**Q. Define iot** Ans. IoT stands for "Internet of Things." It refers to the network of physical devices, vehicles, appliances, and other items that are embedded with sensors, software, and connectivity, allowing them to connect and exchange data with each other and with other systems over the internet. The goal of IoT is to create a seamless, connected ecosystem where data can be collected and analyzed in real-time, enabling automation, optimization, and new services and experiences.

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.

IoT has a wide range of applications across industries, from smart homes and cities, to healthcare, agriculture, manufacturing, and transportation. For example, in a smart home, IoT devices like smart thermostats, security systems, and lighting can all be connected and controlled through a single app on a smartphone or tablet. In healthcare, IoT sensors can be used to monitor patient health remotely, alerting doctors and caregivers if there are any concerns.

Overall, IoT is a powerful technology that has the potential to transform the way we live, work, and interact with the world around us.

**Q.Iot impact** Ans.Projections on the potential impact of IoT are impressive. About 14 billion, or just 0.06%, of “things” are connected to the Internet today. Cisco Systems predicts that by 2020, this number will reach 50 billion. A UK government report speculates that this number could be even higher, in the range of 100 billion objects connected. Cisco further estimates that these new connections will lead to $19 trillion in profits and cost savings.3 Figure 1-2 provides a graphical look at the growth in the number of devices being connected. What these numbers mean is that IoT will fundamentally shift the way people and businesses interact with their surroundings. Managing and monitoring smart objects using real-time connectivity enables a whole new level of data-driven decision making. This in turn results in the optimization of systems and processes and delivers new services that save time for both people and businesses while improving the overall quality of life. The following examples illustrate some of the benefits of IoT and their impact. These examples will provide you with a high-level view of practical IoT use cases to clearly illustrate how IoT will affect everyday life.

**Q.Iot challenges**

**Table 1-4** *IoT Challenges*

| 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. See Chapter 7 for more information on IoT and the challenges it faces from a big data perspective. |

**Q. M2M 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. 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. This conceptual layer adds APIs and middleware supporting third-party services and applications**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.

Figure 2-1 illustrates the oneM2M IoT architecture.

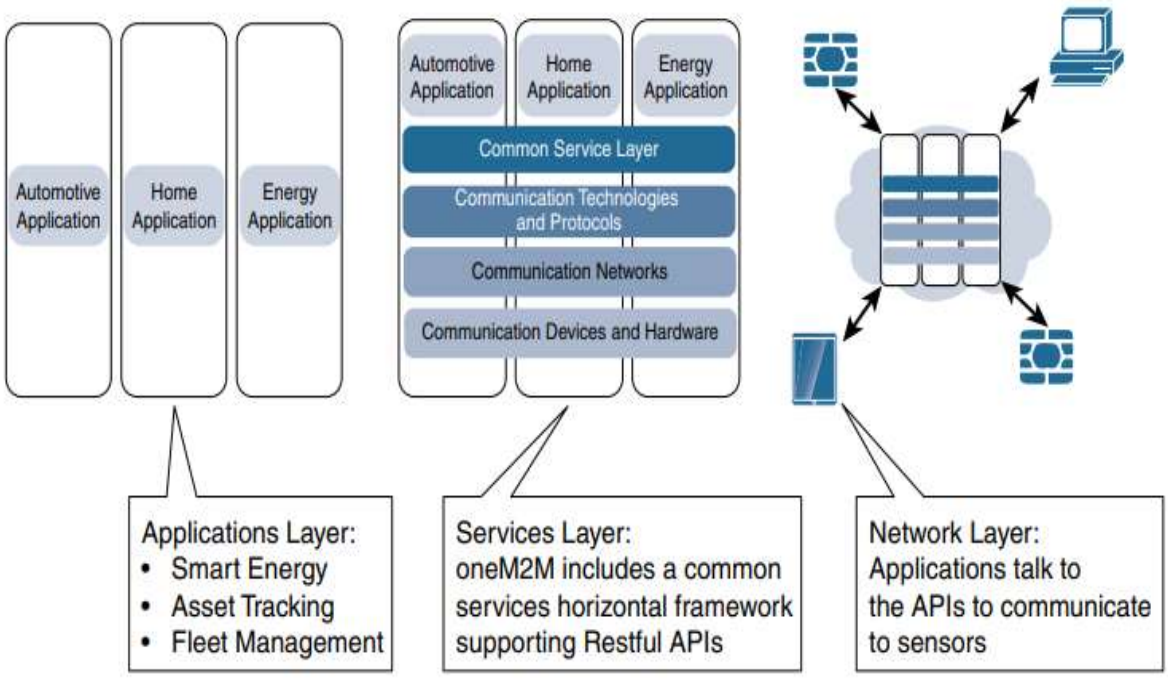


**Figure 2-1** *The Main Elements of the oneM2M IoT Architecture*

**Q. IoTWF architecture**

Ans. In 2014 the IoTWF architectural committee (led by Cisco, IBM, Rockwell Automation, and others) published a seven-layer IoT architectural reference model. While various IoT reference models exist, the one put forth by the IoT World Forum offers a clean, simplified perspective on IoT and includes edge computing, data storage, and access.The World Forum Standardized Architecture (WFSA) is a set of standards developed by the World Forum on the Internet of Things (WF-IoT) to provide a framework for IoT device interoperability and data exchange. The WFSA aims to establish a common language and framework for IoT devices and applications, enabling seamless integration and interoperability between different systems and technologies.

The WFSA includes four layers: ● **Device layer:** This layer defines the hardware and software components of IoT devices, including sensors, actuators, processors, and communication interfaces. The device layer also includes standardized device profiles that define the functionality and capabilities of different types of IoT devices. ● **Network layer:** This layer defines the communication protocols and interfaces used to connect IoT devices to the internet and to other devices. The network layer includes standard protocols such as TCP/IP, HTTP, and MQTT, as well as interfaces for device discovery and configuration. ● **Service layer:** This layer defines the services that are provided by IoT devices and applications, including data collection, storage, processing, and analysis. The service layer also includes standard data models and technologies that enable the semantic interoperability of IoT data. ● **Application layer**: This layer defines the interfaces and protocols used by applications to interact with IoT devices and services. The application layer includes standard APIs and interfaces for accessing IoT data and services, as well as standard data formats for data exchange between applications.

**Applications:**

**Smart cities:**By using the WFSA, different smart city systems can communicate with each other using common protocols and data models, enabling better coordination and more efficient use of resources.

**Healthcare:** The WFSA has been used to develop interoperable and secure solutions for healthcare applications, such as remote patient monitoring and telemedicine. By using the WFSA, different healthcare devices and systems can communicate and exchange data in a standardized way, ensuring that patient data is consistent and accurate.

**Agriculture:** The WFSA has been used in agriculture to develop interoperable and standardized solutions for precision farming applications, such as soil moisture monitoring and crop management. By using the WFSA, farmers can integrate different sensors and devices into their systems, enabling better decision-making and more efficient use of resources.

**FOG COMPUTING,EDGE COMPUTING,CLOUD COMPUTING**

**Edge computing:** This is the layer closest to the devices and sensors that generate the data. Edge computing involves processing data on or near the device itself, rather than sending it to a central server or the cloud. This can be done using low-power, low-latency devices like microcontrollers or single-board computers. Edge computing is useful for applications that require real-time processing and decision-making, such as industrial automation, autonomous vehicles, and smart homes.Example:In the healthcare industry, fog computing can be used to process data from patient monitoring devices in real-time. For example, a hospital could use fog computing to analyze data from wearable devices that track patients' vital signs, such as heart rate and blood pressure, to detect signs of distress and alert medical staff.

**Fog computing:** This layer is a step up from edge computing and involves using a distributed network of servers and devices to process data. Fog computing typically involves processing data in a local network, rather than sending it to a remote data center. This can help reduce latency and improve the reliability and security of the system. Fog computing is useful for applications that require more processing power than edge computing can provide, but still need to be processed locally, such as video analytics, smart cities, and remote monitoring. a retail store could use edge computing to analyze data from sensors that track customer behavior and purchasing patterns to offer personalized discounts and recommendations

**Cloud computing**: This layer is the highest level in the hierarchy and involves using a centralized network of servers to process and store data. Cloud computing typically involves sending data to a remote data center over the internet, where it can be processed and stored in large data warehouses. Cloud computing is useful for applications that require massive amounts of processing power and data storage, such as big data analytics, machine learning, and artificial intelligence.Example:

| | Cloud | Fog | Edge |
|---|---|---|---|
| Latency | Highest | Medium | Lowest |
| Scalability | High, easy to scale | Scalable within network | Hard to scale |
| Distance | Far from the edge | Network close to the edge | At the edge |
| Data analysis | Less time-sensitive data processing, permanent storage | Real-time, decides to process locally or send to cloud | Real-time, instant decision making |
| Computing power | High | Limited | Limited |
| Interoperability | High | High | Low |

## SENSORS AND TRANSDUCERS

The words sensors and transducers are widely used in association with measurement systems. The sensor is an element that produces signals relating to the quantity that is being measured. According to Instrument Society of America, "a sensor is a device that provides usable output in response to a specified quantity which is measured." The word sensor is derived from the original meaning 'to perceive'.
In simple terms, **a sensor is** a device that detects changes and events in a physical stimulus and provides a corresponding output signal that can be measured and/or recorded. Here, the output signal can be any measurable signal and is generally an electrical quantity.
Sensors are devices that perform input function in a system as they sense the changes in a quantity. The measured temperature is converted to a readable value on the calibraled glass a based on the expansion and contraction of liquid mercury. **Transducers** are the devices that convert energy in one form into another form. Generally the energy is in the form of a signal. Transducer is a term collectively used for both sensors and actuators.

### Criteria to Choose a Sensor

The following are certain features that are considered when choosing a sensor.
1. **Type of Sensing**: The parameter that is being sensed like temperature or pressure.
2. **Operating Principle:** The principle of operation of the sensor.
3. **Power Consumption:** The power consumed by the sensor will play an important role in defining the total power of the system.
4. **Accuracy:** The accuracy of the sensor is a key factor in selecting a sensor.
5. **Environmental Conditions:** The conditions in which the sensor is being used will be a factor in choosing the quality of a sensor.
6. **Cost**: Depending on the cost of application, a low cost sensor or high cost sensor can be used.
7. **Resolution and Range:** The smallest value that can be sensed and the limit of measurement are important.
8. **Calibration and Repeatability**: Change of values with time and ability to repeat measurements under similar conditions.

### The basic requirements of a sensor are:

**1. Range**: It indicates the limits of the input in which it can vary. In case of temperature measurement, a thermocouple can have a range of 25 - 250°C.
**2. Accuracy:** It is the degree of exactness between actual measurement and true value. Accuracy is expressed as percentage of full range output.
**3. Sensitivity:** Sensitivity is a relationship between input physical signal and output electrical signal. It is the ratio of change in output of the sensor to unit change in input value that causes change in output.
**4. Stability:** It is the ability of the sensor to produce the same output for constant input over a period of time.
**5. Repeatability:** It is the ability of the sensor to produce same output for different applications with same input value.
**6. Response Time:** It is the speed of change in output on a stepwise change in input.
**7. Linearity:** It is specified in terms of percentage of nonlinearity. Nonlinearity is an indication of deviation of curve of actual measurement from the curve of ideal measurement.
**8. Ruggedness:** It is a measure of the durability when the sensor is used under extreme operating conditions.

**.Sensor Types**

There are many different types of sensors, which can be classified based on various criteria, including their physical principle of operation, their sensing mechanism, and their application domain. Here are some common types of sensors:

**1)Temperature sensors:** These sensors measure the temperature of the environment, typically using a thermocouple, resistance temperature detector (RTD), or thermistor.**2)Pressure sensors:** These sensors measure the pressure of a fluid or gas, typically using a piezoelectric, capacitive, or strain gauge sensor.**3)Accelerometers:** These sensors measure changes in acceleration, typically using a piezoelectric or capacitive sensor.**4)Gyroscopes**: These sensors measure changes in angular velocity, typically using a mechanical or MEMS-based sensor.**5)Proximity sensors:** These sensors detect the presence or proximity of an object, typically using a capacitive, inductive, or optical sensor.**6)Magnetic sensors**: These sensors measure changes in magnetic fields, typically using a magnetoresistive, Hall effect, or fluxgate sensor.**7)Humidity sensors:** These sensors measure the relative humidity of the environment, typically using a capacitive, resistive, or thermal sensor.**8)Optical sensors:** These sensors use light to detect changes in the environment, typically using a photodiode, phototransistor, or photovoltaic sensor.**9)Gas sensors:** These sensors detect the presence or concentration of gases, typically using a catalytic, electrochemical, or optical sensor.**10)Force sensors**: These sensors measure the force applied to an object, typically using a strain gauge or piezoelectric sensor.

**Classification:-**

Sensors are devices that detect and measure physical or chemical properties of the environment and convert them into an electrical signal that can be processed and analyzed.

**1)Optical Sensors:** These sensors use light to detect and measure changes in the environment. They can be classified based on their sensing mechanism, such as photovoltaic, photoconductive, or photoacoustic sensors.

**2)Mechanical Sensors:** These sensors use mechanical properties, such as displacement, strain, or pressure, to detect and measure changes in the environment. They can be classified based on their sensing mechanism, such as resistive, capacitive, or inductive sensors.

**3)Magnetic Sensors**: These sensors use magnetic fields to detect and measure changes in the environment. They can be classified based on their sensing mechanism, such as magnetoresistive, magnetostrictive, or Hall effect sensors.

**4)Chemical Sensors:** These sensors use chemical reactions to detect and measure changes in the environment, such as changes in pH, gas concentration, or humidity. They can be classified based on their sensing mechanism, such as electrochemical, optical, or thermal sensors.

**5)Biological Sensors:** These sensors use biological properties, such as antibodies or enzymes, to detect and measure changes in the environment, such as the presence of specific molecules or pathogens. They can be classified based on their sensing mechanism, such as biosensors or immunosensors.

**6)Environmental Sensors:** These sensors are used to monitor changes in the environment, such as temperature, humidity, or air quality. They can be classified based on their application domain, such as weather sensors, air quality sensors, or water quality sensors.

**ACTUATORS**

**An actuator** is a machine, or rather a part of a machine used to convert externally available energy into motion based on the control signals.

• Much like how hands and legs enable humans to move around and perform actions. actuators let machines perform various mechanical movements.For electromechanical systems, the input is detected and measured by a device called a sensor. The task of a sensor is to sample the signals available to it and convert them into a form understandable by the system. The system then processes the information and decides how to respond.

common types of actuators and their classifications:1**)Electric actuators:** These actuators use electric motors to generate mechanical motion or force. They can be classified based on their motor type, such as DC, stepper, or servo motors.2**)Hydraulic actuators:** These actuators use hydraulic fluid to generate mechanical motion or force. They can be classified based on their operating principle, such as linear or rotary actuators.**3)Pneumatic actuators:** These actuators use compressed air or gas to generate mechanical motion or force. They can be classified based on their operating principle, such as diaphragm or piston actuators.**4)Piezoelectric actuators:** These actuators use the piezoelectric effect to generate mechanical motion or force. They can be classified based on their operating principle, such as stack or bimorph actuators.**5)Shape memory alloy actuators:** These actuators use shape memory alloys, such as Nitinol, to generate mechanical motion or force.**Based on the application domain:Industrial actuators:** These actuators are used in manufacturing and industrial processes, such as robotics, machine tools, and assembly lines.**Aerospace actuators:** These actuators are used in aircraft and spacecraft systems, such as control surfaces, landing gear, and engine controls.**Automotive actuators: T**hese actuators are used in vehicles, such as power windows, door locks, and steering systems.**Medical actuators:** These actuators are used in medical devices and equipment, such as surgical robots, prosthetic limbs, and insulin pumps.**Consumer actuators:** These actuators are used in consumer products, such as home appliances, gaming controllers, and toys.

**Q)Smart object trends**

Ans. Smart objects are physical objects that are embedded with sensors, processors, and communication capabilities, allowing them to collect and exchange data with other devices and systems. Here are some current trends in smart object development:

**1)Internet of Things (IoT) connectivity:** Smart objects are increasingly being designed to connect to the internet and other IoT devices, enabling them to exchange data and communicate with other systems.**2) (AI) integration:** Smart objects are being designed to incorporate AI algorithms and machine learning capabilities, allowing them to learn from data and improve their functionality over time. This can lead to more efficient and effective operation, as well as more personalized user experiences.**3)Edge computing**: Smart objects are being designed to incorporate edge computing capabilities, allowing them to perform data processing and analysis locally rather than sending all data to the cloud. This can lead to faster response times and reduced data transfer costs.**4)Energy efficiency:** Smart objects are being designed with energy efficiency in mind, using low-power sensors and communication protocols to reduce their energy consumption. This allows for longer battery life and reduced environmental impact.

**5)Wearable technology:** Smart objects are increasingly being designed as wearable devices, such as smartwatches, fitness trackers, and medical sensors. These devices allow for more personalized monitoring and feedback, as well as more convenient and unobtrusive operation.

**Q.Architecture of wireless sensor network**.Wireless sensor networks are made up of wirelessly connected smart objects, which are sometimes referred to as motes. The fact that there is no infrastructure to consider with WSNs is surely a powerful advantage for flexible deployments, but there are a variety of design constraints to consider with these wirelessly connected smart objects.

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. The fact that individual sensor nodes are typically so limited is a reason that they are often deployed in very large numbers. As the cost of sensor nodes continues to decline, the ability to deploy highly redundant sensors becomes increasingly feasible. Because many sensors are very inexpensive and correspondingly inaccurate, the ability to deploy smart objects redundantly allows for increased accuracy.Smart objects with limited processing, memory, power, and so on are often referred to as constrained nodes.**The architecture of a WSN consists of several components, including: Sensors**: The sensors are the primary component of the WSN. They are small devices that are equipped with sensors to measure physical parameters such as temperature, humidity, light, and sound. The sensors can also be equipped with processing and storage capabilities to perform local data processing and decision-making.**Wireless communication:** The sensors in a WSN communicate wirelessly with each other using various communication protocols, such as ZigBee, Bluetooth, or Wi-Fi. The communication can be either direct or multi-hop, where the data is transmitted through multiple sensors to reach the sink node.

**Sink node:** The sink node is a special type of node that acts as a gateway between the WSN and the external world. It is typically equipped with more processing power and storage than the regular sensors and is responsible for collecting data from the sensors, processing it, and transmitting it to an external device or system.

**Network topology:** The topology of a WSN can be either a star or a mesh. In a star topology, the sensors communicate directly with the sink node. In a mesh topology, the sensors communicate with each other to relay the data to the sink node.

**Power management:** The sensors in a WSN are typically battery-powered and have limited energy resources. Therefore, power management is a critical aspect of WSN architecture. Techniques such as duty cycling, sleep scheduling, and energy harvesting are used to optimize power consumption and prolong the battery life of the sensors.

**Data management:** The data generated by the sensors in a WSN can be massive and unstructured. Therefore, efficient data management techniques such as compression, aggregation, and filtering are used to reduce the amount of data transmitted and improve network efficiency.

**SCADA**

Supervisory Control And Data Acquisition (SCADA) is a control system arda comprising computers, networked data communications and graphical user interfaces (GUI) for high process supervision, control and data acquisition in manufacturing plants and other industrial sectors

SCADA systems have the following major components.

**1. Facility and equipment sensors and actuators:** There could be several sensors and actuators spread tens plant site for collecting data and controlling various facilities and equipment. These sensors and aches monitor and control temperature, pressure, voltage, current, speed, humidity and probably anytings appropriate.

**2. Programmable Logic Controllers (PLC) :** PLCs are connected to sensors and actuators. They collect data fume and provide control inputs to actuators. PLCs are cheap and provide flexible and programmable funcial typically have a high speed connection to the SCADA server and thus help you to collect and visualise data it m time. You could have several PLCs deployed at a site. A site may or may not use PLCs but only RTUs.

**3. Remote Terminal Units (RTU)** : RTUs are connected to sensors and actuators. They collect data from sess may optionally provide control inputs to actuators. Note here that RTUs and PLCs have several common faces However, RTUs are often considered for collecting sensor data over large geographical areas (where there= continuous power) and they use wireless communication.PLCs are commonly implemented in situations where local control is needed as they are designed for maltiple inputs and outputs. RTUs are often used for remote plant sites. You could have several RTUs deployed at a site. A site may or may not use RTUs but only PLCs.

**4.SCADA Network:** SCADA network may utilise radio, telephone lines, fibre, cable, satellites or other communication mechanisms as appropriate. It allows the transfer of information and data back and forth between the SCADA server and the RTUs or PLCs.

**5. SCADA Server (or Master Terminal Unit)**: SCADA server controls the overall plant operations. It is also called as contro! server. It collects data from RTUs and PLCs, stores it, processes it and provides control mechanisms to regulate actuators through RTUs or PLCs. The server software is programmed to tell the system what and when to monitor, what parameter ranges are acceptable, and what response to initiate when parameters change outside acceptable values.

**6. Human-Machine Interface (HMI):** This could be a single monitor or workstation or could be several depending on the plant size and monitoring and controlling requirements. A user can visually monitor the overall operations in realtime and type commands to send to the RTUs or PLCs via the server. A single interface could be connected to multiple servers or multiple interfaces can show several data points from a single server.

**Distributed Network Protocol 3 (DNP3) i**s a set of communications protocols used between components in process automation systems. Its main use is in utilities such as electric and water companies. Like many of the other SCADA protocols, DNP3 is based on a master/slave relationship. The term master in this case refers to what is typically a powerful computer located in the control center of a utility, and a slave is a remote device with computing resources found in a location such as a substation. DNP3 refers to slaves specifically as outstations.

Outstations monitor and collect data from devices that indicate their state, such as whether a circuit breaker is on or off, and take measurements, including voltage, current, temperature, and so on. This data is then transmitted to the master when it is requested, or events and alarms can be sent in an asynchronous manner. The master also Issues control commands, such as to start a motor or reset a circuit breaker and logs the incoming data.

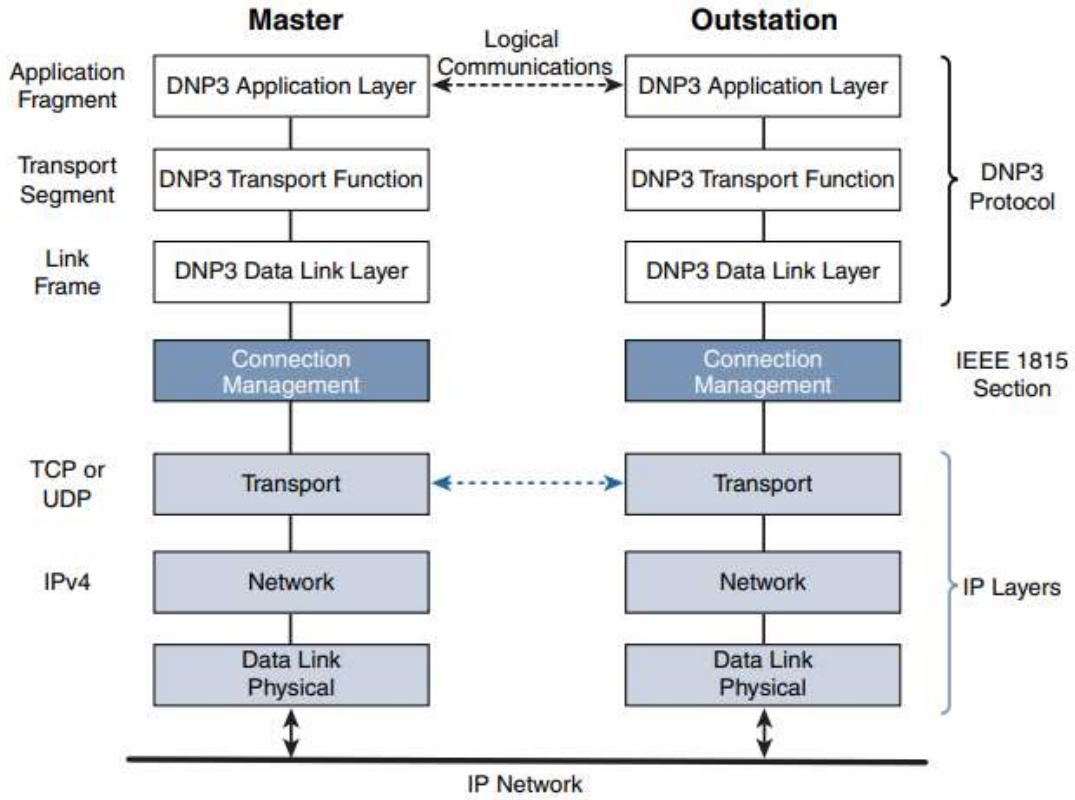


**Figure 6-2** *Protocol Stack for Transporting Serial DNP3 SCADA over IP*

**Q. What is coap ?**

Ans. Constrained Application Protocol (CoAP) resulted from the IETF Constrained RESTful Environments (CoRE) working group's efforts to develop a generic framework for resource-oriented applications targeting constrained nodes and networks. (For more information on the IETF CoRE working group, see https://datatracker.ietf.org/wg/ core/charter/.) Constrained nodes and networks are discussed in Chapter 5. The CoAP framework defines simple and flexible ways to manipulate sensors and actuators for data or device management. The IETF CoRE working group has published multiple standards-track specifications for CoAP, including the following:

■ RFC 6690: Constrained RESTful Environments (CoRE) Link Format

■ RFC 7252: The Constrained Application Protocol (CoAP)

■ RFC 7641: Observing Resources in the Constrained Application Protocol (CoAP)

■ RFC 7959: Block-Wise Transfers in the Constrained Application Protocol (CoAP)

■ RFC 8075: Guidelines for Mapping Implementations: HTTP to the Constrained Application Protocol (CoAP).

The CoAP messaging model is primarily designed to facilitate the exchange of messages over UDP between endpoints, including the secure transport protocol Datagram Transport Layer Security (DTLS). (UDP is discussed earlier in this chapter.) The IETF CoRE working group is studying alternate transport mechanisms, including TCP, secure TLS, and WebSocket. CoAP over Short Message Service (SMS) as defined in Open Mobile Alliance for Lightweight Machine-to-Machine (LWM2M) for IoT device management is also being considered. (For more information on the Open Mobile Alliance, see http://openmobilealliance.org.) RFC 7252 provides more details on securing CoAP with DTLS.

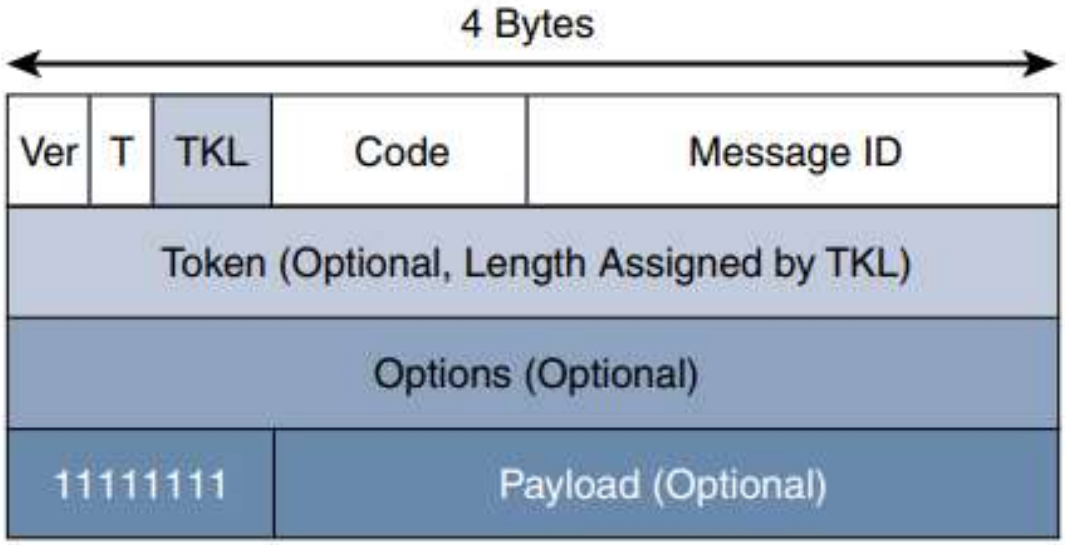


**Figure 6-7** *CoAP Message Format*

**Table 6-1** *CoAP Message Fields*

| CoAP Message Field | Description |
|---|---|
| Ver (Version) | Identifies the CoAP version. |
| T (Type) | Defines one of the following four message types: Confirmable (CON), Non-confirmable (NON), Acknowledgement (ACK), or Reset (RST). CON and ACK are highlighted in more detail in Figure 6-9. |
| TKL (Token Length) | Specifies the size (0–8 Bytes) of the Token field. |
| Code | Indicates the request method for a request message and a response code for a response message. For example, in Figure 6-9, GET is the request method, and 2.05 is the response code. For a complete list of values for this field, refer to RFC 7252. |
| Message ID | Detects message duplication and used to match ACK and RST message types to Con and NON message types. |
| Token | With a length specified by TKL, correlates requests and responses. |
| Options | Specifies option number, length, and option value. Capabilities provided by the Options field include specifying the target resource of a request and proxy functions. |
| Payload | Carries the CoAP application data. This field is optional, but when it is present, a single byte of all 1s (0xFF) precedes the payload. The purpose of this byte is to delineate the end of the Options field and the beginning of Payload. |

CoAP can run over IPv4 or IPv6. However, it is recommended that the message fit within a single IP packet and UDP payload to avoid fragmentation. For IPv6, with the default MTU size being 1280 bytes and allowing for no fragmentation across nodes, the maximum CoAP message size could be up to 1152 bytes, including 1024 bytes for the payload. In the case of IPv4, as IP fragmentation may exist across the network, implementations should limit themselves to more conservative values and set the IPv4 Don't Fragment (DF) bit. While most sensor and actuator traffic utilizes small-packet payloads, some use cases, such as firmware upgrades, require the capability to send larger payloads. CoAP doesn't rely on IP fragmentation but defines (in RFC 7959) a pair of Block options for transferring multiple blocks of information from a resource representation in multiple request/ response pairs. As illustrated in Figure 6-8, CoAP communications across an IoT infrastructure can take various paths. Connections can be between devices located on the same or different constrained networks or between devices and generic Internet or cloud servers, all operating over IP. Proxy mechanisms are also defined, and RFC 7252 details a basic HTTP mapping for CoAP. As both HTTP and CoAP are IP-based protocols, the proxy function can be located practically anywhere in the network, not necessarily at the border between constrained and non-constrained networks. As illustrated in Figure 6-8, CoAP communications across an IoT infrastructure can take various paths. Connections can be between devices located on the same or different constrained networks or between devices and generic Internet or cloud servers, all operating over IP. Proxy mechanisms are also defined, and RFC 7252 details a basic HTTP mapping for CoAP. As both HTTP and CoAP are IP-based protocols, the proxy function can be located practically anywhere in the network, not necessarily at the border between constrained and non-constrained networks.

Just like HTTP, CoAP is based on the REST architecture, but with a “thing” acting as both the client and the server. Through the exchange of asynchronous messages, a client requests an action via a method code on a server resource. A uniform resource identifier (URI) localized on the server identifies this resource. The server responds with a response code that may include a resource representation. The CoAP request/response semantics include the methods GET, POST, PUT, and DELETE

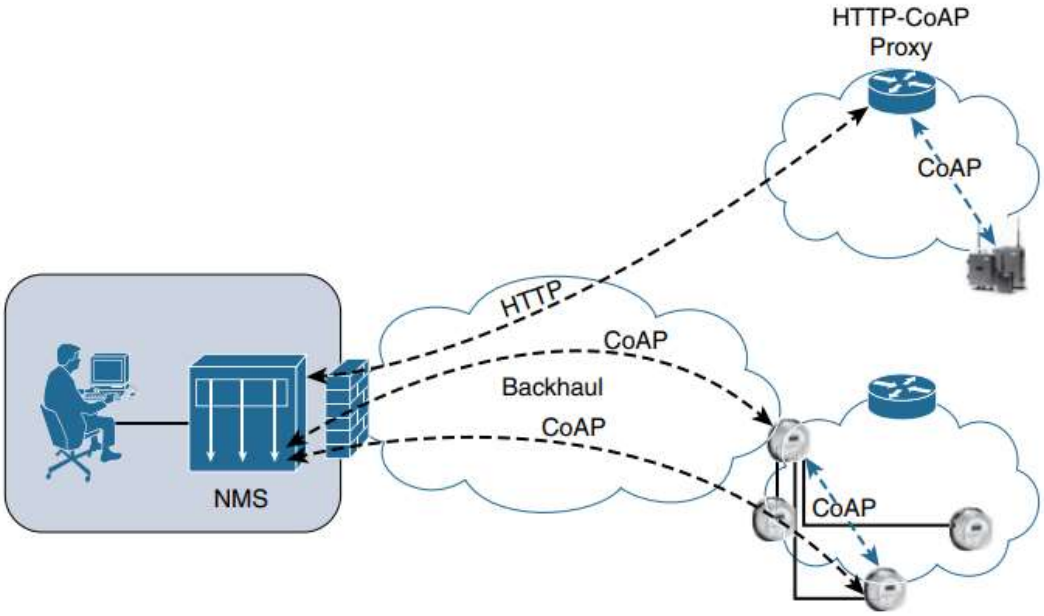


**Figure 6-8** *CoAP Communications in IoT Infrastructures*

**What is mqtt ?**

An MQTT client can act as a publisher to send data (or resource information) to an MQTT server acting as an MQTT message broker. In the example illustrated in Figure 6-10, the MQTT client on the left side is a temperature (Temp) and relative humidity (RH) sensor that publishes its Temp/RH data. The MQTT server (or message broker) accepts the network connection along with application messages, such as Temp/RH data, from the publishers. It also handles the subscription and unsubscription process and pushes the application data to MQTT clients acting as subscribers. The application on the right side of Figure 6-10 is an MQTT client that is a subscriber to the Temp/RH data being generated by the publisher or sensor on the left. This model, where subscribers express a desire to receive information from publishers, is well known. A great example is the collaboration and social networking application Twitter. With MQTT, clients can subscribe to all data (using a wildcard character) or specific data from the information tree of a publisher. In addition, the presence of a message broker in MQTT decouples the data transmission between clients acting as publishers and subscribers. In fact, publishers and subscribers do not even know (or need to know) about each other. A benefit of having this decoupling is that the MQTT message broker ensures that information can be buffered and cached in case of network failures. This also means that publishers and subscribers do not have to be online at the same time. MQTT control packets run over a TCP transport using port 1883. TCP ensures an ordered, lossless stream of bytes between the MQTT client and the MQTT server. Optionally, MQTT can be secured using TLS on port 8883, and WebSocket (defined in RFC 6455) can also be used. MQTT is a lightweight protocol because each control packet consists of a 2-byte fixed header with optional variable header fields and optional payload. You should note that a control packet can contain a payload up to 256 MB. Figure 6-11 provides an overview of the MQTT message format.

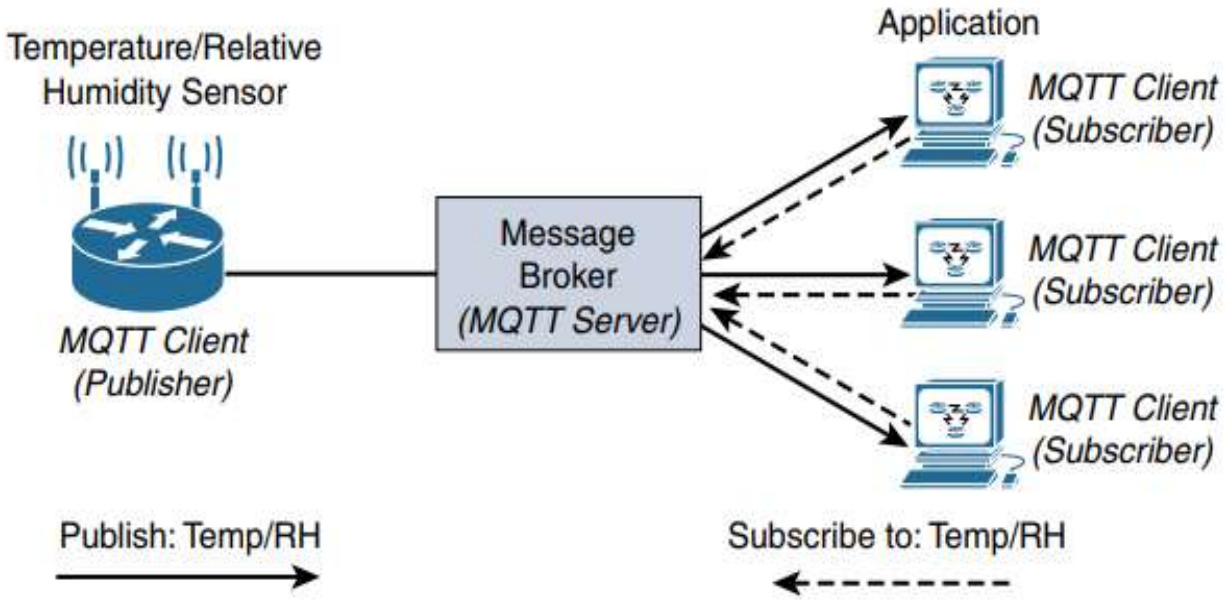


**Figure 6-10** *MQTT Publish/Subscribe Framework*

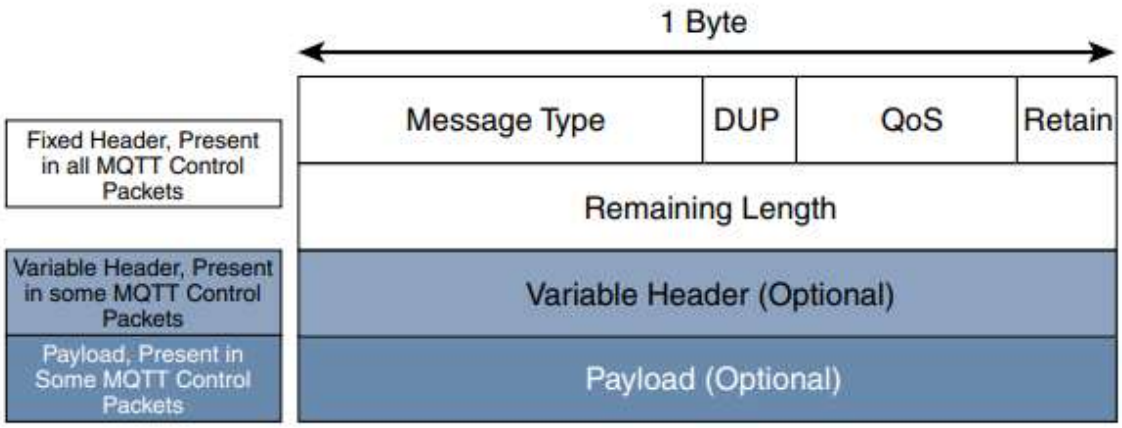


**Figure 6-11** *MQTT Message Format*

Compared to the CoAP message format in Figure 6-7, you can see that MQTT contains a smaller header of 2 bytes compared to 4 bytes for CoAP. The first MQTT field in the header is Message Type, which identifies the kind of MQTT packet within a message. Fourteen different types of control packets are specified in MQTT version 3.1.1. Each of them has a unique value that is coded into the Message Type field.

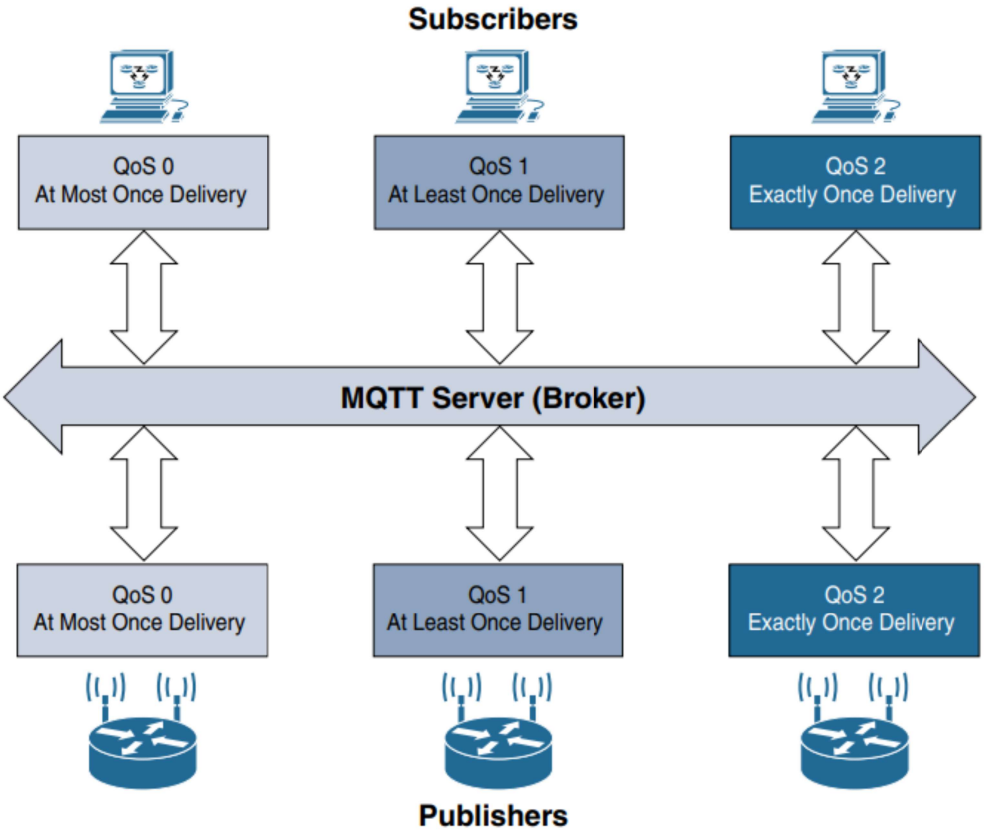


**Figure 6-13** *MQTT QoS Flows*

These are the three levels of MQTT QoS:

■ QoS 0: This is a best-effort and unacknowledged data service referred to as “at most once” delivery. The publisher sends its message one time to a server, which transmits it once to the subscribers. No response is sent by the receiver, and no retry is performed by the sender. The message arrives at the receiver either once or not at all.

■ QoS 1: This QoS level ensures that the message delivery between the publisher and server and then between the server and subscribers occurs at least once. In PUBLISH and PUBACK packets, a packet identifier is included in the variable header. If the message is not acknowledged by a PUBACK packet, it is sent again. This level guarantees “at least once” delivery.

■ QoS 2: This is the highest QoS level, used when neither loss nor duplication of messages is acceptable. There is an increased overhead associated with this QoS level because each packet contains an optional variable header with a packet identifier. Confirming the receipt of a PUBLISH message requires a two-step acknowledgement process

**Q..DIFFERENCE BETWEEN COAP AND MQTT**

**Table 6-3** *Comparison Between CoAP and MQTT*

| Factor | CoAP | MQTT |
|---|---|---|
| Main transport protocol | UDP | TCP |
| Typical messaging | Request/response | Publish/subscribe |
| Effectiveness in LLNs | Excellent | Low/fair (Implementations pairing UDP with MQTT are better for LLNs.) |
| Security | DTLS | SSL/TLS |
| Communication model | One-to-one | many-to-many |
| Strengths | Lightweight and fast, with low overhead, and suitable for constrained networks; uses a RESTful model that is easy to code to; easy to parse and process for constrained devices; support for multicasting; asynchronous and synchronous messages | TCP and multiple QoS options provide robust communications; simple management and scalability using a broker architecture |
| Weaknesses | Not as reliable as TCP-based MQTT, so the application must ensure reliability. | Higher overhead for constrained devices and networks; TCP connections can drain low-power devices; no multicasting support |

**ARDUINO**

Arduino is an open-source platform used for building electronics projects. Arduino consists of both a physical programmable circuit board (often referred to as a microcontroller) and a piece of software, or IDE (Integrated Development Environment) that runs on your computer, used to write and upload computer code to the physical board.The Arduino platform has become quite popular with people just starting out with electronics, and for good reason.
• Unlike most previous programmable circuit boards, the Arduino does not need a separate piece of hardware (called a programmer) in order to load new code onto the board - you can simply use a USB cable. Additionally, the Arduino IDE uses a sins lifted airs. you
C++, making it easier to learn to program. Finally, Arduino provides a standard form factor that breaks out the functions of the micro-controller into a more accessible package.

**IOREF** This provides a logic reference voltage for shields that use it. It is connected to the 5V bus. Use to reset the Arduino board.
**RESET** Used to reset the arduino board
**3.3 V** Power supply
**5 V** Power supply
**GND** Ground pin. In the Arduino Uno pinout, you can find 5 GND pins, which are all interconnected.
**VIN** This pin is used to power the Arduino Uno board using an external power source.
**AO – A5** Analog Input Pins. The Arduino Uno has 6 analog pins, which utilize ADC (Analog to Digital converter). These pins serve as analog inputs but can also function as digital inputs or digital outputs.
**AREF** Analog Reference pin
**Digital Pins 2-13** Digital I/0. Pins 3,5,6,9,10,11 (marked with ~) have PWM capability. Pulse Width Modulation (PWM) is a modulation technique used to encode a message into a pulsing signal.
**Digital Pins 0-**
**1/Serial In/Out -**
**TX/RX**
These pins cannot be used for Digital I/O but for serial 1/0. Serial communication is used to exchange data between the Arduino board and another serial device such as computers, displays, sensors and more. Each Arduino board has at least one serial port.

**ESP32**

ESP32 is a series of low cost, low power system on a chip microcontrollers with integrated Wi-Fi & dual-mode Bluetooth. The ESP32 series employs a Tensilica Xtensa [X6 microprocessor in both dual-core and single-core variations.
ESP32 is created and developed by Espressif Systems, a Shanghai-based Chinese
ESP8266 micro controller.
company, and is manufactured by TSMC using their 40 nm process. It is a successor to the
M 6.2 FEATURES OF THE ESP32 INCLUDE THE FOLLOWING
GQ. Explain features of ESP 32.
.CPU: Xtensa Dual-Core 32-bit LX6 microprocessor, operating at 160 or 240 MHz and performing at up to 600 DMIPS
• Memory: 520 KiB SRAM
Wireless connectivity:
+ Wi-Fi: 802.11 b/g/n/e/i
+ Bluetooth: v4.2 BR/EDR and BLE
•Peripheral interfaces:
+ 12-bit SAR ADC up to 18 channels
+ 2 × 8-bit DACs
+ 10 × touch sensors
+ Temperature sensor
+4 × SPI
+ 2 × 12S

+ 2 × PC
+ 3 × UART
+ SD/SDIO/MMC host
+ Slave (SDIO/SPI)
+ Ethernet MAC interface with dedicated DMA and IBBE 1588 support
+ CAN bus 2.0
+ IR (TX/RX)
+ Motor PWM
+ LED PWM up to 16 channels
+ Hall effect sensor
+ Ultra low power analog pre-amplifier

**RASBERRY PI**

The Raspberry Pi is a series of small single.-board computers developed in the United Kingdom by the Raspberry Pi Foundation to promote teaching of baste connuter seience in schools and in developing countries

Features:

**1. Powerful yet small footprint**: The Raspberry Pi is a low cost, credit-card sized computer that plugs into a computer monitor or TV and uses a standard keyboard and mouse. It is capable of doing everything that you would expect a desktop computer to do, from browsing the internet and playing high-definition video, to making spreadsheets, word-processing, and playing games. Despite such capabilities, it has an extremely small footprint.**2.Low cost:** Raspberry Pi is a low cost device ranging anywhere between R$ 2,000 to Rs. 5,000 depending upon various specifications that you desire. This makes it very preferable for running educational projects, research projects, low cost loT devices, hobby projects or anything else that you wish to experiment with. It Is not cost prohibitive and hence makes an excellent choice for wide use cases. **3. Highly programmable**: Raspberry Pi has several interfaces and GPIO (General Purpose Input Output) pins that makes if highly programmable for various use cases and requirements. You could connect external sensors, actuators, LED lights and other peripherals and boards as desired. It provides several modules that can be used to extend the functionality of the device further. For example, if you are building an loT device that requires a camera to be connected to the device, you can do so.**4. Ease of application development:** Raspberry Pi supports various operating systems and programming languages that makes it an excellent choice for application development.**5.Several connectivity options:** Raspberry Pi provides various connectivity options such as ethernet, WI-Fi, USB, HDMI, and Bluetooth. You can also plug-in external modules to further enrich the connectivity options. This ensures that your loT device can be easily connected to the desired network or other devices.**6 Community Support**: Raspberry Pi is extremely popular in the user community. You get support from not only the Raspberry Pi organisation for your queries but also you could ask your questions and discuss solutions in these well-established communities. This level of support could be really crucial to ensure that you are not left alone when you need help.

**Beagle Board** offers credit-card sized computers under the Beagle Bone brand name. they are based on open source specifications.

.The boards are low-cost, fan-less single-board computers based on low-power Texas Instruments processors featartag

the ARM Cortex-A series core.

•Like Raspberry Pi, these boards could provide a full-fledged computer like experience. It enables simplified physical computing on advanced GUI-enabled and networked-enabled devices.

•It provides ease of application development through simplified learning experience and support for various development environments. Some of the OS that it supports are Ubuntu, QNX, Windows Embedded and Android

•Following are some of the common applications that you could develop.

• Low-cost Linux PC

Network-connected digital signage

• Game console

° LCD-to-picture-frame conversion kit

• Web services development

• Google Talk video phone

**.IOT FUNCTIONAL STACK**

The Core loT Functional Stack represents the three layers that simplify the loT architecture into its most foundational building blocks. Each block in the stack could be further expanded based on the technologies you choose to implement de stack For example, as you understand, there are several networking protocols that could be used in loT systems. The eats OSt layer itself has seven layers that cover the various aspects of networking. Similarly, the bottom most layer of The Care loT Functional Stack could have various types of sensors and actuators connected through various mechanisms and protocols.

The three layers are further explained as following.

**1."Things" Layer**: At this layer, the physical devices (sensors and actuators) are used as per the constraints of the environment in which they are deployed.

The physical devices carry out tasks such as information collection (through sensors) and taking actions (through actuators). Today, there are thousands of physical devices that could be used as per your requirements. They come in varlety of types, shapes, functionalities, and operate using various protocols and mechanisms. You will learn more
about them in the subsequent chapters.

**2.Communications Network Layer:** Communication layer is the heart of any loT system. This is the layer that actually connects the physical devices to the external network and make them really "smart" and accessible over different networks. The communication network layer could use either wired or wireless medium to connect the physical devices to the network. However, wireless technologies are more common for loT systems. This layer could have four sublayers as following.

**(a)Access network sublayer:** Access network sublayer connects physical devices to the network The physical devices could be directly accessed and operated using the access network sublayer. It is usually based off the wireless technologies such as WI-FI, ZigBee and Bluetooth. However, note here that the physical devices could also have this layer connected through the wired medium. For example, you could turn on a smart bulb in your home using home WI-FI network.

**(b) Gateways and backhaul network sublayer:** The various access network sublayer endpoints could be connected to a common communication system called a gateway.

The devices on the same network (subnet) could talk to each other without the gateway. But, if the devices need to connect to other networks than its own network, then a gateway is required. For example, you can connect two phones, in close proximity, over Bluetooth and send data. But, if you need to send the data to a different phone, which is not in the local proximity, you will require to connect your phone to an external network, say a WI-FI, via a gateway. A common communication system organises multiple smart objects in a given area around a common gateway. The gateway communicates directly with the smart objects.

The role of the gateway is to forward the collected information through a longer-range medium (called the backhaul) to a central information processing station where the information is further processed through several applications. For example, if you want to remotely control your smart bulb at home, you would require a connection mechanism to control the bulb over cellular or WI-Fi network via an application that could connect you to the gateway setup at your home using which you can operate the bulb.

**(c) Network transport sublayer**: This sublayer refers to the OSI model layers 3 and 4 where IP, TCP and UDP protocols are used for sending and receiving the information.The "things" could send the information via the gateway and could receive the control and management instructions via the gateway. For example, a temperature sensor could periodically send (via the gateway) temperature data to the cloud based storage system or application for processing.

(d) loT network management sublayer: At this layer, additional networking protocols could be used to exchange data with "things using lower level protocols such as TCP and UDP. Some of the examples of such higher level protocols could be CoAP, DDS, AMQP, and MQTT.

**3. Application and Analytics Layer:** At this layer, there could be several applications that process, analyse, visualise, control, manage and report the collected data from "things".
You could build several useful applications based on your requirements. Some of the applications could just control, manage and operate the IoT systems while others could synthesise the collected information and generate meaningful reports and actionable insights.

**Micro-Electro-Mechanical Systems (MEMS)**
One of the most interesting advances in sensor and actuator technologies is in how they are packaged and deployed.
Micro-electro-mechanical systems (MEMS), sometimes simply referred to as micro-machines, can integrate and combine electric and mechanical elements, such as sensors and actuators, on a very small (millimetre or less) scale. One of the keys to this technology is a microfabrication technique that is similar to what is used for microelectronic integrated circuits. This approach allows mass production at very low costs. 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.
MEMS are made up of components between 1 and 100 micrometres in size (i.e., 0.001 to 0.1 mm), and MEMS devices generally range in size from 20 micrometres to a millimetre (i.e., 0.02 to 1.0 mm). They usually consist of a central unit that processes data (an integrated circuit chip such as microprocessor) and several components that interact with the surroundings (such as microsensors). MEMS devices have already been widely used in a variety of different applications and can be found in very familiar everyday devices. For example, inkjet printers use micropump MEMS. Smart phones also use MEMS technologies for things like accelerometers and gyroscopes. In fact, automobiles were among the first to commercially introduce MEMS into the mass market, with airbag accelerometers.

**RFID**
RFID basically has two components.
**1. RFID Tag:** RFID tag contains a circuit and an antenna. It contains the information that helps to identify and track the object. RFID tags could be active or passive. Active RFID tags have their own power source (such as a battery) whereas passive RFID tags are activated using external power source. You usually see passive RFID tags at shops where the tag gets activated when it comes near the RFID reader bars.
**2. RFID Reader:** RFID reader collects the information from the RFID tags and processes it as desired. It could be sounding alarms or sending the information further for tracking. For example, you can track the movement of wheelchair in a hospital and find out where exactly it is at a particular time.
1. The RFID reader continuously scans for radio signals.
2. As soon as a RF enabled tag comes near the reader, the reader activates the RF circuitry in the RF tag and extracts the information from it.
3. The extracted information is sent to the processing center which can carry out the desired actions such as sounding alarm, updating tracking database, sending emails or just reducing the inventory information. The processing center could run various applications (such as FASTag toll collection) and could make the appropriate use of the extracted information through RFID.

**Advantages of RFID**
1. RFID tags can store a good amount of information.2. RFID tags are re-writable.
3. RFID technology is robust and proven.4. RFID is cost-effective.
**Disadvantages of RFID**
1. RFID tags can be read by anyone with a RFID reader. Hence, there could be a privacy issue.
2. It might be labour intensive to program RFID tags and then attach to each object.
3. Any electromagnetic interference can interrupt the functioning of RFID.

**BLUETOOTH**

Bluetooth is one technology that probably requires no introduction. It is one of the most widely used technologie connecting devices for data transfer, remote control, audio / video streaming location services, and several ode Bluetooth-based new developments and use-cases such as Aarogya Setu app that was developed for contact tracing dog Covid-19.

Bluetooth is a short-range wireless technology standard that is used for exchanging data between fixed and mobi devices over short distances using UHF radio waves in the ISM bands, from 2.402 GHz to 2.48 GHz, and building Persed Area Networks (PANs).Bluetooth is managed by the Bluetooth Special Interest Group (SIG), which has more than 35.000 member companies in the areas of telecommunication, computing networking, and consumer electronics. The im standardised Bluetooth as IEEE 802.15.1, but no longer maintains the standard. The Bluetooth SIG oversees development the specification, manages the qualification program, and protects the trademarks.

**1. Bluetooth Classic :**The Bluetooth Classic radio, also referred to as Bluetooth Basic Rate/Enhanced Data Ba (BR/ED), is a low power radio that streams data over 79 channels in the 2.4GHz unlicensed Industrial, Scientic al Medical (ISM) frequency band. Supporting point-to-point device communication, Bluetooth Classic is mainly selF enable wireless audio streaming and has become the standard radio protocol behind wireless speakers, headpbes and in-car entertainment systems. The Bluetooth Classic radio also enables data transfer applications, including made printing.

**Bluetooth Low Enengy (LE)** iThe Bluetooth Low Energy (LB) radio is designed for very low power operation, Transmiting data over 40 channels in the 2.4CH# unlicensed ISM frequency band, the Bluetooth LE radio provides developers a tremendous amount of flexiblity to bulld products that meet the unique connectivity requirements of their market Bluetoth LE suppart hitsibly to buld prod topologies, expanding from point-to-point to broadease and, most recently, mesh, enabling Bluetooth technology to support the creation of reliable, large-scale device networks. While initially known for its device communications capabllities, Bluetooth LE is now also widely used as a device positioning technology to address the increasing demand for high accuracy indoor location services. Initially supporting simple presence and proximity capabilities, Bluetooth LE now supports Bluetooth Direction Finding and soon, high-accuracy distance measurement. Bluetooth LE is one of the most used technologies for loT devices and loT.

**NFC**

Near Field Communication (NFC) is a contactless communication technology based on a radio frequency (RF) field using a base frequency of 13.56 MHz. NFC technology is perfectly designed to exchange data between two devices through a simple touch gesture.

the RF held generated by an NFC Forum (compatible) device to communicate with an NFC Forum (compatible)tag has

the following three tasks.

**1. To transfer power from the NFC Forum Device to the NFC Forum Tag.** Therefore, the NFC Forum Tags dost net batteries or other power supplies for operation as the necessary power for communication is provided by the RF field.

This technology is also ideal for small loT devices acting as an NFC Forum Tag as no additional power is needed for the NFC communication.For Wireless Charging the primary goal of NFC Technology is to transfer power thus extending communication In this case NFC communication is used to regulate the power transfer. When Wireless Charging mode is active the feld strength of the RF field can be increased allowing a power transfer of up to 1 W.

**2. The NFC** device is sending information to an NFC Forum Tag by modulating the RF field signal (signal modulation!

**3. The NFC** device is receiving information from an NFC Forum Tag by sensing the modulation of the load generated by the NFC Forum tag (load modulation).

NFC technology is designed for an operation distance of a few centimetres. This makes it more difficult for attackers to record the communication between an NFC Forum Device and an NFC Forum Tag compared to other wireless technologies which have a working distance of several meters. In addition, the user of the NFC Forum Device determines by the touch gesture which entity the NFC communication should take place, which makes it more difficult for the attacker to get connected. As a result, the security level of the NFC communication is by default higher compared to other wireless communication protocols. Additionally, the NFC Forum has added Peer to Peer communication which is a mechanism to cipher all exchanged data to avoid that a spy can interpret recorded communication.