UNIT-II

IOT PROTOCOLS: Protocol Standardization for IoT – Efforts – M2M and WSN Protocols – SCADA and RFID Protocols – Issues with IoT Standardization – Unified Data Standards – Protocols – IEEE802.15.4–BACNet Protocol– Modbus – KNX – Zigbee– Network layer – APS layer – Security

---

Protocol Standardization for IoT

IoT communication protocols are modes of communication that protect and ensure optimum security to the data being exchanged between connected devices.

The IoT devices are typically connected to the Internet via an IP (Internet Protocol) network. However, devices such as Bluetooth and RFID allow IoT devices to connect locally. In these cases, there's a difference in power, range, and memory used. Connection through IP networks are comparatively complex, requiring increased memory and power from the IoT devices while the range is not a problem. On the other hand, non-IP networks demand comparatively less power and memory but have a range limitation.
As far as the IoT communication protocols or technologies are concerned, a mix of both IP and non-IP networks can be considered depending on usage.

Types of IoT ProtocolsTypes of IoT Protocols: IoT protocols and standards can be broadly classified into two separate categories.

1. **IoT Network Protocols:** IoT network protocols are used to connect devices over the network. These are the set of communication protocols typically used over the Internet. Using IoT network protocols, end-to-end data communication within the scope of the network is allowed. Following are the various IoT Network protocols:

- **HTTP (HyperText Transfer Protocol):** HyperText Transfer Protocol is the best example of IoT network protocol. This protocol has formed the foundation of data communication over the web. It is the most common protocol that is used for IoT devices when there is a lot of data to be published. However, the HTTP protocol is not preferred because of its cost, battery-life, energy saving, and more constraints.

  Additive manufacturing/3D printing is one of the use cases of the HTTP protocol. It enables computers to connect 3D printers in the network and print three-dimensional objects and pre-determined process prototypes.
- **LoRaWan (Long Range Wide Area Network):** It is a long-range low power protocol that provides signal detection below the noise level. LoRaWan connects battery operated things wirelessly to the Internet in either private or global networks. This communication protocol is mainly used by smart cities, where there are millions of devices that function with less power and memory. Smart street lighting is the practical use case of LoRaWan IoT protocol. The street lights can be connected to a LoRa gateway using this protocol. The gateway, in turn, connects to the cloud application that controls the intensity of light bulbs automatically based on the ambient lighting, which helps in reducing the power consumption during day-times.
- **Bluetooth:** Bluetooth is one of the most widely used protocols for short-range communication. It is a standard IoT protocol for wireless data transmission. This communication protocol is secure and perfect for short-range, low-power, low-cost, and wireless transmission between electronic devices. BLE (Bluetooth Low Energy) is a low-energy version of Bluetooth protocol that reduces the power consumption and plays an important role in connecting IoT devices. Bluetooth protocol is mostly used in smart wearables, smartphones, and other mobile devices, where small fragments of data can be exchanged without high power and memory. Offering ease of usage, Bluetooth tops the list of IoT device connectivity protocols.
- **ZigBee:** ZigBee is an IoT protocol that allows smart objects to work together. It is commonly used in home automation. More famous for industrial settings, ZigBee

is used with apps that support low-rate data transfer between short distances. Street lighting and electric meters in urban areas, which provides low power consumption, use the ZigBee communication protocol. It is also used with security systems and in smart homes.

2. **IoT Data Protocols:** IoT data protocols are used to connect low power IoT devices. These protocols provide point-to-point communication with the hardware at the user side without any Internet connection. Connectivity in IoT data protocols is through a wired or a cellular network. Some of the IoT data protocols are:
    - **Message Queue Telemetry Transport (MQTT):** One of the most preferred protocols for IoT devices, MQTT collects data from various electronic devices and supports remote device monitoring. It is a subscribe/publish protocol that runs over Transmission Control Protocol (TCP), which means it supports event-driven message exchange through wireless networks. MQTT is mainly used in devices which are economical and requires less power and memory. For instance, fire detectors, car sensors, smart watches, and apps for text-based messaging.
    - **Constrained Application Protocol (CoAP):** CoAP is an internet-utility protocol for restricted gadgets. Using this protocol, the client can send a request to the server and the server can send back the response to the client in HTTP. For light-weight implementation, it makes use of UDP (User Datagram Protocol) and reduces space usage. The protocol uses binary data format EXL (Efficient XML Interchanges). CoAP protocol is used mainly in automation, mobiles, and microcontrollers. The protocol sends a request to the application endpoints such as appliances at homes and sends back the response of services and resources in the application.
    - **Advanced Message Queuing Protocol (AMQP):** AMQP is a software layer protocol for message-oriented middleware environment that provides routing and queuing. It is used for reliable point-to-point connection and supports the seamless and secure exchange of data between the connected devices and the cloud. AMQP consists of three separate components namely Exchange, Message Queue, and Binding. All these three components ensure a secure and successful

exchange and storage of messages. It also helps in establishing the relationship of one message with the other. AMQP protocol is mainly used in the banking industry. Whenever a message is sent by a server, the protocol tracks the message until each message is delivered to the intended users/destinations without failure.

- **Machine-to-Machine (M2M) Communication Protocol:** It is an open industry protocol built to provide remote application management of IoT devices. M2M communication protocols are cost-effective and use public networks. It creates an environment where two machines communicate and exchange data. This protocol supports the self-monitoring of machines and allows the systems to adapt according to the changing environment. M2M communication protocols are used for smart homes, automated vehicle authentication, vending machines, and ATM machines.
- **Extensible Messaging and Presence Protocol (XMPP):** The XMPP is uniquely designed. It uses a push mechanism to exchange messages in real-time. XMPP is flexible and can integrate with the changes seamlessly. Developed using open XML (Extensible Markup Language), XMPP works as a presence indicator showing the availability status of the servers or devices transmitting or receiving messages. Other than the instant messaging apps such as Google Talk and WhatsApp, XMPP is also used in online gaming, news websites, and Voice over Internet Protocol (VoIP).

Issues with IoT Standardization

- **Platform:** This part includes the form and design of the products (UI/UX), analytics tools used to deal with the massive volume of data streaming from all products in a secure way, and scalability which means that wide adoption of protocols like IPv6 in all vertical and horizontal markets is needed.
- **Business Model:** The bottom line is a big motivation for starting, investing in, and operating any business; without a sound and solid business model for IoT we will have another bubble , this model must satisfy all the requirements for all kinds of e-commerce;

vertical markets, horizontal markets and consumer markets. But this category is always a victim of regulatory and legal scrutiny.

- **Killer Applications**: In this category there are three functions needed to have killer applications: control "things", collect "data", and analyze "data". IoT needs killer applications to drive the business model using a unified platform.
- **Security:** IoT encompasses everything from wireless communications, sensors, Radio-Frequency Identification (RFID) to Machine-to-Machine (M2M). However, the IoT industry is still unregulated, which has led to wider security and privacy implications. The ease with which IoT devices can be hacked, packet data sniffed and unsecured firmware can be modified, is alarming. Attacks are heterogeneous in nature and can occur at every layer of IoT's protocol stack. We need to have regulation, robust security mechanisms and stricter controls over authentication of devices that are connected to the Internet
- **Governance:** Effective governance within the IoT industry is an important consideration. Due to IoT's entry into almost every industry, malicious back-door passage led by vulnerable devices may not be immediately apparent, but it opens up new avenues of cyber attack on a much larger scale. Governance on an international level, such as rules, processes, procedures, audits, accountability and coherence are also currently non-existent in the IoT domain, due to the absence of general legislation in the IoT industry. Such levels of legislation at an industry, national and international level can be extremely helpful in aiding the organisations with improved efficiency and reliability of systems, as well as reduce the possibility of future errors. The involvement of heterogeneous technologies and the broad range of services used to support IoT, an effective governance plan is harder to achieve, but not impossible.
- **Connectivity:** Connecting billions of devices or things is a major challenge. Connectivity impacts the scale of business, profit margin, and societal impact of the operation. Though cloud-based deployments rule the IoT world, edge-based deployments are picking up due to (i) low latency, (ii) ease of deployment, (iii) better security and privacy, and (iv) high data aggregation.
- **Interoperability:** The IoT is growing in various directions, and different technologies are playing different roles. Today, Wireless Fidelity (WiFi), Zigbee, Long-Term Evolution

(LTE), LTE Advanced (LTE-A), Low-Power Wide Area Network (LPWAN), Bluetooth, etc., are some of the major communication technologies rule the IoT world. Seamless connectivity with different devices operating in different technologies is a major challenge. Interoperation at higher layers of the network protocol stack involving semantics, and domain-specific operations is another challenge.

- **IoT analytics:** The basic nature of the IoT is to obtain and to act on information. Therefore, IoT analytics play a major role. For practical deployment, placing the analytics platform in the IoT architecture is the major issue. Since information is generated or gathered at the devices and is communicated to the cloud with/without the support of edge, decision has to be taken such that parts of the analytics platform have to be deployed in appropriate places of the framework, i.e. whether at edge/fog or at the cloud. Factors such as delay, regulatory issues, cost, scale and ease of operation, etc., play significant roles on this.
- **Security and privacy:** It has been observed that IoT deployments are prone to security and privacy issues at device, edge, and cloud platform level. Therefore, security and privacy of the data, device, application, and the server are to be considered while deciding appropriate deployment architecture. Instead of considering security and privacy as afterthoughts of deployment, today, these are the prime concerns for any kind of deployment.
- **Business or return on investment (RoI):** Deployment decision can impact the vertical, horizontal, and consumer markets of IoT industry while struggling with the regulatory and legal aspects of the society. Based on the deployment usage and client base, IoT can be divided into (i) consumer IoT, which impacts the mass (like wellness, education, etc.) and the governance in the society; (ii) industrial IoT, which governs the communication framework of Industry 3.0 or Industry 4.0 scenarios; and (iii) commercial IoT, which includes retail and warehouse inventory controls, device tracking, health services, and so on.
- **Societal:** Societal challenges also play a major role in IoT deployment as IoT has to satisfy the customer, developer, and regulator needs of the society. This includes the mode of usage, the energy consumption, environmental impact, societal impact, etc.

M2M: Machine-to-Machine Communications

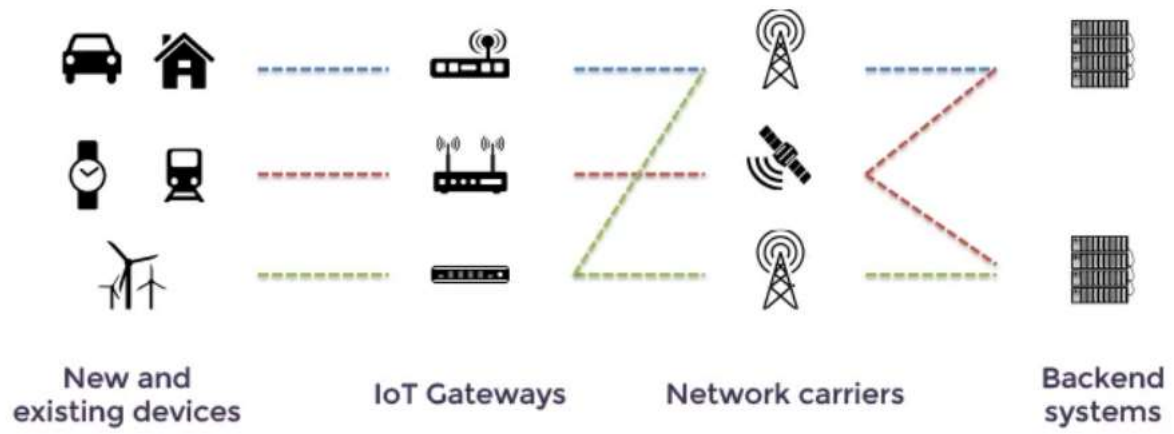
M2M stands for Machine to Machine communication. It is a direct communication system between the devices using wired or wireless communications channels without any human interaction. It collects the data and shares it with other connected devices. It is a technology that allows devices without the use of the internet to connect between devices. Various applications, such as defense, monitoring and tracking, production and facility management, are provided by M2M communications.

M2M technology may be present in offices, shopping malls, houses, and many other places. A common example of a machine to machine is controlling electrical devices like fans and bulbs using Bluetooth from the smartphone. Here, the smartphone and electrical devices are the two interacting devices with each other.

Key applications are :

- Connecting machines to other machines -e.g. Remote Production Environment
- Connecting machines to service centers — e.g. reporting maintenance issues

M2M protocols are well-defined architecture consisting of communication parameters and paradigm to exchange the data or information over the network. Each protocol defines the packet size, rules of communication, security over a network, communication requirements and other properties of the M2M network so that it will help to connect low powered, lossy devices to the world of the Internet. The structured communication scenario with system tools and processing devices at the various level of communication in IoT comprising M2M concept is well shown in the Figure.



Main Differences between the IoT and M2M:

Some of IoT and M2M differences are as follows:

- IoT is a subset of M2M technology. In IoT, the communication between two machines without human instruction, making it a part of the M2M communication system.
- The point-to-point communication of M2M is the main difference between M2M and IoT technology. Meanwhile, an IoT system usually locates its devices within a global cloud network that facilitates larger-scale automation and more advanced applications.
- Another key difference between IoT and M2M is scalability. IoT is designed to be highly scalable because devices may also be included in the network and integrated into existing networks with minimal issues. In contrast, maintaining and setting up M2M networks could also be more labor-intensive, as new point-to-point connections must be built for each system.

Protocols used in M2M:

1. **MQTT (Message Queuing Telemetry Transport) protocol:** MQTT stands for Message Queuing Telemetry Transport. MQTT is a machine to machine internet of things connectivity protocol. It is an extremely lightweight and publish-subscribe messaging transport protocol. This protocol is useful for the connection with the remote location where the bandwidth is a premium. These characteristics make it useful in various situations, including a constant environment such as for communication machine to machine and internet of things contexts. It is a publish and subscribe system where we can publish and receive the messages as a client. It makes it easy for communication

between multiple devices. It is a simple messaging protocol designed for the constrained devices and with low bandwidth, so it's a perfect solution for the internet of things applications.

Characteristics of MQTT

The MQTT has some unique features which are hardly found in other protocols. Some of the features of an MQTT are given below:

- It is a machine to machine protocol, i.e., it provides communication between the devices.
- It is designed as a simple and lightweight messaging protocol that uses a publish/subscribe system to exchange the information between the client and the server.
- It does not require that both the client and the server establish a connection at the same time.
- It provides faster data transmission, like how WhatsApp/messenger provides a faster delivery. It's a real-time messaging protocol.
- It allows the clients to subscribe to the narrow selection of topics so that they can receive the information they are looking for.

MQTT Architecture

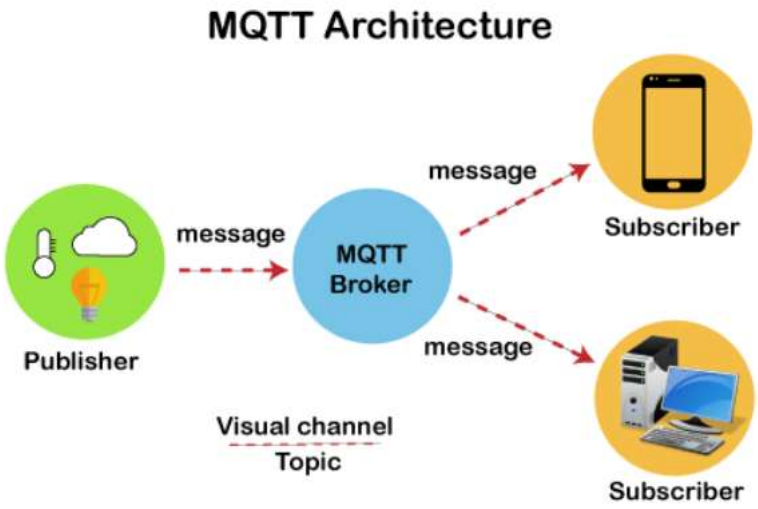
To understand the MQTT architecture, we first look at the components of the MQTT.

- **Message:** The message is the data that is carried out by the protocol across the network for the application. When the message is transmitted over the network, then the message contains the following parameters:
    - ❖ Payload data
    - ❖ Quality of Service (QoS)
    - ❖ Collection of Properties
    - ❖ Topic Name
- **Client:** In MQTT, the subscriber and publisher are the two roles of a client. The clients subscribe to the topics to publish and receive messages. In simple words, we can say that if any program or device uses an MQTT, then that device is referred to as a client. A device is a client if it opens the network connection to the server, publishes messages that other clients want to see, subscribes to the messages that it is interested in receiving, unsubscribes to the messages

that it is not interested in receiving, and closes the network connection to the server. In MQTT, the client performs two operations:

- **Publish:** When the client sends the data to the server, then we call this operation as a publish.
- **Subscribe:** When the client receives the data from the server, then we call this operation a subscription.

- **Server**: The device or a program that allows the client to publish the messages and subscribe to the messages. A server accepts the network connection from the client, accepts the messages from the client, processes the subscribe and unsubscribe requests, forwards the application messages to the client, and closes the network connection from the client.
- **TOPIC:** The label provided to the message is checked against the subscription known by the server as TOPIC.



Suppose a device has a temperature sensor and wants to send the rating to the server or the broker. If the phone or desktop application wishes to receive this temperature value on the other side, then there will be two things that happened. The publisher first defines the topic; for example, the temperature then publishes the message, i.e., the temperature's value. After

publishing the message, the phone or the desktop application on the other side will subscribe to the topic, i.e., temperature and then receive the published message, i.e., the value of the temperature. The server or the broker's role is to deliver the published message to the phone or the desktop application.

2. **CoAP:** Constrained Application Protocol (CoAP) is a specialized web transfer protocol for use with constrained nodes and constrained networks in the Internet of Things. CoAP is designed to enable simple, constrained devices to join the IoT even through constrained networks with low bandwidth and low availability. It is generally used for machine-to-machine (M2M) applications such as smart energy and building automation. The protocol was designed by the Internet Engineering Task Force (IETF)

CoAP is a customary client-server IoT protocol. It enables clients to make requests for web transfers as per the need of the hour. On the other hand, it also lets supporting servers to respond to arriving requests. In summary, devices' nodes in the IoT ecosystem are enabled to interact over through CoAP only.

CoAP and HTTP follow the same working procedure. However, CoAP attains its functionality via asynchronous transactions (using UDP). It utilizes the POST, GET, PUT, and DELETE calls.

Key traits of CoAP are:

- Works for devices in the same network types.
- Enables data transmission, to and fro, for the general internet-enabled nodes and network-connected devices.
- Works really fine for SMSs shared over mobile network connectivity.
- Suitable for internet-operative applications that use connected devices/sensors and have resource limitations.
- Capable of translating HTTP, supports multicast, and exerts the bare minimum cost burden.
- Only helps machines to communicate (in the network).

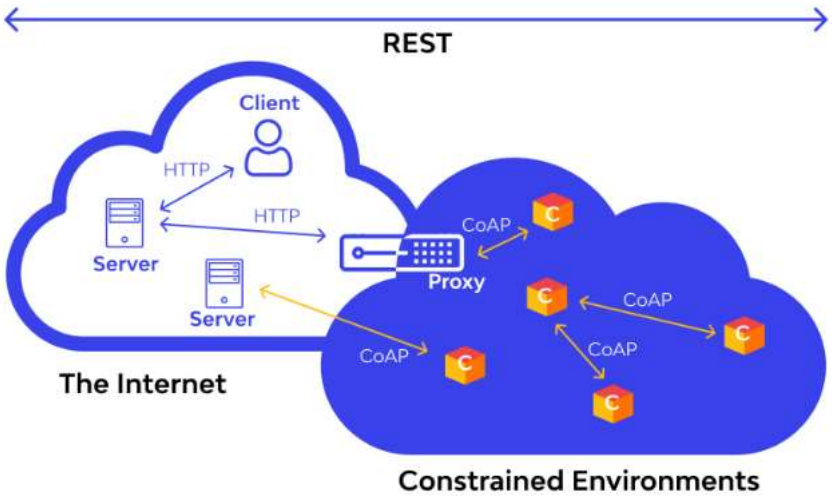
CoAP Architecture

The WWW and the constraints ecosystem are the 2 foundational elements of the CoAP protocol architecture. Here, the server monitors and helps in communication happening using CoAP and HTTP while proxy devices bridge the existing gap for these 2 ecosystem, making the communication smoother.

CoAP allows HTTP clients (also called CoAP clients here) to talk or exchange data/information with each other within resource constraints.

While one tries to understand this architecture, gaining acquaintances with some key terms is crucial:

- Endpoints are the nodes that host have knowledge of;
- Client sends requests and replies to incoming requests;
- Server gets and forwards requests. It also gets and forwards the messages received in response to the requests it had processed.
- Sender creates and sends the original message.
- Recipient gets the information sent by the client or forwarded by the server.



3. **OMA LWM2M :** Lightweight M2M is an open protocol from the Open Mobile Alliance (OMA) that is designed for addressing the needs of mobile low-power devices with very

little compute power. LWM2M is being adopted widely by telecom operators and is emerging as the standard protocol for device management and service enablement.

Use of LWM2M

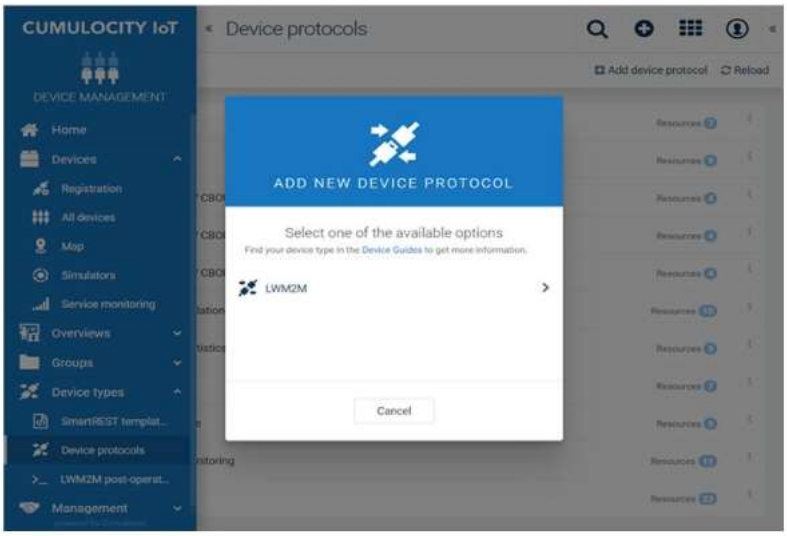
As the use of Internet of Things continues to grow so will the need to manage and use remote sensors and devices in areas with intermittent connectivity and situated far from power connections. LWM2M provides a standardized way to manage these devices and send telemetry data drawn in by the sensors quickly and cost effectively to the cloud.

LWM2M has been designed to reduce power and data usage for low-power devices, which are limited in processing power and bandwidth. The protocol is ideal when people or devices are a long way from power and need to use battery-powered local devices, have a SIM card and no power cord.

So sensors and devices can be managed centrally and viewed remotely, LWM2M defines a common language for the communication between devices and IoT platforms. With LWM2M, metadata (which describes the data) needed to understand the capabilities of a given device and interpret the data sent by the device is stored in a central repository in the cloud. This allows devices to minimize the transmission of data, so that only key data is sent. Saving bandwidth in particular for remote devices accelerates transmission, as well as reduces communication costs.

Sample use cases

Example uses include tracking shipper containers, cargo railways, farming where sensors monitor and optimize irrigation fertilization, smart cities, and water and energy metering. LWM2M is also used across telecommunications, the automotive industry, security devices, by utilities companies and in manufacturing.



No coding, easy-to-use integration with your LWM2M-enabled devices

Benefits of LWM2M

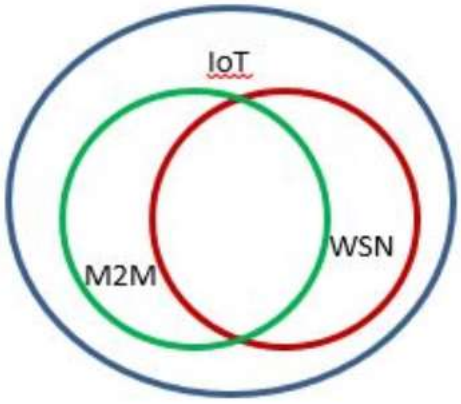
The Cumulocity IoT platform natively supports LWM2M as an IoT device management and service enablement protocol.

1. **Self-service, plug and play:** You can connect any LWM2M server and device without coding. Direct integration with LWM2M devices is quick and easy with our plug-and-play integration.
2. **Remote management:** Even though your devices are in hard-to-reach locations you need to be able to update the firmware and be aware of any issues. With its native integration, Cumulocity IoT provides firmware updates and monitoring capabilities out of the box and enables you to troubleshoot devices remotely.
3. **Easy-to-use interface to map with the Cumulocity IoT data model:** Cumulocity IoT's device management allows you to define which data you want to receive from the device and at which frequency. Additionally, you can integrate data from the device into your IoT application's domain model, allowing you to treat an LWM2M device in the same way as any other device connected to your Cumulocity IoT tenant.

WSNs: Wireless Sensor Networks

IoT configurations often involve sensors, which can be connected by wireless networks. Such sensor networks are termed "Wireless Sensor Networks" or WSNs. A WSN comprises spatially distributed autonomous devices equipped with sensors, connected through a wireless network to some type of gateway. The sensors typically monitor physical or environmental conditions. The gateway communicates with another set of devices that can act on the information from the sensors. Application examples include patient monitoring; environmental monitoring of air, water, and soil; structural monitoring for buildings and bridges; industrial machine monitoring; and process monitoring. The wireless network could be WiFi or Bluetooth, and the protocol one of the three listed above.

The boundaries between these networks are not clearly drawn, and in practice they overlap considerably. Figure 1 shows the relationship schematically:



WSN Protocols:

1. **WIFI:** WiFi stands for Wireless Fidelity. WiFiIt is based on the IEEE 802.11 family of standards and is primarily a local area networking (LAN) technology designed to provide in-building broadband coverage. Current WiFi systems support a peak physical-layer data rate of 54 Mbps and typically provide indoor coverage over a distance of 100 feet.
   WiFi has become the de facto standard for last mile broadband connectivity in homes, offices, and public hotspot locations. Systems can typically provide a coverage range of only about 1,000 feet from the access point.

WiFi offers remarkably higher peak data rates than do 3G systems, primarily since it operates over a larger 20 MHz bandwidth, but WiFiWiFi systems are not designed to support high-speed mobility. One significant advantage of WiFi over WiMAX and 3G is its wide availability of terminal devices. A vast majority of laptops shipped today have a built-in WiFi interface. WiFi interfaces are now also being built into a variety of devices, including personal data assistants (PDAs), cordless phones, cellular phones, cameras, and media players.

WiFi is Half Duplex

All WiFi networks are contention-based TDD systems, where the access point and the mobile stations all vie for use of the same channel. Because of the shared media operation, all WiFi networks are half duplex. There are equipment vendors who market WiFi mesh configurations, but those implementations incorporate technologies that are not defined in the standards.

WIFI – WORKING CONCEPTS

Radio Signals: Radio Signals are the keys, which make WiFi networking possible. These radio signals transmitted from WiFi antennas are picked up by WiFi receivers, such as computers and cell phones that are equipped with WiFi cards. Whenever a computer receives any of the signals within the range of a WiFi network, which is usually 300 — 500 feet for antennas, the WiFi card reads the signals and thus creates an internet connection between the user and the network without the use of a cord. Access points, consisting of antennas and routers, are the main source that transmit and receive radio waves. Antennas work stronger and have a longer radio transmission with a radius of 300-500 feet, which are used in public areas while the weaker yet effective router is more suitable for homes with a radio transmission of 100-150 feet.

2. **Bluetooth:** Bluetooth simply follows the principle of transmitting and receiving data using radio waves. It can be paired with the other device which has also Bluetooth but it should be within the estimated communication range to connect. When two devices start to share data, they form a network called piconet which can further accommodate more than five devices.

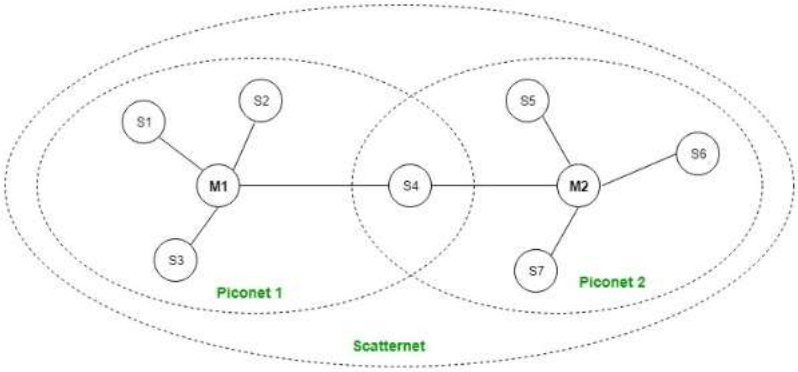
Points to remember for Bluetooth:

- Bluetooth Transmission capacity 720 kbps.
- Bluetooth is Wireless.
- Bluetooth is a Low-cost short-distance radio communications standard.
- Bluetooth is robust and flexible.
- Bluetooth is cable replacement technology that can be used to connect almost any device to any other device.
- The basic architecture unit of Bluetooth is a piconet.

Bluetooth Architecture:

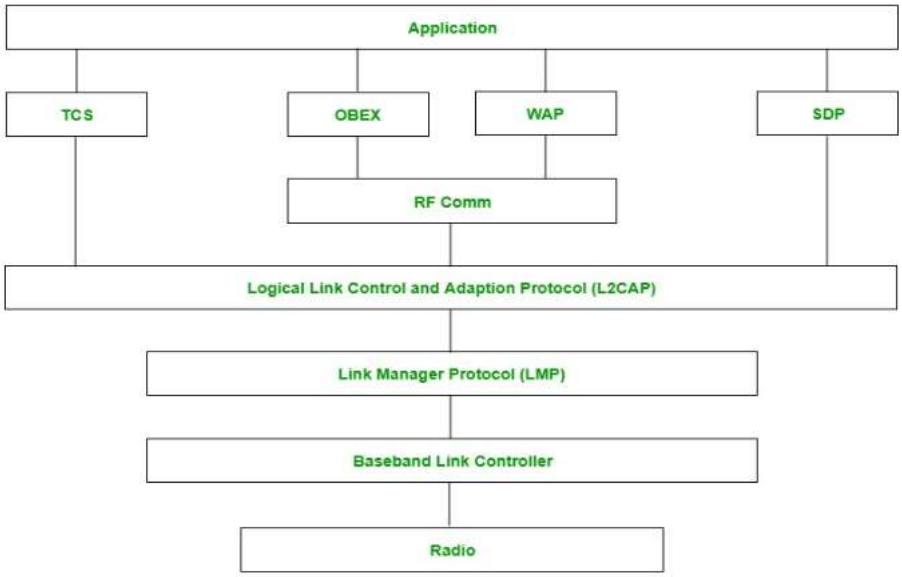
The architecture of Bluetooth defines two types of networks:

1. Piconet
2. Scatternet



Piconet: Piconet is a type of Bluetooth network that contains one primary node called the master node and seven active secondary nodes called slave nodes. Thus, we can say that there is a total of 8 active nodes which are present at a distance of 10 meters. The communication between the primary and secondary nodes can be one-to-one or one-to-many. Possible communication is only between the master and slave; Slave-slave communication is not possible. It also has 255 parked nodes, these are secondary nodes and cannot take participation in communication unless it gets converted to the active state.

Scatternet: It is formed by using various piconets. A slave that is present in one piconet can act as master or we can say primary in another piconet. This kind of node can receive a message from a master in one piconet and deliver the message to its slave in the other piconet where it is acting as a master. This type of node is referred to as a bridge node. A station cannot be mastered in two piconets.



Radio (RF) layer: It specifies the details of the air interface, including frequency, the use of frequency hopping and transmit power. It performs modulation/demodulation of the data into RF signals. It defines the physical characteristics of Bluetooth transceivers. It defines two types of physical links: connection-less and connection-oriented.

Baseband Link layer: The baseband is the digital engine of a Bluetooth system and is equivalent to the MAC sublayer in LANs. It performs the connection establishment within a piconet, addressing, packet format, timing and power control.

Link Manager protocol layer: It performs the management of the already established links which includes authentication and encryption processes. It is responsible for creating the links, monitoring their health, and terminating them gracefully upon command or failure.

Logical Link Control and Adaption (L2CAP) Protocol layer: It is also known as the heart of the Bluetooth protocol stack. It allows the communication between upper and lower layers of the Bluetooth protocol stack. It packages the data packets received from upper layers into the form expected by lower layers. It also performs segmentation and multiplexing.

Service Discovery Protocol (SDP) layer: It is short for Service Discovery Protocol. It allows discovering the services available on another Bluetooth-enabled device.

RF comm layer: It is a cabal replacement protocol. It is short for Radio Frontend Component. It provides a serial interface with WAP and OBEX. It also provides emulation of serial ports over the logical link control and adaption protocol(L2CAP). The protocol is based on the ETSI standard TS 07.10.

OBEX: It is short for Object Exchange. It is a communication protocol to exchange objects between 2 devices.

WAP: It is short for Wireless Access Protocol. It is used for internet access.

TCS: It is short for Telephony Control Protocol. It provides telephony service. The basic function of this layer is call control (setup & release) and group management for the gateway serving multiple devices.

Application layer: It enables the user to interact with the application.

Types of Bluetooth

Various types of Bluetooth are available in the market nowadays. Let us look at them.

In-Car Headset: One can make calls from the car speaker system without the use of mobile phones.

Stereo Headset: To listen to music in car or in music players at home.

Webcam: One can link the camera with the help of Bluetooth with their laptop or phone.

Bluetooth-equipped Printer: The printer can be used when connected via Bluetooth with mobile phone or laptop.

Bluetooth Global Positioning System (GPS): To use GPS in cars, one can connect their phone with car system via Bluetooth to fetch the directions of the address.

Advantage:

- It is a low-cost and easy-to-use device.
- It can also penetrate through walls.
- It creates an Ad-hoc connection immediately without any wires.
- It is used for voice and data transfer.

Disadvantages:

- It can be hacked and hence, less secure.
- It has a slow data transfer rate: of 3 Mbps.
- It has a small range: 10 meters.
- Bluetooth communication does not support routing.
- The issues of handoffs have not been addressed.

Applications:

- It can be used in laptops, and in wireless PCs, printers.
- It can be used in wireless headsets, wireless PANs, and LANs.
- It can connect a digital camera wirelessly to a mobile phone.
- It can transfer data in terms of videos, songs, photographs, or files from one cell phone to another cell phone or computer.
- It is used in the sectors of Medical health care, sports and fitness, Military.

3. Zigbee:

ZigBee is a Personal Area Network task group with low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensing the

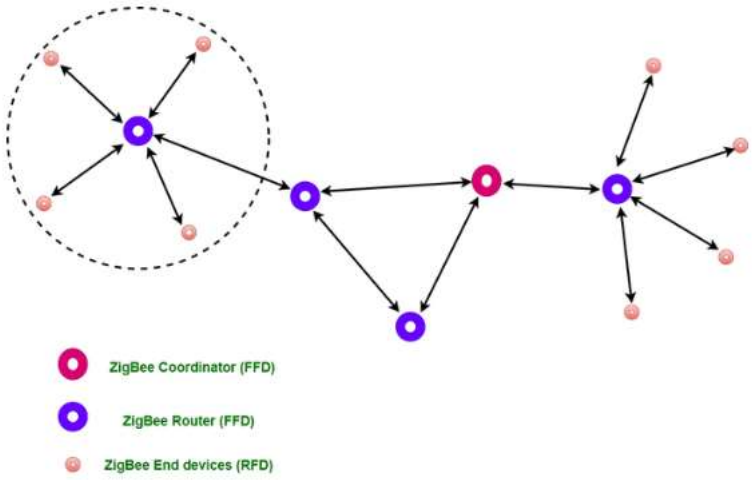
network. As we know that ZigBee is the Personal Area Network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.

ZigBee is an open, global, packet-based protocol designed to provide an easy-to-use architecture for secure, reliable, low power wireless networks. Flow or process control equipment can be place anywhere and still communicate with the rest of the system. It can also be moved, since the network doesn't care about the physical location of a sensor, pump or valve. ZigBee is a standard that addresses the need for very low-cost implementation of Low power devices with Low data rates for short-range wireless communications.

IEEE 802.15.4 supports star and peer-to-peer topologies. The ZigBee specification supports star and two kinds of peer-to-peer topologies, mesh and cluster tree. ZigBee-compliant devices are sometimes specified as supporting point-to-point and point-to-multipoint topologies.

Types of ZigBee Devices:

- Zigbee Coordinator Device: It communicates with routers. This device is used for connecting the devices.
- Zigbee Router: It is used for passing the data between devices.
- Zigbee End Device: It is the device that is going to be controlled.



General Characteristics of Zigbee Standard:

- Low Power Consumption

- Low Data Rate (20- 250 kbps)
- Short-Range (75-100 meters)
- Network Join Time (~ 30 msec)
- Support Small and Large Networks (up to 65000 devices (Theory); 240 devices (Practically))
- Low Cost of Products and Cheap Implementation (Open Source Protocol)
- Extremely low-duty cycle.
- 3 frequency bands with 27 channels.

Features of Zigbee:

1. Stochastic addressing: A device is assigned a random address and announced. Mechanism for address conflict resolution. Parents node don't need to maintain assigned address table.
2. Link Management: Each node maintains quality of links to neighbors. Link quality is used as link cost in routing.
3. Frequency Agility: Nodes experience interference report to channel manager, which then selects another channel
4. Asymmetric Link: Each node has different transmit power and sensitivity. Paths may be asymmetric.
5. Power Management: Routers and Coordinators use main power. End Devices use batteries.

Advantages of Zigbee:

Designed for low power consumption.

Provides network security and application support services operating on the top of IEEE.

Zigbee makes possible completely networks homes where all devices are able to communicate and be

Use in smart home

Easy implementation

Adequate security features.

Low cost: Zigbee chips and modules are relatively inexpensive, which makes it a cost-effective solution for IoT applications.

Mesh networking: Zigbee uses a mesh network topology, which allows for devices to communicate with each other without the need for a central hub or router. This makes it ideal for

use in smart home applications where devices need to communicate with each other and with a central control hub.

Reliability: Zigbee protocol is designed to be highly reliable, with robust mechanisms in place to ensure that data is delivered reliably even in adverse conditions.

Disadvantages of Zigbee :

Limited range: Zigbee has a relatively short range compared to other wireless communications protocols, which can make it less suitable for certain types of applications or for use in large buildings.

Limited data rate: Zigbee is designed for low-data-rate applications, which can make it less suitable for applications that require high-speed data transfer.

Interoperability: Zigbee is not as widely adopted as other IoT protocols, which can make it difficult to find devices that are compatible with each other.

Security: Zigbee's security features are not as robust as other IoT protocols, making it more vulnerable to hacking and other security threats.

Zigbee Network Topologies:

Star Topology (ZigBee Smart Energy): Consists of a coordinator and several end devices, end devices communicate only with the coordinator.

Mesh Topology (Self Healing Process): Mesh topology consists of one coordinator, several routers, and end devices.

Tree Topology: In this topology, the network consists of a central node which is a coordinator, several routers, and end devices. the function of the router is to extend the network coverage.

Architecture of Zigbee:

Zigbee architecture is a combination of 6 layers.

Application Layer

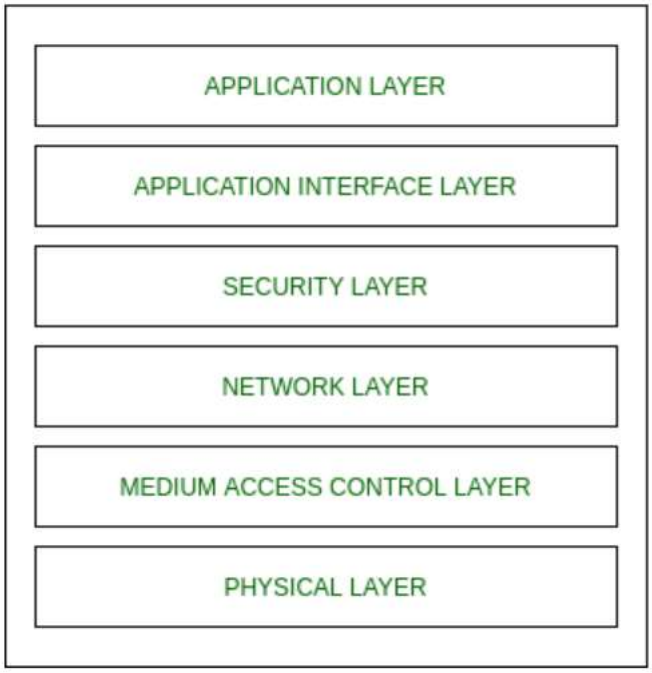
Application Interface Layer

Security Layer

Network Layer

Medium Access Control Layer

Physical Layer



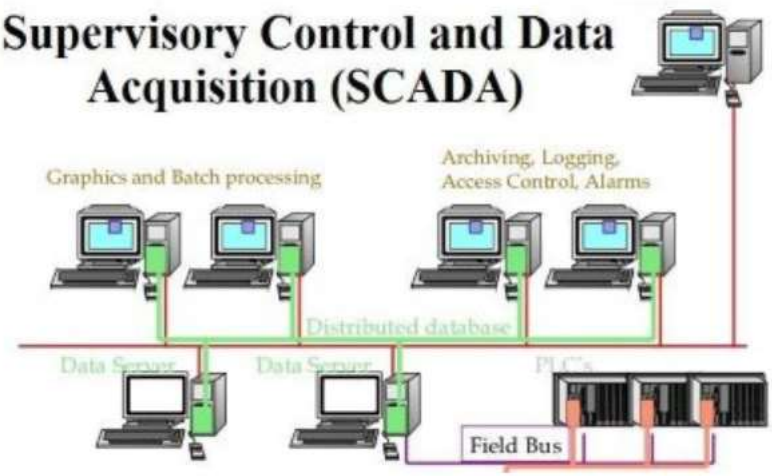
- Physical layer: The lowest two layers i.e the physical and the MAC (Medium Access Control) Layer are defined by the IEEE 802.15.4 specifications. The Physical layer is closest to the hardware and directly controls and communicates with the Zigbee radio. The physical layer translates the data packets in the over-the-air bits for transmission and vice-versa during the reception.
- Medium Access Control layer (MAC layer): The layer is responsible for the interface between the physical and network layer. The MAC layer is also responsible for providing PAN ID and also network discovery through beacon requests.
- Network layer: This layer acts as an interface between the MAC layer and the application layer. It is responsible for mesh networking.
- Application layer: The application layer in the Zigbee stack is the highest protocol layer and it consists of the application support sub-layer and Zigbee device object. It contains manufacturer-defined applications.
- Channel Access: Contention Based Method (Carrier-Sense Multiple Access With Collision Avoidance Mechanism) Contention Free Method (Coordinator dedicates a specific time slot to each device (Guaranteed Time Slot (GTS)))

Zigbee Applications:

- Home Automation
- Medical Data Collection
- Industrial Control Systems
- meter reading system
- light control system
- Commercial
- Government Markets Worldwide
- Home Networking

SCADA: Supervisory Control and Data Acquisition

It is a computer system designed to gather and analyze real-time data. It is used to control and monitor the equipment and manufacturing processes in various industries in different fields such as water and waste control, telecommunications, oil and gas refining, power generation, and transportation. SCADA systems were used for the first time in the 1960s.



It is also used by industrial organizations to accomplish the following tasks.

- To control industrial processes locally as well as at remote locations
- To monitor, gather and process real-time data
- To interact with devices such as sensors, valves, motors, pumps, and more using human-machine interface (HMI) software

- It comprises both software and hardware

How SCADA Systems Work:

Let us take an example of a leak on a pipeline. When a pipeline starts leaking, the SCADA system gathers information and forwards it to a central site and thus alerts the home station about the leak. It also analyses the situation, such as how big is the leak and how much water is being released.

A SCADA system can be very simple such as which are used to monitor the environmental conditions of a small office building or complex or can be very advanced such as which are used to monitor the activity in a nuclear power plant or the activity of a municipal water system.

SCADA Protocols:

1. **MODBUS:** MODBUS Protocol is a messaging structure, widely used to establish master-slave communication between intelligent devices. A MODBUS message sent from a master to a slave contains the address of the slave, the 'command' (e.g. 'read register' or 'write register'), the data, and a check sum (LRC or CRC). Since Modbus protocol is just a messaging structure, it is independent of the underlying physical layer. It is traditionally implemented using RS232, RS422, or RS485

   The Request: The function code in the request tells the addressed slave device what kind of action to perform. The data bytes contains any additional information that the slave will need to perform the function. For example, function code 03 will request the slave to read holding registers and respond with their contents. The data field must contain the information telling the slave which register to start at and how many registers to read. The error check field provides a method for the slave to validate the integrity of the message contents.

   The Response: If the slave makes a normal response, the function code in the response is an echo of the function code in the request. The data bytes contain the data collected by the slave, such as register values or status. If an error occurs, the function code is modified to indicate that the response is an error response, and the data bytes contain a code that describes the error. The error check field allows the master to confirm that the message contents are valid.

   Controllers can be setup to communicate on standard Modbus networks using either of two transmission modes: ASCII or RTU.

ASCII Mode: When controllers are setup to communicate on a Modbus network using ASCII (American Standard Code for Information Interchange) mode, each eight-bit byte in a message is sent as two ASCII characters. The main advantage of this mode is that it allows time intervals of up to one second to occur between characters without causing an error.

ASCII Coding System

- Hexadecimal ASCII printable characters 0 ... 9, A ... F
- Bits per Byte
- 1 start bit
- 7 data bits, least significant bit sent first
- 1 bit for even / odd parity-no bit for no parity
- 1 stop bit if parity is used-2 bits if no parity
- Error Checking
- Longitudinal Redundancy Check (LRC)

RTU Mode: When controllers are setup to communicate on a Modbus network using RTU (Remote Terminal Unit) mode, each eight-bit byte in a message contains two four-bit hexadecimal characters. The main advantage of this mode is that its greater character density allows better data throughput than ASCII for the same baud rate. Each message must be transmitted in a continuous stream.

RTU Coding System

- Eight-bit binary, hexadecimal 0 ... 9, A ... F
- Two hexadecimal characters contained in each eight-bit field of the message
- Bits per Byte
- 1 start bit
- 8 data bits, least significant bit sent first
- 1 bit for even / odd parity-no bit for no parity
- 1 stop bit if parity is used-2 bits if no parity
- Error Check Field
- Cyclical Redundancy Check (CRC)

2. **DNP3:** Distributed Network Protocol (DNP or DNP3) has achieved a large-scale acceptance since its introduction in 1993. This protocol is an immediately deployable

solution for monitoring remote sites because it was developed for communication of critical infrastructure status, allowing for reliable remote control.

GE-Harris Canada (formerly Westronic, Inc.) is generally credited with the seminal work on the protocol. This protocol is, however, currently implemented by an extensive range of manufacturers in a variety of industrial applications, such as electric utilities.

DNP3 is composed of three layers of the OSI seven-layer functions model. These layers are application layer, data link layer, and transport layer. Also, DNP3 can be transmitted over a serial bus connection or over a TCP/IP network.

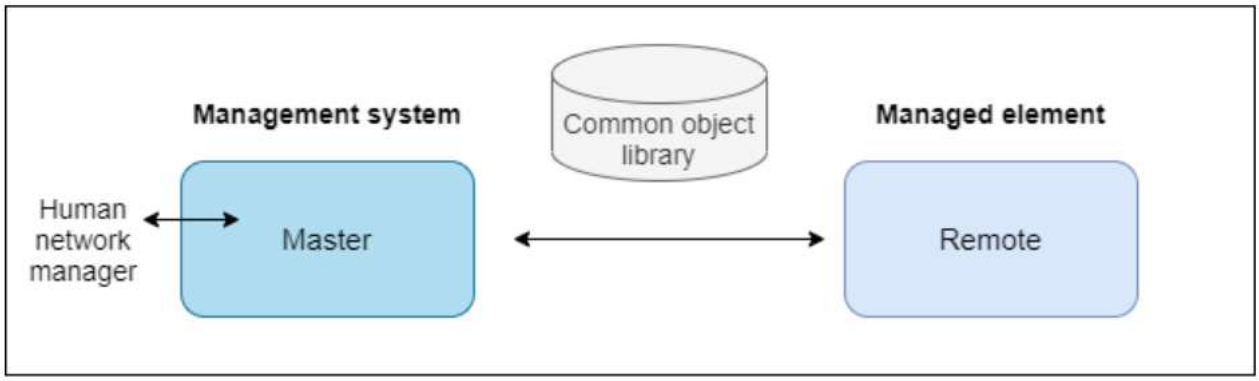
The DNP3 Protocol Specification is Based An Object Model

DNP3 is based on an object model. This model reduces the bit mapping of data that is traditionally required by other less object-oriented protocols. It also reduces the wide disparity of status monitoring and control paradigms generally found in protocols that provide virtually no pre-defined objects.

Purists of these alternate protocols would insist that any required object can be 'built' from existing objects. Having some pre-defined objects though makes DNP3 a somewhat more comfortable design and deployment framework for SCADA engineers and technicians.

DNP3 uses a Master/Remote Model

DNP3 is typically used between centrally located masters and distributed remotes. The master provides the interface between the human network manager and the monitoring system. The remote (RTUs and intelligent electronic devices) provides the interface between the master and the physical device(s) being monitored and/or controlled.



A typical DNP3 master/remote monitoring system architecture.

The master and remote both use a library of common objects to exchange information. The DNP3 protocol contains carefully designed capabilities. These capabilities enable it to be used reliably even over media that may be subject to noisy interference.

The DNP3 protocol is a polled protocol. When the master station connects to a remote, an integrity poll is performed. Integrity polls are important for DNP3 addressing. This is because they return all buffered values for a data point and include the current value of the point as well.

Main DNP3 Capabilities

As an intelligent and robust SCADA protocol, DNP3 gives you many capabilities. Some of them are:

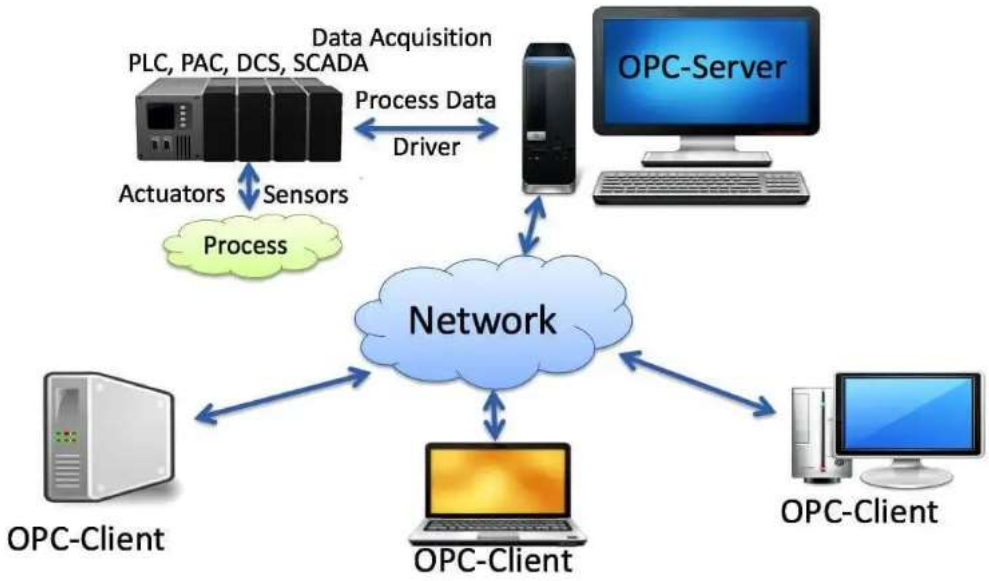
- DNP3 can request and respond with multiple data types in single messages
- Response without request (unsolicited messages)
- It allows multiple masters and peer-to-peer operations
- It supports time synchronization and a standard time format
- It includes only changed data in response messages

3. **OPC :** OPC stands for Open Platform Communications or some say OLE (Object Linking and Embedding) for Process Control. It is a type of protocol used in Industrial Automation.

   The OPC is always used in the Client/Server pair. The OPC server converts the hardware communicated data from PLC into OPC protocol. So that other software like SCADA can access the data.

   The OPC server is a program that often connects with hardware like HMI to get the data and convert it into OPC protocol.

   The OPC client communicates with the OPC server to receive data or send commands to the hardware.



Usually, the OPC is implemented in a Single Server – Client in a single system format. But there are some famous alternate methods,

- OPC aggregation – In this method, the OPC Client is connected to several OPC servers to acquire data
- OPC bridging – In this method, the OPC server is connected with another OPC server to share data.
- OPC tunneling – In this method, the OPC client is connected to an OPC server over a network.

The combination of OPC server and OPC client supports many connections. The OPC datahub is designed in such a way to handle all those connections.

In addition to improving OPC server and client connections, the OPC datahub can connect any OPC server or client to other applications as well, including Excel, a web browser, or any other database.

The Following are some of the OPC specifications that are used in Industries,

- OPC AE (Alarms and Events) – OPC AE servers are used to accept and exchange process alarms and events.
- OPC-HDA (Historical Data Access) – This is used to retrieve historical process data for analysis. This data is typically stored in files, databases, or remote telemetry systems.

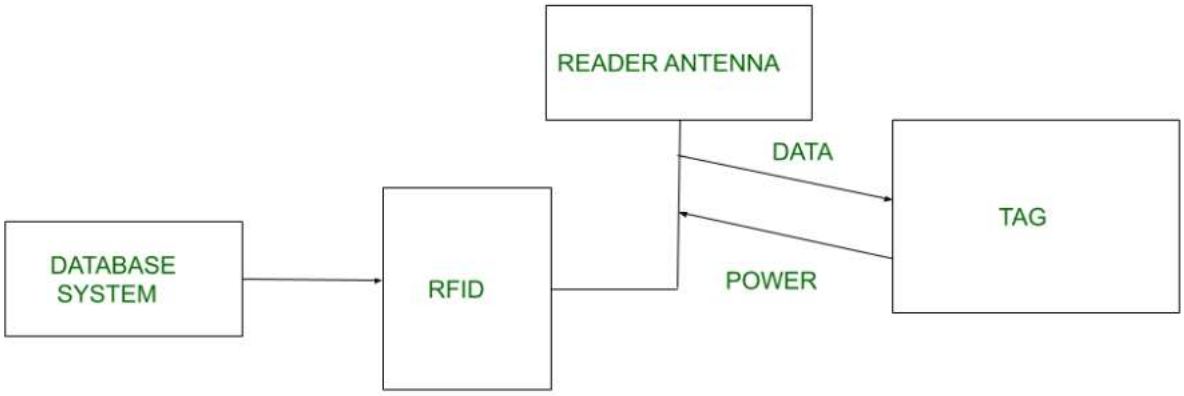
- OPC-DA (Data Access) – Provides access to real-time data. We can query the most recent values of temperature, pressure, density, acceleration, and other types of process control data from the OPC-DA server.

Advantages of OPC

- Interoperability.
- Since the client software is always going to access data from the server, the Client software has no need to know the hardware protocol.
- Scalability of the system.

RFID

Radio Frequency Identification (RFID) is a form of wireless communication that incorporates the use of electromagnetic or electrostatic coupling in the radio frequency portion of the electromagnetic spectrum to uniquely identify an object, animal or person. It uses radio frequency to search ,identify, track and communicate with items and people. it is a method that is used to track or identify an object by radio transmission uses over the web. Data digitally encoded in an RFID tag which might be read by the reader. This device work as a tag or label during which data read from tags that are stored in the database through the reader as compared to traditional barcodes and QR codes. It is often read outside the road of sight either passive or active RFID.



Kinds of RFID :

There are many kinds of RFID, each with different properties, but perhaps the most fascinating

aspect of RFID technology is that most RFID tags have neither an electric plug nor a battery. Instead, all of the energy needed to operate them is supplied in the form of radio waves by RFID readers. This technology is called passive RFID to distinguish it from the(less common) active RFID in which there is a power source on the tag.

UHF RHID (Ultra-High Frequency RFID). It is used on shipping pallets and some driver's licenses. Readers send signals in the 902-928 MHz band. Tags communicate at distances of several meters by changing the way they reflect the reader signals; the reader is able to pick up these reflections. This way of operating is called backscatter.

HF RFID (High-Frequency RFID). It operates at 13.56 MHz and is likely to be in your passport, credit cards, books, and noncontact payment systems. HF RFID has a short-range, typically a meter or less because the physical mechanism is based on induction rather than backscatter.

There are also other forms of RFID using other frequencies, such as LF RFID(Low-Frequency RFID), which was developed before HF RFID and used for animal tracking

There are two types of RFID :

1. **Passive RFID –** Passive RFID tags does not have thier own power source. It uses power from the reader. In this device, RF tags are not attached by a power supply and passive RF tag stored their power. When it is emitted from active antennas and the RF tag are used specific frequency like 125-134MHZ as low frequency, 13.56MHZ as a high frequency and 856MHZ to 960MHZ as ultra-high frequency.

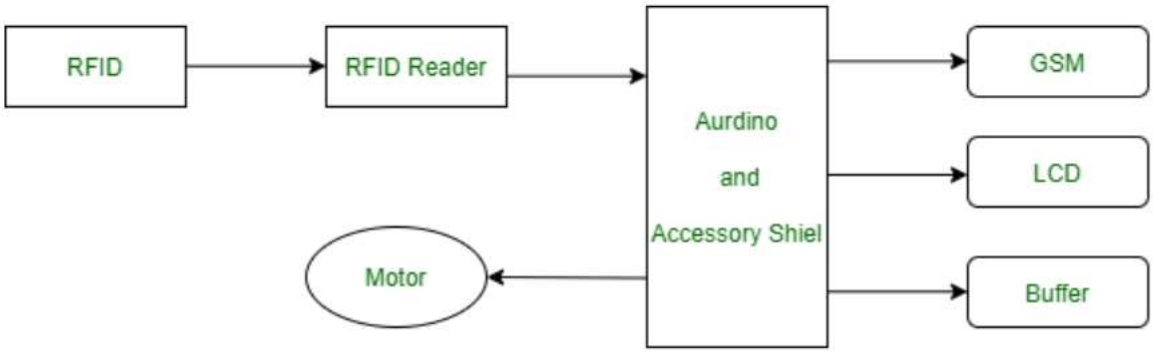
2. **Active RFID –** In this device, RF tags are attached by a power supply that emits a signal and there is an antenna which receives the data. means, active tag uses a power source like battery. It has it's own power source, does not require power from source/reader.

Working Principle of RFID :

Generally, RFID uses radio waves to perform AIDC function. AIDC stands for Automatic

Identification and Data Capture technology which performs object identification and collection and mapping of the data.

An antenna is an device which converts power into radio waves which are used for communication between reader and tag. RFID readers retrieve the information from RFID tag which detects the tag and reads or writes the data into the tag. It may include one processor, package, storage and transmitter and receiver unit.



Working of RFID System :

Every RFID system consists of three components: a scanning antenna, a transceiver and a transponder. When the scanning antenna and transceiver are combined, they are referred to as an RFID reader or interrogator. There are two types of RFID readers — fixed readers and mobile readers. The RFID reader is a network-connected device that can be portable or permanently attached. It uses radio waves to transmit signals that activate the tag. Once activated, the tag sends a wave back to the antenna, where it is translated into data.

The transponder is in the RFID tag itself. The read range for RFID tags varies based on factors including the type of tag, type of reader, RFID frequency and interference in the surrounding environment or from other RFID tags and readers. Tags that have a stronger power source also have a longer read range.

Features of RFID :

- An RFID tag consists of two-part which is an microcircuit and an antenna.

- This tag is covered by protective material which acts as a shield against the outer environment effect.
- This tag may active or passive in which we mainly and widely used passive RFID.

Application of RFID :

- It utilized in tracking shipping containers, trucks and railroad, cars.
- It uses in Asset tracking.
- It utilized in credit-card shaped for access application.
- It uses in Personnel tracking.
- Controlling access to restricted areas.
- It uses ID badging.
- Supply chain management.
- Counterfeit prevention (e.g., in the pharmaceutical industry).

Advantages of RFID :

- It provides data access and real-time information without taking to much time.
- RFID tags follow the instruction and store a large amount of information.
- The RFID system is non-line of sight nature of the technology.
- It improves the Efficiency, traceability of production.
- In RFID hundred of tags read in a short time.

Disadvantages of RFID :

- It takes longer to program RFID Devices.
- RFID intercepted easily even it is Encrypted.
- In an RFID system, there are two or three layers of ordinary household foil to dam the radio wave.
- There is privacy concern about RFID devices anybody can access information about anything.
- Active RFID can costlier due to battery.

RFID Protocols

1. ISO/IEC 18000 Series

ISO/IEC 18000 series standards are most eye-catching among RFID wireless interface standards, which cover the communication frequency from 125 kHz to 2.45GHz, with reading distances ranging from a few centimeters to dozens of meters, mainly passive tags but also active tags for containers. There are seven standards with the ISO 18000 series as follows:

- 18000–1: Generic parameters for air interfaces for globally accepted frequencies
- 18000–2: Air interface for 135 kHz
- 18000–3: Air interface for 13.56 MHz
- 18000–4: Air interface for 2.45 GHz
- 18000–5: Air interface for 5.8 GHz
- 18000–6: Air interface for 860 MHz to 930 MHz
- 18000–7: Air interface at 433.92 MHz

2. ISO 11784/11785 (134.2 kHz)

ISO 11784 and ISO 11785 are international standards that regulate the RFID of animals, which is usually accomplished by implanting, introducing, or attaching a transponder containing a microchip to an animal.

ISO 11784- Code Structure

ISO 11784 specifies the structure of the identification code, including transponder data transmission method and reader specification, working on 134.2 kHz.

ISO 11785- Technical Standard

ISO 11785 specifies how a transponder is activated and how the stored information is transferred to a transceiver.

RFID tags from different manufacturers can be read using a common reader according to this standard. Besides, transponder size is not specified in the standard, so it can be designed in a variety of shapes to suit different animals, such as glass tubes, earmarks, or collars.

3、ISO/IEC 14443 (13.56 MHz)

ISO/IEC 14443 is one of a series of International Standards describing the parameters for identification cards as defined in ISO 7810 and the use of such cards for international interchange.

ISO/IEC14443 protocol is divided into two types: TypeA & TypeB, both operating at 13.56 MHz (RFID HF). They are close-reading protocols. Label read-write distance is 0~10cm. The main difference between A and B lies in their modulation, coding schemes, and anti-collision methods.

ISO/IEC 14443A

Strong anti-interference ability but poor power stability, mainly used in the field of transportation, urban construction access cards, bus cards, and small stored value consumption cards, with a high market share.

ISO/IEC 14443B

Good stability, high security, but relatively vulnerable to external environment interference. Because the encryption coefficient is relatively high, it is more suitable for CPU card, generally used for ID card, passport, bank card, etc.

4、ISO/IEC 15693(13.56 MHz)

ISO/IEC 15693 is a long-distance reading protocol and also a popular HF (13.56 MHz) standard for High RFIDs widely used for non-contact smart payment and credit cards.

It is compatible with ISO 18000-3 and allows long-distance communication. The maximum reading distance is 100mm, and the application is more flexible. It widely used in production automation, medical management, jewelry inventory, asset management, parking management and product anti-counterfeiting, access control, asset management, logistics & supply chain, library management, etc.

5、EPC Gen2 (860~960 MHz)

EPC Gen2 is the second generation standard of the Class1UHF RFID air interface developed by EPCglobal. The standard is similar to ISO18000-6. EPC Gen2 was approved by ISO in 2006 and incorporated into the ISO standard system known as ISO 18000-6C.

ISO 18000-6C (EPC Gen2) protocol is the most widely used protocol in medium and long-distance. Tags under the EPC Gen2 protocol can be read and written repeatedly, and have a good confidentiality performance.

IEEE802.15.4

IEEE 802.15.4 is a low-cost, low-data-rate wireless access technology for devices that are operated or work on batteries. This describes how low-rate wireless personal area networks (LR-WPANs) function.

802.15.4e for industrial applications and 802.15.4g for the smart utility networks (SUN). The 802.15.4e improves the old standard by introducing mechanisms such as time slotted access, multichannel communication and channel hopping.

IEEE 802.15.4e introduces the following general functional enhancements:

1. Low Energy (LE): This mechanism is intended for applications that can trade latency for energy efficiency. It allows a node to operate with a very low duty cycle.
2. Information Elements (IE) It is an extensible mechanism to exchange information at the MAC sublayer.
3. Enhanced Beacons (EB): Enhanced Beacons are an extension of the 802.15.4 beacon frames and provide a greater flexibility. They allow to create application-specific frames.
4. Multipurpose Frame: This mechanism provides a flexible frame format that can address a number of MAC operations. It is based on IEs.
5. MAC Performance Metric: It is a mechanism to provide appropriate feedback on the channel quality to the networking and upper layers, so that appropriate decision can be taken.
6. Fast Association (FastA) The 802.15.4 association procedure introduces a significant delay in order to save energy. For time-critical application latency has priority over energy efficiency.

IEEE 802.15.4e defines five new MAC behavior modes.

1. Time Slotted Channel Hopping (TSCH): It targets application domains such as industrial automation and process control, providing support for multi-hop and multichannel communications, through a TDMA approach.

2. Deterministic and Synchronous Multi-channel Extension (DSME): It is aimed to support both industrial and commercial applications.

3. Low Latency Deterministic Network (LLDN): Designed for single-hop and single channel networks

4. Radio Frequency Identification Blink (BLINK): It is intended for application domains such as item/people identification, location and tracking.

5. Asynchronous multi-channel adaptation (AMCA): It is targeted to application domains where large deployments are required, such as smart utility networks, infrastructure monitoring networks, and process control networks.

Properties:

1. Standardization and alliances: It specifies low-data-rate PHY and MAC layer requirements for wireless personal area networks (WPAN).
IEEE 802.15. Protocol Stacks include:

- **ZigBee:** ZigBee is a Personal Area Network task group with a low rate task group 4. It is a technology of home networking. ZigBee is a technological standard created for controlling and sensing the network. As we know that ZigBee is the Personal Area network of task group 4 so it is based on IEEE 802.15.4 and is created by Zigbee Alliance.
- **6LoWPAN:** The 6LoWPAN system is used for a variety of applications including wireless sensor networks. This form of wireless sensor network sends data as packets and uses IPv6 – providing the basis for the name – IPv6 over Low power Wireless Personal Area Networks.

- **ZigBee IP:** Zigbee is a standards-based wireless technology that was developed for low-cost and low-power wireless machine-to-machine (M2M) and internet of things (IoT) networks.
- **ISA100.11a:** It is a mesh network that provides secure wireless communication to process control.
- **Wireless HART:** It is also a wireless sensor network technology, that makes use of time-synchronized and self-organizing architecture.
- **Thread:** Thread is an IPv6-based networking protocol for low-power Internet of Things devices in IEEE 802.15. 4-2006 wireless mesh network. Thread is independent.

2. Physical Layer: This standard enables a wide range of PHY options in ISM bands, ranging from 2.4 GHz to sub-GHz frequencies. IEEE 802.15.4 enables data transmission speeds of 20 kilobits per second, 40 kilobits per second, 100 kilobits per second, and 250 kilobits per second. The fundamental structure assumes a 10-meter range and a data rate of 250 kilobits per second. To further reduce power usage, even lower data rates are possible. IEEE 802.15.4 regulates the RF transceiver and channel selection, and even some energy and signal management features, at the physical layer. Based on the frequency range and data performance needed, there are now six PHYs specified. Four of them employ frequency hopping techniques known as Direct Sequence Spread Spectrum (DSSS). Both PHY data service and management service share a single packet structure so that they can maintain a common simple interface with MAC.

3. MAC layer: The MAC layer provides links to the PHY channel by determining that devices in the same region will share the assigned frequencies. The scheduling and routing of data packets are also managed at this layer. The 802.15.4 MAC layer is responsible for a number of functions like:

- Beaconing for devices that operate as controllers in a network.
- used to associate and dissociate PANs with the help of devices.
- The safety of the device.
- Consistent communication between two MAC devices that are in a peer-to-peer relationship.

Several established frame types are used by the MAC layer to accomplish these functions. In 802.15.4, there are four different types of MAC frames:

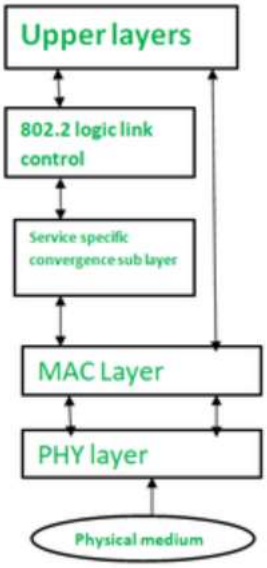
- frame of data
- Frame for a beacon
- Frame of acknowledgement
- Frame for MAC commands

4. Topology: Networks based on IEEE 802.15.4 can be developed in a star, peer-to-peer, or mesh topology. Mesh networks connect a large number of nodes. This enables nodes that would otherwise be out of range to interact with each other to use intermediate nodes to relay data.

5. Security: For data security, the IEEE 802.15.4 standard employs the Advanced Encryption Standard (AES) with a 128-bit key length as the basic encryption technique. Activating such security measures for 802.15.4 significantly alters the frame format and uses a few of the payloads. The very first phase in activating AES encryption is to use the Security Enabled field in the Frame Control part of the 802.15.4 header. For safety, this field is a single bit which is assigned to 1. When this bit is set, by taking certain bytes from its Payload field, a field known as the Auxiliary Security Header is formed following the Source Address field.

6. Competitive Technologies: The IEEE 802.15.4 PHY and MAC layers serve as a basis for a variety of networking profiles that operate in different IoT access scenarios. DASH7 is a competing radio technology with distinct PHY and MAC layers.

The architecture of LR-WPAN Device:



IEEE 802.15.4

Advantages of IEEE 802.15.4:

IEEE 802.15.4 has the following advantages:

- cheap cost
- long battery life,
- Quick installation
- simple
- extensible protocol stack

Disadvantages of IEEE 802.15.4:

IEEE 802.15.4's drawbacks include:

- IEEE 802.15.4 causes interference and multipath fading.
- doesn't employ a frequency-hopping approach.
- unbounded latency
- interference susceptibility

Applications of IEEE 802.15.4:

IEEE 802.15.4 Applications:

- Wireless sensor networks in the industry
- Building and home automation
- Remote controllers and interacting toys
- Automotive networks