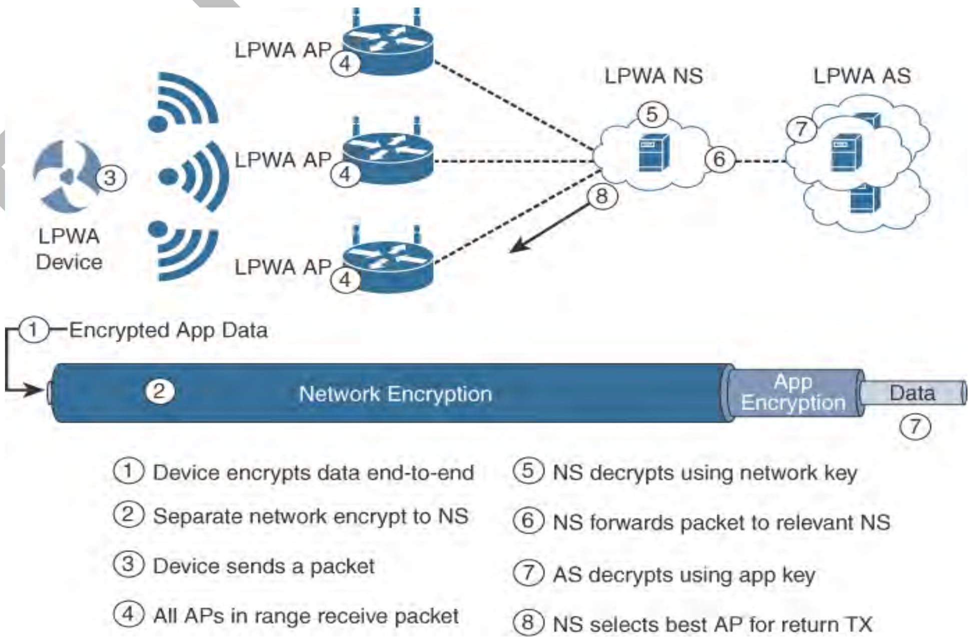

LPWA AP 4
LPWA AP 4
LPWA AP 4
LPWA NS
LPWA AS
5
6
7
8
3
LPWA Device
1 Encrypted App Data
2 Network Encryption
App Encryption
Data
7
1 Device encrypts data end-to-end
2 Separate network encrypt to NS
3 Device sends a packet
4 All APs in range receive packet
5 NS decrypts using network key
6 NS forwards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

Figure 2.19: 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.
- 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 netwrk 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:

- Because the new LTE-M device category was not sufficiently close to LPWA capabilities, in 2015 3GPP approved a proposal to standardize a new narrowband radio access technology called Narrowband IoT (NB-IoT).
- 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.

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.

- Category 0 includes important characteristics to be supported by both the network and end devices 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.
- 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

- 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 NB-OFDMA
  - Narrowband LTE (NB-LTE), Alcatel-Lucent, Ericsson, and Nokia proposal
  - Cooperative Ultra Narrowband (C-UNB), Sigfox proposal
- 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.
- **Guard band:** An NB-IoT carrier is between the LTE or WCDMA bands. This requires coexistence between LTE and NB-IoT bands.

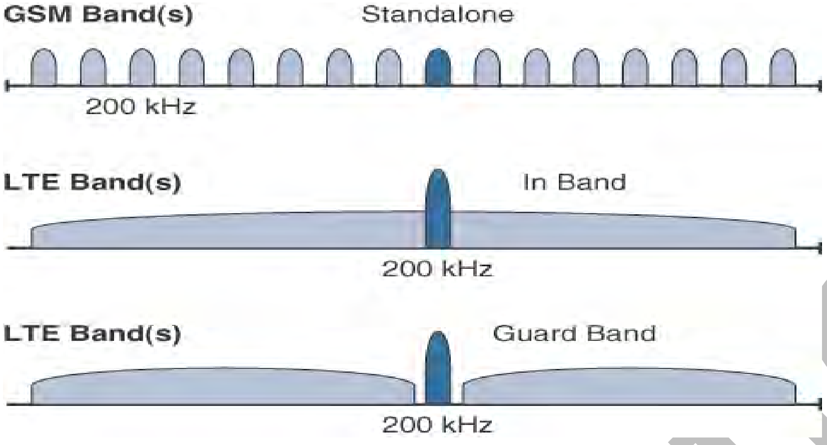


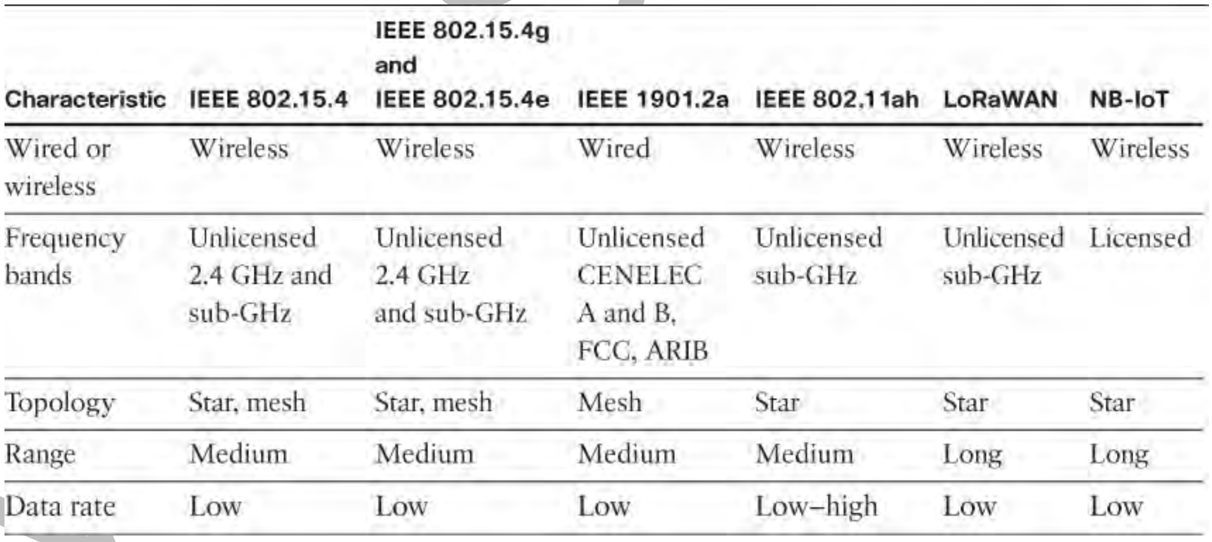
Figure 2.20: NB-IoT Deployment Options

- 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.
- 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.

Main Characteristics of Access Technologies is given in Table 2.5



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

Table 2.5 : Characteristics of Access Technologies

MODULE - 5

IOT physical Devices and Endpoints - Arduino UNO

Introduction to Arduino

Arduino is an open-source advancement prototying platform which depends on simple to-utilize equipment and programming.

Arduino can read inputs - such as detecting the power of light, events triggered by a button or a twitter message and can respond into a yield.

The Arduino is a small computer that you can program to read information from the world around you and to send commands to the outside world.

- Arduino is a tiny computer that you can connect to electrical circuits. This makes it easy to read inputs - and control outputs - send a command to the outside.

Why Arduino ?

Arduino is an open source product, software/hardware which is accessible and flexible to customers.

Arduino is flexible because of offering variety of digital and analog pins, SPI and PWM outputs.

Arduino is easy to use, connected to computer via a USB and communicates using serial protocol.

Arduino has growing online community where lots of source code is available for use.

Arduino is cross-platform, which can work on Windows, Mac or Linux platforms.

Arduino follows simple, clear programming environment as C language.

Which Arduino?

There are hundreds of "Arduino boards" available in the market serving every kind of purpose. Among all we almost focus on popular Arduino UNO which is used in almost 99% of projects use.

→ Some of the Boards from Arduino family are given below

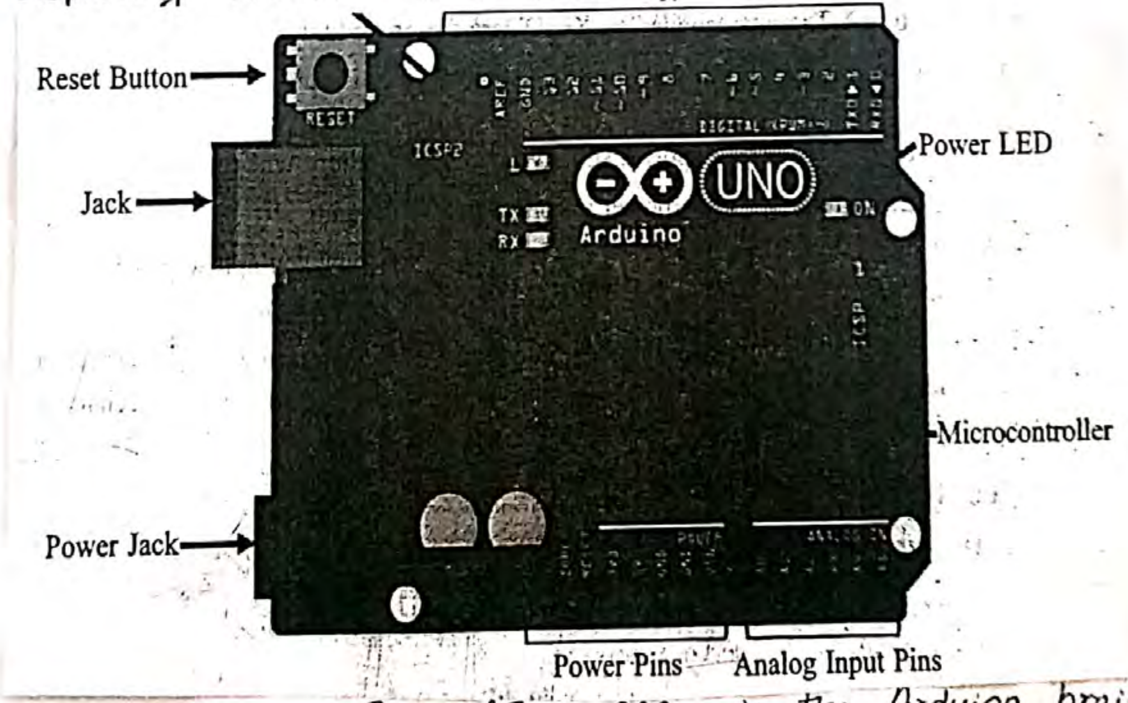
Arduino Mega is a big sister to the UNO with more memory and pins with a different chip the ATmega2560.

Flora is an Arduino compatible from Adafruit which is a round wearable which can be sewed into clothing.

The Arduino MKR1000 is a little like an Arduino Micro but has a more powerful32-bit ATSAM ARM chip and built-in Wifi.

Arduino Micro is bit smaller with a chip Atmega32u4 that can act like a Keyboard or mouse.

Exploring Arduino UNO Learning Board



* Microcontroller : The ATmega328p is the Arduino brain. Everything on the Arduino board is meant to support this microcontroller.

* Digital pins : Arduino has 14 digital pins, labeled from 0 to 13 that can act as inputs or outputs.

* PWM pins : These are digital pins marked with a ~ (pins 11, 10, 9, 6, 5 and 3). PWM stands for "pulse width modulation" and allows to make digital pins output "fake" varying amounts of voltage.

* TX and RX pins : digital pins 0 and 1. The T stands for "transmit" and the R for "receive".

* LED attached to digital pin 13 : This is useful for an easy debugging of the Arduino sketches.

* Analog pins : The analog pins are labeled from A0 to A5 and are most often used to read analog sensors.

* Power pins : The Aurdino has 3.3V or 5V Supply, Which is really useful since most components require 3.3V or 5V.

* Reset button : When you press that button, the program that is currently being run in your Arduino will start from the beginning.

* Power ON LED : will be on since power is applied to the Arduino.

* USB jack : Connecting a male USB A to male USB B cable is how you upload programs from your computer to your Arduino board.

* Power jack : The power jack is where you connect a component to power up your Arduino.

Things that Arduino can do

Motion Sensor : It allows you detect movement

Light Sensor : this allows you to "measure" the quantity of light in the outside world.

Humidity and temperature Sensor : this is used to measure the humidity and temperature.

Ultrasonic Sensor : this sensor allows to determine the distance to an object through sonar.

Installing the Software (Arduino IDE)

The Arduino IDE (Integrated Development Environment) is where you develop your programs that will tell your Arduino what to do.

To download your Arduino IDE, browse on the following link https://www.arduino.cc/en/Main/Software.

Select which Operating System you're using and download it.

Fundamentals of Arduino Programming

1) Structure

The structure of Arduino programming contains of two parts as shown below

```
void setup()
{
   Statement(s);
}
void loop()
{
   Statement();
}
```

2) void setup()

```
   void loop()
{
   digitalWrite(pin,HIGH);
   delay(10000);
   digitalWrite(pin,Low);
   delay(10000);
}
```

3) Functions

A function is a piece of code that has a name and set of statements executed when function is called.

Functions are declared by its type followed with name of a function.

```
Syntax : type functionName (parameters)
         {
           Statement(s);
         }
```

4) { } Curly braces

They define beginning and end of function.

5) Semicolon

It is used to end a statement and separate elements of a program.

Syntax : int x=14;

Differences between Analog, Digital and PWM Pins

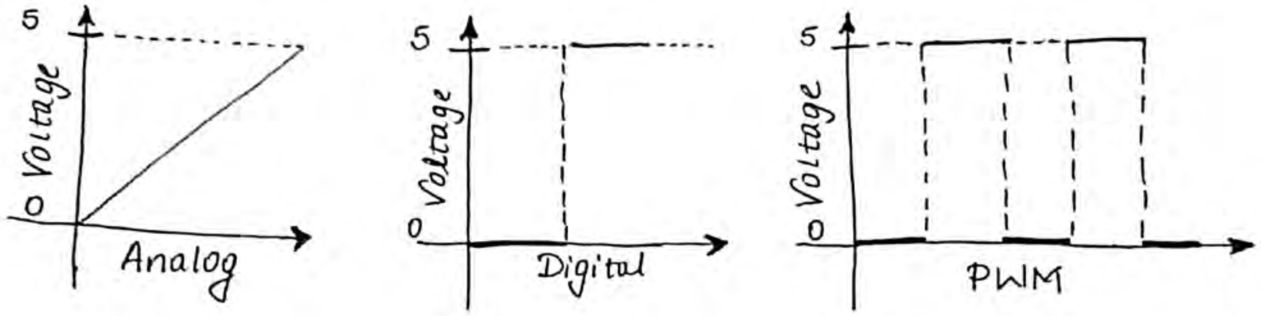
In analog pins, you have unlimited possible states between 0 and 1023, This allows you to read Sensor Values for example, with a light sensor, if it is very dark, you'll read 1023, if it is very bright you'll read 0 If there is a brightness between dark and very bright you'll read a value between 0 and 1023.

In digital pins, you have just two possible states, which are on or off. These can also be referred as High or Low, 1 or 0 and 5V or 0V. For example, if an LED is on, then, its state is high or 1 or 5V. If it is off, you'll have Low, or 0 or 0V.

PWM pins are digital pins, so they output either 0 or 5V. However these pins can output "fake" intermedia voltage values between 0 and 5V, because they can perform "Pulse Width Modulation" (PWM). PWM allows to "simulate" varying levels of power by oscillating the output voltage of the Arduino.

The below figure shows the representation of Analog,

Digital and PWM pins of Arduino.



IOT Physical Devices and Endpoints : RaspberryPi

Introduction to RaspberryPi

The RaspberryPi is a series of credit card sized single-board computers developed in the United Kingdom by Raspberrypi foundation to promote the teaching of basic computer science in school and developing Countries.

The original model became far more popular than anticipated, selling outside its target market for uses such as robotics. It does not include peripherals and cases. However, some accessories have been included in several official and unofficial bundles.

The Organisation behind the Raspberry Pi consists of two arms. The first two models were developed by the Raspberry Pi Foundation. After the Pi Model B was released, the Foundation setup Raspberry Pi Trading, with Eben Upton as CEO, to develop the third model the B+.

"Why RaspberryPi?" - Inexpensive, Cross-platform, Simple, clear programming environment, Open source and extensible Software and Open source and extensible hardware.

Exploring The Raspberrypi Learning Board

GPIO Pinout Diagram

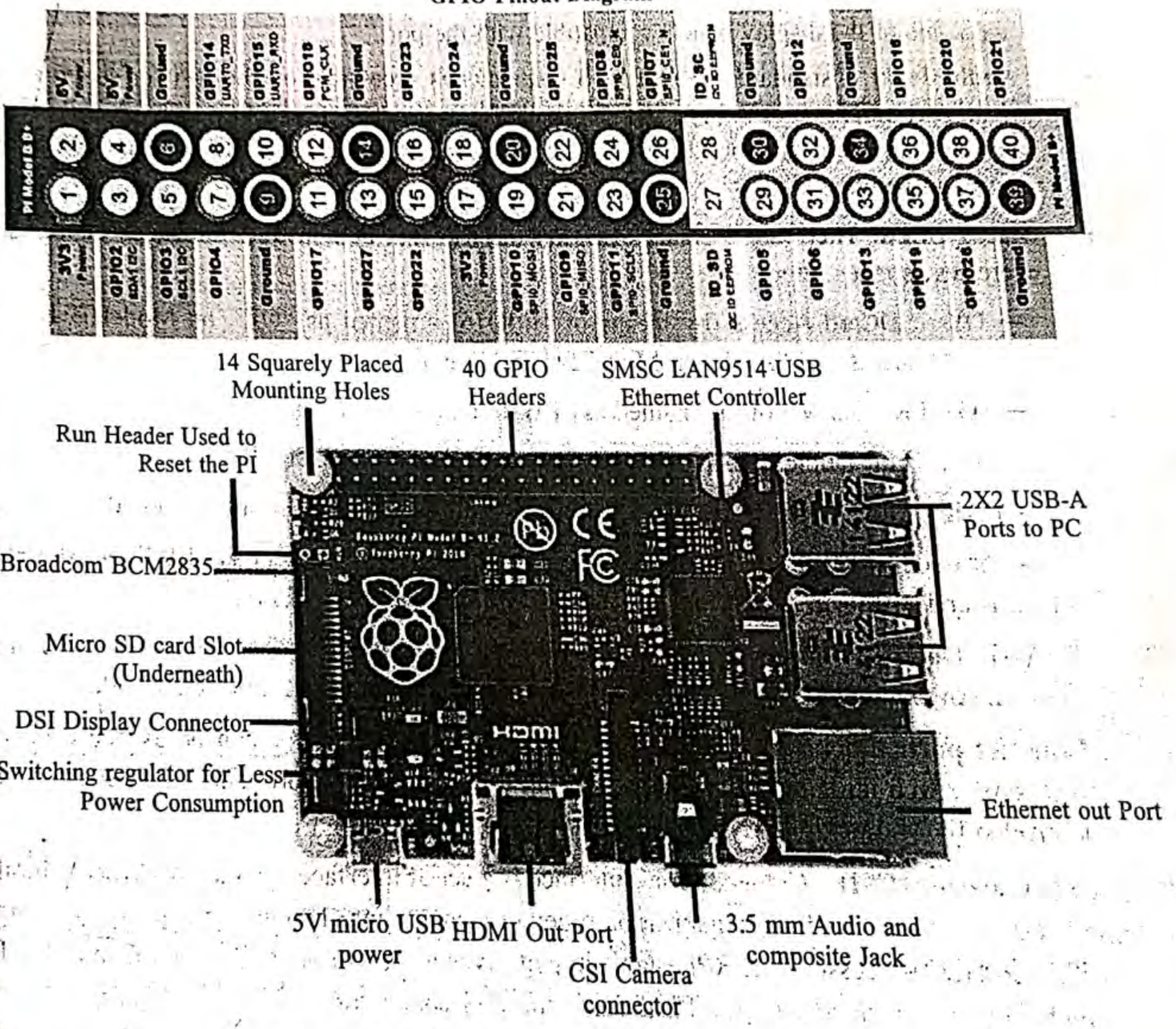


Figure 8-1: Raspberry Pi2 Model B and its GPIO

Processor : The Broadcom BCM2835 SoC used in the first generation Raspberrypi is somewhat equivalent to the chip used in first generation smart phones, which includes a 700 MHz ARM 1176JZF-S processor, Video Core IV graphics processing Unit (GPU) and RAM. This has a level 1 cache of 16KB and a level 2 cache of 128KB.

Power Source : The recommended and easiest way to power the Raspberrypi is Via the Micro USB port on the side of the unit.

SD Card : The Raspberry Pi does not have any locally available storage accessible. The working framework is stacked on a SD card which is embedded on the SD card space on the Raspberry Pi.

GPIO (General Purpose Input Output) : GPIO is a non specific pins on a coordinated circuit to know is an input or output pin which can be controlled by the client at run time. GPIO pins have no exceptional reason characterized, and go unused as a matter of course.

DSI Display X : The Raspberrypi Connector S2 is a display serial interface (DSI) for connecting a liquid crystal display (LCD) panel using a 15-pin ribbon cable.

Audio Jack : A standard 3.5mm TRS connector is accessible on the RPi for stereo sound yield. Any earphone or 3.5mm sound link can be associated straightforwardly.

Ethernet Port : It is accessible on Model B and B+. It can be associated with a system or web utilizing a standard LAN link on the Ethernet port.

CSI connector(CSI) : Camera Serial Interface is a serial interface outlined by MIPI (Mobile Industry Processor Interface) organization together went for interfacing computerized cameras with a portable Processor.

JTAG headers : JTAG is an acronym for 'Join Test Action Group', an association that began back in the mid 1980's to address test point get to issues on PCB with surface mount gadgets.

Description of System on Chip (SoC)

A System on a chip (SoC) is an integrated Circuit (IC) that co-ordinates all parts of a PC or other electronic framework into a Solitary chip.

It might contained advanced, simple, blended flag, and regularly radio-recurrence works - all on a Solitary chip Substrate. SoCs are exceptionally regular in the portable gadgets advertise in view of their low power utilization. A run of the mill application is in the range of implanted frameworks.

An SoC comprises of:

★ A microcontroller, chip or DSP core(s). Some SoCs - called multiprocessor framework on chip (MPSoC) - incorporate more than one processor center.

★ Memory pieces including a choice of ROM, RAM, EEPROM and Streak memory.

★ Timing Sources including oscillators and Stage bolted circles.

★ Simple interfaces including ADCs and DACs.

★ Voltage controllers and power administration circuits.

Raspberry Pi interfaces

Raspberry Pi has Serial, SPI and I2C interfaces as shown in the figure of Raspberry Pi Learning board.

★ Serial : The Serial interface on Raspberry Pi has receive (rx) and transmit (Tx) pins for Communication with Serial peripherals.

★ SPI : Serial Peripheral Interface (SPI) is a Synchronous Serial data Used for communicating with one or more peripheral devices.

★ I2C : The I2C interface pins on Raspberry Pi allow you to connect hardware modules. I2C interface allows Synchronous data transfer with just two pins-SDA (data line) and SCL (clock ~~line~~ line).

Raspberry Operating Systems

Various operating systems can be installed on Raspberry through SD cards. Most use a MicroSD slot located on the bottom of the board.

The Raspberrypi primarily uses Raspbian, a Debian-based Linux operating System.

Operating Systems (not Linux based)

- RISC OS Pi
- FreeBSD
- NetBSD
- Plan 9 from Bell Labs and Inferno
- Windows 10 IOT Core - a no cost edition of Windows 10 offered by Microsoft that runs natively on the RaspberryPi 2.

Operating Systems (Linux based)

- Xbian - using Kodi open source digital media center
- openSUSE
- Raspberry Pi Fedora remix
- Pidora, another fedora Remix optimised for Raspberry Pi
- Gentoo Linux
- Diet Pi
- CentOS\Open Wrt
- Kali Linux
- Ark OS
- Kano OS
- Nard SDK

Media center operating system

- OSMC
- OpenELEC
- LibreELEC
- Xbian
- Rasplex

Audio operating Systems

- Volumio
- Pimusicbox
- Runeaudio
- moOdeaudio

Recalbox

- Happi Game Center
- Lakka
- ChameleonPi
- Piplay

Operating System Setup On RaspberryPi

Preinstalled NOOBS operating system is already available in many authorized as well as independent seller, there are many other operating system for RaspberryPi in the market like NOOBS, Raspbian and third party Operating Systems are also available like UBUNTU MATE, OSMC, RISC OS etc. To setup an operating system we need a SD card with minimum capacity of 8GB.

Formatting SD card

Format the SD card before copying NOOBS onto it. To do this -

- Download SD formatter 4.0 from SD Association website for either Windows or Mac.

Follow the instructions to install the Software

- Insert the SD card into the computer or laptops SD card reader and make a note of the drive letter allocated to it.
- In SD formatter, select the drive letter the SD card is and format it.

OS Installation

Follow the step to install operating system in SD card

- Go to RaspberryPi foundation website and click on DOWNLOAD section.
- Click on NOOBS, then click on "Download zip" button under NOOBS and select a folder to save this zip file.
- Extract all the files from ZIP.
- Once SD card has been formatted, drag all the files in the extracted NOOBS folder and drop them onto the SD card drive.
- The necessary file will then be transferred to the SD card.
- When this process has finished, safely remove the SD card and insert it into the RaspberryPi.

First Boot

- Plug in the Keyboard, mouse, and monitor cables.
- Now plug the USB cable into the RaspberryPi
- Now Raspberrypi will boot, and a window will appear with a list of different operating system.
- Raspbian will then run through its installation Process.

Programming RaspberryPi with Python

RaspberryPi runs Linux and Supports python out of the box. Henceforth you can run any python program that runs on a normal computer. However it is the general purpose input/output capability provided by the GPIO pins on Raspberry Pi that makes it useful device for Internet of things.

Simple python Programs on RaspberryPi

Program | Code

1. Print hello world

```
print("hello world")
```

2. Program to add two numbers

```
a=1.2
b=5.3
sum = float(a) + float(b)
print("the sum of{0} and {1} is {2}".
                    format(a,b,sum))
```

3. Program to print fibonacci series

```
a,b = 0,1
while b<200:
    print(b)
     a,b = b,a+b
```

4. Program to display calender of given month of the year

```
import calender
yy = 2017
mm = 11
print(calender.month(yy.mm))
```

5. Program to find the ip address of raspbrerrypi

```
import urllib
import re
print("we will try to open this url, in order
        to get ip address")
url = http://checkip.dyndns.org
print(url)
```