Draft Study Material

Telecom Technician – IoT Device/ Systems

(Job Role)

(Qualification Pack: Ref. Id. TEL/Q6210)

Sector: Telecom

Textbook for Class XI

विद्या ऽमृतमश्नुते

एन सी ई आर टी
NCERT

PSS CENTRAL INSTITUTE OF VOCATIONAL EDUCATION
(a constituent unit of NCERT, under Ministry of Education, Government of India)
Shyamla Hills, Bhopal- 462 002, M.P., India
https://www.psscive.ac.in

Preface

Vocational Education is a dynamic and evolving field, and ensuring that every student has access to quality learning materials is of paramount importance. The journey of the PSS Central Institute of Vocational Education (PSSCIVE) toward producing comprehensive and inclusive study material is rigorous and time-consuming, requiring thorough research, expert consultation, and publication by the National Council of Educational Research and Training (NCERT). However, the absence of finalized study material should not impede the educational progress of our students. In response to this necessity, we present the draft study material, a provisional yet comprehensive guide, designed to bridge the gap between teaching and learning, until the official version of the study material is made available by the NCERT. The draft study material provides a structured and accessible set of materials for teachers and students to utilize in the interim period. The content is aligned with the prescribed curriculum to ensure that students remain on track with their learning objectives.

The contents of the modules are curated to provide continuity in education and maintain the momentum of teaching-learning in vocational education. It encompasses essential concepts and skills aligned with the curriculum and educational standards. We extend our gratitude to the academicians, vocational educators, subject matter experts, industry experts, academic consultants, and all other people who contributed their expertise and insights to the creation of the draft study material.

Teachers are encouraged to use the draft modules of the study material as a guide and supplement their teaching with additional resources and activities that cater to their students' unique learning styles and needs. Collaboration and feedback are vital; therefore, we welcome suggestions for improvement, especially by the teachers, in improving upon the content of the study material.

This material is copyrighted and should not be printed without the permission of the NCERT-PSSCIVE.

Deepak Paliwal
(Joint Director)
PSSCIVE, Bhopal

Date: 16 April 2025

STUDY MATERIAL DEVELOPMENT COMMITTEE

Members

Prof Dr Prakash Khanale, Senior Academic Coordinator, Yashwantrao Chavan Maharashtra Open University, Nashik., Maharashtra and Ex. Head Department of Computer Science, DSM College, Parbhani, Maharashtra

Mrs. Rita Jain, Professor in Electronic and Communication, LNCT, Bhopal and Director (COI IOT), Workspace, Bhopal

Member Coordinator

Prof Dr Deepak D. Shudhalwar, Professor (CSE), Head, Department of Engineering and Technology, PSSCIVE, NCERT, Bhopal, Madhya Pradesh

TABLE OF CONTENTS

Module 1 IoT Devices and Systems

Module Overview

Internet of Things (IoT) is a revolutionary concept that is transforming the way we interact with the world around us. IoT involves the integration of devices, sensors, and systems with the power of the internet, enabling them to communicate, share information, and perform intelligent actions. In this journey, we will explore how IoT is shaping our future, enhancing efficiency, and creating innovative solutions for a wide range of applications. From smart homes and cities to healthcare and industry, understanding IoT devices and systems will not only expand our technological knowledge but also empower us to contribute to the evolving digital landscape.

This Module begins by outlining the crucial responsibilities of a Telecom Technician in managing IoT devices and systems, emphasizing their role in maintaining seamless connectivity in the complex landscape of telecommunications and IoT technologies.

Moving forward, the Module covers fundamental IoT concepts, it helps in understanding how everyday objects transform into intelligent entities, seamlessly communicating and enhancing our daily lives.

This Module includes the significance of microprocessors and microcontroller boards. It delves into the pivotal functions of sensors and actuators, highlighting their role in data collection and real-time decision-making.

Additionally, the Module explores the architectural components of IoT networks such as gateways, nodes, and edge devices, providing insights into their critical functions. Finally, it delves into communication technologies and protocols, crucial for efficient data transmission in diverse IoT applications.

This Module serves as a strong foundation for further exploration and mastery in the field of IoT.

Learning Outcomes

After completing this module, you will be able to:

- Understand the basic concept, features, and applications of the Internet of Things (IoT).
- Identify different types of controller boards and explain their role in IoT systems.
- Describe the functions and working principles of sensors and actuators in IoT.

Module Structure

Session 1. Basic Concept of IoT

Minnie and Mickey enter an expansive library filled with books stretching in every direction, forming towering stacks throughout the space. Faced with this vast collection as shown in Figure 1.1, Mickey asked Minnie how would you go about locating a specific book?

Fig. 1.1: An image of Library

Minnie plans to ask the librarian for help finding a book. Mickey prompts her to consider how the librarian has information on all books. Minnie explains that new books are marked, and their details, including location, are entered into the computer.

Mickey proposes the idea of electronic tags or sensors on every book, sending real-time location information to the computer. Minnie likes the idea, anticipating easier tracking and retrieval. Mickey expands the concept globally and includes the whole world that if all the physical things like vehicles, devices, TV, Microwave, refrigerator, healthcare devices etc have these smart sensors to gather information and also a way to send this information across using the internet. It is depicted in Figure 1.1.

Well, I guess, whenever a new book arrives in the library, it is marked and the details about the book including location is fed to the librarian computer
Exactly. Now suppose if every book has some electronic tag or sensor and could send the information about its location to the librarian computer in real-time

Fig. 1.2: Use of IoT in Library management

1.1 Introduction to IoT (Internet of Things)

Internet of Things (IoT) is a massive network of physical devices embedded with sensors, software, electronics, and network which allows the devices to exchange or collect data and perform certain actions. Basically, IoT is made up of two words: Internet & Things.

Things – physical devices, appliances, gadgets, etc.

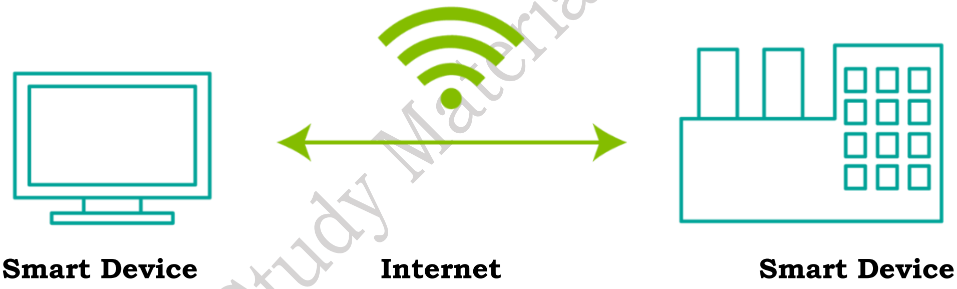
Internet – through which these devices are connected.

IoT aims at extending internet connectivity beyond computers and smartphones to other devices which people use at home or for business. The technology allows devices to get controlled across network infrastructure remotely. As a result, it cuts down the human effort and paves the way for accessing the connected devices easily. With autonomous control, the devices are operable without involving human interaction. IoT makes things virtually smart through algorithms, data collection and networks enhancing our lives.

Examples: Smart switches, AC sensors to adjust the temperature based on the outside temperature, smart wearables, Pet tracking devices, Health monitors, and many more.

IoT comprises things that have unique identities and are connected to internet. By 2028 there will be a total of 75 billion devices /things connected to internet. IoT is not limited to just connecting things to the internet but also allow things to communicate and exchange data.

Definition: The Internet of Things (IoT) is a network of 'smart' devices that connect and communicate via the Internet.



A smart device is a thing which has senses and has a unique identity which connects it to a communication network so that we can communicate with it from any part of the world.

So, Things in IOT refers to any physical object with a device that has its own IP address and can connect to a network and also sends/receives data via a network.

Thus, Internet of things (IoT) is a system of interrelated computing devices, mechanical and digital machines provided with unique identifiers (UIDs) and the ability to transfer data over a network without requiring human-to-human or human-to-computer interaction.

IOT is a dynamic global network infrastructure with self-configuring capabilities based on standard and interoperable communication protocols. In IOT every physical and virtual things have identities as we have our names and family names. These things with unique identifiers get seamlessly integrated into the internet so as to communicate data associated with users and their environments.

Characteristics of IoT

1) Dynamic & Self Adapting: IoT devices and systems may have the capability to dynamically adapt with the changing contexts and take actions based on their operating conditions, user 's context or sensed environment. Eg: the surveillance system is adapting itself based on context and changing conditions.

2) Self Configuring: It allows a large number of devices to work together to provide certain functionality.

3) Inter-Operable Communication Protocols: IOT supports a number of interoperable communication protocols and its devices can communicate with other devices and also with infrastructure.

4) Unique Identity: Each IoT device has a unique identity and a unique identifier (IP address).

5) Integrated into Information Network: This allows them to communicate and exchange data with other devices and systems.

IoT is a network of connected devices with unique identifiers in the form of an IP address which have embedded technologies or are equipped with technologies that enable them to sense, gather data and communicate about the environment in which they reside and/or themselves.

1.2 Building Blocks of IoT

The important components of an IoT system are Devices and sensors, Cloud Computing, User interface, Connectivity, Gateways are shown in Figure 1.4.

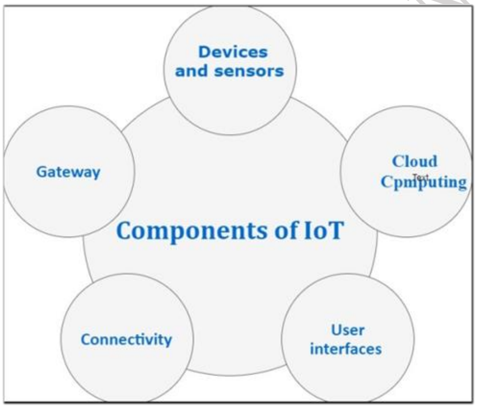


Fig. 1.4: Building blocks of IoT

1.1.1 Devices and sensors – Devices and sensors are components of the connectivity layer. These smart sensors continuously collect information about the environment and transmit it to the next layer. For example, our phone is a device that has several sensors such as GPS, camera, motion, etc. There are some common sensors used in IoT are as follows:

Temperature and Thermostats Sensors: They sense the temperature of the environment.

Pressure Sensor: It measure the pressure or force per unit area applied to the sensor.

Humidity Sensor: It is a device used to measure the moisture level in the environment

Light Intensity Detector: It detects the intensity of Light

Soil Moisture Sensors: It is a device used to measure the moisture level in the soil

Proximity Detector: It detects the presence of nearby objects

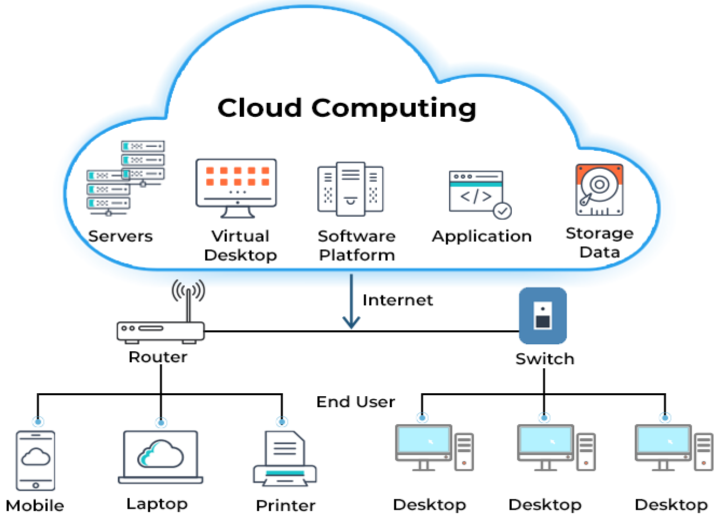
RFID Tag: An electronic tag used for tracking an object.

1.1.2 Cloud Computing – Cloud computing is a technology that enables us to create, configure, and customize applications through an internet connection. Cloud computing allows resources located at remote locations to be made available to anyone anywhere. In simple words, cloud computing permits you to rent as an alternative to buy your IT. Instead of investing heavily in databases, software, and hardware. Enterprises opt to access their compute power via the internet, or the cloud, and pay for it as they utilize it.

IoT systems transmit a large amount of data from devices, and this data must be effectively managed to deliver meaningful results. IoT technology uses cloud services to store large amounts of data. It provides tools for data collection, processing and storage. Information is readily available and remotely accessible via the Internet. It also provides an analytics platform. The IoT cloud is an advanced network of high-performance servers for fast processing of large amounts of data.

Activity: Google Classroom is a cloud-based tool that allows teachers to create and manage classes, share resources, and communicate with students. It allows teachers to post announcements, assignments, and quizzes, and for students to submit their work and collaborate on group projects. Explain how it works?

Google Classroom is implemented through different components of Cloud computing which correspond to platforms such as front end, back end, and cloud-dependent delivery and the utilized network. Thus, the Google classroom framework of cloud computing is broadly categorized as three specifically clients, datacentre and cloud-based delivery and network.



Clients: Clients in cloud computing are in general to the operation of Local Area Networks (LAN's). These help users access their systems and applications by using any device from anywhere. They are just the desktops where they have their place on desks. These might be also in the form of laptops, mobiles, tablets to enhance mobility. Clients hold the responsibility of interaction which pushes for the management of data on cloud servers. This is the place where the teacher creates the classes, upload notes, quizzes, announcements etc. They are free to use any device e.g. laptop, Mobile phone, Desktop, Tab, desktop etc. to create content and upload too.

Datacentre: It is an array of servers that houses the subscribed applications with several servers for storage and processing. Management of Applications logic is managed through servers and effective data handling is provided by storage. The combination of these platforms at the backend offers the processing power, and capacity to manage and store data behind the cloud. This is the place where the data uploaded by the teacher is stored safely.

Cloud-based delivery and Network

On-demand access to the computer and resources is provided over the Internet, Intranet, and Intercloud. The Internet comes with global accessibility, the Intranet helps in internal communications of the services within the organization and the Intercloud enables interoperability across various cloud services. This dynamic network connectivity ensures an essential component of cloud computing architecture on guaranteeing easy access and data transfer. This is the facility through which the associate students of the Google classroom can access the data from anywhere in the world.

Activity 2: Smart traffic management

This project primarily uses cloud computing power to reduce your vehicle's waiting time request during peak traffic hours. After analyzing real-time traffic, such management will be represented by an application that can potentially simulate the movement of vehicles.

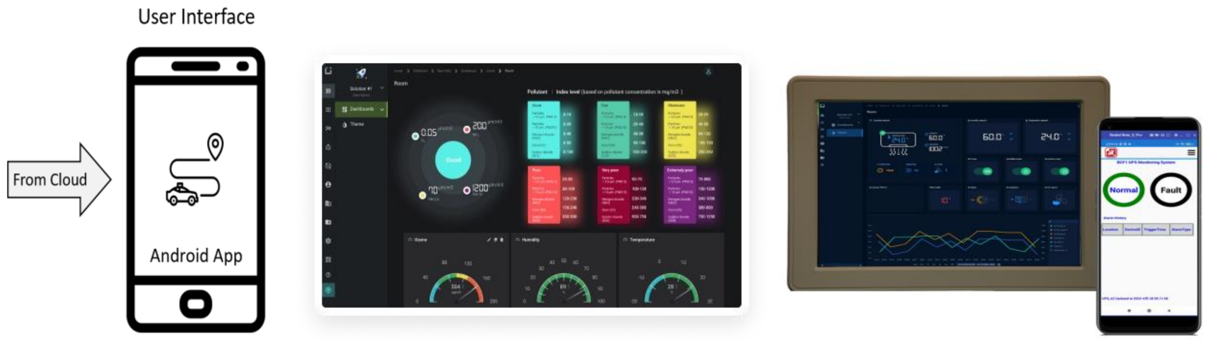
This project will help beginners afraid of applying traffic management techniques to real-world problems strengthen their decision-making process.

Cloud services can be Infrastructure as a Service (IaaS), Platform as a Service (PaaS), and Software as a Service (SaaS).

1.1.3 User interface – User interface is the physical and visible part of an IoT system that is accessible to users. User interface design is more important in today's competitive market because it often allows the user to choose a particular device or equipment for effective interaction between the user and services. There are two types of applications in IOT:

Mobile Application: iOS and Android

Web Application: Single page application on website

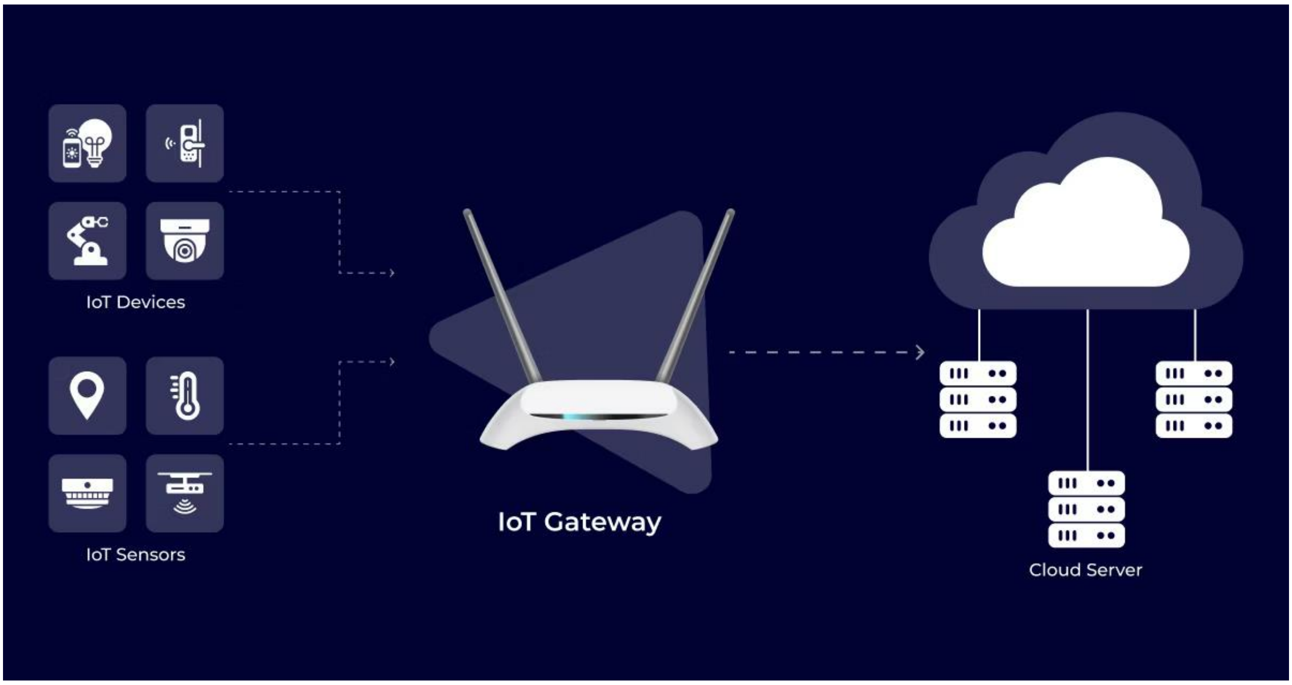


Users are interested in buying new smart devices if they are easy to use and compatible with current wireless standards. Modern technology offers many interactive designs to facilitate complex operations with simple touch screen controls. Multi-colour touch screens have replaced the hardware switches in our devices, and this trend is increasing in almost all smart home devices.

1.1.4 Connectivity – Internet connection is required for communication. An Internet connection gives each device an IP address. Although fewer addresses depend on the IP address.

1.1.5 IoT Gateway – IoT Gateway manages two-way data traffic between different networks and protocols. Another task of the gateway is to translate different network protocols and ensure interoperability of connected devices and sensors. The IoT gateway provides a certain level of data security to the network and to the data transmitted through higher order encryption techniques.

It acts as a middle layer between the devices and the cloud, protecting the system against malicious attacks and unauthorized access. The gateway can be configured to pre-process data collected from thousands of sensors locally before forwarding it to the next stage. In some cases, this would be necessary for TCP/IP protocol compatibility.



Activity: Demonstrate the connection of IOT things to IOT Network through IOT Gateway.

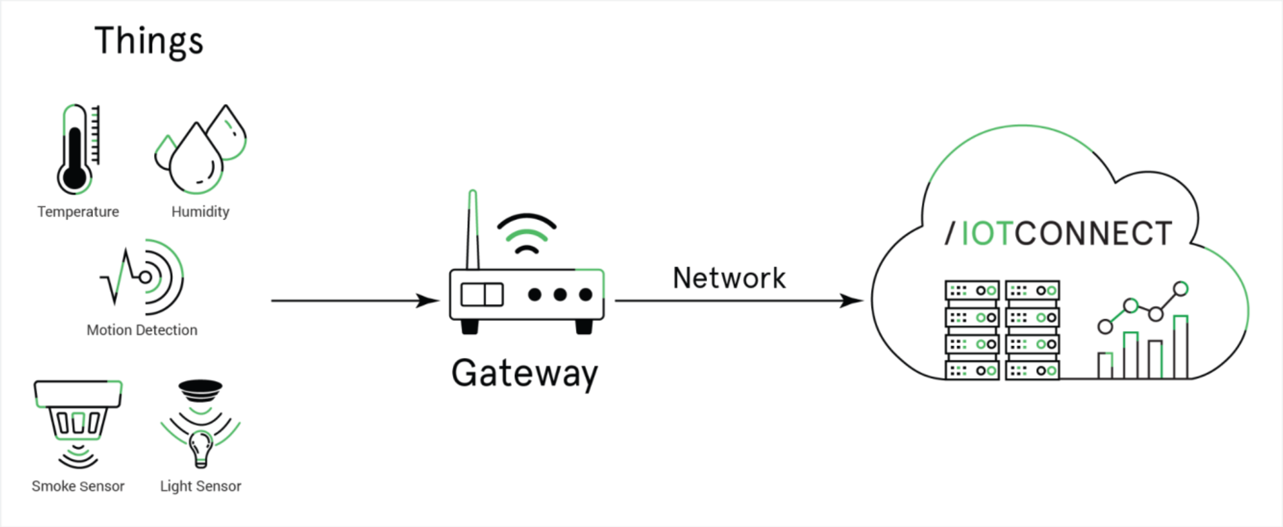
Considering a use case of a connected office environment, there will be several sensors associated with equipment like lights, HVAC system, security systems, CCTVs, etc. These sensors are used to capture data such as:

1. Temperature
2. Humidity
3. Noise
4. Position of people and equipment
5. Light

Each of these devices use different protocols like WiFi, Bluetooth and Ethernet to connect to the network. They connect to different control environments and have different models for management and security. Some of these sensors or controllers might use low energy and may not support energy-intensive protocols like WiFi and Bluetooth, which may affect their connectivity.

To connect all of them to the IOT Network, we need an IOT Gateway which have the provision like:

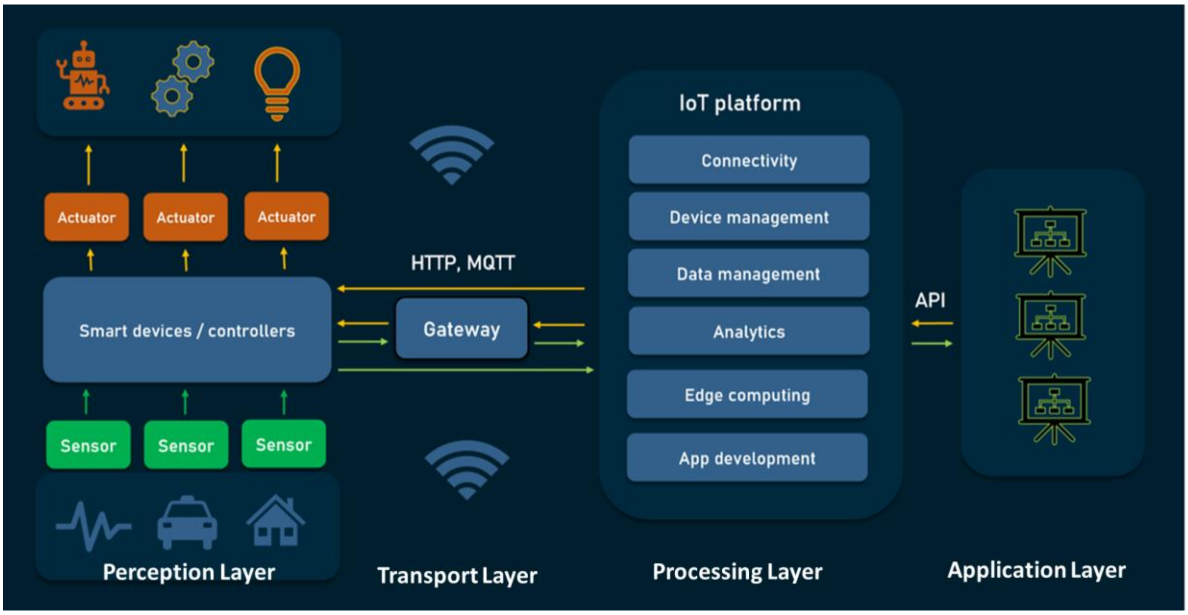
1. Device connectivity
2. Protocol translation
3. Data filtering and processing
4. Security management



Thus, the IOT gateway will help all the IOT devices working at different operating speeds and protocols be able to access the Internet as shown in the above image.

1.3 Architecture of IoT

IoT architecture is the structural framework that defines how Internet of Things devices communicate, process data, and interact within a network.



The Architecture of Internet of Things comprises four layers – 1) Sensing or Perception Layer (sensors and actuators) 2) Transport Layer (gateways and nodes) 3) Processing Layer and 4) Application Layer (cloud-based platforms and end-user interfaces).

This architecture enables seamless connectivity, data collection, and real-time decision-making, forming the foundation for a smart and interconnected ecosystem.

Sensing layer (sensors and actuators): The main purpose of the sensing layer is to recognize any phenomena in the peripheral devices and obtain information from the real world.

Network layer (IoT gateways and nodes): The network layer acts as a communication channel that transfers the information collected in the sensing layer to other connected devices. The network layer is implemented in IoT devices by using different communication technologies (e.g. Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, cellular network, etc.) to allow data flow between other devices on the same network.

Data Processing layer (cloud server): The data processing layer consists of the main data processing unit of IoT devices. The data processing layer gathers data collected in the sensing layer and analyses the data to make decisions based on the outcome. In some IoT devices (e.g. smart watches, smart home hub, etc.), data processing the layer also saves the previous analysis to improve the result. This layer can share the processed data with other connected devices through the network layer.

Application layer (end-user interface/mobile applications): The application layer implements and presents the results of the data processing layer to run various applications of IoT devices. The application layer is the user-centric layer which performs various tasks for users. There exist different IoT applications like smart transportation, smart home, personal care, healthcare, etc.

Activity: Demonstrate IOT architecture

Considering a use case of a smart home where Temperature, Humidity, Pressure, Motion and Lux Sensors are used to capture useful data of the House. The client needs to monitor all the sensors 24x7 through an application.

Following are the steps to demonstrate the architecture of IOT in a system.

Step 1: Identify the components of the sensing layer: Temperature, Humidity, Pressure, Motion and Lux Sensors. All these sensors measure the environmental data and send it to an intelligent device for processing.

Step 2: Identity the network layer components: As all these are wired devices a simple wired connection is more suitable to act as a communication channel. We can use the IOT Gateway for transfer of data from sensors to processing unit.

Step 3: Identify the Processing layer components: All the data collected by different sensors are first processed in the cloud server and meaningful information is extracted for the client.

Step 4: Identify the Application components: A mobile is a necessity of every human being. Especially when they are out of home they use this portable device to monitor every minute details related to home, office, business, clients etc. Thus, mobile applications are the best application to monitor the data measured by individual sensors inside the house.

Thus, the connectivity of all four layer are shown in the fig.----- as per the architecture of IoT.

1.3 Architecture of IoT

IoT architecture is the structural framework that defines how Internet of Things devices communicate, process data, and interact within a network.

Internet of things is based on four simple building blocks – 1) Sensors 2) Internet of Things (IoT) framework & gateway 3) cloud server 4) mobile app. These are also called IoT architecture layers. It is shown in Figure 1.5.

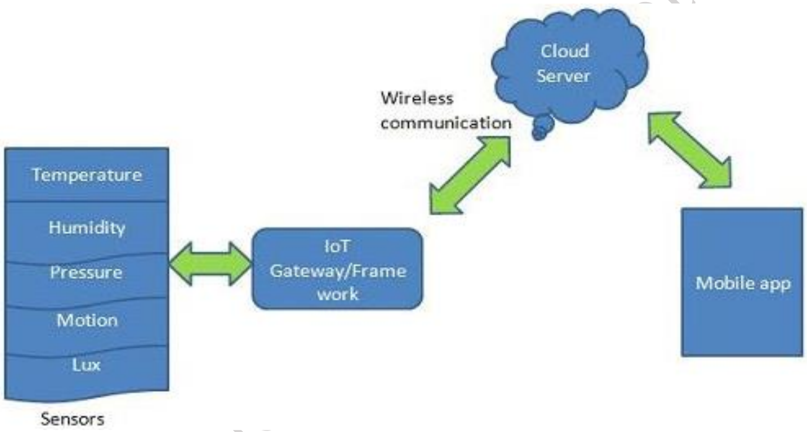


Fig. 1.5: Basic connection between different components of IoT in a Network

IoT architecture consists of four main layers: the sensing layer (sensors and actuators), the network layer (gateways and nodes), data processing layer and the application Layer (cloud-based platforms and end-user interfaces). This architecture enables seamless connectivity, data collection, and real-time decision-making, forming the foundation for a smart and interconnected ecosystem.

Sensing layer (sensors and actuators): The main purpose of the sensing layer is to recognize any phenomena in the peripheral devices and obtain information from the real world.

This layer consists of several sensors. Use of multiple sensors for applications is one of the main features of Internet of Things devices. Sensors are everywhere, sensors sense data from the atmosphere or place, for example temperature sensor senses temperature from the room and shares it through IoT gateway. Sensor will sniff a wide variety of information ranging from Location, Weather/Environment conditions, running machine, from the human body, engine maintenance data to health essentials of a vehicle.

Network layer (IoT gateways and nodes): The network layer acts as a communication channel that transfers the information collected in the sensing layer to other connected devices. The network layer is implemented in IoT devices by using different communication technologies (e.g. Wi-Fi, Bluetooth, Zigbee, Z-Wave, LoRa, cellular network, etc.) to allow data flow between other devices on the same network.

This layer consists of IoT Gateways & frameworks. As the name rightly explains, it is a gateway to the internet for all the things/devices that we want to interact with. Gateways act as a carrier between the internal network of sensor nodes with the external Internet or World Wide Web. They do this by collecting the data from sensor nodes and transmitting them to the internet infrastructure.

Data Processing layer (cloud server): The data processing layer consists of the main data processing unit of IoT devices. The data processing layer gathers data collected in the sensing layer and analyses the data to make decisions based on the outcome. In some IoT devices (e.g. smart watches, smart home hub, etc.), data processing the layer also saves the previous analysis to improve the result. This layer can share the processed data with other connected devices through the network layer.

Here a cloud server is used to store the data. The data transmitted through the gateway is stored & processed securely within the cloud server i.e. in data centres. This processed data is then used to perform intelligent actions that make all our devices Smart Devices. In the cloud, all analytics and decision making happen considering user comfort.

Application layer (end-user interface/mobile applications): The application layer implements and presents the results of the data processing layer to run various applications of IoT devices. The application layer is the user-centric layer which performs various tasks for users. There exist different IoT applications like smart transportation, smart home, personal care, healthcare, etc.

The intuitive mobile apps will help end-users to control & monitor their devices (ranging from the room thermostat to vehicle engines) from remote locations. These apps push important information from the cloud on your smartphones, tablets. After analytics, Information is in the form of graphs, bars and in pi-diagram and display to the user in a user-friendly manner. From mobile application, we can send a command to sensors to change default values, like changing default temperature of air conditioner and many more. The architecture of IoT comprising these four layers are shown in Figure 1.6.

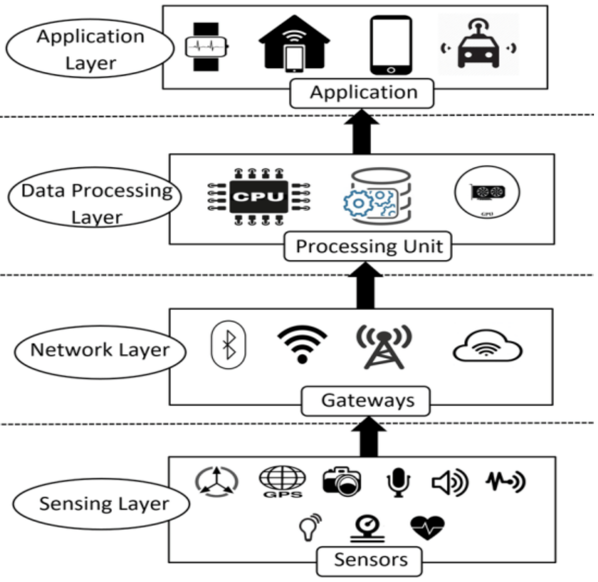


Fig. 1.6: Architecture of IoT

Assignment 1. Draw the diagram of the architecture of the Internet of Things on a sheet.

1.4 Applications of Internet of Things

IoT transforms healthcare, smart homes, agriculture, and industries through remote monitoring, energy efficiency, predictive maintenance, and streamlined processes. It also influences transportation, wearables, and smart cities, showcasing its versatile impact across diverse sectors as shown in Figure 1.7.

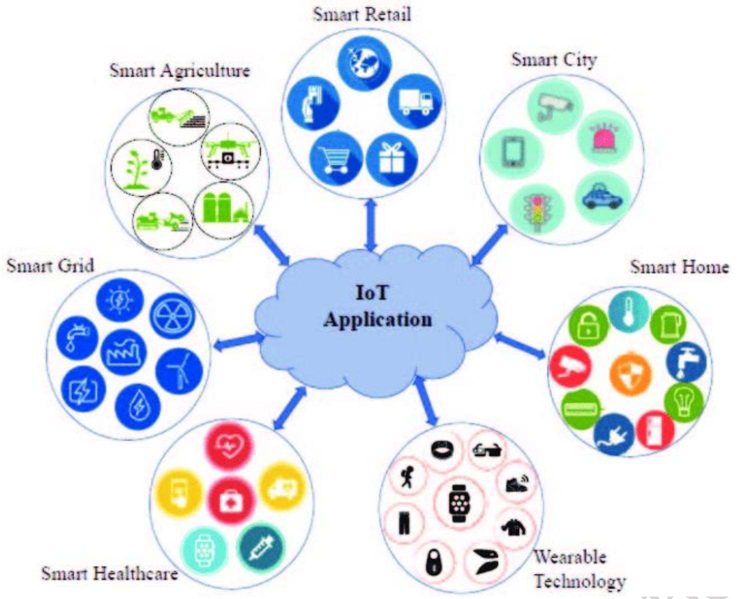


Fig. 1.7: Applications of IoT

1.4.1 Smart Homes – Developing smart homes has caused a revolution in designing residential homes. Smart home products would save energy, time and money. A Smart Home would enable the owner to control household jobs at the house even from a remote location. For example, switching on the air conditioner or heaters minutes before reaching home, switching on / off the lights, controlling the washing machine, etc. It is depicted in the Figure 1.8.

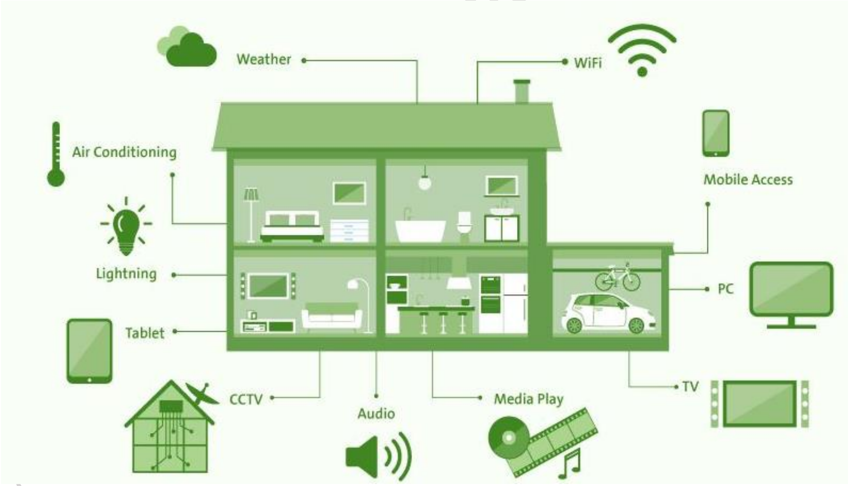


Fig. 1.8: Smart Homes

1.4.2 Wearable Devices – Wearable devices include wrist watches or glasses that are installed with sensors and software which collect and analyse data. Companies like Google and Samsung have invested heavily in building such devices. These devices broadly cover fitness, health and entertainment requirements. A major challenge for developing such systems is that it should be lightweight, small in size and should have very low power consumption as shown in Figure 1.9.

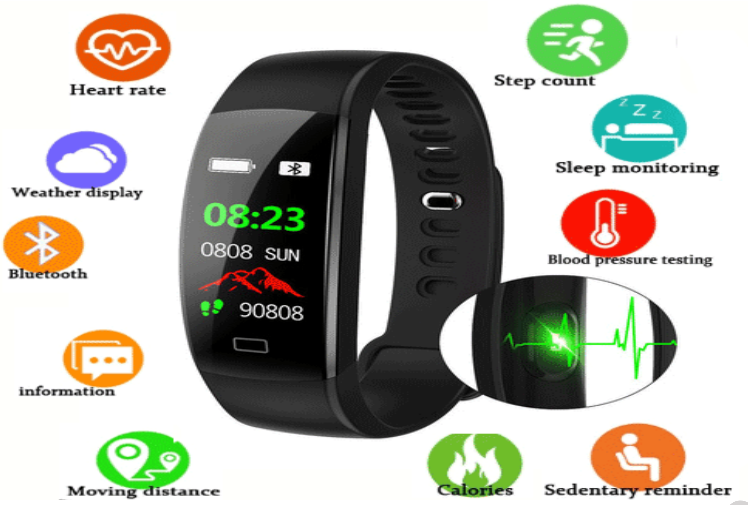


Fig. 1.9: Wearable Devices

1.4.3 Traffic Monitoring – Vehicles should be capable of optimizing its operation, fuel consumption, pollution control, maintenance and comfort of passengers. A breakthrough will be achieved if such smart traffic could be developed as it would drastically reduce road accident casualties. By installing sensors and using web applications, citizens can also find free available parking slots across the city. It can be understood by the Figure 1.10.

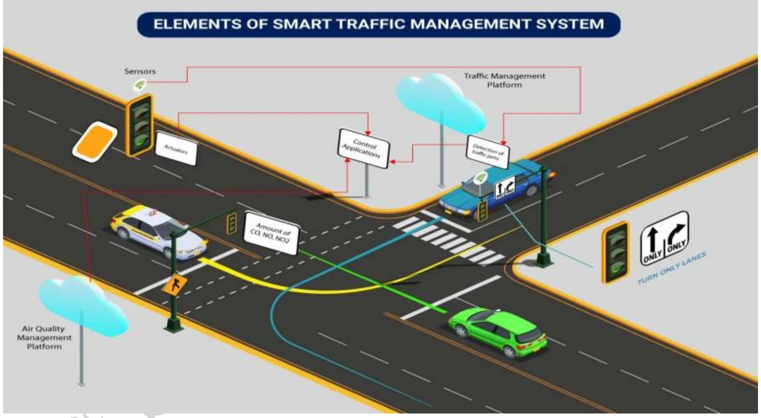

ELEMENTS OF SMART TRAFFIC MANAGEMENT SYSTEM
Sensors
Traffic Management Platform
Actuators
Control Applications
Detection of traffic jams
Amount of CO, NO, NO2
ONLY
ONLY
TURN ONLY LANES
Air Quality Management Platform

Fig. 1.10: Traffic Monitoring System using IoT

1.4.4 Industrial IoT – Industrial IoT (IIoT) is the new buzz in the industrial sector. It is empowering industrial engineering with sensors, software and big data analytics to create brilliant machines. IoT holds great potential for quality control and sustainability. Applications for tracking goods, real time information exchange about inventory among suppliers and retailers and automated delivery will increase the supply chain efficiency. It is shown in Figure 1.11.

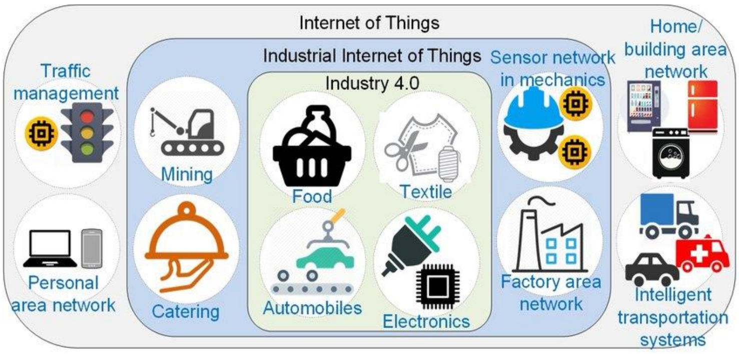


Fig. 1.11: Industrial Internet of things

1.4.6 Smart Cities – Smart cities are another area gaining immense interest from the public. Smart surveillance, automated transportation, smarter energy management systems, water distribution, urban security and environmental monitoring all are examples of internet of things applications for smart cities. It will solve major problems faced by the people living in cities like pollution, traffic congestion and shortage of energy supplies etc. Products like cellular communication enabled Smart trash will send alerts to municipal services when a bin needs to be emptied. Example of this application is given in Figure 1.12.

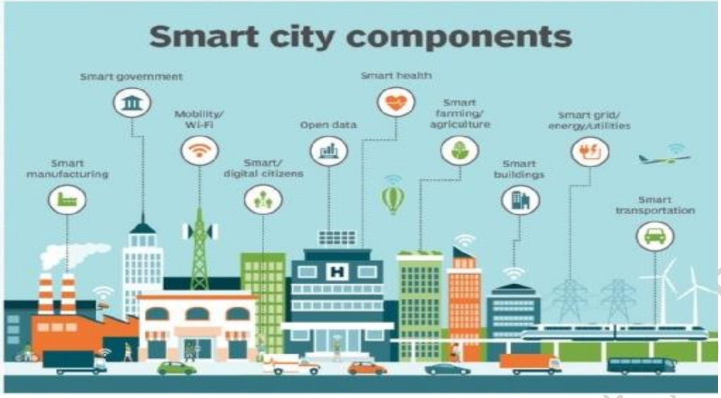


Fig. 1.12: Smart Cities

1.4.7 Agriculture: With the continuous increase in world's population, demand for food supply is extremely high. Governments are helping farmers to use advanced techniques and research to increase food production. Smart farming is one of the fastest growing fields in IoT. Farmers are using meaningful insights from the data to yield better return on investment. Sensing for soil moisture and nutrients, controlling water usage for plant growth and determining custom fertilizer are some simple uses of IoT as shown in Figure 1.13.

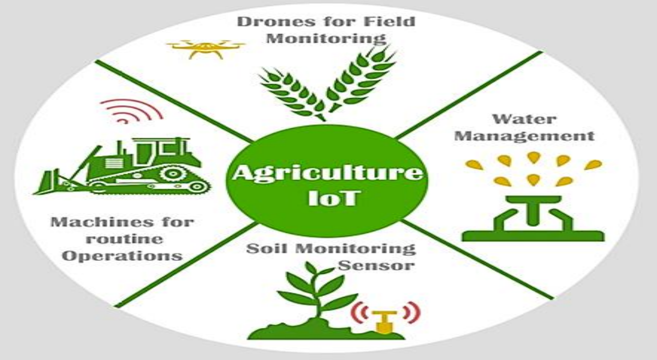


Fig. 1.13: Agriculture

1.4.8 Healthcare – The concept of a connected healthcare system and smart medical devices bears enormous potential not just for companies, but also for the well-being of people in general. Research shows IoT in healthcare will be massive in coming years. IoT in healthcare is aimed at empowering people to live healthier lives by wearing connected devices. The collected data will help in personalized analysis of an individual's health and provide tailor made strategies to combat illness as illustrated in Figure 1.14.

Fig. 1.14: Healthcare

Assignment 1. List the applications of the Internet of Things with examples on a chart.

1.5 Use of Mobile applications in IoT systems

In the domain of the Internet of Things (IoT), mobile applications serve as an essential interface, facilitating seamless communication and control between users and their networked devices.

These applications, often developed for iOS or Android platforms, are designed to optimize user experience in managing and monitoring IoT devices through smartphones or tablets. The technical integration involves leveraging specific programming languages, frameworks, and protocols tailored to IoT requirements.

Mobile apps in IoT typically interact with backend servers, databases, and application programming interfaces (APIs) to retrieve and update real-time data from connected devices. The development process involves utilizing integrated development environments (IDEs) and software development kits (SDKs) compatible with the target platforms. Additionally, mobile apps in IoT often employ security measures such as encryption and secure communication protocols to safeguard sensitive data transmitted between devices and applications. An example of a mobile app is shown in Figure 1.15.

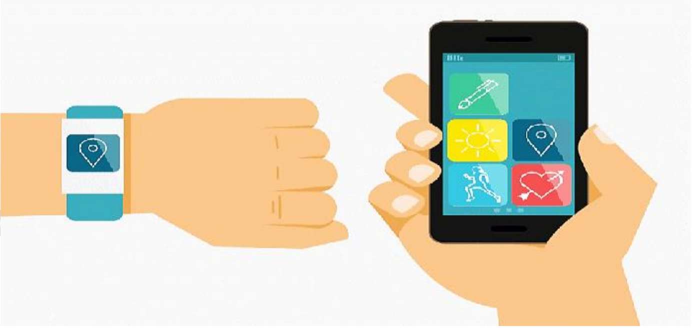


Fig. 1.15: Mobile app

These applications act as command centers, enabling users to remotely configure device parameters, receive sensor data, and execute commands within the IoT ecosystem. The intricate interplay between mobile apps and IoT contributes to a dynamic and responsive user experience, shaping the landscape of interconnected smart environments.

1.6 Different types of mobile applications used in IoT

In the context of the Internet of Things (IoT), various types of mobile applications serve distinct purposes, enhancing the functionality and user experience across diverse IoT ecosystems. Here are different categories of mobile applications commonly used in conjunction with IoT:

1.6.1Control Apps – Control apps empower users to actively manage and manipulate IoT devices remotely. They provide interfaces for adjusting settings, initiating actions, and controlling the behaviour of connected devices.

Example: A smart home control app that allows users to turn on/off lights, adjust thermostat settings, or manage security systems.

1.6.2 Monitoring Apps – Monitoring apps offer real-time updates and insights into the status and performance of IoT devices. Users can receive notifications, view data trends, and keep track of key metrics.

Example: An industrial monitoring app that provides real-time information about machinery operation, production metrics, and system health.

1.6.3 Configuration Apps – Configuration apps assist users in setting up and customizing their IoT devices. They often guide users through the initial setup process, enabling personalization and fine-tuning of device parameters.

Example: A wearable device configuration app that helps users set up preferences, update firmware, and customize features.

1.6.4 Health and Fitness Apps – These apps are often associated with wearable IoT devices and focus on health and fitness tracking. They monitor activities, record vital signs, and provide insights into users' well-being.

Example: A fitness tracker app that monitors steps taken, calories burned, and sleep patterns, syncing with a wearable IoT device.

1.6.5 Location-Based Apps – Location-based apps use IoT technology to provide services based on the user's geographic location. They can offer navigation, geofencing, or location-aware content.

Example: An IoT-based navigation app that considers real-time traffic data and suggests the fastest route based on current conditions.

1.6.6 Automation Apps – Automation apps allow users to create rules and scenarios for their IoT devices. These rules automate certain actions or responses based on predefined conditions.

Example: A smart home automation app that sets rules for lights to automatically turn off when no motion is detected for a specified period.

1.6.7 Communication Apps-Communication apps enable interaction between users and IoT devices or facilitate communication between devices. They may include chat interfaces or voice control features.

Example: A voice-controlled smart assistant app that allows users to verbally command and control various IoT devices in their environment.

These types of mobile applications collectively contribute to the seamless integration of IoT into various aspects of daily life, offering users flexibility, customization, and real-time control over their connected devices.

Summary

- In this chapter the concept of IoT (Internet of Things). IoT refers to a network of interconnected devices or "things" that can collect, exchange, and process data over the Internet.
- IoT devices are equipped with sensors or other means to gather data, and they are connected to the internet or other networks, enabling communication and data exchange.
- Data collected by IoT devices needs to be processed and analysed. This can occur on the device itself or in the cloud.
- IoT has diverse applications, including smart homes, industrial automation, healthcare, agriculture, transportation, and more.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the full form of IoT? (a) Internet of Technology (b) Incorporate of Things (c) Internet of Things (d) Incorporate of Technology
2. What is IoT? (a) Network of physical objects embedded with sensors (b) Network of virtual objects (c) Network of objects in the ring structure (d) Network of sensors
3. Which of the following is used to capture data from the physical world in IoT devices? (a) Sensors (b) Actuators (c) Microprocessors (d) Microcontrollers
4. Which of the following is an example of an IoT device? (a) Laptop (b) Fitness tracker (c) A television set (d) A landline telephone
5. IoT is based on _____ technology. (a) Hardware (b) Software (c) None (d) Both of these
6. What is the main purpose of IoT? (a) To collect and analyse data from connected devices (b) To control home appliances remotely (c) To improve online shopping experiences (d) To create a virtual reality environment
7. What is a sensor in IoT? (a) A device that converts physical or environmental parameters into digital signals (b) A device that connects to the internet and sends data (c) A device that provides a graphical user interface (d) A device that runs software programs
8. What is a gateway in IoT? (a) A device that connects IoT devices to the internet (b) A device that stores data collected by IoT devices (c) A device that analyses data collected by IoT devices (d) A device that provides a user interface for IoT devices
9. Which of the following is an example of an IoT application in healthcare? (a) Online shopping for medical supplies (b) Remote patient monitoring (c) Electronic medical record management (d) Telemedicine consultations
10. Which of the following is an example of an IoT application in agriculture? (a) Online crop sales platform (b) Farm management software (c) Weather forecasting app (d) Smart irrigation system

B. Fill in the blanks

1. IoT is the intersection of the __________.
2. ____________ acts as a communication channel that transfers the information collected in the sensing layer to other connected devices.
3. IoT technology uses _________ to store large amounts of data.
4. Devices and sensors are components of the_______________.
5. An Internet connection gives each device an_________.
6. Applications of Internet of Things are________________.
7. A Smart Home would enable the owner_________.
8. ___________implements and presents the results of a data processing layer to run various applications of IoT devices.
9. User interfaces are _________of an IoT system that is accessible to users.
10. ________ acts as a middle layer between the devices and the cloud.

C. State true or False for the following

1. A sensor is a device that runs software programs.
2. Smart grid technology is an example of an IoT application in energy management.
3. RFID is a part of IoT.
4. The Internet of Things can help organizations improve the efficiency and productivity of manufacturing processes and operations.
5. Once connected to the home gateway, smart devices can be controlled from a smartphone, tablet, or PC.
6. Microcontrollers are used to capture data from the physical world in IoT devices.
7. Smoke Alarm is not an IoT device?
8. Arduino is not an application of IoT?
9. Cloud is the way in which an IoT device is associated with data.
10. The network layer acts as a communication channel that transfers the information collected in the sensing layer to other connected devices.

D. Short Answer Type Questions

1. What is the Internet of Things (IoT)?
2. What is the main purpose of IoT?
3. What is a sensor in IoT?
4. What is a gateway in IoT?
5. What is a smart home in IoT?
6. How is IoT used in daily life?
7. What are the fundamental components of IoT?
8. List the most used sensor types in IoT.
9. Which devices are used in IoT?
10. Which types of sensors can be used in agriculture?

Session 2. Controller Boards

Ramesh had lots of wonderful qualities like he is capable of doing several tasks in a very short time without demanding anything. He is ready to work all day without any breaks. He never makes mistakes, neither exhausted, and never wastes time on unnecessary things. Because of having such qualities people like him and respect him as a leader and depend on him to fulfil their requirements. Microprocessors and microcontrollers are the leader in technology requirements nowadays. A Microprocessor is capable of doing several million tasks round the clock without any break with 100% efficiency. It is used in various applications of daily uses like in banking sectors, railways (IRCTC), E-commerce (AMAZON), etc.

2.1 Microprocessor

Microprocessors are semiconductor single-chip devices that act as miniaturized computers but not as full-fledged computers. On a single chip, its CPU houses registers, an interrupts circuit, an arithmetic and logic unit (ALU), a stack pointer, and a program counter. Typically, ROM and RAM, a memory decoder, an oscillator, and a number of serial and parallel ports must be added to create a complete microcomputer as shown in Figure 2.1.

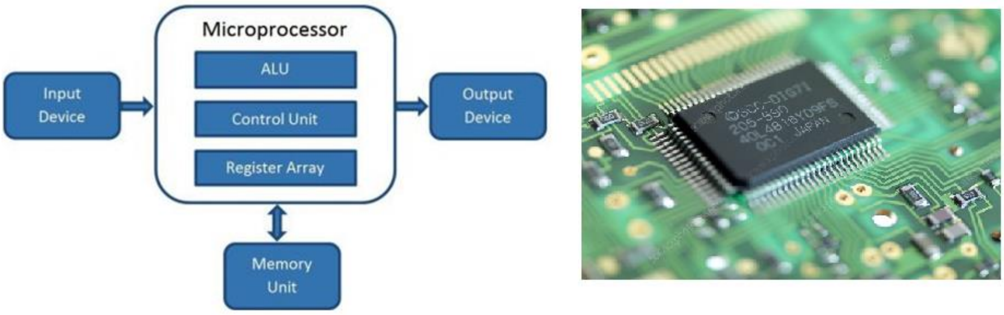


Fig. 2.1: Microprocessor (a) Simple block diagram (b) Microprocessor chip

Application of microprocessor includes Desktop PC's, Laptops, notepads etc.

2.2 Microcontroller

A microcontroller (or VLSI microcomputer) is a computing device integrated on a single chip. Unlike a microprocessor, a microcontroller has a CPU with RAM, ROM, and other necessary peripherals, all embedded on a single chip.

It is a kind of minicomputer in a circuit that allows any hardware to communicate effectively with other devices. Microcontrollers are the heart of any IoT device because they are small, require less power, and perform the necessary functions like any advanced microprocessor. In IoT applications, the microcontroller is cheap as most of the internal pins are user programmable and all components can be integrated on a single board, which reduces the size of the entire computing unit.

All microcontrollers are designed to perform specific tasks. Microcontrollers can be of 4-bits, 8-bit, 64-bit, or 128-bits configuration, depending on the functionality of the embedded system. The Figure 2.2(a) shows the block diagram of the microcontroller and Figure 2.2(b) shows the microcontroller chip.

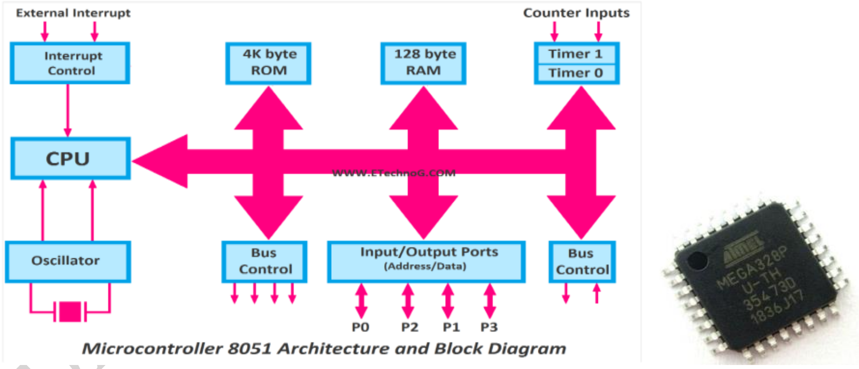


Fig.2.2: Microcontroller a) block diagram of microcontroller b) Microcontroller chip.

2.1.1 Types of Microcontroller

There are numerous types of microcontrollers available, each tailored to specific applications and industry. Some of the widely used microcontrollers include:

8051 Microcontroller	A popular and versatile microcontroller with a simple architecture, commonly used in embedded systems and educational projects.
PIC Microcontroller	Manufactured by Microchip Technology, PIC (Peripheral Interface Controller) microcontrollers are widely used in industrial automation, automotive applications, and consumer electronics.
Arduino Microcontroller	Although not a specific microcontroller, the Arduino platform often uses ATmega series microcontrollers. Arduino is popular for its ease of use in prototyping and educational projects.

AVR Microcontroller	Developed by Atmel (now a part of Microchip Technology), AVR microcontrollers are known for their efficiency and are commonly used in various applications, including robotics and IoT.
Raspberry Pi (System on a Chip-SoC)	Although not strictly a microcontroller, Raspberry Pi is a credit-card-sized computer that includes a microprocessor and various peripherals. It is used for a wide range of applications, including education and hobbyist projects.
ESP Microcontroller	Popular in IoT applications, ESP microcontrollers, such as the ESP8266 and ESP32, offer built-in Wi-Fi capabilities, making them suitable for connected devices and projects.
STM32 Microcontroller	Produced by STMicroelectronics, STM32 microcontrollers are based on the ARM Cortex-M architecture. They find applications in industrial control, automotive systems, and consumer electronics.
MSP430 Microcontroller	Developed by Texas Instruments, MSP430 microcontrollers are known for their ultra-low power consumption and are commonly used in battery-operated devices.
Zilog Z80 Microcontroller	An older but still relevant microcontroller, the Z80 is known for its role in early home computers and embedded systems.

These are just a few examples, and the field of microcontrollers is vast and continually evolving. The choice of a specific microcontroller depends on the requirements of the project, including factors such as processing power, memory, peripherals, and power consumption.

2.1.2 Applications of Microcontroller

Microcontrollers are used in multiple industries and applications, including in the home and enterprise, building automation, manufacturing, robotics, automotive, lighting, smart energy, industrial automation, communications and internet of things (IoT) deployments.

One very specific application of a microcontroller is its use as a digital signal processor. Frequently, incoming analog signals come with a certain level of noise. Noise in this context means ambiguous values that cannot be readily translated into standard digital values. A microcontroller can use its ADC and DAC to convert the incoming noisy analog signal into an even outgoing digital signal.

The simplest microcontrollers facilitate the operation of electromechanical systems found in everyday convenience items, such as ovens, refrigerators, toasters, mobile devices, video game systems, televisions and lawn-watering systems. They are also common in office machines such as photocopiers, scanners, fax machines and printers, as well as Smart meters, ATMs and security systems.

More sophisticated microcontrollers perform critical functions in aircraft, spacecraft, ocean-going vessels, vehicles, medical and life-support systems as well as in robots. In medical scenarios, microcontrollers can regulate the operations of an artificial heart, kidney or other organs. They can also be instrumental in the functioning of prosthetic devices.

2.3 Comparison of microprocessor and microcontroller

The table 2.1 lists the difference between a microprocessor and a microcontroller:

Table 2.1 Comparison of a microprocessor and a microcontroller

Comparison Parameters	Microprocessor	Microcontroller
Functional Units	ALU, registers, CU.	ALU, register, CU, IO port, RAM, ROM, ADC, DAC, timer and counters.

Data transfer instructions	It has large number of data transfer instructions.	Comparatively a smaller number of such instructions.
Cost	High	Comparatively low.
Size of PCB	Large	Small in comparison to microprocessor.
Weight	Bulky	Less bulky
Processing speed	1 GHz	8 to 50 MHz
Uses	Finds its use in general purpose computing systems.	Uses in systems that are manufactured for specific application.
Efficiency	Less efficient	More efficient
Power consumptions	High	Low in comparison to microcontroller
Reliability	Less reliable	More reliable
Example	8085, 8086 etc	8051, 8951 etc.

2.4 IoT Development Boards

A development board is essentially a printed circuit board with circuitry and hardware for experimenting with specific microcontrollers, microprocessors, or other complex integrated circuits (IC). Specifically, an IoT development board includes:

- A programming interface to program the microcontroller from a computer.
- A power circuit used to provide stable DC power to the microcontroller.
- Input components: buttons, switches, etc.
- Output components such as LEDs.
- Various I/O pins used for compatibility with sensors, motors, screens, and any other components.

IoT development boards allow for tinkering and easy access to I/O pins to build custom circuitry and easily develop firmware.

2.5 IoT Development Board Categories

There are three broad categories of IoT boards as shown in Figure 2.2.

1. Microcontroller-based Boards
2. Single board Computer (SBC)
3. System -on -Chip (SOC)board

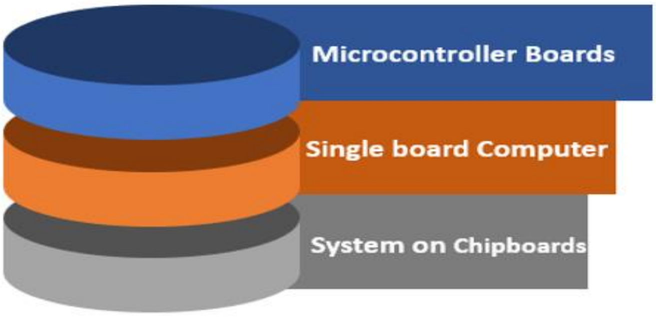


Fig. 2.3 Board Categories

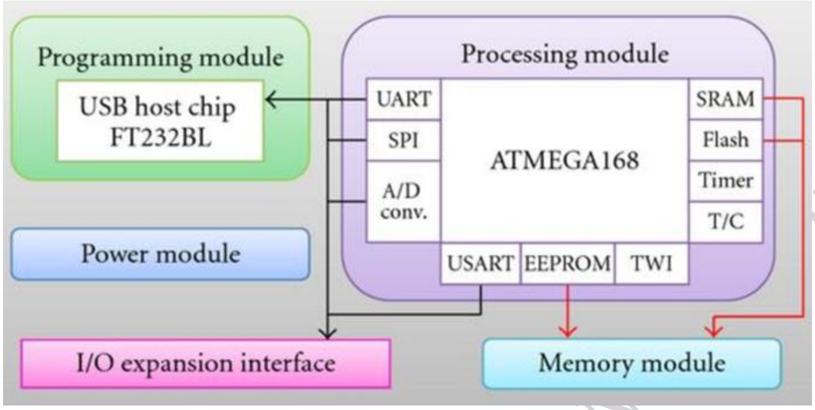
The most common IoT development boards are – *Arduino, Node MCU ESP8266, Raspberry Pi.*

2.6 Arduino Uno Board

It is an ATmega328P microchip-based open-source microcontroller board produced by Arduino Uno, a tech company. The board has arrays of digital and analog input/output pins that can be interfaced with different boards for expansion and other circuits.

Block Diagram of Arduino Uno Board

The major blocks in Arduino Uno consist of Processing Module, Programming Module, Power Module, I/O Expansion Interface etc.



Processing Module

The Processing Module is ATmega328 microcontroller (MCU) used in Arduino UNO R3 as a main controller. ATmega328 is from the AVR family and is an 8-bit device. 8-bit device can handle 8 parallel data signalsat a time because its data-bus architecture and internal registers are of 8-bit.

ATmega328 has three types of memory:

Flash Memory: 32KB nonvolatile memory. This is used for storing application, which explains why you don't need to upload your application every time you unplug arduino from its power source.

SRAM Memory: 2KB volatile memory. This is used for storing variables used by the application while it's running.

EEPROM Memory: 1KB nonvolatile memory. This can be used to store data that must be available even after the board is powered down and then powered up again.

UART Peripheral: A UART (Universal Asynchronous Receiver/Transmitter) is a serial interface. The ATmega328 has only one UART module.

The pins (RX, TX) of the UART are connected to a USB-to-UART converter circuit. Serial communication is carried out through two pins called Pin 0 (Rx) and Pin 1 (Tx).

SPI Peripheral: Another serial interface is SPI (Serial Peripheral Interface). Besides using it as a serial interface, it can also be used to program the MCU using a standalone programmer. One can reach the SPI's pins from the header next to the MCU in the Arduino UNO board or from the digital header as below:

10<->SS

11<->MOSI

12<->MISO

13<->SCK

SPI communication takes place with the help of the SPI library.

Two Wire Interface: The I2C or TWI is an interface consisting of only two wires, serial data, and a serial clock: SDA, SCL. TWI communication is accessed through Wire Library. A4 and A5 pins are used for this purpose.

A/D Converter: Analog signals take on any value within a range of values. ADC is an interface between the sensor and microcontroller. It converts an analog signal into a digital signal and gives it to the microcontroller. Arduino Uno has 6 0n-board ADC channels which can be used to read analog signal in the range 0-5V.

Power Module: This module helps in connecting the Arduino uno to the power source. The option available are the USB or a DC Jack. It consists of a 5V regulator NCP1117ST50T3G and the Vin of this regulator is connected via DC jack input through the M7 diode. The output of the 5V regulator is connected to the rest of 5V net in the circuit and also to the input of the 2.3V regulator, LP2985-33DBVR. You can access 5V directly from the power header 5V pin.

I/O Expansion Interface – This block provides digital inputs and outputs (digital I/O) on the Arduino. It allows the connection of digital sensors, actuators, and other ICs to the Arduino Uno. This block helps in doing some really useful things, such as reading switch inputs, lighting indicators, and controlling relay outputs. Digital signals have two distinct values: HIGH (1) or LOW (0). You use digital signals in situations where the input or output will have one of those two values. For example, one way that you might use a digital signal is to turn an LED on or off.

Programming Module: This module provide communication between Arduino Uno and the USB port of the PC simply by connecting them with a USB cable. Programs (sketches) created on the PC can be written to the Arduino Uno, and the Arduino Uno can be controlled from the PC via serial communication. The Arduino Uno can also be powered via USB instead of the power jack.

Arduino Uno consists of 6 analog inputs,14 Input/output pins, 16MHz quartz crystal, a reset option, and an ICSP header. Since this board fully supports the microcontroller, it can simply be connected to a device with a USB cable or power to start with an AC-to-DC converter or battery.

Arduino Uno board can be programmed to perform specific functions. It can be programmed using the Arduino Integrated development environment (IDE) which is open source. This allows the user to design and program electronics and IoT systems. An Arduino board can be connected to other boards and circuits using its input/output (I/O) pins. This open-source board's communication interfaces are comparable to USB, which enables computer program loading. The Figure 2.4 shows an Arduino Uno board.

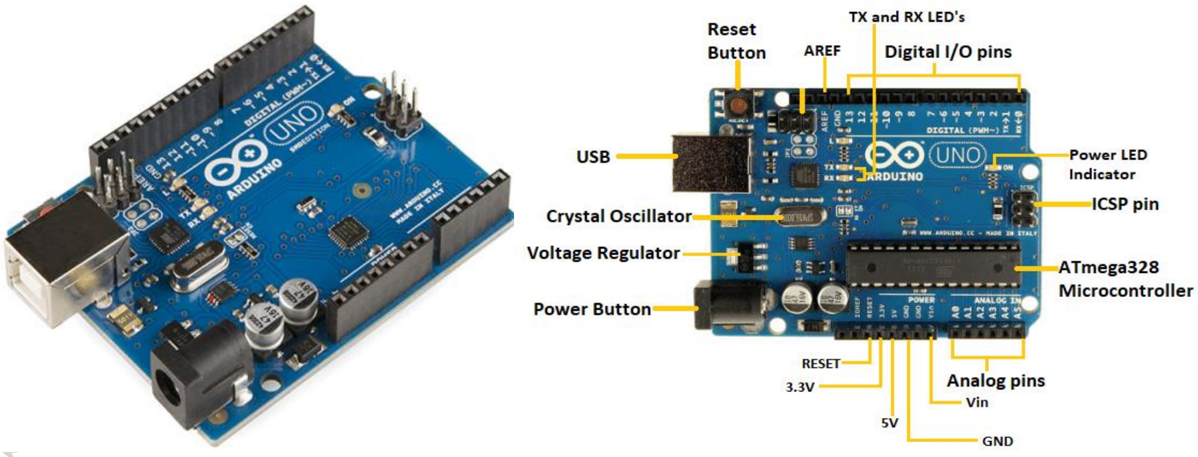


Fig.2.4: Arduino Uno Board

2.6.1 Pin Configuration of an Arduino Uno Board

The Arduino microcontroller has several pins which are used for different functions. The pin layout of an Arduino board is displayed in the Figure 2.5.

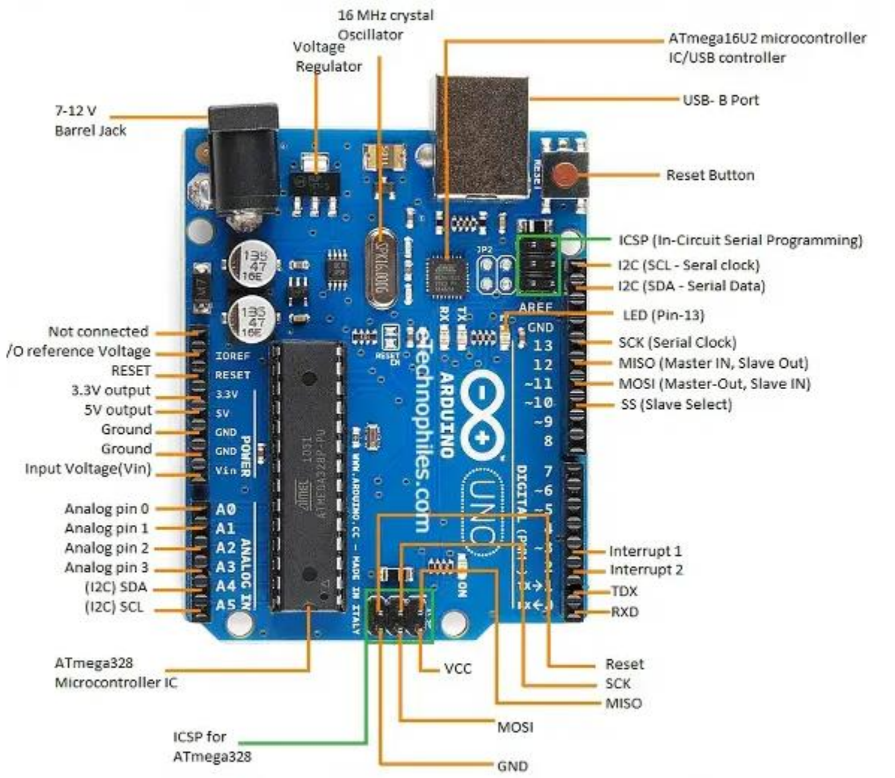


Fig.2.5: Pin configuration of an Arduino Uno board

The functions of important pins are as follows:

- **USB –** The computer's USB connector can be connected to the Arduino board with a USB port.
- **Voltage Regulator –** A voltage regulator controls the voltage supplied to the Arduino board. It regulates the DC voltage supplied to the processor or other components.
- **Crystal Oscillator –** This is an electronic oscillator that creates electric voltage signals by utilizing the mechanical resonance produced by the vibration of piezoelectric quartz crystals. The crystal oscillator is used to keep track of time and frequency for the Arduino board. The crystal oscillator normally has a frequency of 16MHz.
- **Reset –** Arduino reset is required to reset the values of the Arduino board to their inherent values. This is useful when coding a new program function. Although Arduino comes with its own reset button, the user can also have an external Arduino reset button, so that it can be reset externally. An Arduino board can be reset to its factory settings. The UNO board can be reset by two methods. By using the reset button on the board or connecting the external reset button to the Arduino pin labelled RESET.
- **Power Button –** Arduino can be powered from the Barrel Jack or USB connector.
- **GND Pin –** This is the "Ground pin" which is used to ground the circuit.
- **2.3VPin –** Supply 2.3 output volt.
- **5V Pin –** Supply 5 output volt.
- **Vin –** This pin can be used to power the Arduino board from an external power source.
- **Analog Pins –** The Arduino UNO board has six analog input pins - A0, A1, A2, A3, A4 and A5. Analog sensors like temperature sensor or humidity sensor read signals from these pins by converting it into a digital value which acts as an input for the microprocessor.
- **Microcontroller** (Atmega 328 microcontroller): The main microcontroller on the Arduino Uno board is used to perform all the complex functions of an IoT device.

- **ICSP Pin –** ICSP is an AVR tiny programming header for the Arduino. It is also known as Serial Peripheral Interface (SPI), which is a kind of "expansion" of the output, and the output device is a slave to the master of the SPI bus.
- **Power LED Indicator –** The power LED indicator denotes the power supply in the microcontroller device. Power LED indicator lights up when the Arduino is connected to a power source. If the light is not turned on then there is some kind of fault with the connection. Power LED indicators use various modes to indicate the status which are as follows:
  - **Slow flashing green** – On aircraft mode using low power
  - **Flashing green** – Using battery power with good battery power
  - **Fast flashing amber** – Using a battery with low power
  - **Rapid flashing red** – Power on with very low power using battery
  - **No LED** – Power off or battery empty
- **Tx and Rx LEDs –** On the Arduino Uno board, there are two labels, TX (transmit) and RX (receive), which are placed separately. The orange/yellow colored TX and RX pins are used for USB connection. They indicate the data transmission flow in a circuit. TX LED represents the flow of data from the Arduino to the computer, while RX LED shows the data transmission from the computer to the microcontroller. Figure 2.6 shows these two LEDs.

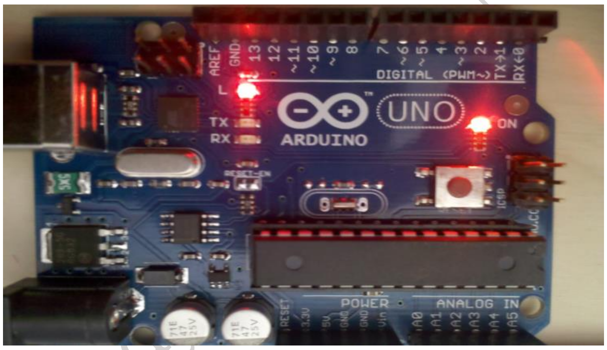


Fig.2.6: Tx and Rx LEDs on Arduino board

- **Digital I/O –** Arduino UNO board comes with 14 digital I/O pins, out of which 6 are used for Pulse Width Modulation (PWM) output. These pins can be coded as input digital pins to read logic values (0 or 1) or as digital output pins for connecting LEDs, relays and so on. The pins marked "~" can be used to generate PWM.
- **Analog Reference (AREF) –** AREF feeds the reference voltage from external power supply in the Arduino. The voltage supplied from a voltage regulator IC of a maximum of 2.3V is directed to the AREF pin.

Practical Activity 2.1. To identify the parts of an Arduino board in the given Figure 2.7.

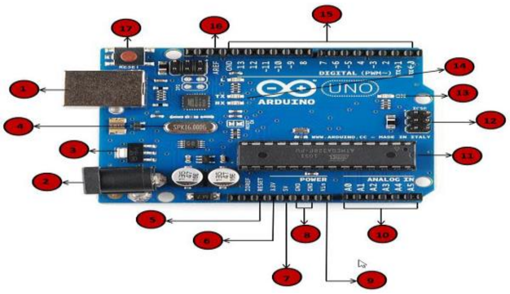


Fig.2.7: Arduino board

Material Required: Arduino Board, jumper wires

Procedure:

Step 1. Study the pin diagram of Arduino board given in Figure 2.8.

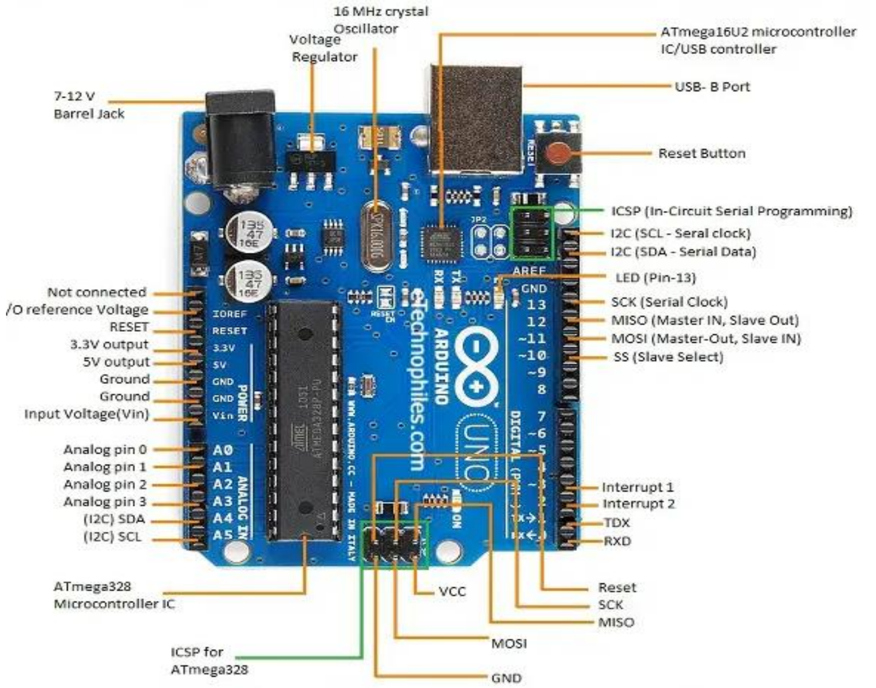


Fig.2.8: Pin diagram of Arduino board

Step 1. Label the pin numbers given in the practical activity as shown in Figure 2.9.

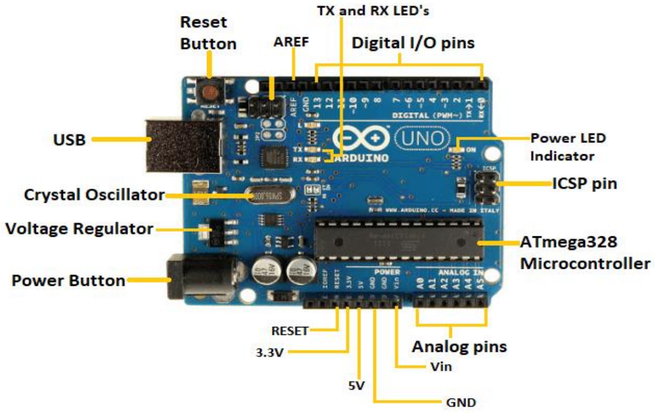


Fig.2.9: Labelled diagram of Arduino board

2.7 Node MCU ESP8266 IoT-enabled Board

Node MCU is an open-source platform based on ESP8266 created by Expressive Systems which can connect objects and let data transfer using the Wi-Fi protocol. A Wi-Fi module called ESP8266 enables microcontrollers to join a network and create basic Wi-Fi applications. It has several general-purpose input/output (GPIO) pins that are useful for interacting with external sensors and devices. It is used to enable the internet connection to various applications of embedded systems. The general features of this board are as follows:

- Easy to use
- Programmability with Arduino IDE or other programming languages such as Python, Micro python etc.
- Available as an access point or station.

- practicable in Event-driven API applications.
- Having an internal antenna.

The Node MCU ESP8266 IoT-enabled Board is shown in Figure 2.10.

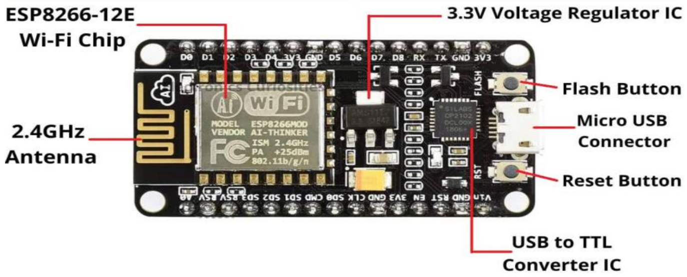


Fig.2.10: Node MCU ESP8266 IoT-enabled Board

2.7.1 Node MCU Development Board Pinout Configuration

The pin configuration of Node MCU ESP8266 is shown in Figure 2.11.

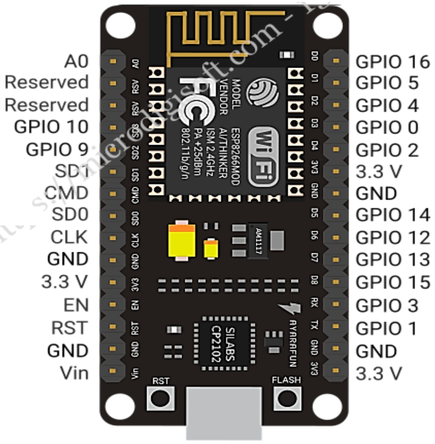


Fig.2.11: Node MCU ESP8266 Pin Diagram

The functions of important pins are discussed in table 2.1.

Table 2.2: Node MCU Development Board Pin Configuration

Pin Category	*Name*	*Description*
Power	Micro-USB, 2.3V, GND, Vin	**Micro-USB:** Node MCU can be powered through the USB port **2.3V:** Regulated 2.3V can be supplied to this pin to power the board **GND:** Ground pins **Vin:** External Power Supply
Control Pins	EN, RST	The pin and the button reset the microcontroller
Analog Pin	A0	Used to measure analog voltage in the range of 0-2.3V
GPIO Pins	GPIO1 to GPIO16	Node MCU has 16 general purpose input-output pins on its board
SPI Pins	SD1, CMD, SD0, CLK	Node MCU has four pins available for SPI communication.

UART Pins	TXD0, RXD0, TXD2, RXD2	Node MCU has two UART interfaces, UART0 (RXD0 & TXD0) and UART1 (RXD1 & TXD1). UART1 is used to upload the firmware/program.
I2C Pins		Node MCU has I2C functionality support but due to the internal functionality of these pins, you have to find which pin is I2C.

Practical Activity 2.1. To demonstrate the LED Blinking with NodeMCU.

Materials Needed: NodeMCU board, Breadboard, LED (any color), Resistor (220 ohms), Jumper wires

Procedure:

Step 1. Insert the NodeMCU into the breadboard. Then, insert the LED into the breadboard, ensuring the longer leg (anode) is connected to a digital pin on the NodeMCU through a resistor (to limit current flow), and the shorter leg (cathode) is connected to the ground (GND) pin.

Step 1. Use jumper wires to connect the components as follows:

Step 2. Connect the anode of the LED to a digital pin (e.g., D1) on the NodeMCU.

Step 4. Connect the cathode of the LED to the ground (GND) pin on the NodeMCU.

Step 5. Optionally, use a resistor between the LED anode and the digital pin to limit current flow and protect the LED.

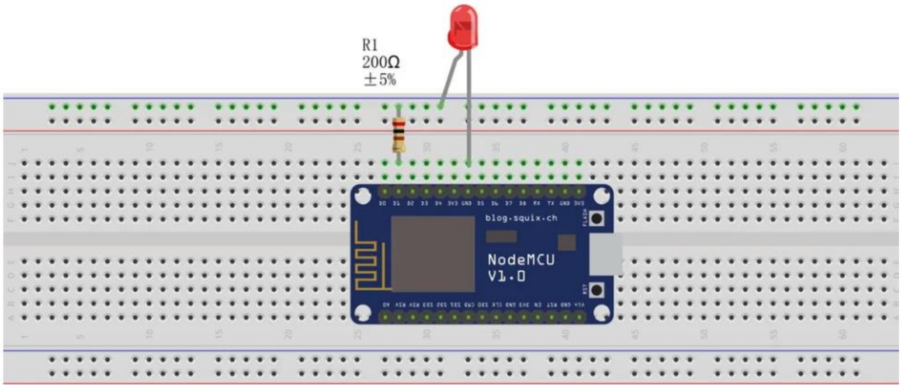
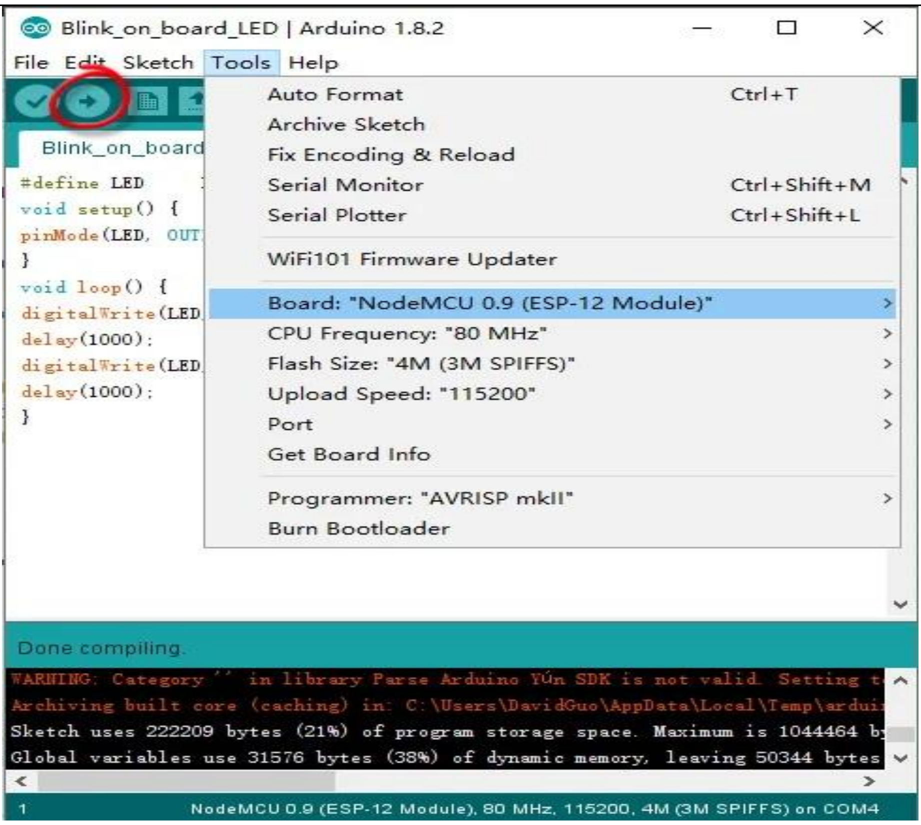


Fig.2.12: Connection of Node MCU

Step 6. Double-check all connections to ensure they are secure and correctly made.

Step 7. Power Up the NodeMCU: Connect the NodeMCU to a power source (e.g., USB port) to power it up.

Step 8. Select the board on Arduino IDE.


Blink_on_board_LED | Arduino 1.8.2
File Edit Sketch Tools Help
Blink_on_board
Auto Format Ctrl+T
Archive Sketch
Fix Encoding & Reload
Serial Monitor Ctrl+Shift+M
Serial Plotter Ctrl+Shift+L
WiFi101 Firmware Updater
Board: "NodeMCU 0.9 (ESP-12 Module)"
CPU Frequency: "80 MHz"
Flash Size: "4M (3M SPIFFS)"
Upload Speed: "115200"
Port
Get Board Info
Programmer: "AVRISP mkII"
Burn Bootloader
Done compiling.
1
NodeMCU 0.9 (ESP-12 Module), 80 MHz, 115200, 4M (3M SPIFFS) on COM4

```
#define LED
void setup() {
pinMode(LED, OUT
}
void loop() {
digitalWrite(LED
delay(1000);
digitalWrite(LED
delay(1000);
}
```

```
WARNING: Category '' in library Parse Arduino Yún SDK is not valid. Setting t
Archiving built core (caching) in: C:\Users\DavidGuo\AppData\Local\Temp\ardui
Sketch uses 222209 bytes (21%) of program storage space. Maximum is 1044464 b
Global variables use 31576 bytes (38%) of dynamic memory, leaving 50344 bytes
```

Step 9. Upload below code to Arduino IDE.

```
#define LED D1 // Led in NodeMCU at pin GPIO16 (D0).
void setup() {
pinMode(LED, OUTPUT); // set the digital pin as output.
}
void loop() {
digitalWrite(LED, HIGH);// turn the LED off.(Note that LOW is the voltage level but actually
                      //the LED is on; this is because it is acive low on the ESP8266.
delay(1000);          // wait for 1 second.
digitalWrite(LED, LOW); // turn the LED on.
delay(1000);         // wait for 1 second.
}
```

Step 10. Observe LED Behaviour: Once powered, the LED should start blinking if everything is connected correctly. If it doesn't blink, double-check the connections and troubleshoot any issues.

2.8 Raspberry Pi

Raspberry Pi is a series of low-cost, credit-card-sized single-board computers that can be used for a variety of purposes, such as learning to program, running basic computer applications, and building DIY projects. The Raspberry Pi was first introduced in 2012 by the Raspberry Pi Foundation, a UK-based charity that aims to promote computer science education and the use of technology for social good.

The Raspberry Pi is designed to be an affordable and accessible platform for learning and experimentation. It is equipped with a processor, memory, USB ports, HDMI port, and other components that are found in traditional computers. It can be used as a standalone computer, or as a component in a larger project, such as a home automation system, a media center, or a gaming console.

The Raspberry Pi runs on Linux-based operating systems, such as Raspbian, which is specifically designed for the Raspberry Pi. It can also run other operating systems like Ubuntu, Windows 10 IoT Core, and others.

One of the key features of the Raspberry Pi is its versatility. It can be used in a wide range of applications, from basic programming projects to complex industrial control systems. It has become a popular platform for makers, hobbyists, educators, and researchers.

Raspberry Pi includes a series of small single-board computers that run on the Raspbian operating system created for Raspberry Pi.

It is a compact single-board computer created by the Raspberry Pi Foundation to support computer literacy initiatives in underdeveloped nations. A Raspberry Pi's processor has evolved from the Broadcom BCM2835 SoC to the most recent generation Broadcom BCM2838 SoC, which has a 1.2 GHz 64-bit quad-core ARM Cortex-A53 processor. RAM can be anywhere from 256 MB to 1 GB. It comprises a power unit, 4 USB ports, and an extendable board. A USB keyboard and mouse make operating the single-board computer simple. The Raspbian operating system, which is based on Debian, works best with the Raspberry Pi, but it can also be used with Windows 10 IoT Core, Snappy Ubuntu Core, and Ubuntu MATE. A Raspberry Pi can be seen in the Figure 2.12.

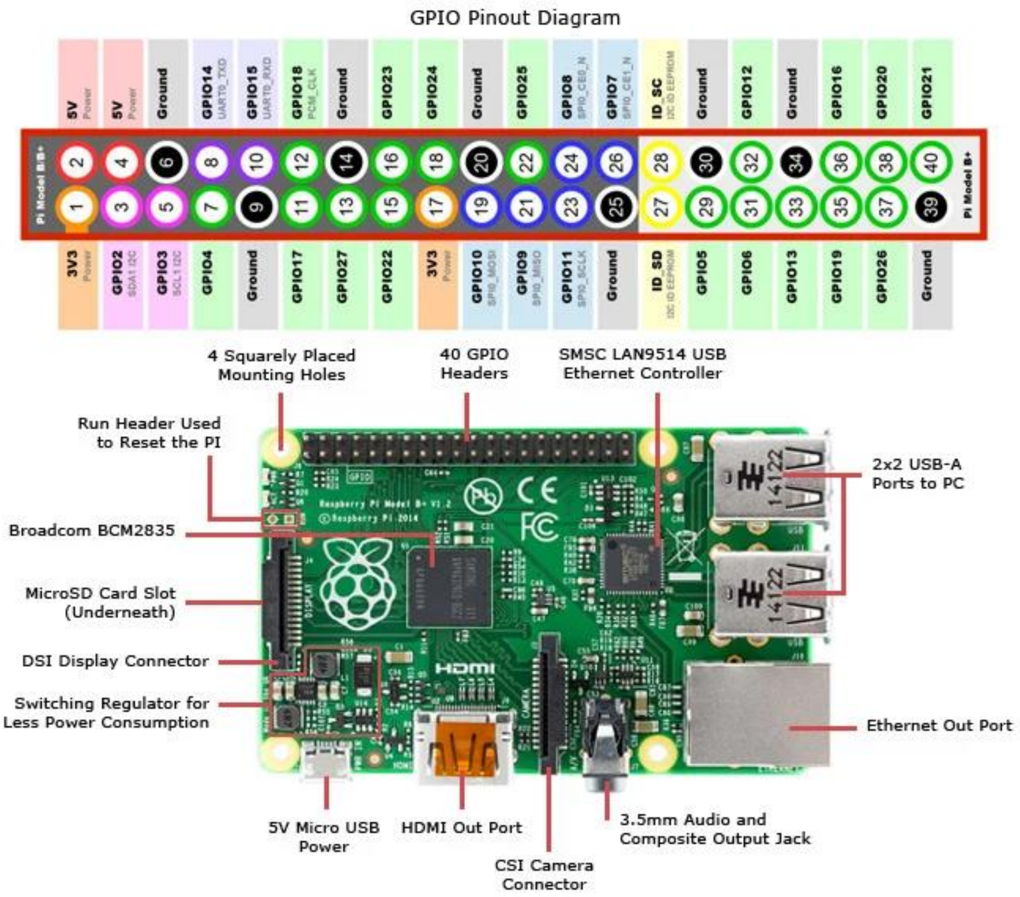


Fig. 2.13: Raspberry Pi Board

2.8.1 Pin Configuration of Raspberry Pi Board

An open-source board that was initially developed for the Linux operating system serves as Raspberry Pi's main chip (a System-on-a-chip application). The CPU, graphics, memory, and USB controller are all onboard components that are controlled by this. The Raspberry Pi version has the following features:

- Broadcom BCM2837B0, Cortex-A53 (ARMv8) 64-bit SoC @ 1.4GHz
- 1GB LPDDR2 SDRAM
- 1.4GHz and 5GHz IEEE 801.11.b/g/n/ac wireless LAN, Bluetooth 4.2, BLE
- Gigabit Ethernet over USB 1.0 (maximum throughput 300 Mbps)

- Extended 40-pin GPIO header
- Full-size HDMI®
- 4 USB 1.0 ports
- CSI camera port for connecting a Raspberry Pi camera
- DSI display port for connecting a Raspberry Pi touchscreen display
- 4-pole stereo output and composite video port
- Micro SD port for loading your operating system and storing data
- 5V/1.5A DC power input
- Power-over-Ethernet (PoE) support (requires separate PoE HAT)
  - Lower power consumption
  - Better audio output

Practical Activity 2.2. Setting Up a Simple Raspberry Pi LED Circuit

Materials Needed:

Raspberry Pi board (any model), Breadboard, LED (any color), Resistor (220 ohms), Jumper wires, Micro USB power supply for Raspberry Pi, HDMI cable and monitor

Procedure:

Step 1. Insert the Raspberry Pi board into the breadboard.

Step 1. Connect the LED: Insert the LED into the breadboard, ensuring the longer leg (anode) is connected to a GPIO pin on the Raspberry Pi through a resistor, and the shorter leg (cathode) is connected to a ground (GND) pin.

Step 2. Connect the anode of the LED to a GPIO pin (e.g., GPIO17) on the Raspberry Pi.

Step 4. Connect the cathode of the LED to a ground (GND) pin on the Raspberry Pi.

Step 5. Connect a resistor between the LED anode and the GPIO pin to limit current flow and protect the LED.

Step 6. Connect the micro USB power supply to the Raspberry Pi to power it up.

Step 7. the LED should light up if everything is connected correctly. If it doesn't light up, double-check the connections and troubleshoot any issues. The connections are shown in Figure 2.14.

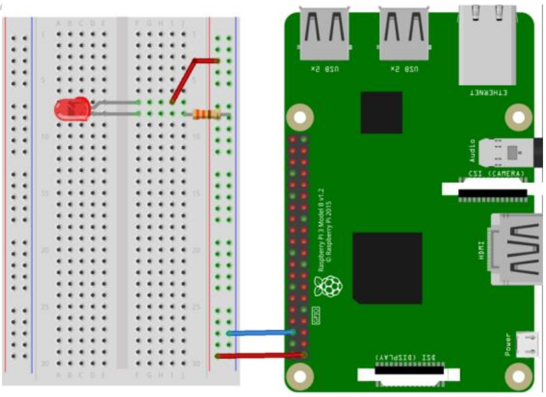


Fig.2.14: Raspberry Pi board connection with the breadboard

2.9 Comparison of various parameters of different controller boards

The table 2.3 shows a comparison between different types of controller boards used in IoT:

Table 2.3 Comparison of various parameters of Controller boards

Controller Boards	***Arduino***	***Raspberry Pi***	***ESP 8266***
CPU	ATmega328P	ARM1186	ESP 8266
GPU	None	Broadcom VideoCore IV	None
External Storage	MicroSD (AR9331)	SD card	--
Networking	By default, none Ethernet, Wi-fi, Bluetooth with shields	Ethernet, Wi-fi, Bluetooth	Wi-fiWi
Core	Single Core	Dual Core	Single Core
Architecture	8 bit RISC	64 bit ARM v8	32 bit LX106
Clock Speed	16 MHz	Up to 1.4GHz	Up to 160 MHz
Operating Voltage	5V	2.3V	2.3V
GPIO Voltage	5V	2.3V	2.3V
Digital Pins	14	26	16
PWM Pins	6	16	16
Analog Pins	6	3	1
Wi-fi	NO	YES	YES
Bluetooth	NO	YES	NO
Built-in Sensor	NO	Temperature Sensor	NO
Programming Language	Arduino IDE, C/C++	Micro python, C/C++	Arduino IDE, C/C++, Micro python, Java Script
On board Programming LED	D13 pin	GP 25 Pin	D0 Pin
RAM	264KB	1 GB	128KB
EEPROM	1KB	NO	520KB
Applications	Best for beginners and pro as there are many modules and library.	Best for machine learning	Best for internet of things

2.10 Programming a Controller Board

In order for the PCB sensors to work according to the desired function, they are programmed with different coding languages by the board developers. Different boards are supported and coded in various languages.

There are various languages in which a program can be written for controller boards. The language can be C, C++, Python, etc. The code is written on the related editor that comes with the board.

For example, Arduino programming can be done on Arduino IDE in the form of Arduino sketch. The code is opened in the editor and the “Upload” is clicked. If there are no errors in the program, there will be a message “Uploading Complete” at the bottom of the sketch. If there is any error, the section will show the lines with the error along with the line number.

2.11 Connectivity Options for controller boards

Smart gadgets are now widely used. The connection may be wired (such as Ethernet, phone, or power line) or wireless (such as RF transmission, spread spectrum, cellular, Wi-Fi, or Bluetooth). Home connectivity is provided by wired connections, which can either be phone lines or power lines and use short-range RF as the transmission medium. Therefore, controllers may need to send and receive messages while interacting with the hardware. There are various connectivity options for a microcontroller. The most commonly used are as follows:

2.11.1 Embedded Wi-Fi – Wi-Fi modules in controller boards have embedded WLAN modules that support IEEE 801.11 b/g/n Wi-Fi standards. They make it simple for users to enable Wi-Fi connectivity on embedded devices. These Wi-Fi modules, like the embedded WLAN stack, TCP/IP (Network) stack, and small-sized security supplicants, are plug-and-play gadgets. It is a self-contained solution actuated by a simple, 8/16/32 bit, low-cost, low-power MCU for Wi-Fi modules. Such microcontroller-based Wireless LAN modules, that is, Wi-Fi modules and subsystems mean high Wi-Fi throughputs.

2.11.2 Bluetooth – Some controller boards use Bluetooth connections. These self-contained modules are low-power and used mainly for wearables or IoT devices that need Bluetooth Low Energy IP Stack or radio frequency (RF) experience. This ensures ultra-low-power connections with extended battery life by 2 to 4 times compared to existing modules. The Bluetooth connectivity is used for the following applications:

- Battery-powered sensor devices
- Wearables
- Smart appliances
- Health and fitness trackers
- Home automation devices
- Consumer electronics
- Retail beacons
- Asset tracking devices

2.11.3 Low Power Wide Area Network – The technology for setting up low power WANs are Long-range Wireless (LoRa). LoRa uses modulation of digital spread spectrum and proprietary protocol in the sub-GHz RF band range. This makes low power consuming long-range high network capacity possible for more than 10 miles. For low power, WAN's gateways and cloud systems need to be in place.

SIGFOX uses an Ultra Narrow Band (UNB) based radio technology for connecting devices to its global network. It ensures a scalable, high-capacity network with low energy consumption. All this is done while maintaining an easy-to-implement star-based cell infrastructure.

2.11.4 Embedded Wireless – This can be divided into two bands as follows:

RF Remotes-Unlicensed Sub-GHz radio frequency bands - Industrial, Scientific, and Medical (ISM) are used for short-range, low-data-rate, and low-power wireless applications.

Sub-Ghz – License-free ISM frequency bands running at 1.4 GHz, 868 to 928 MHz, 433 MHz, and 315 MHz are used mainly for RF devices. They have compatibility for both unidirectional or bidirectional data communication. Such bands are used for target proprietary and standard-based wireless applications like smart metering, alarm systems, home automation, and the ever-popular IoT applications. For example, sensors in garage doors or radio-controlled outlets work with 433 MHz radio signals. In radio-controlled outlets, the radio sockets can be switched individually by reading the codes of the remote control with a receiver.

2.11.5 ZigBee (801.15.4) – ZigBee and IEEE 801.15.4 are standardized protocols essential for wireless sensor network applications. While 801.15.4 establishes the physical and MAC layers, ZigBee focuses on the network and application layers. Sensor network design necessitates prolonged battery life, affordability, compact size, and mesh networking capabilities. These requirements enable seamless communication among numerous devices within an interoperable, multi-application environment.

2.12 Optimization of the Controller Boards

Technological advancement has permitted the facility of getting a high CPU performance with low consumption of power within a small-scale unit. This is beneficial for various systems such as Wireless Sensor Networks (WSN). It is essential that a microcontroller gets optimum power. After the framework has been installed on a microcontroller, the technician is required to perform certain steps for optimizing the power consumption in the microcontroller chip. These steps are as follows:

1. Optimise the Pull-up Resistor – The resistor value should be optimized to its greatest possible value after the current value testing needed for signal transmission has been done. Power pull-up of resistors can be done by utilizing spare I/O pins.
2. Back up the Powering Devices – Buffers can be utilized to divide power domains for controlling the output quantity of the signal to the attached devices.
3. Decrease the Needed Voltage – The microcontroller board design should be such that the least voltage is needed for transmitting the signals; the lesser the voltage, the less the consumption of power.
4. Alter the Clock Frequency – Power consumption rises according to the clock frequency. If the clock frequency is decreased, the power consumption of the microcontroller will only be for operation times.
5. Choose the Right Oscillators – The time required for a capacitor to be charged or discharged can be reduced by selecting a lower capacitance and consequently the power consumption can also be decreased.
6. Voltage Drop and the Diode Leakage – Check the diodes for voltage drop or reverse leakage current as these causes significant power loss in the microcontroller. In a 1.4 GHz receiver/transmitter, the commands are sent with a signal/data package. A Raspberry Pi or an Arduino board can be equipped with a 1.4 GHz receiver / transmitter to receive commands from a base station and send back data.

2.13 Connecting IP-Enabled and Non-IP Enabled Devices

The IoT devices can be connected using IP-Enabled and Non-IP Enabled services. This is described as following:

2.12.1 Non-IP Enabled Devices

In IoT, the smart things are primarily connected via non-IP enabled services such as Z wave, ZigBee or Bluetooth. The steps for connecting the non-IP-enabled devices are as follows:

1. The control settings page of the ZigBee device gives access to the control panel which allows control of the devices.
2. The control panel should be accessed in addition to a new device.
3. Devices that are available for the required connections should be checked.
4. It should be ensured that the other device can be discovered and is ready for connection.
5. When the screen displays the other device, it should be selected for connection.
6. The indication that the device is paired confirms that the connection has been established.
7. Sometimes, a password is required for pairing. If this is so, enter identical passwords on both of the devices.

A sensor hub is used to process the data from individual sensors and produce app-ready data in order to connect the non-IP sensors. A compact, low-power microcontroller serves as this hub's implementation. The sensors could be co-packaged MEMS sensors, discrete devices, or fully integrated sensor devices. On-board sensors, for instance, might combine accelerometer, gyroscope, and magnetometer components with a microcontroller that processes the sensor data and makes the fused data, such as rotation vector, linear acceleration, or gravity, available.

2.12.2 IP Enabled Devices

An IP address is needed for connecting IP enabled devices via the Internet. The steps in connecting devices through IP are as follows:

1. The control panel should be accessed from one device.
2. The network and the sharing option should be opened.
3. The LAN, and WAN connection across which the device has to be connected should be selected.
4. Then, the properties window should be opened and the IPv4 option should be selected.
5. "Use the following IP address" should be selected.
6. The IP address 191.168.128.XXX should be entered; XXX can have any value less than 254.
7. The subnet mask should be SET to default 255.255.255.0.
8. The settings should then be saved by selecting OK.
9. It should be ensured that the other device is discoverable and linked to the LAN or WAN.
10. It should be ensured that the IP settings of the first device is set close to that of the other device.

IP enabled devices refer to those devices that are designed for non-IP-based communications but have been upgraded to provide IP-based communications with a single device. For example, the devices that can be connected through Wi-Fi and Ethernet have IP enabled microcontroller boards integrated in them.

Summary

- In this chapter, the distinction between a microprocessor, which is a general-purpose processor, and a microcontroller, which is specialized for specific tasks or device control is given.
- The introduction of various IoT development boards are given here, with popular boards including Arduino, Raspberry Pi, and ESP8266.
- The primary difference between Arduino and Raspberry Pi lies in their architecture. Arduino is a microcontroller board, while Raspberry Pi is a microprocessor-based single board computer (SBC).
- Additionally, an overview of the Node MCU ESP8266 board is also provided here, which is Wi-Fi enabled and known for its versatile applications.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. Which of the following is true about a microprocessor? (a) It has built-in memory and I/O ports. (b) It is a standalone computing device (c) It requires external memory and I/O devices (d) It is primarily used in embedded systems
2. What is the function of the Arithmetic Logic Unit (ALU) in a microprocessor? (a) Performs arithmetic and logic operations (b) Manages memory and I/O operations (c) Executes control instructions (d) Converts analog signals to digital signals
3. How does a microcontroller differ from a microprocessor? (a) A microcontroller is a standalone device, while a microprocessor needs external components (b) A microcontroller integrates memory, I/O ports, and a CPU on a single chip (c) A microcontroller is used in high-performance computing, while a microprocessor is used in low-power applications (d) A microcontroller has a higher clock speed than a microprocessor
4. What is the significance of embedded memory in a microcontroller? (a) It allows the microcontroller to store large amounts of data (b) It stores the firmware and data required for the microcontroller's

operation (c) It provides additional processing power to the microcontroller (d) It enables the microcontroller to connect to external devices

5. Which component of an Arduino board is responsible for controlling input and output operations? (a) Microcontroller (b) Voltage Regulator (c) Crystal Oscillator (d) USB Connector
6. In the pin diagram of an Arduino board, which pin is typically used for connecting external power? (a) VIN (b) GND (c) A0 (d) RX
7. What is the primary purpose of a Raspberry Pi board? (a) Microcontroller programming (b) Network routing and switching (c) General-purpose computing and coding projects (d) Graphic design and video editing
8. How many digital pins are available on a standard Arduino Uno board? (a) 6 (b) 8 (c) 12 (d) 14
9. Which of the following is primarily designed to perform arithmetic and logic operations on data in a computer system? (a) Microcontroller (b) Microprocessor (c) Memory module (d) Input device
10. What is the main function of a microcontroller? (a) Process instructions and data (b) Store large amounts of data (c) Display graphics on a screen (d) Provide internet connectivity

B. Fill in the Blanks

1. ____________operating systems are commonly used with Raspberry Pi.
2. Microprocessor is a circuit that functions as______ of the computer.
3. A Raspberry Pi Model typically has ___USB ports.
4. Raspberry Pi is a type of __________.
5. IoT development boards are of _______types.
6. _________ is an open-source electronics platform based on easy-to-use hardware and software in embedded systems.
7. The programming language commonly used with Arduino boards is_____.
8. A microcontroller board has a number of _____that can be used for various control functions.
9. The Raspberry Pi runs on Linux-based operating systems, such as ____ .
10. A ___________ controls the voltage supplied to the Arduino board.

C. State true or False for the following

1. Microcontrollers have built-in memory and peripherals, making them suitable for embedded systems.
2. Microcontrollers are generally more powerful than microprocessors.
3. The peripheral interface in a microcontroller is responsible for connecting to external devices and sensors.
4. The "GND" (Ground) pin on an Arduino board serves as a common reference voltage for connecting components.
5. Arduino board is a microprocessor -based board.
6. The HDMI port on a Raspberry Pi is primarily used for connecting external sensors.
7. Microcontrollers are designed for specific tasks include built-in memory and peripherals.
8. Microprocessors are primarily used in embedded systems and IoT devices.
9. The microcontroller requires less hardware devices.
10. Analog pins on an Arduino board can only read analog sensor values and cannot generate PWM signals.

D. Short Answer Type Questions

1. Define a microprocessor and provide an example of its application.
2. What distinguishes a microcontroller from a microprocessor? Give an example of an application where microcontrollers are commonly used.
3. What is an Arduino board?
4. Name two common programming languages used with Arduino boards.
5. What is Raspberry Pi, and what are its main applications?
6. What are some benefits of using microcontrollers and microprocessors in embedded systems?
7. What are some common operating systems compatible with Raspberry Pi?
8. Name three components commonly found on a microcontroller board.
9. Explain the role of input/output pins in microcontroller programming.
10. What are the connectivity ports in the microcontroller?

Session 3. Functions of Sensors and Actuators in IoT

Rahul and Iqbal found sensors and actuators all around them in a town. Due to a light sensor, they witnessed a lamppost lighting up at dusk. A crosswalk button changed the direction of the traffic lights. Motion sensors activated doors in a shopping mall, temperature sensors managed the air conditioning, and humidity sensors directed misters in a store. Bus doors were opened by pressure sensors, and a digital piano's music was improved by touch sensors. They became interested in the world of sensors and actuators after realizing how these technologies had subtly improved their lives.

3.1 Sensors

A sensor is a device designed to identify and react to specific inputs from the surrounding physical environment. These inputs may include light, heat, motion, moisture, pressure, or various other environmental phenomena. Typically, the sensor produces an output, often in the form of a signal, which can either be converted into a human-readable display at the sensor's location or transmitted electronically over a network for reading or subsequent processing. It is depicted in Figure 3.1.

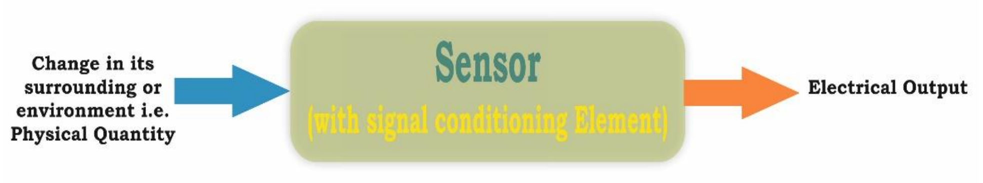

Change in its surrounding or environment i.e. Physical Quantity
Sensor
(with signal conditioning Element)
Electrical Output

Fig.3.1: Block Diagram of Sensor

Generally, sensors are used in the architecture of IOT devices. Sensors are used for sensing physical parameters, things, and devices. In order to detect the presence of a specific physical quantity, the sensor acquires a physical parameter and transforms it into a signal that can be processed (e.g., electrically, mechanically, or optically). The sensor's output is a signal that can be read by humans, such as changes in characteristics, resistance, capacitance, impedance, etc.

- The Internet of Things (IoT) technology, along with the sensors, are integrated using microcontrollers to produce a more accurate and reliable display of data than can be obtained using individual sensors. Sensors enable intelligent devices to have a much greater range than humans.

- These are at the front end of the IoT devices. These are the "Things" of the system. The main purpose of the sensor is to either collect data from its surroundings or to send out data to its surroundings (actuators).
- These have to be active which means that they should be able to collect real-time data. These can either work on their own (autonomous) or can be made to work by the user depending on their needs (user-controlled).
- For example - Door sensors are used to sense the door opening or closing.

3.1.1 Working of Sensors in IoT

Sensors are incorporated into IoT devices. These sensors have the ability to sense their environment. The information is kept on the devices as data in some format. Appliances like cell phones, coffee makers, microwaves, geysers, air conditioners, fire alarms, cars, and so forth are examples of these devices.

The embedded sensors in these devices continuously release information about their environment and operational details. All of the data collected by these devices can be processed and sent to the cloud via an IoT gateway, access point, or hub using various communication techniques. It is illustrated in Figure 3.1.

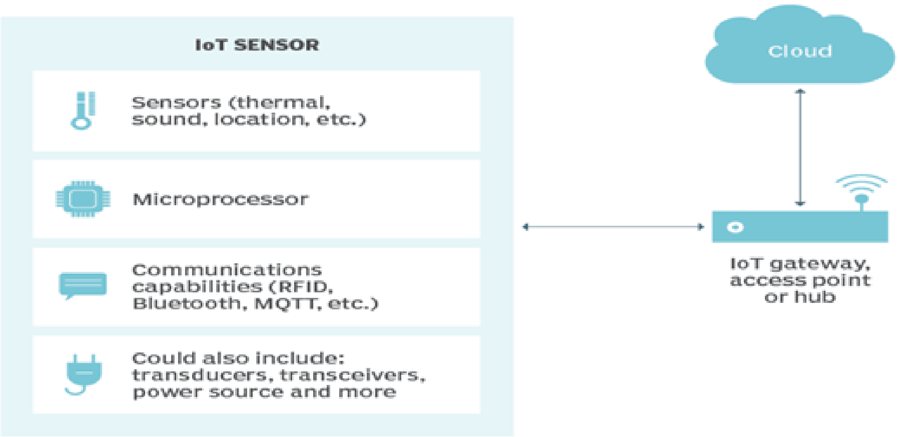

IoT SENSOR
Sensors (thermal, sound, location, etc.)
Microprocessor
Communications capabilities (RFID, Bluetooth, MQTT, etc.)
Could also include: transducers, transceivers, power source and more
Cloud
IoT gateway, access point or hub

Fig. 3.2: Working of IoT sensor

3.2 Sensor Classification

Sensors are categorized based on the physical quantities they measure, such as temperature, pressure, light, and motion. They can also be classified by their transduction mechanisms or operating principle, including resistive, capacitive, inductive, optical, and piezoelectric sensors.

Furthermore, sensors find application in diverse fields like industry, automotive, medicine, environment, and consumer electronics, highlighting their versatility in meeting specific measurement and detection needs across various domains. They can be also classified based upon the power requirements, output signal, etc. as shown in Figure 3.3.

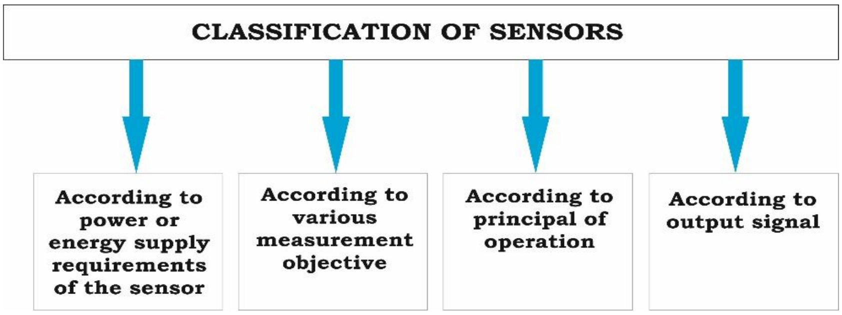

CLASSIFICATION OF SENSORS
According to power or energy supply requirements of the sensor
According to various measurement objective
According to principal of operation
According to output signal

Fig. 3.3: Classification of sensors

3.1.1 According to power or energy supply requirements of the sensor

Passive & Active

Passive Sensors cannot independently sense the input. Ex- Accelerometer, soil moisture, water level and temperature sensors.

Active Sensor can Independently sense the input. Example- Radar, sounder and laser altimeter sensors.

3.1.2 According to output signal

Analog & Digital

Sensors that produce an analog output signal that is a continuous function with respect to time input are called analog sensors. The signals generated by these sensors are measured proportionally. There are various analog sensors. Accelerometers, pressure sensors, light sensors, sound sensors and temperature sensors are some of the examples of analog sensors.

Sensors in which data conversion and transmission is done digitally are called digital sensors. A digital sensor mainly consists of three parts: the sensor, cable and transmitter. The measured signal is internally converted to a digital signal by the digital sensor itself. Cable transmits this digital information digitally. They are different types of digital sensors. A digital accelerometer and a digital temperature sensor are examples of digital sensors.

3.1.3 According to various measurement objective

Scalar & vector

Scalar sensor detects the input parameter only based on its magnitude. The response of the sensor is a function of the magnitude of some input parameter and it is not affected by the direction of input parameters. Example – temperature, gas, strain, color and smoke sensor.

In the working of vector sensor, the response of the sensor depends on the magnitude of the direction and orientation of the input parameter. Example – Accelerometer, gyroscope, magnetic field and motion detector sensors.

3.3 Different Types of Sensors used in IoT

There are various types of sensors available according to the application and requirement as shown in Figure 3.3.

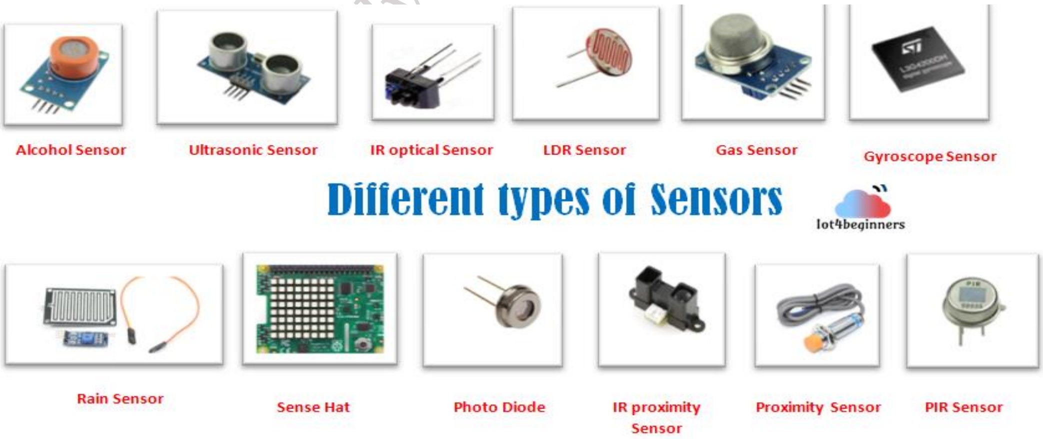


Fig. 3.4: Different types of sensors

In the IoT arena, there are some sensors that are extensively used for all types of applications. Based on their functionality, sensors can be classified as follows:

3.3.1 Temperature Sensor – Devices that monitor and track the temperature and give temperature measurement as an electrical signal are termed temperature sensors. These electrical signals will be in the form of voltage and are directly proportional to the temperature measurement. Earlier temperature sensors were only used for sensing temperature in appliances. For example, they were used in air conditioners and refrigerators to detect accurate temperatures. But with IoT, temperature sensors are now being used in every industry and application. These sensors dynamically measure the slightest of changes in temperature for accurate measurement.

Applications – The most basic example of a temperature sensor is a digital thermometer. The sensors measure the temperature of an object, detect any change in the temperature, and generate a signal in case of any change. These sensors are used in thermostats to maintain the temperature in the houses. Some common examples of temperature sensors are given in Figure 3.5.

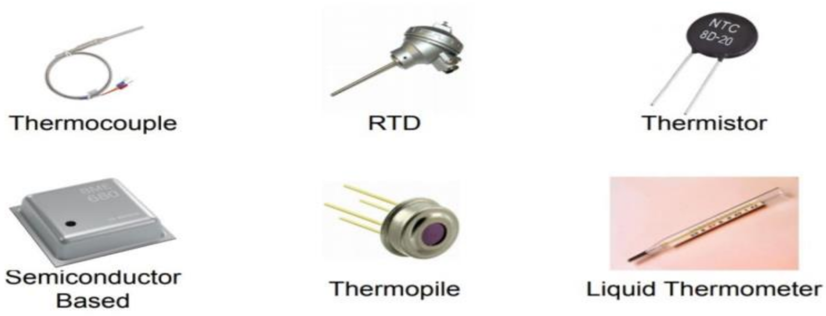


Fig. 3.5: Examples of temperature sensor

3.3.2 Proximity Sensor – This sensor is capable of detecting the movement of an object that is in its field of view. An electromagnetic field or electromagnetic control radiation is used for this, and then read variations in the return signal. Such sensors are used in mobile devices, autonomous vehicles or home monitoring devices that detect an intended purpose. Image of proximity sensor is shown in Figure 3.6.

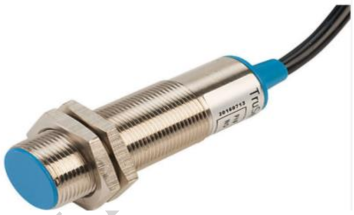


Fig. 3.6: Proximity Sensor

Applications: Garage doors use proximity sensors to open and close them when a car is nearby. They'll also be utilized in vehicles of the future that can detect other vehicles on the road.

3.3.3 Pressure sensor – These are used to measure a valid measurement per unit area of the pressure level of gases or liquids. The measured pressure level is converted into an analog electrical signal. It is depicted in Figure 3.7 given.

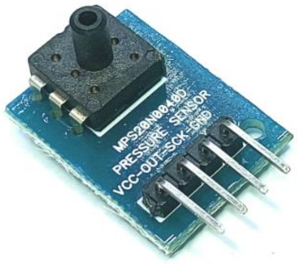


Fig. 3.7: Pressure Sensor

Applications – Applications for these sensors include manufacturing, aerospace, automotive, and hydraulic measurement. One typical illustration is a touch screen smartphone with pressure screen sensors that react to even the lightest pressure from a finger or pen. A car engine's pressure sensors, which control how much power is needed in accordance with throttle input, are another example. Pressure sensors are used in industries where pressure is related to warnings of a system of unfair conditions.

3.3.4 Accelerometer Sensor – These are dynamic sensors that can measure speed target speed change using microelectromechanical sensors (MEMS). These sensors are used to measure the vibration of machines or to detect a change in the speed moving objects. The accelerometer measures the change of speed in one, two, or three axes. Data transmission interface of accelerometers can be either analog, digital or pulse width modulated. Accelerometer Sensors look like as shown in Figure 3.8.

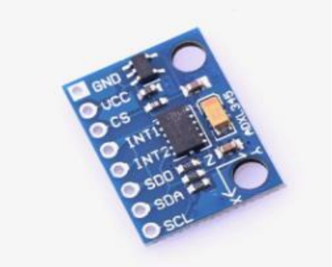


Fig. 3.8: Accelerometer Sensor

***Applications* –** An acceleration sensor is used to control acceleration in cars and machine parts and warns of inappropriate acceleration conditions. The sensor can be installed in a system that detects speed, vibration, position or gravitational acceleration and sets the orientation of the device.

For example, the sensors in smart phones help to rotate their display depending on how the phone is tilted. The Figure 3.9 shows the changing of the display orientation of a smart phone.

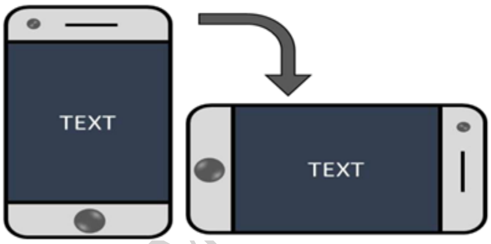


Fig. 3.9: Changing the display orientation of smartphone

3.3.5 Gyroscope Sensor – Utilizing acceleration sensors Along with the change in velocity detected by the accelerometer, gyroscope sensors also measure the angular rate of spin or rotation. The sensor measures deviation in a balanced position movement and corrects the movement in robotics or autonomous navigation systems. A gyroscope's user interface can be digital or analog. The image of this type of sensor is shown in Figure 3.10.

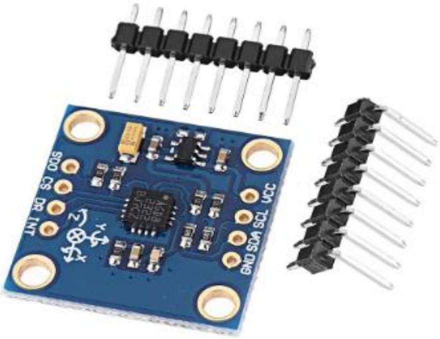


Fig. 3.10: Gyroscope Sensors

***Applications* –** Gyroscope sensors allow mobile apps to trigger an event. Modern self-balancing scooters or hoverboards and virtual reality goggles both use gyroscopic sensors as shown in Figure 3.11.

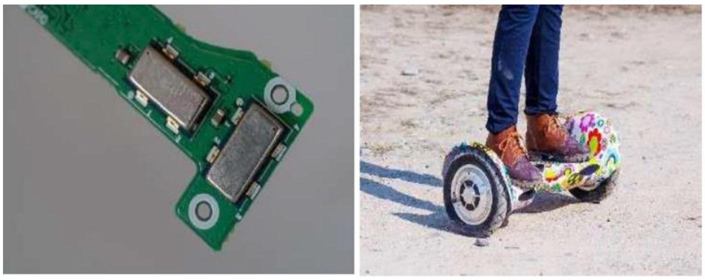


Fig. 3.11: Use of Gyroscopic sensors

3.3.6 Humidity Sensor – A humidity sensor, also known as a hygrometer, measures humidity level in the environment. It calculates relative humidity, which is the ratio of the amount of water in the air to the amount of moisture that can be kept constant at the specified air temperature. This is done by monitoring changes in electric current or temperature. It is depicted in Figure 3.11.

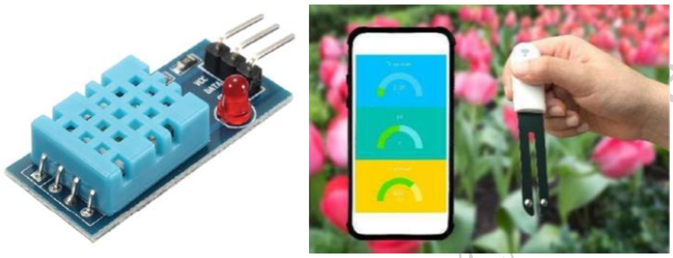


Fig. 3.12: Humidity sensor and Humidity sensor device

***Applications* –** Basically, these sensors are used in refrigerators and air conditioners to keep the area moist. The Figure 3.13 shows the device with the humidity sensor installed, as well as the display of a device that shows the temperature and humidity detected by the sensor.

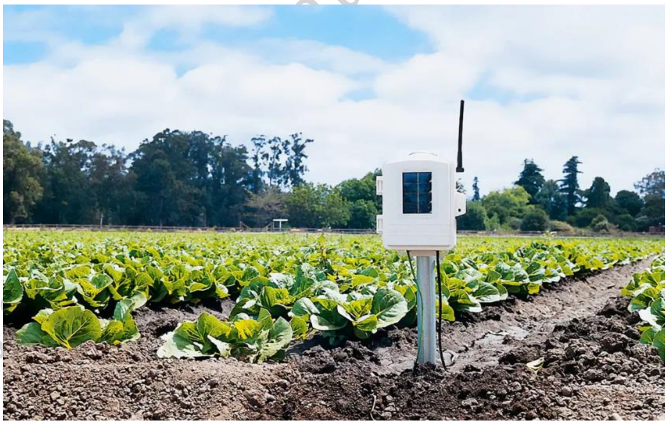


Fig. 3.13: Application of Humidity sensor device

3.3.7 Touch Sensor – A touch sensor is a sensitive device that detects physical contact and carries out the required operations. Detection of something like a touch of a finger or a stylus is known as a touch sensor. It is depicted in Figure 3.13.

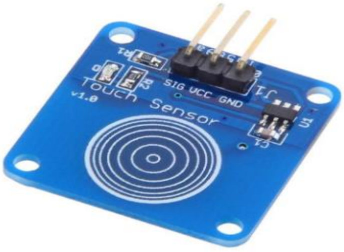


Fig. 3.14: Touch sensor

Touch sensors are sensitive to touch, force or pressure. They are one of the simplest and useful sensors. The working of a touch sensor is similar to that of a simple switch.

When there is contact with the surface of the touch sensor, the circuit is closed inside the sensor and there is a flow of current. When the contact is released, the circuit is opened and no current flows. The pictorial representation of working of a touch sensor is shown in the Figure 3.15.

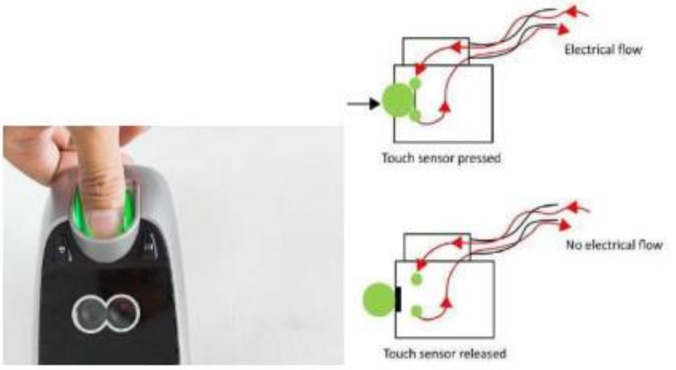


Fig. 3.15: Touch sensor (a) used in a door (b) working

Touch sensors are classified into two types:

1. Resistive type
2. Capacitive type

Today almost all modern touch sensors are of capacitive types. Because they are more accurate and have a better signal-to-noise ratio. These sensors are used to initiate a specific operation in mobile devices, home equipment, and other business equipment. The controller and software collaborate with the touch sensor to provide the necessary input and function.

Applications – These sensors are now widely used in security systems and locks, for example, used in offices and mobile phones.

3.3.8 Reed Sensor – It is an electromagnetic switch that regulates an electric current in the circuit and is constructed from ferrous reeds. The magnetization of the reed inside a tiny glass tube causes it to move in the direction of the switch. Electricity flows in the circuit when these reeds are in contact. Physical pressure is applied to such sensors, which have no mechanical wear. Reed sensor looks like as shown in Figure 3.16.

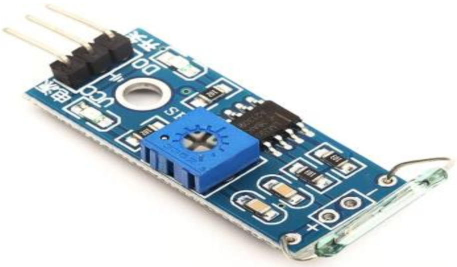


Fig. 3.16: Touch sensor

Applications – These sensors are employed in intelligent voltage regulators to regulate power supply voltage fluctuations.

3.3.9 Light sensor – Light sensor is also known as a photo sensor and one of the important sensors. Light dependent resistor or LDR is a simple light sensor available today as depicted in Figure 3.17.

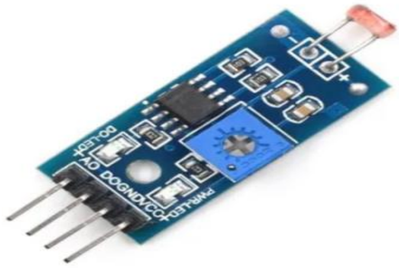


Fig. 3.17: Light sensor

The property of LDR is that its resistance is inversely proportional to the intensity of the ambient light i.e. when the intensity of light increases, its resistance decreases and vice versa.

Applications **–** Different types of light sensors can be used to measure illuminance, respond to changes in the amount of light received, or convert light to electricity.

3.3.10 Range sensor – Range sensors detect how near or far a component is from the sensing position. They can also be used as proximity sensors. Range or distance or sensors use non-contact analog techniques. It is shown in Figure 3.18.

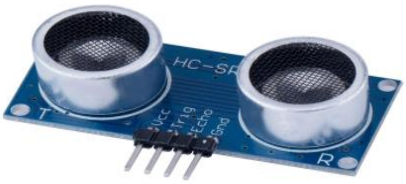


Fig. 3.18: Range sensor

Short-range sensing, between a few millimetres and a few hundred millimetres is carried out using electrical capacitance, inductance and magnetic technique.

Longer range sensing is carried out using transmitted energy waves of various types e.g. radio waves, sound waves and lasers.

Applications **–** Distance sensors are commonly used in robotics, automation, and other applications where accurate distance measurements are necessary. They can be used for obstacle detection, object tracking, and positioning, among other things.

3.3.11 Video Surveillance camera

This is a video recording device that captures footage of home and property that can be viewed on a smartphone, tablet, or computer from anywhere using an internet connection. Most video surveillance cameras are motion-activated and will record when they detect any motion, and simultaneously send an alert to the authorized person. It is shown in Figure 3.19.

Fig. 3.19: Video Surveillance camera

Applications

The video surveillance cameras are used in video surveillance systems. There are many applications of this type of cameras including Home Security systems, traffic monitoring, public safety systems. It can be used in educational institutions, healthcare facilities for monitoring and vigilance.

Assignment 1. List the various types of sensors with their applications in IoT on a chart.

Practical Activity 3.1: To test temperature sensor TMP36 using a multi meter.

Material Required: TMP36sensor, multi meter, connecting wires, AA batteries

Procedure:

Step 1. Connect a power supply that provides 1.7-5.5V (like 2-4 AA batteries) to the pins of TMP36 sensor as shown in Figure 3.20.

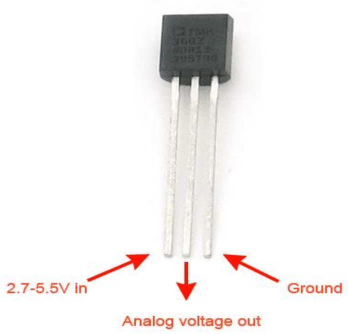


Fig.3.20: TMP36 sensor pin connections

Step 2. Make sure the ground is connected to pin 3 (the right pin), and power is connected to pin 1 (the left pin).

Step 3. Now, connect your multi meter in DC voltage mode to ground and the remaining pin 2 (the middle pin).

Step 4. As the TMP36 sensor is used here and the temperature is around room temperature (25°C), the reading on the multi meter should be about 0.75 V. However, if an LM35 sensor is used, the voltage will be around 0.25V. It is shown in Figure 3.21.

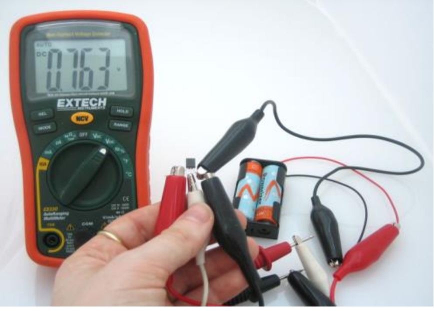


Fig.3.21: TMP36 sensor testing at room temperature

The sensor is indicating that the temperature is 26.3°C also known as 79.3°F.

Step 5. Now, the voltage range can be changed by pressing the plastic case of the sensor with fingers, a rise in temperature/voltage can be seen as shown in Figure 3.22.

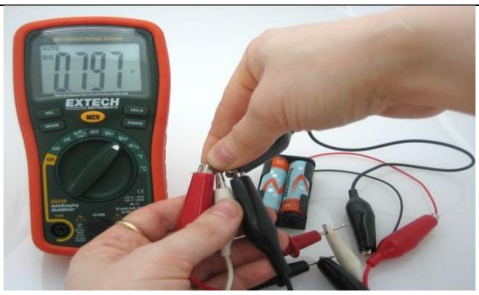


Fig.3.22: TMP36 sensor testing at high temperature

By putting fingers on the sensor, heating it up a little, the temperature reading is now 29.7°C / 85.5°F.

Step 6. Next, by touching the sensor with an ice cube (preferably in a plastic bag so it doesn't get water on your circuit) a drop in the temperature/voltage can be seen as depicted in Figure 3.23.

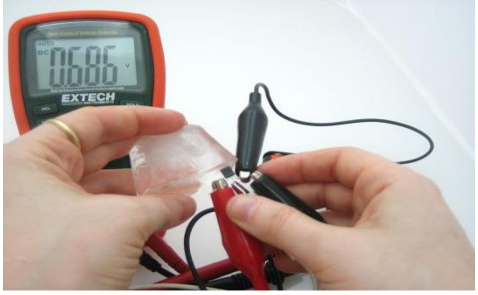


Fig.3.23: TMP36 sensor testing at low temperature

As an ice-cube is pressed against the sensor, temperature drops down to 18.6°C / 65.5°F.

Practical Activity 3.2. To demonstrate Light Sensing with a Light-Dependent Resistor (LDR)sensor

Materials Required:

Light-dependent resistor (LDR)Resistor (around 10kΩ), Breadboard, LED, BC547 Transistor Power source (e.g., battery or power supply), Multi meter (optional, for measuring resistance)

Procedure:

Step 1. Collect all the components as shown in Figure 3.24.

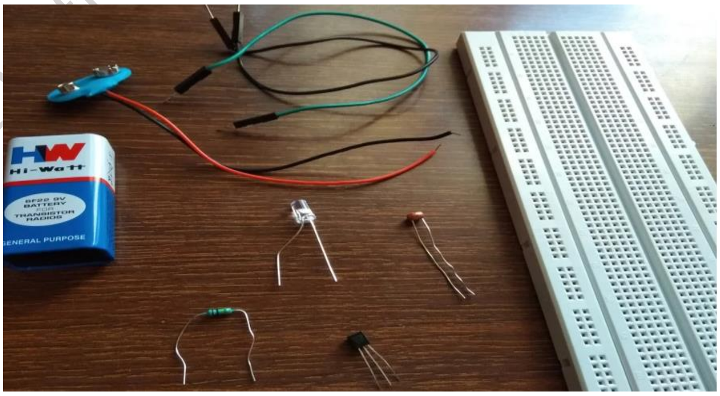


Fig.3.24: Components required

Step 2. Insert BC547 transistor on breadboard as shown in Figure 3.25.

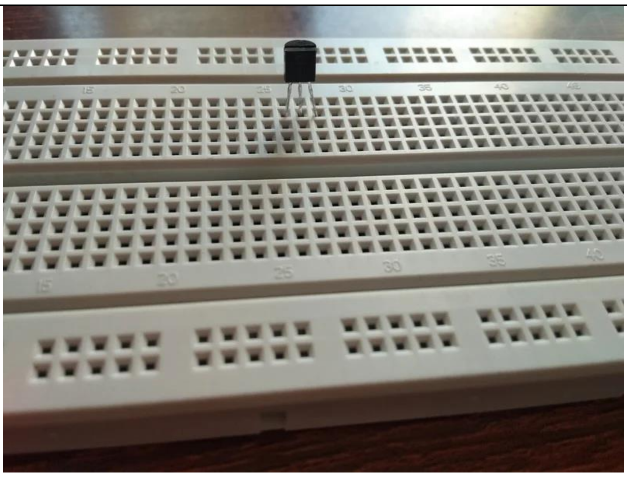


Fig.3.25: transistor on breadboard

Step 3. Connect the LDR to the ‘base' and 'emitter' of the BC547 transistor.

Step 4. Then connect one end if the 100-k ohm resistor from the 'base' of the BC547 transistor and the other end of the 100k resistor to anode (+) side of the L.E.D.

Step 5. The cathode (-) side of the LED will get connected to the 'collector' of the BC547 transistor. It is shown in Figure 3.26.

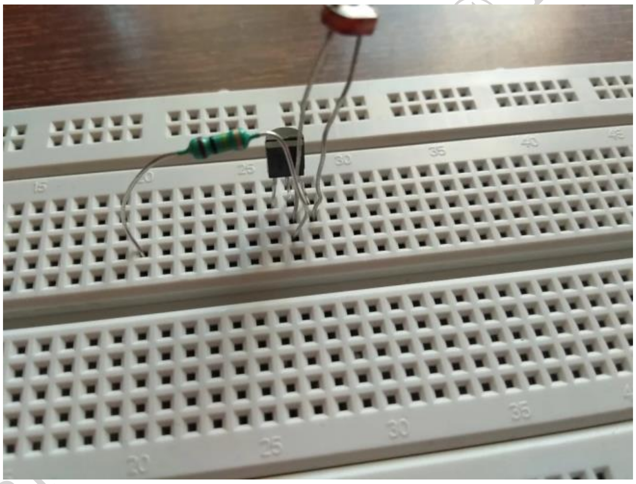


Fig.3.26: Connection on breadboard

Step 6. Join the wires as shown. One end of wire to end of emitter and the other wire connect to end of the resistor as shown in Figure 3.27.

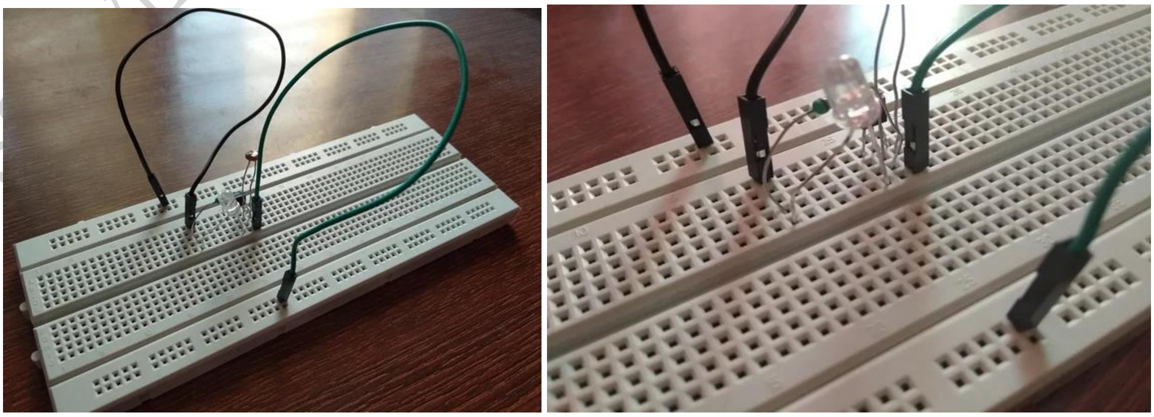


Fig.3.27: Connection of wires on breadboard

Step 7. The positive side of the battery will get connected to the 100k ohm resistor and anode (+) of the led while the negative side of the battery will get connected to the 'emitter' of the BC547 transistor and the other end of the LDR. It is shown in Figure 3.28.

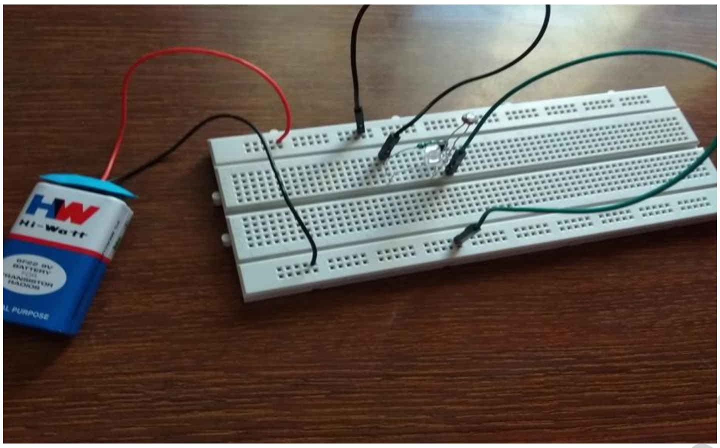


Fig.3.28: battery Connection with components on breadboard

Step 8. Observe the brightness of the LED in the room lighting conditions When there is light the LED will not glow but as the circuit is kept in dark the LED glows as shown in Figure 3.29.

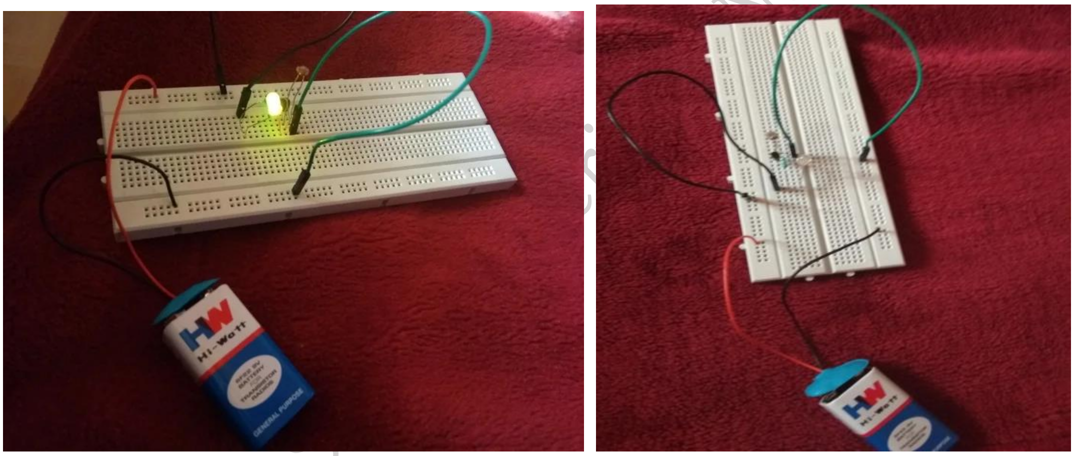


Fig.3.29: variation in brightness of the LED in the room lighting conditions

Practical Activity 3.3. To demonstrate the working of PIR motion sensor

Materials Needed

PIR motion sensor, jumper wires,9V batteries, LED or buzzer

Procedure

Step 1. Connect Batteries are connected across VCC and GND of the sensor.

Step 2. Connect a LED to the output pin through a 220Ω current limiting resistor. A buzzer can also be connected here. It is shown in Figure 3.30.

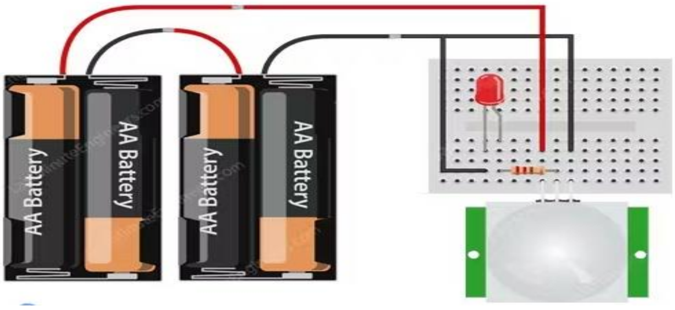


Fig.3.30: circuit connection

Step 3. Now, when the PIR detects any motion around, the output pin will go "high" and this will light up the LED.

3.4 Actuators

An actuator is a device that converts energy, which may be electric, hydraulic, pneumatic, etc., to mechanical in such a way that it can be controlled. It is illustrated in Figure 3.31.

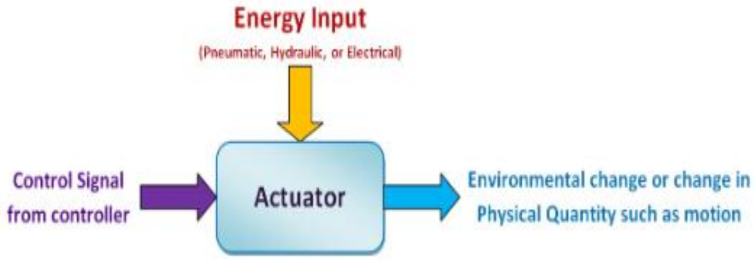

Energy Input
(Pneumatic, Hydraulic, or Electrical)
Control Signal
from controller
Actuator
Environmental change or change in
Physical Quantity such as motion

Fig. 3.31: Block diagram of an actuator

The quantity and the nature of input depends on the kind of energy to be converted and the function of the actuator. Electric and piezoelectric actuators, for instance, work on the input of electric current or voltage, for hydraulic actuators, it's incompressible liquid, and for pneumatic actuators, the input is air. The output is always mechanical energy.

The process is compared to the functioning of a human body. Like muscles in a body that enable energy to be converted to some form of motion like the movement of arms or legs, actuators work in a machine to perform a mechanical action.

Actuators come in a variety of forms, each with specific benefits and drawbacks, such as pneumatic, hydraulic, electric, magnetic, thermal and mechanical etc. The kind of actuator used in a given application is determined by its particular needs, including the required level of force, response time, and durability.

3.5 Working of Actuator

In a typical IoT system, a sensor may collect information and route to a control centre. There, previously defined logic dictates the decision. As a result, a corresponding command controls an actuator in response to that sensed input. Thus, sensors and actuators in IoT work together from opposite ends. It is illustrated in the given Figure, where temperature sensor detects the temperature, sends information to the control centre that gives command to the actuator. The actuator that is a water sprinkler start working after getting the command. So, the information obtained in the form of temperature is converted into the mechanical form. It is illustrated below in Figure 3.31.

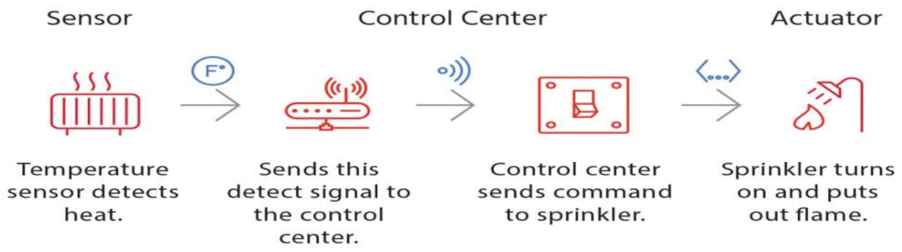

Sensor
Control Center
Actuator
F°
Temperature sensor detects heat.
Sends this detect signal to the control center.
Control center sends command to sprinkler.
Sprinkler turns on and puts out flame.

Fig. 3.32: Working of an actuator

3.6 Actuators Classification

Actuators can be categorized based on their movement type, either linear or rotary. Linear actuators produce linear motion in a straight line, while rotary actuators produce rotary motion in a circular path.

The linear and rotary actuators can be classified based on the energy they use to move the shaft of the motors. Here is a list of actuator classes that use different energy to create movement.

3.6.1 Pneumatic actuators – Pneumatic actuators produce motion by compressing air. They can be employed in a number of ways, like controlling valve positions or moving machine parts. This type of actuators is used in the applications that require high force, quick response times, or explosion-proof environment. It is shown in Figure 3.33.

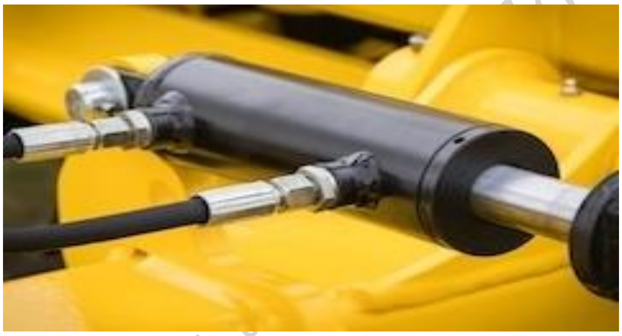


Fig. 3.33: Pneumatic actuator

3.6.2 Hydraulic actuators – These devices produce motion by applying fluid pressure. They are frequently employed in heavy-duty applications like industrial robots, manufacturing machinery, and construction equipment. A common example of a hydraulic actuator system is JCB as shown in Figure 3.33.

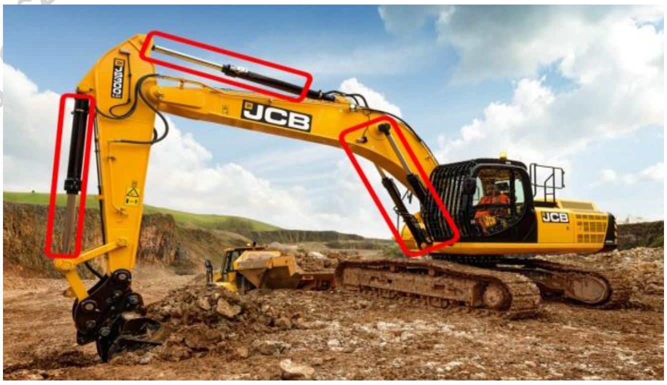


Fig. 3.34: Hydraulic actuator

3.6.3 Electric actuators – To create motion, electric actuators use electrical energy. They can be driven by AC or DC motors and are often used in applications that require precise control, low noise, and low maintenance. This actuator converts electric energy into linear or rotary motion.

Electric actuators are commonly used in automation systems, robotics, medical devices, and laboratory equipment. The electric actuator can be AC/DC actuators. Mostly, DC actuators are used in robotics. Different types of DC actuators that are used in robots are shown in Figure 3.35.

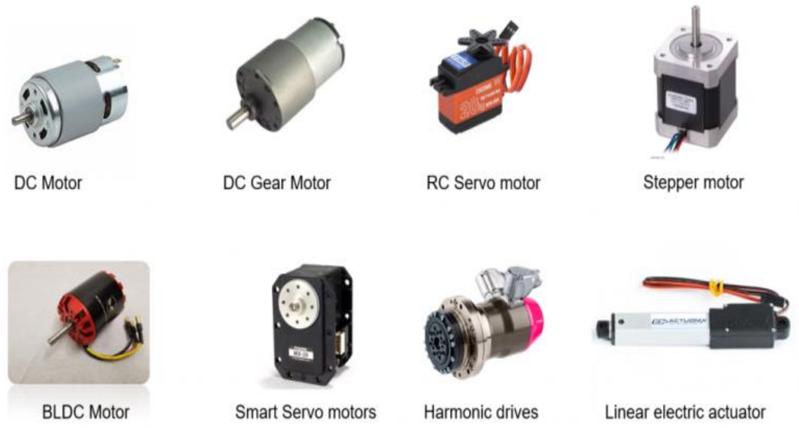


Fig. 3.35: Electric actuator

DC Motor – DC motor converts the electrical signal into mechanical rotation dc motor operates only on DC voltage. A typical DC motor is shown in the Figure 3.36.

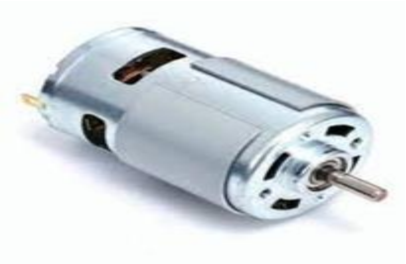


Fig. 3.36: DC motor

AC Motor – AC motor converts the electrical signal into mechanical rotation it works on AC voltage. a typical AC motor is shown in Figure 3.37.

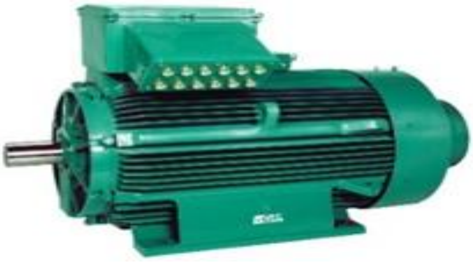


Fig. 3.37: AC motor

Relay module – A relay is an electromechanical switching device which is electrically operated. It works on the principle of electromagnet. It consists of a set of input terminals for single or multiple control signals, and a set of operating contact terminals. A typical relay is shown in Figure 3.38.

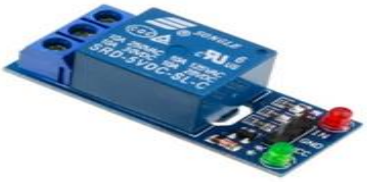


Fig. 3.38: Relay module

3.6.4 Magnetic and thermal actuators – Actuators that use magnetic or thermal changes to produce motion are referred to as magnetic actuators and thermal actuators, respectively. Magnetic actuators produce force by means of magnetic fields. The expansion or contraction of materials in response to temperature changes is used by thermal actuators. Micro-electromechanical systems (MEMS) and other miniaturized applications frequently use both actuators.

3.6.5 Mechanical actuators – To create motion, mechanical actuators rely on tangible components like gears, levers, or cams. When durability, ease of use, and affordability are crucial, mechanical actuators are frequently employed. Mechanical locks, manual valve systems, and hand crank machines are a few examples.

3.7 Difference between Sensor and Actuator

In IoT applications, the accuracy of data is of utmost importance, and actuators with sensors make sure of that. A comparison between sensor and actuators is shown in table 3.1 given below.

Table: 3.1 Comparison between sensor and actuators

SN	*Sensor*	*Actuator*
1	Sensor converts physical quantities and characteristics into electrical signals.	Actuator converts electrical signals into physical action such as force and motion.
2	It acts as an input device in any control system and placed in input port	It acts as an output device in a control system and placed in output port
3	Sensor takes input from environment and senses surroundings condition.	Actuator takes input from output signal conditioning unit of system.
4	Sensor gives output to input signal conditioning unit of the system to convert into electrical form.	It gives output to environment and makes an impact on load to control parameters.
5	It gives information to the system about environment condition to monitor and control.	It accepts command from system to deliver physical action.
6	Sensors are often used to measure process pressure, temperature, fluid levels, flow, vibration, speed etc.	Actuators are often used to operate control valves, dampers, guide vanes, and to move objects from one place to another, to move conveyor belts in robotic arms movement etc.
7	Sensor examples- Thermocouple, photo cell, RTD, LVDT, strain gauge, Load cell, hall sensors, differential flow meters, speed probes, PH meter etc	Actuator examples- motor actuator, servo motor, stepper motor, heaters, electro pneumatic actuator, electro-hydraulic actuator, magnetic actuator etc

Practical Activity 3.3. To observe the working of Remote-controlled LED using Wi-Fi-enabled smart plug

Materials needed

Wi-Fi-enabled smart plug (such as TP-Link Smart Plug, Wemo Mini Smart Plug, etc.), LED bulb or LED strip with compatible socket, Smartphone with Wi-Fi capabilities, Wi-Fi network

Procedure

Step 1. Plug the LED bulb or LED strip into the Wi-Fi-enabled smart plug.

Step 2. connect the smart plug to your Wi-Fi network using the accompanying smartphone app. Typically, this involves plugging in the smart plug, downloading the app, and following the on-screen instructions to connect it to your Wi-Fi network.

Step 3. Once the smart plug is connected to your Wi-Fi network, you can control it remotely using the smart phone app. Most smart plug apps allow you to turn the connected device (in this case, the LED bulb or LED strip) on and off, set schedules, and even monitor energy usage.

Step 4. Test the setup by remotely turning the LED bulb or LED strip on and off using the smart phone app.

3.8 Sensor Calibration

Sensor calibration is a crucial process to ensure the accuracy of measurements. It involves adjusting sensor settings to align with a standard reference, minimizing discrepancies. This is essential for various applications, including scientific and industrial uses. Calibration compensates for factors like environmental conditions and aging, maintaining precision over time. Regular calibration ensures compliance with quality standards, allowing sensors to consistently provide accurate and reliable data.

Calibration process for any sensor can be understood with the help of the example given in the following section.

3.8.1 Calibration process of Temperature Sensor with Indicator

Temperature sensors equipped with indicators are integral in industries and applications requiring precise temperature measurements. Regular calibration is indispensable to maintain accuracy in readings. This process involves comparing the sensor's output with a known reference to assess accuracy and make necessary adjustments as needed.

The calibration process is vital for temperature sensors equipped with indicators, guaranteeing the precision and dependability of temperature measurements. Factors such as aging, environmental conditions, or mechanical stress can cause temperature sensors to deviate from their initial calibration over time. Without routine calibration, there is a risk of increasingly inaccurate readings, compromising the accuracy of temperature monitoring and potentially posing quality or safety concerns.

Temperature sensors with indicators come with a display or indicator offering temperature readings. Depending on the sensor's design and purpose, these indicators can be digital, analog, or color-coded. The indicator converts the sensor's electrical signal into a temperature value that is easily readable. Calibration of a temperature sensor with an indicator is the process of confirming the accuracy of both the sensor and its display, ensuring precise temperature readings. The arrangement for calibration is shown in Figure 3.39.

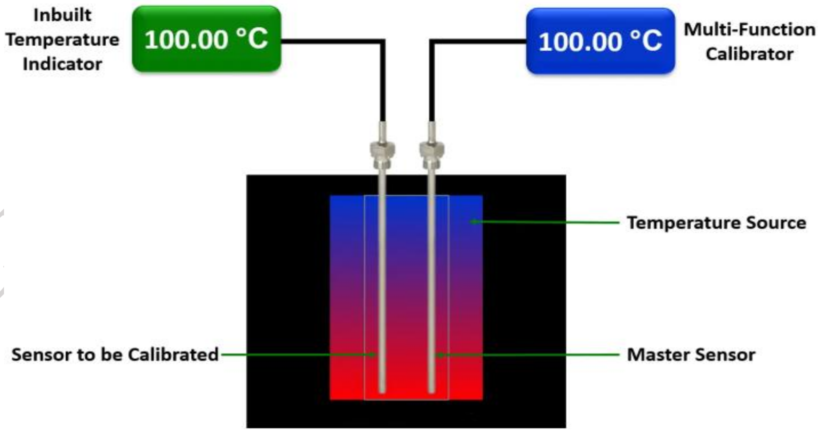


Fig. 3.39: Calibration process of Temperature Sensor with Indicator

Step 1. Preparing for Calibration

Prior to commencing the calibration procedure, assemble the required equipment, including a calibrated reference temperature source, a digital thermometer or temperature calibrator, and any tools specified by the sensor manufacturer. Ensure that both the temperature source and the reference device used for calibration adhere to national or international standards.

Step 2. Confirming Indicator Accuracy

Initiate the calibration process by validating the accuracy of the temperature indicator on the sensor. Compare the displayed readings with those obtained from the reference temperature source. If any disparities are detected, take note of the deviations for subsequent adjustment during the calibration process.

Step 3. Choosing Calibration Points

Select a set of temperature points across the sensor's range for calibration. These points should encompass the desired operational range and include critical temperatures pertinent to the specific application. It is advisable to include a minimum of three calibration points, typically spanning the minimum, middle, and maximum temperature range.

Step 4. Executing Calibration Adjustments

Position the temperature sensor in the reference temperature source and allow sufficient time for stabilization. Compare the sensor's output readings with the reference temperature measurements at each calibration point. If discrepancies from the desired values are identified, make the necessary adjustments to the sensor or its indicator to align the readings with the reference measurements.

Step 5. Verification and Documentation

Following the calibration adjustments, reconfirm the sensor's readings at each calibration point to ensure alignment with the reference measurements. Document the calibration results, noting the adjustment values made, for future reference and traceability purposes.

3.8.2 Benefits of Calibration

Calibration stands as a crucial element in preserving the precision and dependability of temperature sensors equipped with indicators. Through adherence to a systematic calibration procedure and recognizing the significance of indicator accuracy, organizations can guarantee accurate measurements, thereby improving process control, compliance, and product quality. Consistent calibration is imperative to reduce measurement uncertainties and optimize the performance of applications sensitive to parameter values.

3.9 Sensor Nodes

A sensor node is a node in the IoT network that is capable of

- Gathering sensory information
- Performing processing
- Communicating with other connected nodes in the network

In a wireless sensor network (WSN), various sensor nodes are connected. The following Figure 3.40 shows a WSN:

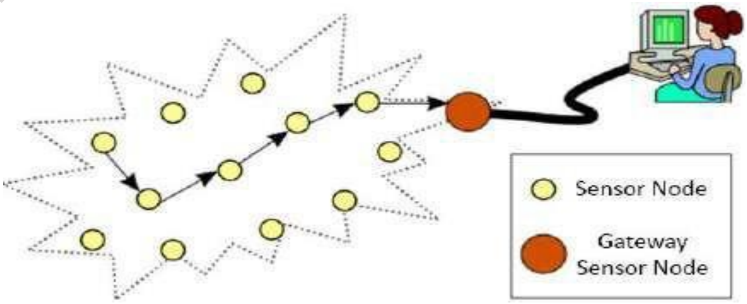


Fig. 3.40: WSN

3.9.1 Structure of a Sensor Node

In the structure of a sensor nodes following components are present:

Controller – The controller processes data and controls functions of other components in the node. Digital Signal Processors (DSPs) are generally used for wireless communication applications.

Transceiver – A transceiver is a device that combines both a transmitter and a receiver. The operational states of transceivers are as follows:

- Transmit
- Receive
- Idle
- Sleep

External Memory – External memory is used based on the purpose of storage that are as follows:

- **User memory** – To store application related or personal data
- **Program memory** – To perform programming of the device

Power Source: It is difficult to connect a wireless sensor to the mains supply. Power is required for the sensor node to sense, communicate and process data. The power can be stored in batteries or capacitors. Batteries are the main power source for the sensor nodes.

The structure of a sensor node is shown in following Figure 3.41.

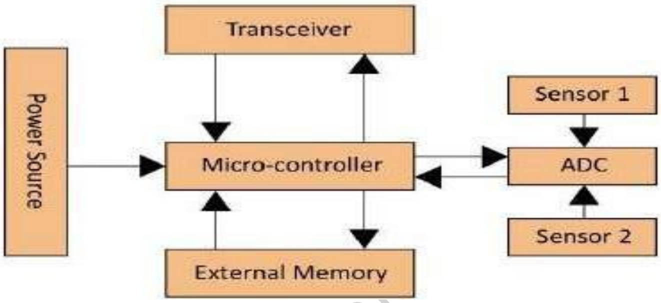


Fig.3.41: Structure of a sensor node

Assignment 2. Sketch a neat diagram on a sheet showing the structure of a sensor node.

3.10 Sensor Connectivity in IOT

The connectivity requirements of IoT networks depend on the purpose of the system and the resource constraints. A range of several wireless and wired technologies are used to provide complete IoT connectivity. The Figure 3.42 shows a sensor connectivity model.

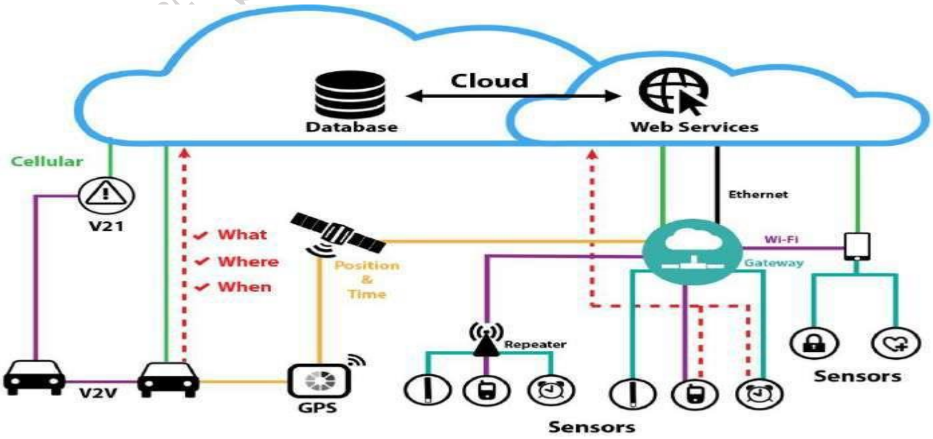


Fig.3.42: Sensor connectivity model

Summary

- Sensors are components of IoT devices that measure physical quantities, converting them into data that can be interpreted by humans or machines.
- The data gathered by IoT sensors enables various types of control and automation.

- Sensors are important for capturing data, but in order for them to be truly useful, they must be coupled with actuators, which are devices that can physically respond to sensor input.
- Actuators, which include electric motors, pneumatic and hydraulic actuators, etc. are devices that transform energy into mechanical motion.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. A Sensor is a (a) Subsystem (b) Machine (c) Module (d) All of the above
2. The function of a sensor is to (a) Detect events within a specified environment (b) Separate physical parameters (c) Track and transfer data to computer processor (d) Both a and c
3. Sensor provides output signal depending on (a) Input (b) Physical quantity (c) Both a and b (d) None of the above
4. Sensors can be (a) Temperature (b) Light (c) Motion (d) All of the above
5. Proximity type sensor is which type of sensor? (a) Contact type (b) Non-contact type (c) Both a and b (d) Partially contact
6. Actuators can be (a) Displays (b) Motors (c) Sound (d) All of the above
7. On which of the following factors does the design of a sensor depend? (a) Application property (b) Quantity measurement (c) Quality of environment (d) None of the above
8. Which of the following are the applications of proximity sensors? (a) Car (b) Mobile phones (c) Industries (d) All the above
9. Examples of sensors are (a) Motors (b) Pumps (c) Moisture sensor (d) All of these
10. Actuators include (a) Gears (b) Pistons (c) Valves (d) All of the above

B. Fill in the blanks

1. Sensors fetch ________ data to control devices.
2. A transceiver is a device that combines both a ______.
3. Actuators can be categorized based on their movement type _____.
4. The most basic example of a temperature sensor is a___________.
5. ___________ is a process to remove structural errors from the output of the sensor.
6. A Proximity Sensoris capable of detecting the __________that is in its field of view.
7. An actuator is a which actuates the movement by converting______________.
8. A touch sensor is a sensitive device that detects _________and carries out the required operations.
9. Sensors are categorized based on the physical quantities they measure, such as __________________.
10. The connectivity requirements of IoT networks depend on the ____________.

C. State true or False for the following

1. A sensor is not a machine.
2. IoT devices and systems include sensors that track and measure activity in the world.
3. A sensor may not be a transducer.
4. The sensor is an input device while the actuator is an output device.

5. Electrical switches are the choice of actuators for most of the on-off type control action.
6. A thermocouple is an electric temperature detector that uses thermoelectric resistance created by heat.
7. A transducer is any which converts one form of energy into another.
8. A light bulb is a transducer for converting electrical energy into optical energy.
9. An electric motor is a transducer for the conversion of electricity into mechanical energy or motion.
10. The data in digital sensors, which are used for conversion and transmission, is analog in nature.

D. Short answer type questions

1. What is a sensor?
2. What is an actuator?
3. Are sensors can be used along with other electronic devices?
4. List different types of sensors.
5. What are the characteristics of sensors?
6. What are the applications of proximity sensors?
7. Give the applications of light sensors.
8. What is a humidity sensor?
9. What is the use of a touch sensor?
10. Define sensor accuracy and calibration.

Module 2 Networking of IoT Devices

Module Overview

This module provides learners with a comprehensive understanding of how Internet of Things (IoT) devices connect, communicate, and operate within a network. Beginning with the initialization and configuration of nodes, gateways, and control edge appliances, the module introduces the fundamental components required to build a functional IoT system. Learners will then explore how to establish communication and connectivity between devices, enabling seamless data exchange. The importance of security in IoT systems is addressed through the implementation of authentication and authorization mechanisms. The module also covers key communication technologies and protocols used in IoT, such as MQTT, CoAP, and HTTP. Finally, learners are introduced to the role of cloud computing in IoT, focusing on data storage, processing, and remote access. By the end of this module, learners will be equipped with essential networking skills needed to build secure, scalable, and efficient IoT solutions.

Learning Outcomes

After completing this module, you will be able to:

- Initialize and configure IoT nodes, gateways, and control edge devices for seamless integration.
- Establish reliable communication and connectivity among various IoT devices.
- Implement secure authentication and authorization mechanisms in IoT networks.
- Identify and apply suitable communication technologies and protocols used in IoT.
- Understand the role of cloud computing in managing and storing IoT data effectively.

Module Structure

Session 1. Initialize and Configure Nodes, Gateways, and Control Edge Appliances

Session 2. Establish Communication and Connectivity between devices

Session 3. Authentication and Authorization Mechanism in IoT

Session 4. Communication Technologies and Protocols for IoT

Session 5. Cloud Computing

Session 1. Initialize and Configure Nodes, Gateways, and Control Edge Appliances

Setting up and configuring nodes, gateways, and control edge appliances is essential for building effective IoT systems. Nodes collect data, gateways facilitate communication, and control edge appliances process data at the network edge. Proper setup ensures smooth operation and secure connectivity in IoT networks. This guide explores the key steps involved in initializing and configuring these components, enabling users to establish reliable and scalable IoT infrastructures.

Setting up a username and password on routers and IoT devices is known as initializing a node and gateway. The technician must finish the full installation of the IoT setup before initializing the nodes and gateways. This involves working with IoT devices, such as setting up a router, an IoT camera, and a functional Internet connection. For instance, using the procedures depicted in Figure 1.1, an IoT camera can be set up alongside the IoT framework, and then, finally, a node gateway can be initialized.

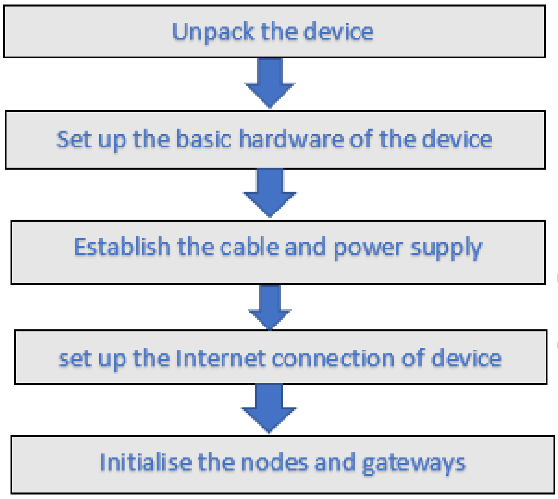

Unpack the device
Set up the basic hardware of the device
Establish the cable and power supply
set up the Internet connection of device
Initialise the nodes and gateways

Fig. 1.1: Prerequisite steps for an IoT device installation

1.1 IoT Device Installation

In the process of installation of IoT devices like cameras, motion sensors, an IoT camera, certain steps need to be performed.

Unpack the Camera

Remove the camera and its accessories from the package carefully.

1.1.2 Set Up the Basic Camera Hardware

Once unpacked, the foundational hardware requires setup, including mounting the camera and its stand. The following steps illustrate the basic hardware setup procedures:

1. Slide the camera onto the stand to connect it.
2. Mount the screws and secure them tightly.

The Figure 1.2 shows the camera hardware assembly.

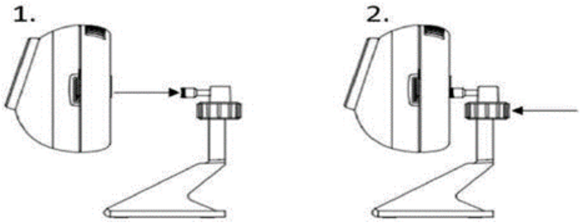


Fig. 1.2: Camera hardware setup

Figure 1.3 shows the mounting of a camera on the wall.

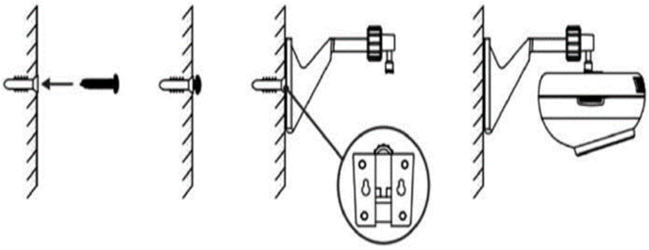


Fig. 1.3: Mounting of the camera on a wall

1.1.3 Ensure the Power Supply and Cable Connection

Connect the power adaptor end to the power supply port on the camera's back. Next, attach the power supply plug to a power supply port that is close as shown in Figure 1.5.

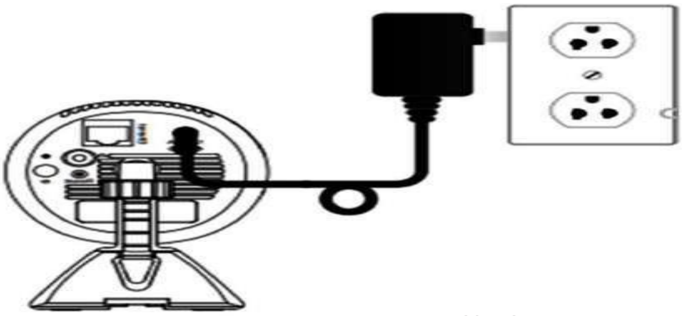


Fig. 1.5: Connection for the power adaptor

1.1.4 Set Up the Internet Connection of Camera Device

For the IoT camera to operate via wireless internet using Wi-Fi, it must connect to the router. Depending on the customer's needs or site requirements, there may already be a pre-installed wireless internet connection available, or the technician may need to install a router to enable wireless connectivity.

If a pre-installed wireless internet connection is accessible then following steps should be carried out to complete a wireless setup automatically

Step 1. Verify that the router device's wireless Internet connection is functioning properly.

Step 1. Ascertain that the camera is positioned within the router's coverage area.

Step 1. For 1 to 5 seconds, press the WPS (Wi-Fi Protected Setup) button on the router or gateway. so that the WPS LED begins to flash.

Step 4. Next, press the WPS button on the camera's back to make the WiFi LED start blinking and turn green. Figure 1.6 shows the steps of the automatic connection of router and camera:

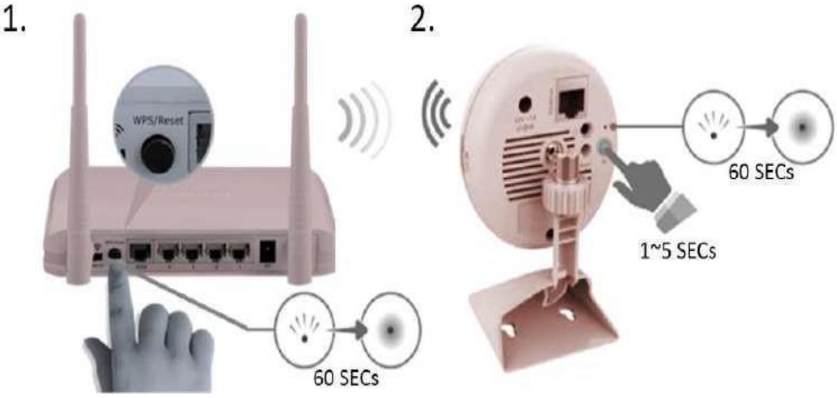


Fig. 1.6: Automatic router and camera connection

If the automatic connection fails, establish a manual connection using a utility program like EnViewer that was included on the CD that came with the IoT camera's packaging. EnViewer Finder by EnGenius is being used in this illustration. The procedure to manually connect the camera is as follows:

Step 1. Turn on the laptop or desktop, wait until the system starts up, and check that the window opens and runs.

Step 1. Run the utility tool disc by inserting it into the disc drive. The following are the steps to run the disc:

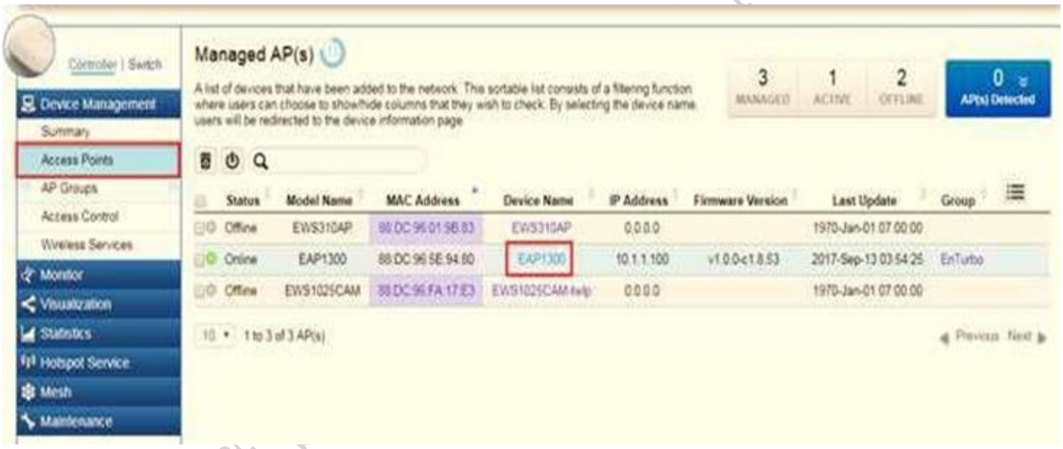
1. Click the start button to launch "My Computer."
2. Select "Run the disc as administrator" by performing a right-click on the disk drive.
3. To finish installing, adhere to the installation instructions.

Step 1. To use the tool after completing the installation, follow these steps:

4. Access the desktop of the computer. Pressing "window" and "R" on the keyboard will open and run the window.
5. Type the name of the tool and press “Enter”.

Step 4. From the list provided in the tool window, select the camera linked to the router network. If the camera isn't showing up in the list, click Refresh to see it. The device will display the hostname, IP (in this case, the camera's IP is assumed to be 191.168.0.101), and version in the list's camera row.

6. The screenshot in Figure 1.7 shows the camera listed in the utility tool.



Managed AP(s)

A list of devices that have been added to the network. This sortable list consists of a filtering function where users can choose to show/hide columns that they wish to check. By selecting the device name, users will be redirected to the device information page

Status	Model Name	MAC Address	Device Name	IP Address	Firmware Version	Last Update	Group
Offline	EWS310AP	88:DC:96:01:9B:83	EWS310AP	0.0.0.0		1970-Jan-01 07:00:00	
Online	EAP1300	88:DC:96:5E:94:80	EAP1300	10.1.1.100	v1.0.0-c1.8.53	2017-Sep-13 03:54:25	EnTurbo
Offline	EWS1025CAM	88:DC:96:FA:17:E3	EWS1025CAM-kelp	0.0.0.0		1970-Jan-01 07:00:00	

10 ▾ 1 to 3 of 3 AP(s)

Fig. 1.7: Screenshot showing the camera listed in the utility tool

Select the camera from the list, enter the username and the password in the column given on the top right corner, and then click next for the configuration shown in Figure 1.7. The default username and password are given in the camera packaging or in the user manual. Figure 1.8 shows the username and password on a camera packing.

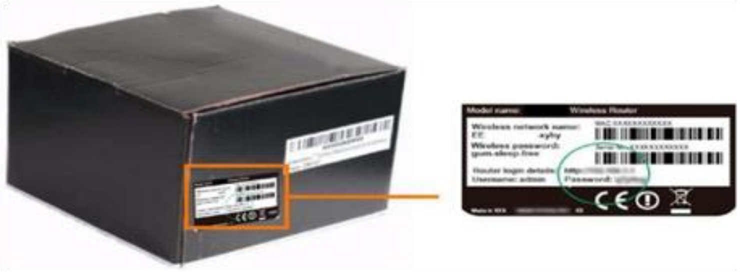
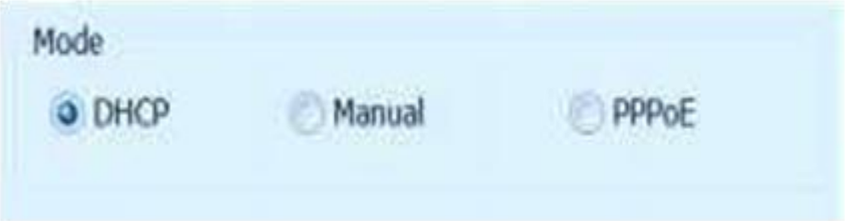


Fig. 1.8: Username and password on camera packing

Click the network tab given in the options in the utility tool and select the mode of connecting the camera with the network. Figure 1.9 shows the modes of network connection – DHCP, Manual, PPPoE.



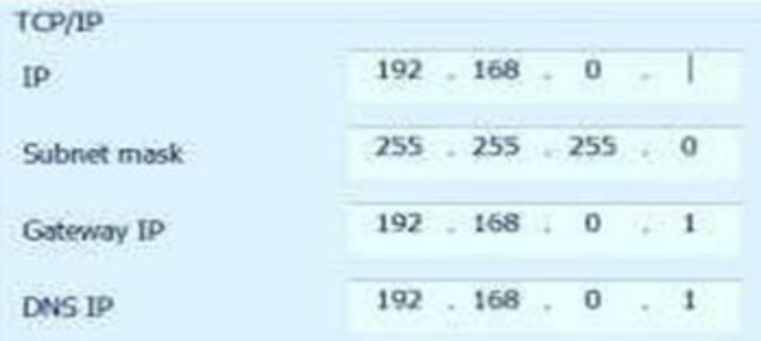
Mode

● DHCP ○ Manual ○ PPPoE

Fig. 1.9: Screenshot showing the modes of network connection

Dynamic Host Configuration Protocol (DHCP) – DHCP allows to connect to the network without providing any IP. The camera automatically requests the IP from the router.

Manual – In this option, IP address is to be provided in the TCP/IP section. Make sure that the IP is not used by some other network. Figure 1.10 shows the manual network setup wizard.



TCP/IP

IP: 192 . 168 . 0 . |

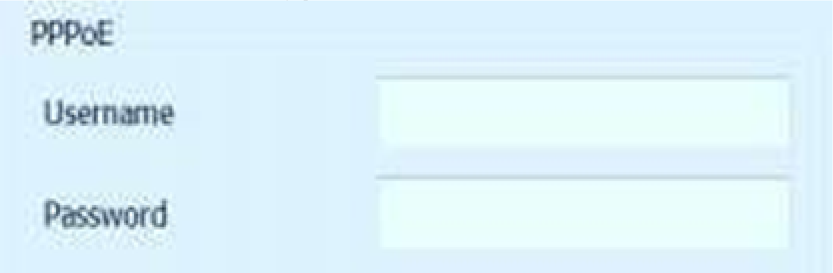
Subnet mask: 255 . 255 . 255 . 0

Gateway IP: 192 . 168 . 0 . 1

DNS IP: 192 . 168 . 0 . 1

Fig. 1.10: Manual network setup wizard

***Point-to-Point Protocol over Ethernet (PPPoE)* –** The camera and modem can be directly connected when the Internet service is using the PPPoE Internet protocol. This calls for getting in touch with the service provider to get the necessary information details. In the same PPPoE protocol setting on the router, only the username and password are required as shown in Figure 1.11.



PPPoE

Username

Password

Fig. 1.11: Setting up the PPPoE protocol

1.1.5 Installation of edge devices

Edge devices in IoT refer to hardware components deployed at the network edge to collect, process, and transmit data from IoT sensors and devices. Examples include gateways, edge servers, routers, and computing nodes.

A) Installation of the Router

Following steps has to be followed by the technician to install a router for a wireless internet connection at site.

1. Unpacking the router device.

2. Connecting the ethernet wire with router.

3. Configuring the router device Initialising the router device.

1. Unpacking the Router Device

The technician may get the router from the Internet Service Provider (ISP) or the manufacturer, based on the requirement of the job. The table 1.1 lists some of the specifications that need to be checked with the camera:

Table 1.1 Specifications to be checked

Interface	RJ45
Wi-Fi	801.11 b/g
Secured access	WPA/WPA2-PSK and WEP
Data transmission rate	Up to 54 Mbps

Unpack the router, then check the accessories and devices for any damage. The following list shows the items provided in the packaging:

1. Router device
2. RJ 45 cable
3. Power adaptor
4. Product manual

1. Connecting the Ethernet and Power Cable with Router

Step 1. Connect the power cable end to the back of the router and the adapter plug to a power socket. Ensure that the power LED indicator light on the router turns ON. Figure 1.12 shows the LED indicator on a router.

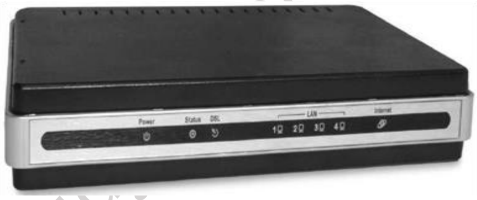


Fig. 1.12: Router LED indicator

Step 1. Connect the Ethernet cable given in the kit to the back of the router in the WAN port and the other end of the cable to the modem installed at the site. Figure 1.13 shows the power and Ethernet cable connection with the router.

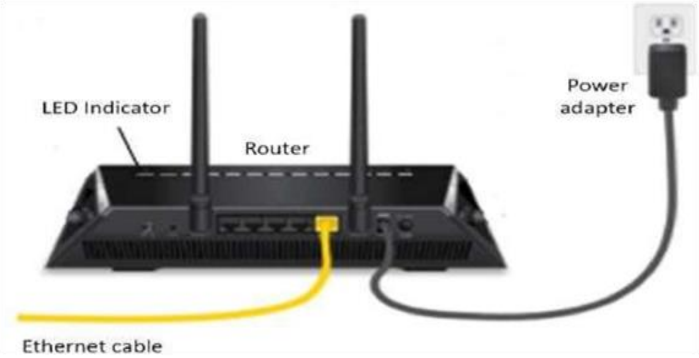
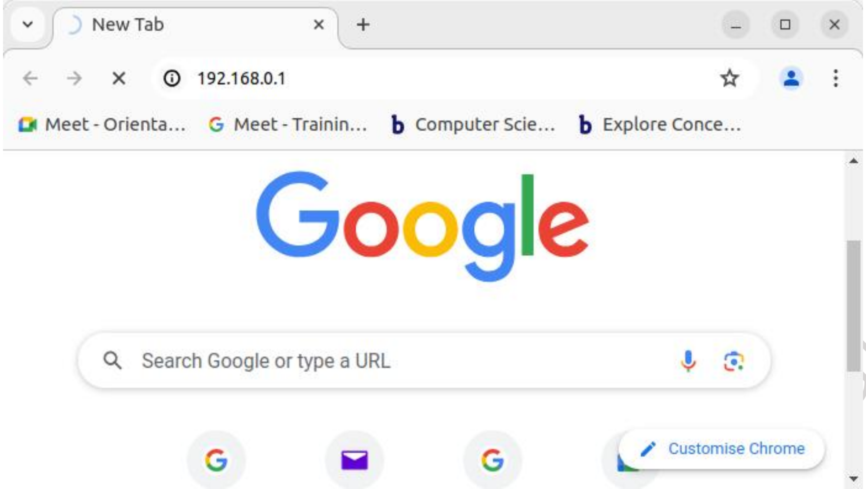


Fig. 1.13: Power and Ethernet cable connection with router

1. Configuring the Router Device

To configure the router, a technician can connect the router with a desktop/laptop through a LAN wire or with the help of the IP address. For this following step need to be performed:

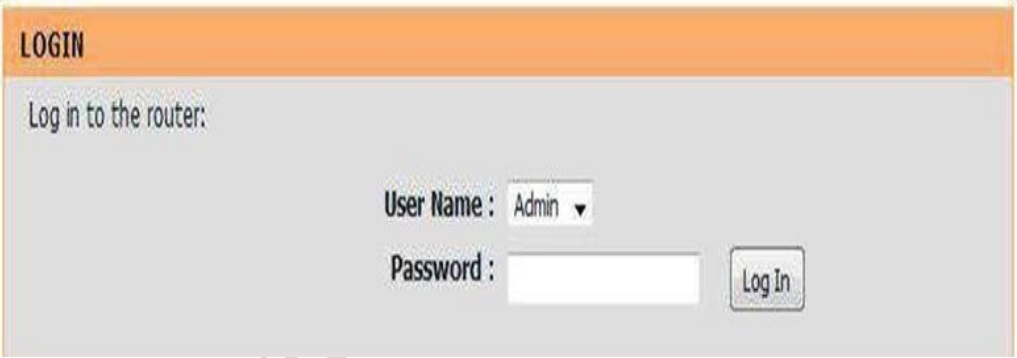
Step 1. Open a web browser and in the address, bar enter the IP address for the router which is given in the product manual. Suppose 191.168.0.1 is the IP address of the router, then enter it in the browser as shown in Figure 1.14.



192.168.0.1

Fig. 1.14: IP address for router configuration – IoT Devices/Systems

Step 1. Then, enter the default username and password given in the router manual or within the packing in the window that opens. Figure 1.15 shows the window:



LOGIN

Log in to the router:

User Name : Admin

Password :

Fig. 1.15: Window for router configuration

After completing the hardware setup of the IoT device and connecting it to the Internet, the final step is to initialize the node devices and the gateway routers. The initialization of gateways and nodes means configuring the network settings, that is, the TCP/IP configuration setting, securing the network, and commissioning the IoT device framework.

Node Initialization

Setting a login and password for the system default user is necessary when using a node or device for the first time. Initialization of nodes (IoT devices) is another name for this action. The system will become secure and configured as a result. As an illustration, initialization through network video recorder (NVR) software is mentioned for a camera setup using NVR, in which the NVR device is initialized with the router. A typical NVR device is shown in Figure 1.16.

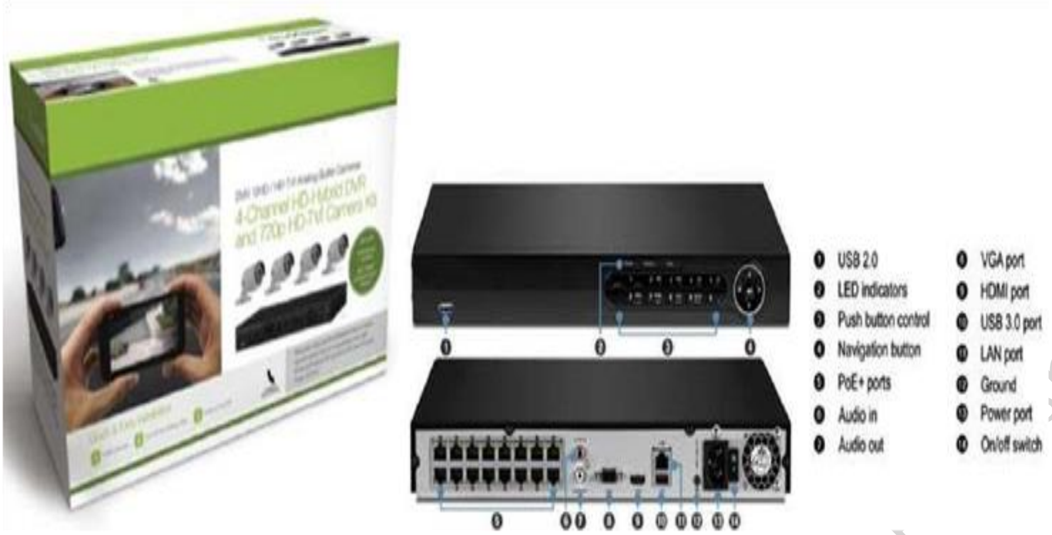


Fig. 1.16: Front and back view of an NVR

Practical Activity 1.1. Demonstrate to establish the connection between an NVR device, a camera, and a router.

Material Required

NVR device, camera, router, ethernet cable

Procedure

Step 1. Unpack the NVR device and connect the device to the router using an Ethernet cable. Figure 1.17 shows the connection of IoT camera, a router, and an NVR device setup:

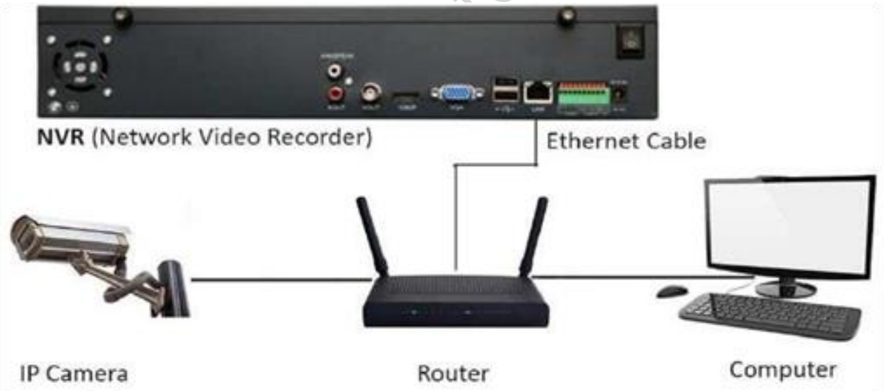


Fig. 1.17: NVR device connection with router and camera

Step 2. Power ON the NVR device and let it boot into the initialization interface. The power indicator of an NVR device is displayed in Figure 1.18.

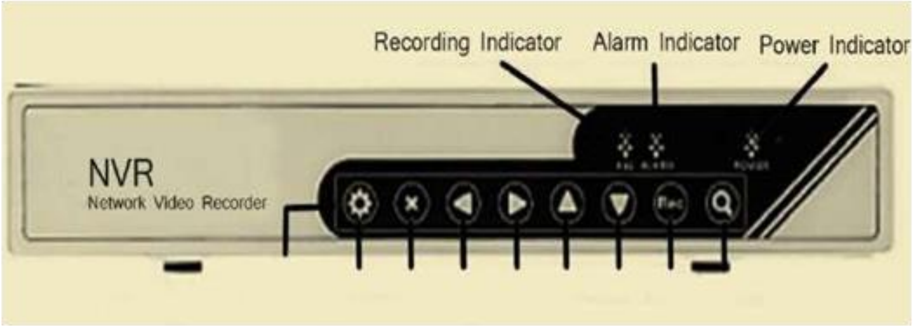


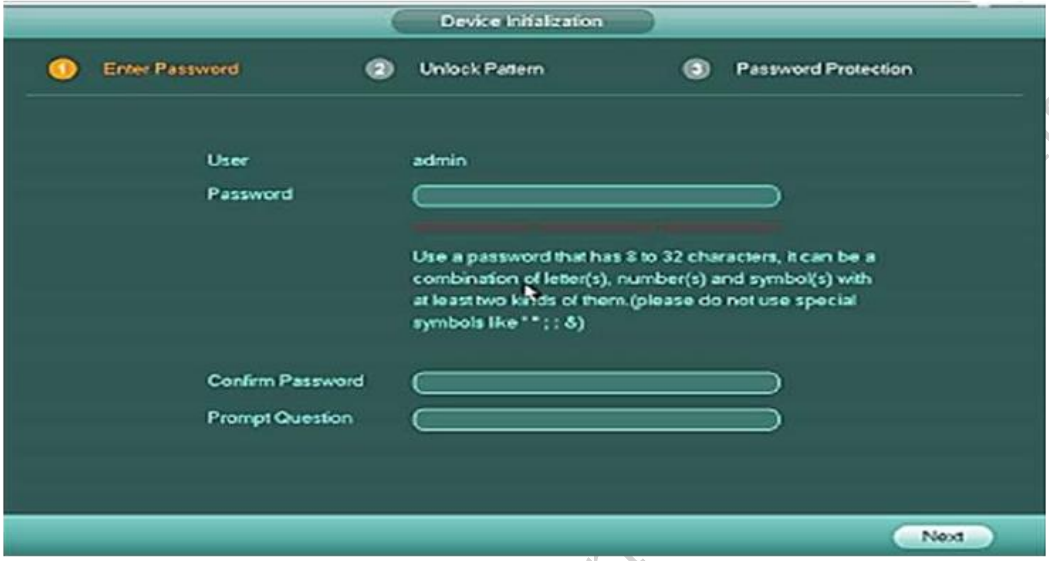
Fig. 1.18: NVR device indicators

Step 3. Either the NVR device comes with software, or it can be downloaded from the Internet. For example, the NVR software for Genius Vision camera setup can be downloaded from the link:

https://geniusvision.net/community/GeniusVisionNVRCommunitySetup_v960.exe

Step 4. Install and activate the NVR software on a computer system linked to the same network as the IP camera and NVR device.

Step 5. Configure the default login details for the camera. Figure 1.19 shows the device login screen of NVR software on a computer system.



Device Initialization

1 Enter Password 2 Unlock Pattern 3 Password Protection

User admin

Password

Use a password that has 8 to 32 characters, it can be a combination of letter(s), number(s) and symbol(s) with at least two kinds of them.(please do not use special symbols like ' " ; : &)

Confirm Password

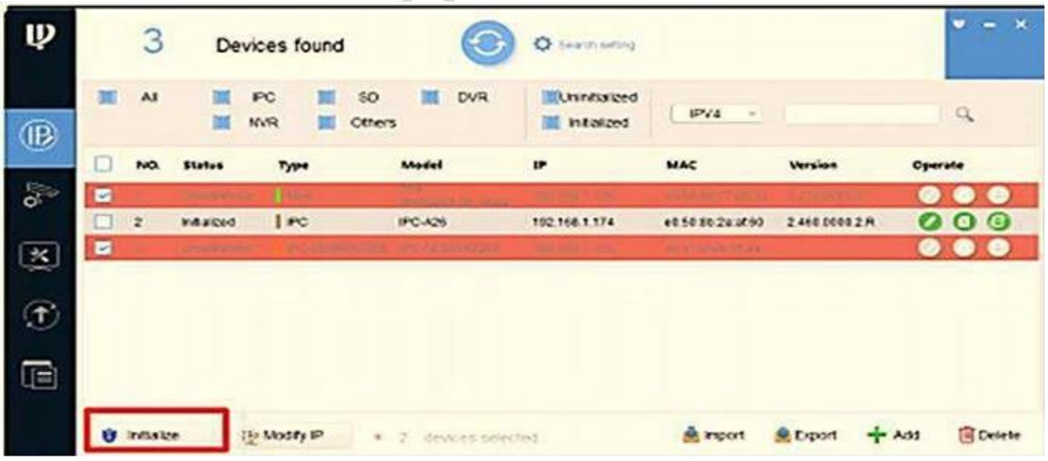
Prompt Question

Next

Fig. 1.19: Device login screen

Step 6. For initialization of the camera device, connected through the same LAN, launch the interface on the desktop and check the connected device list.

Figure 1.20 shows the screenshot of the list of devices connected to the network.



3 Devices found

Search setting

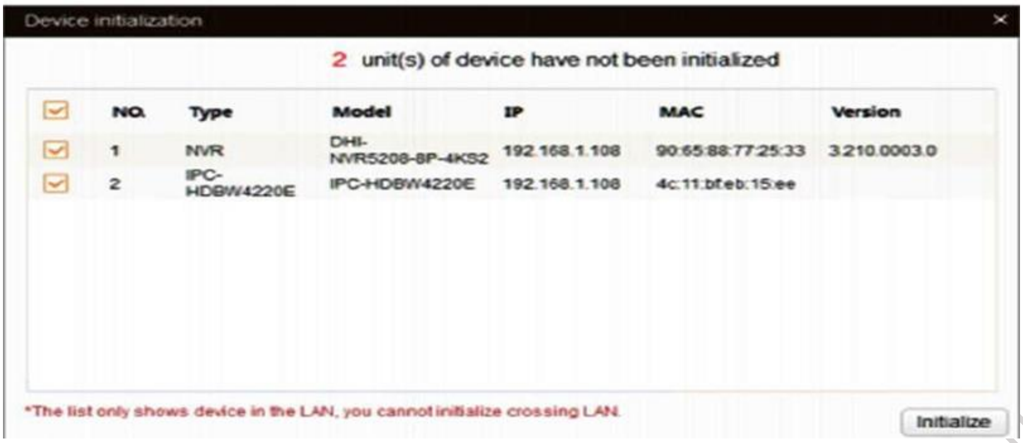
All, IPC, SD, DVR, NVR, Others, Uninitialized, Initialized, IPV4

□	NO.	Status	Type	Model	IP	MAC	Version	Operate
☑	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	
□	2	Initialized	IPC	IPC-A26	192.168.1.174	e0:50:8b:2a:af:90	2.460.0000.2.R	
☑	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]	[illegible]		

Initialize Modify IP 2 devices selected Import Export Add Delete

Fig. 1.20: Screenshot of the list of devices connected to the network

Step 7. Select the uninitialized camera device from the list and enter the initializing interface by clicking on the **"Initialize"** button. Figure 1.21 shows the initializing interface.



Device initialization ×

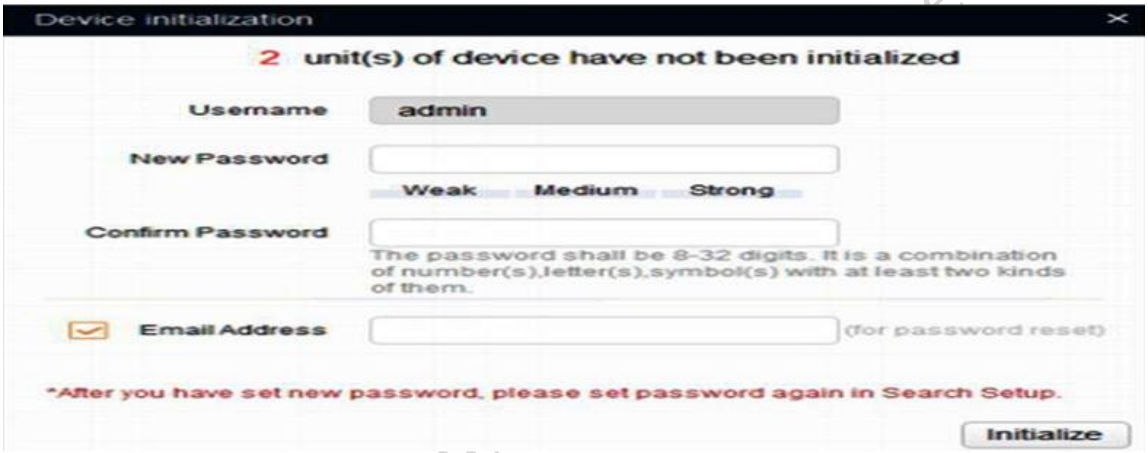
2 unit(s) of device have not been initialized

☑	NO.	Type	Model	IP	MAC	Version
☑	1	NVR	DHI-NVR5208-8P-4KS2	192.168.1.108	90:65:88:77:25:33	3.210.0003.0
☑	2	IPC-HDBW4220E	IPC-HDBW4220E	192.168.1.108	4c:11:bf:eb:15:ee	

*The list only shows device in the LAN, you cannot initialize crossing LAN.

Fig. 1.21: Initializing interface

Step 8. Select the devices and click **"Initialize"** and set the initialization parameters. Figure 1.22 shows the setting up the password of the device.



Device initialization ×

2 unit(s) of device have not been initialized

Username: admin

New Password:

Weak Medium Strong

Confirm Password:

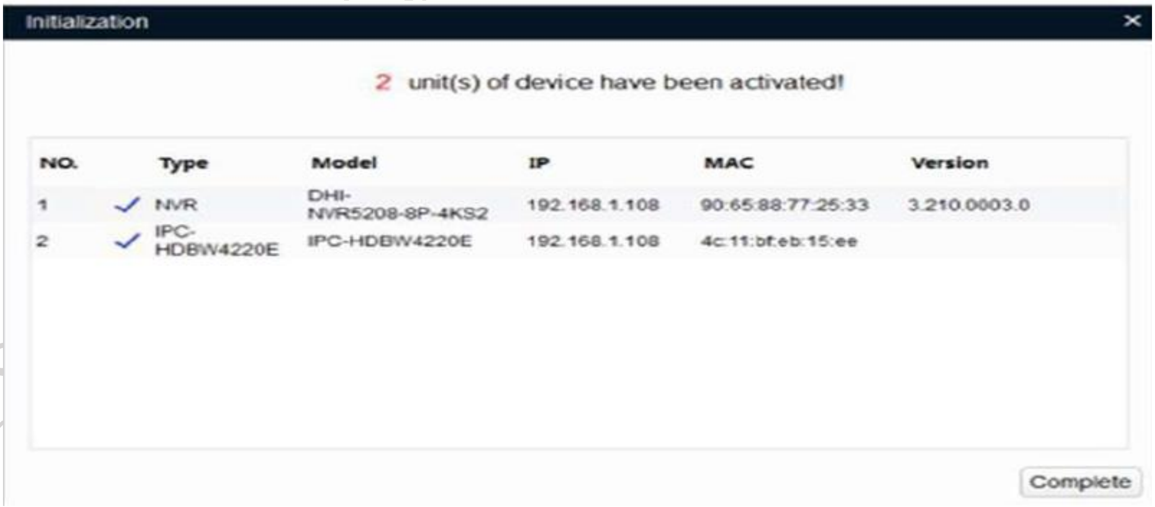
The password shall be 8-32 digits. It is a combination of number(s),letter(s),symbol(s) with at least two kinds of them.

☑ Email Address: (for password reset)

*After you have set new password, please set password again in Search Setup.

Fig. 1.22: Setting up of password of the device

Step 9. Figure 1.23 shows the detected devices after initialization.



Initialization ×

2 unit(s) of device have been activated!

NO.		Type	Model	IP	MAC	Version
1	✓	NVR	DHI-NVR5208-8P-4KS2	192.168.1.108	90:65:88:77:25:33	3.210.0003.0
2	✓	IPC-HDBW4220E	IPC-HDBW4220E	192.168.1.108	4c:11:bf:eb:15:ee	

Fig. 1.23: Detected devices after initialization

Gateway Initialization

To establish an Internet connection between the network provider and the gateway, which is the router installed at the location, the gateway or router must first be initialized.

Gateway initialization is the vital process of setting up a gateway device to enable communication between different networks. It involves configuring hardware, installing software, assigning network addresses, setting up routing, implementing security measures, and enabling monitoring. Through thorough testing and validation, the gateway ensures reliable and secure network operation.

Practical Activity 1.2. Demonstrate to initialize a gateway or router.

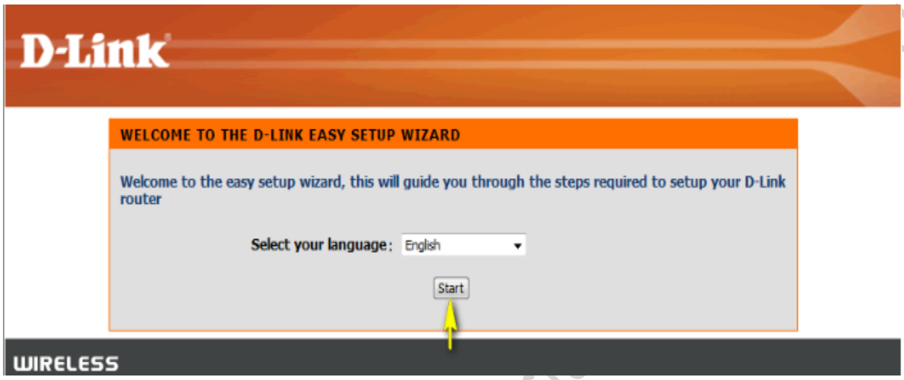
Material required

D-Link router, computer, Ethernet cable

Procedure

Step 1. Attach the power adapter to the router's back panel.

Step 2. Connect the computer and router with an Ethernet cable. Figure 1.24 represents the window that will open on the screen.



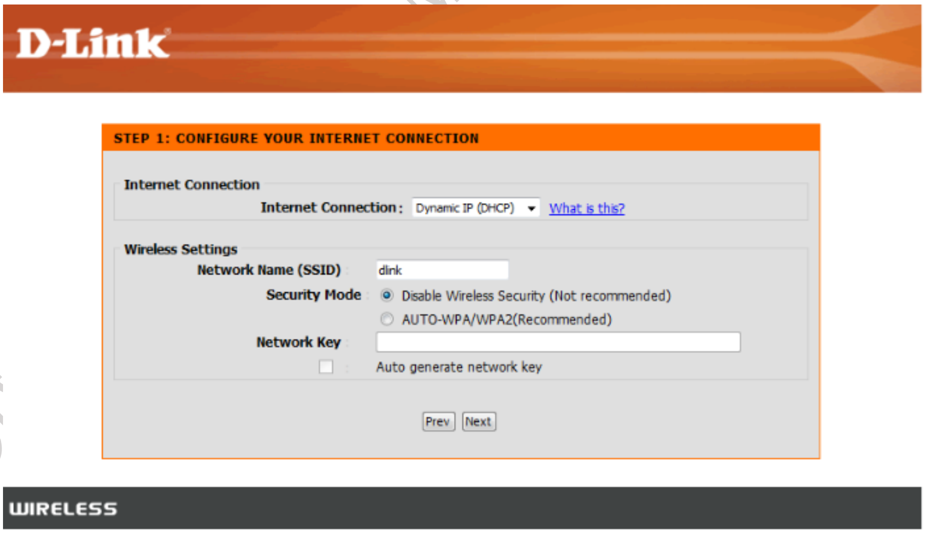
WELCOME TO THE D-LINK EASY SETUP WIZARD

Welcome to the easy setup wizard, this will guide you through the steps required to setup your D-Link router

Select your language : English

Fig. 1.24: Router setup wizard

Step 3. Configure the Internet connection and set up a password. Figure 1.25 shown the configuration of Internet connection and password.



STEP 1: CONFIGURE YOUR INTERNET CONNECTION

Internet Connection

Internet Connection : Dynamic IP (DHCP)

Wireless Settings

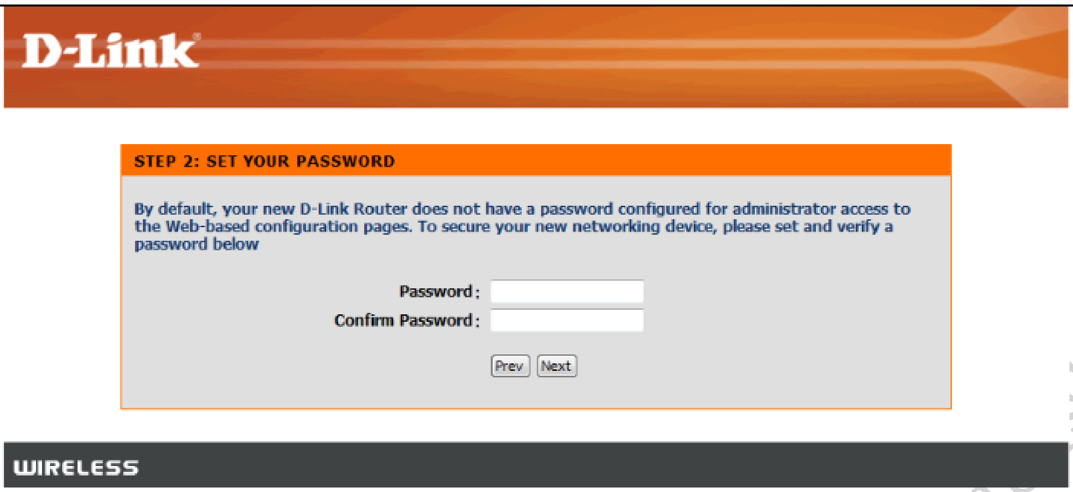
Network Name (SSID) : dlink

Security Mode : ● Disable Wireless Security (Not recommended) ○ AUTO-WPA/WPA2(Recommended)

Network Key :

□ Auto generate network key

Fig. 1.25 (a): Internet connection configuration window



STEP 2: SET YOUR PASSWORD

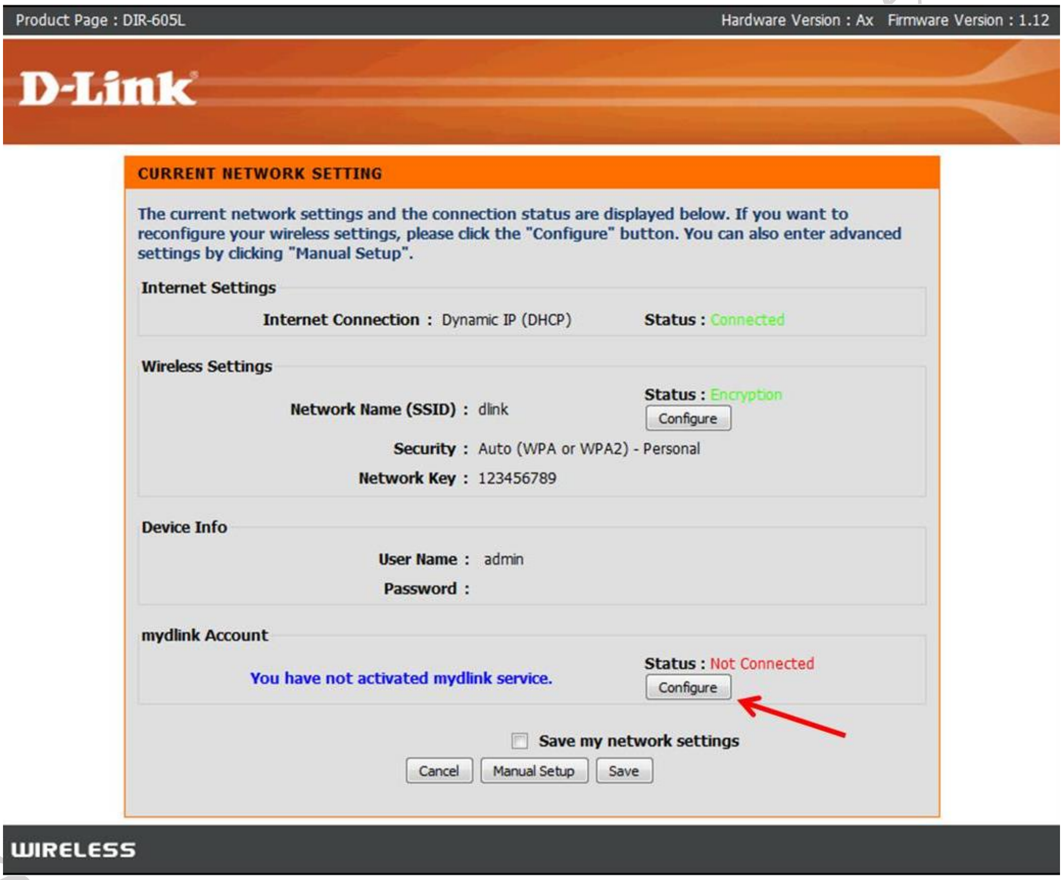
By default, your new D-Link Router does not have a password configured for administrator access to the Web-based configuration pages. To secure your new networking device, please set and verify a password below

Password :

Confirm Password :

Fig. 1.25 (b): Password setup window

Step 4. Check the setup details as shown in Figure 1.26 (a).



Product Page : DIR-605L Hardware Version : Ax Firmware Version : 1.12

CURRENT NETWORK SETTING

The current network settings and the connection status are displayed below. If you want to reconfigure your wireless settings, please click the "Configure" button. You can also enter advanced settings by clicking "Manual Setup".

Internet Settings

Internet Connection : Dynamic IP (DHCP) Status : Connected

Wireless Settings

Network Name (SSID) : dlink Status : Encryption

Security : Auto (WPA or WPA2) - Personal

Network Key : 123456789

Device Info

User Name : admin

Password :

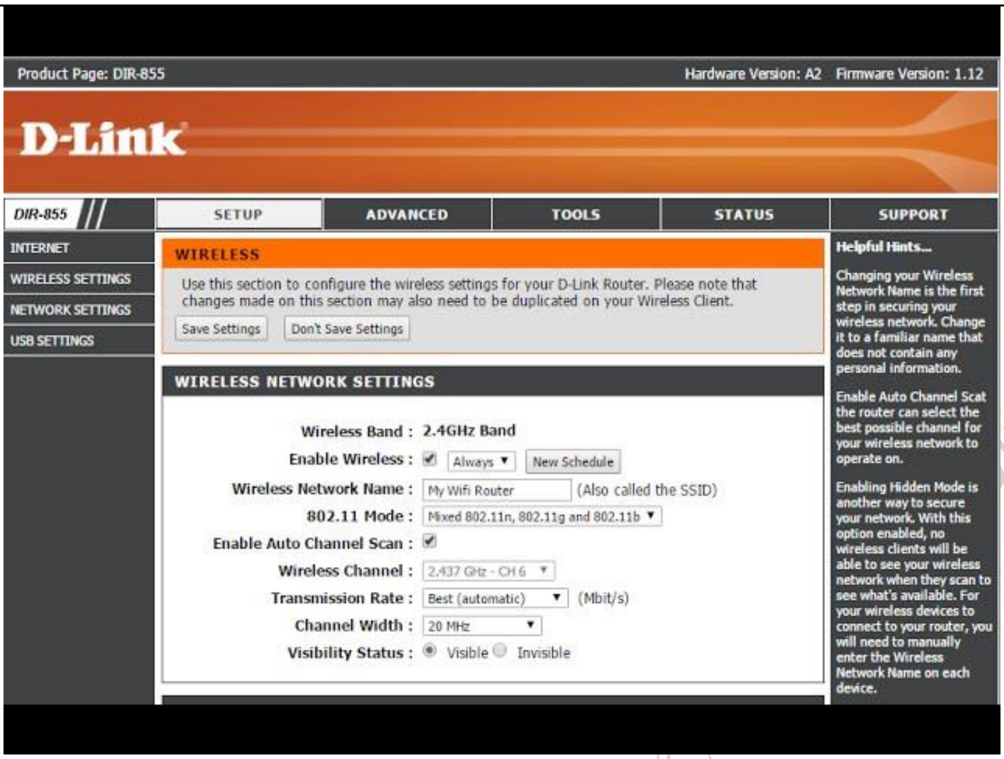
mydlink Account

You have not activated mydlink service. Status : Not Connected

□ Save my network settings

Fig. 1.26 (a): Router configuration

Step 5. Open the Internet browser and type the default gateway address on the address bar. Login to the account and the router details' window will open. Figure 1.26 (b), (c), (d), (e) shows the screenshots of router settings.



Product Page: DIR-855 Hardware Version: A2 Firmware Version: 1.12

WIRELESS

Use this section to configure the wireless settings for your D-Link Router. Please note that changes made on this section may also need to be duplicated on your Wireless Client.

WIRELESS NETWORK SETTINGS

Wireless Band : 2.4GHz Band

Enable Wireless : ☑ Always

Wireless Network Name : My Wifi Router (Also called the SSID)

802.11 Mode : Mixed 802.11n, 802.11g and 802.11b

Enable Auto Channel Scan : ☑

Wireless Channel : 2.437 GHz - CH 6

Transmission Rate : Best (automatic) (Mbit/s)

Channel Width : 20 MHz

Visibility Status : ● Visible ○ Invisible

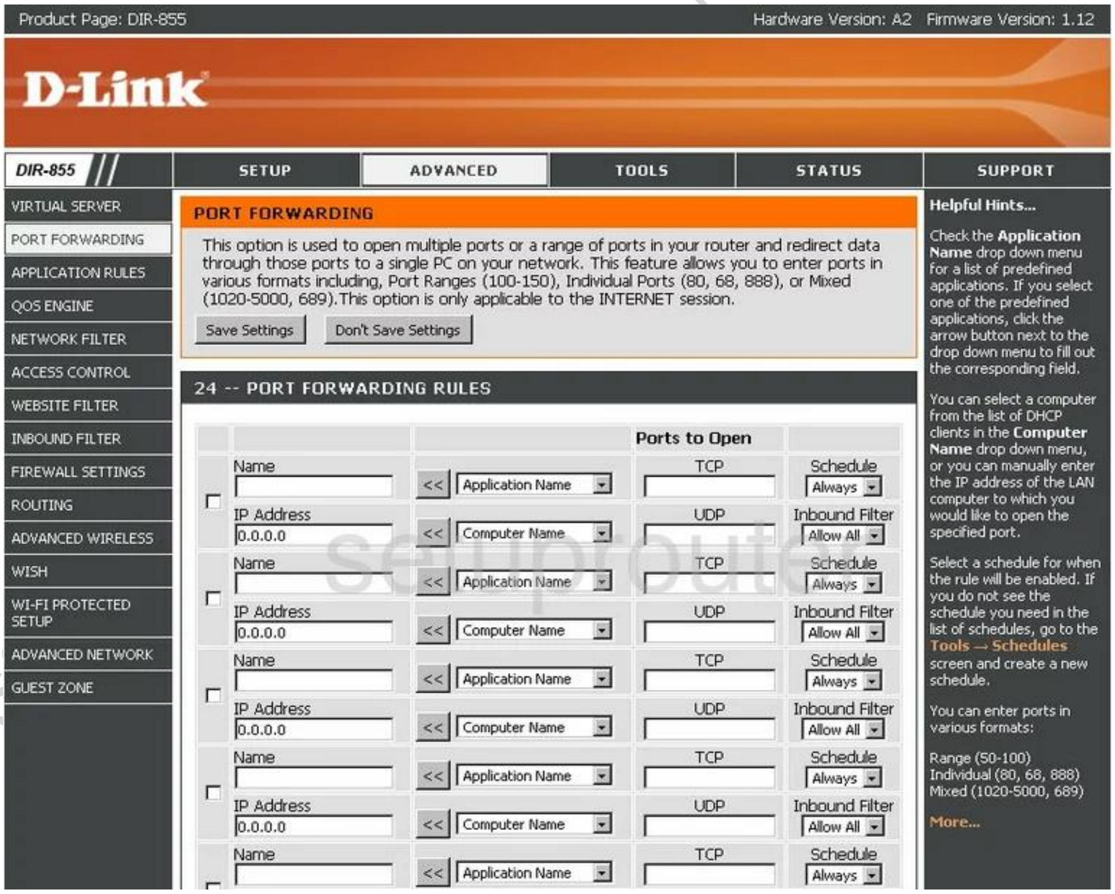
Helpful Hints...

Changing your Wireless Network Name is the first step in securing your wireless network. Change it to a familiar name that does not contain any personal information.

Enable Auto Channel Scat the router can select the best possible channel for your wireless network to operate on.

Enabling Hidden Mode is another way to secure your network. With this option enabled, no wireless clients will be able to see your wireless network when they scan to see what's available. For your wireless devices to connect to your router, you will need to manually enter the Wireless Network Name on each device.

Fig.1.26 (b): Router settings



Product Page: DIR-855 Hardware Version: A2 Firmware Version: 1.12

PORT FORWARDING

This option is used to open multiple ports or a range of ports in your router and redirect data through those ports to a single PC on your network. This feature allows you to enter ports in various formats including, Port Ranges (100-150), Individual Ports (80, 68, 888), or Mixed (1020-5000, 689).This option is only applicable to the INTERNET session.

24 -- PORT FORWARDING RULES

			Ports to Open	
□	Name	<< Application Name	TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	UDP	Inbound Filter Allow All
□	Name	<< Application Name	TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	UDP	Inbound Filter Allow All
□	Name	<< Application Name	TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	UDP	Inbound Filter Allow All
□	Name	<< Application Name	TCP	Schedule Always
	IP Address 0.0.0.0	<< Computer Name	UDP	Inbound Filter Allow All
□	Name	<< Application Name	TCP	Schedule Always

Helpful Hints...

Check the **Application Name** drop down menu for a list of predefined applications. If you select one of the predefined applications, click the arrow button next to the drop down menu to fill out the corresponding field.

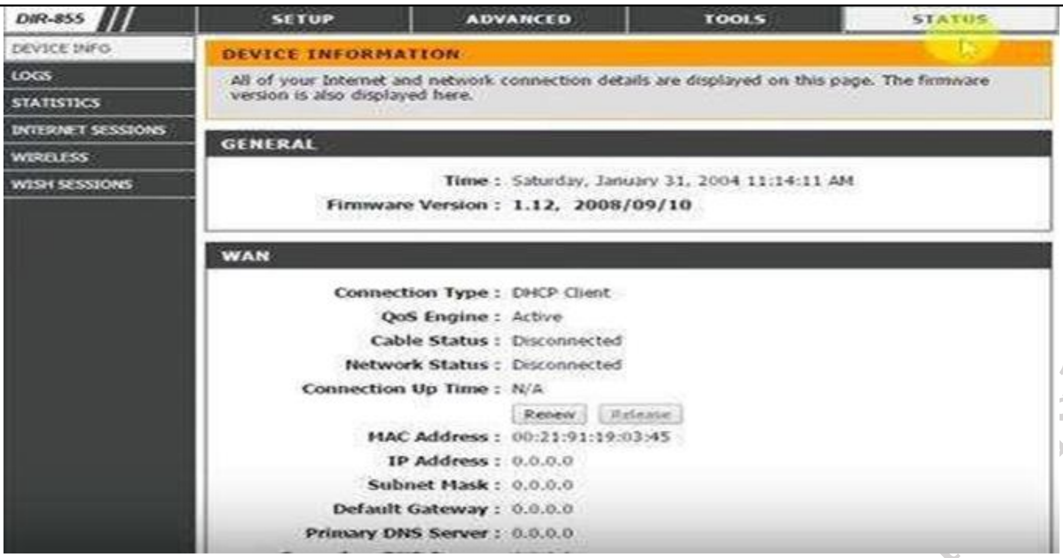
You can select a computer from the list of DHCP clients in the **Computer Name** drop down menu, or you can manually enter the IP address of the LAN computer to which you would like to open the specified port.

Select a schedule for when the rule will be enabled. If you do not see the schedule you need in the list of schedules, go to the **Tools → Schedules** screen and create a new schedule.

You can enter ports in various formats:

Range (50-100)
Individual (80, 68, 888)
Mixed (1020-5000, 689)

Fig. 1.26 (c): Router settings



DEVICE INFORMATION

All of your Internet and network connection details are displayed on this page. The firmware version is also displayed here.

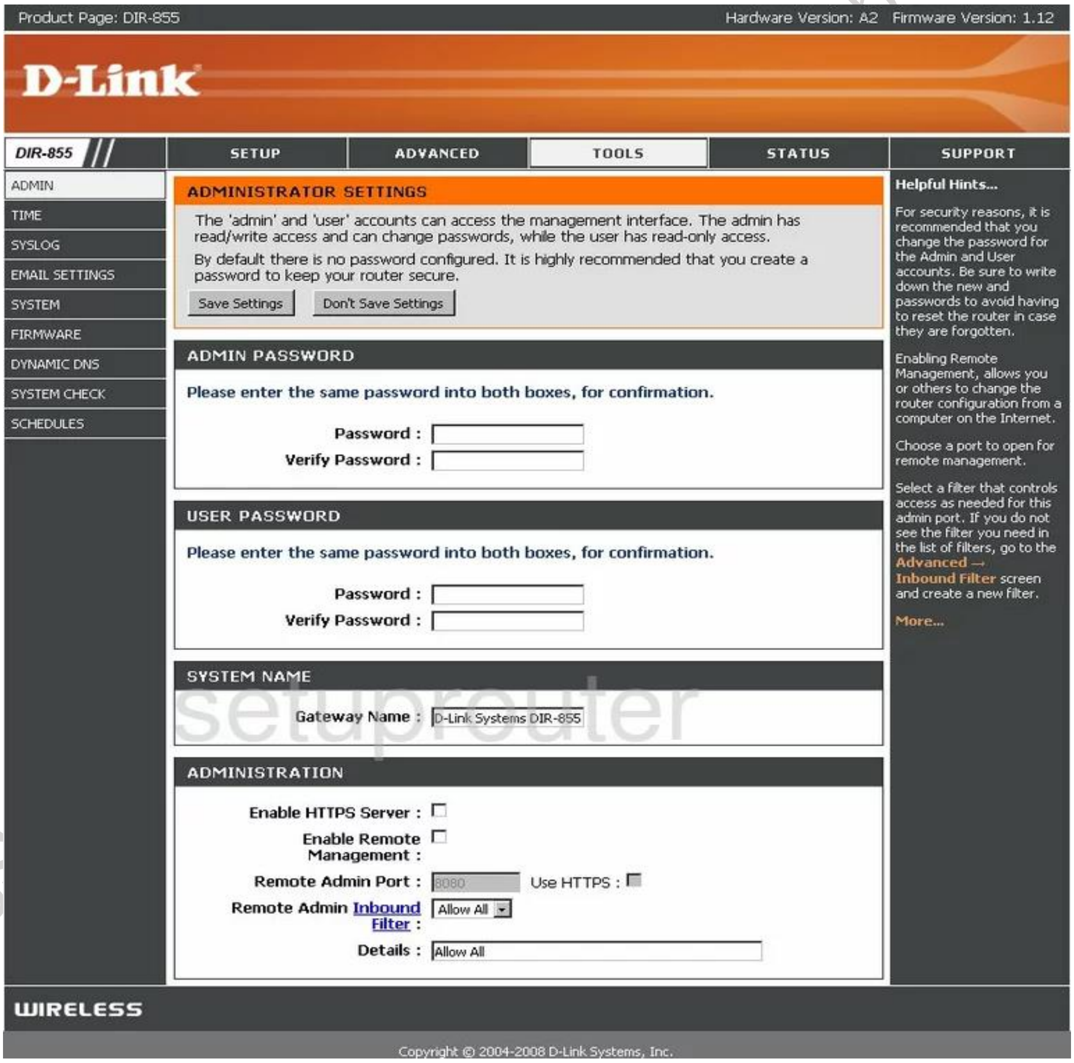
GENERAL

Time : Saturday, January 31, 2004 11:14:11 AM
Firmware Version : 1.12, 2008/09/10

WAN

Connection Type : DHCP Client
QoS Engine : Active
Cable Status : Disconnected
Network Status : Disconnected
Connection Up Time : N/A
Renew Release
MAC Address : 00:21:91:19:03:45
IP Address : 0.0.0.0
Subnet Mask : 0.0.0.0
Default Gateway : 0.0.0.0
Primary DNS Server : 0.0.0.0

Fig. 1.26 (d): Router settings



ADMINISTRATOR SETTINGS

The 'admin' and 'user' accounts can access the management interface. The admin has read/write access and can change passwords, while the user has read-only access.

By default there is no password configured. It is highly recommended that you create a password to keep your router secure.

Save Settings Don't Save Settings

ADMIN PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
Verify Password :

USER PASSWORD

Please enter the same password into both boxes, for confirmation.

Password :
Verify Password :

SYSTEM NAME

Gateway Name : D-Link Systems DIR-855

ADMINISTRATION

Enable HTTPS Server : □
Enable Remote Management : □
Remote Admin Port : 8080 Use HTTPS : □
Remote Admin Inbound Filter : Allow All
Details : Allow All

Helpful Hints...

For security reasons, it is recommended that you change the password for the Admin and User accounts. Be sure to write down the new and passwords to avoid having to reset the router in case they are forgotten.

Enabling Remote Management, allows you or others to change the router configuration from a computer on the Internet.

Choose a port to open for remote management.

Select a filter that controls access as needed for this admin port. If you do not see the filter you need in the list of filters, go to the Advanced → Inbound Filter screen and create a new filter.

More...

Copyright © 2004-2008 D-Link Systems, Inc.

Fig. 1.26 (e): Router settings

Step 6. After initializing the node device which is an IoT camera in the above-given case and the gateway which is a D Link router in the above case, the technician should check the connectivity of the node devices to the gateways.

1.2 Testing of network connectivity

After estatblishing the network connection, it should be tested for proper functioning. The network connectivity can be tested by **ipconfig** and **ping** command. Follow the steps below to test the network connectivity.

Step 1. Enter the command **ipconfig** on the command line and and press enter. If the screen shows the connection details, it means that there is no problem with the network connection.

Step 2. In the same way enter the **ping** command followed by <gateway address> to test. If it executes, it shows that there is no loss of packets and the router is working well.

Testing the network connectivity in Ubuntu Linux is shown in Figure ...

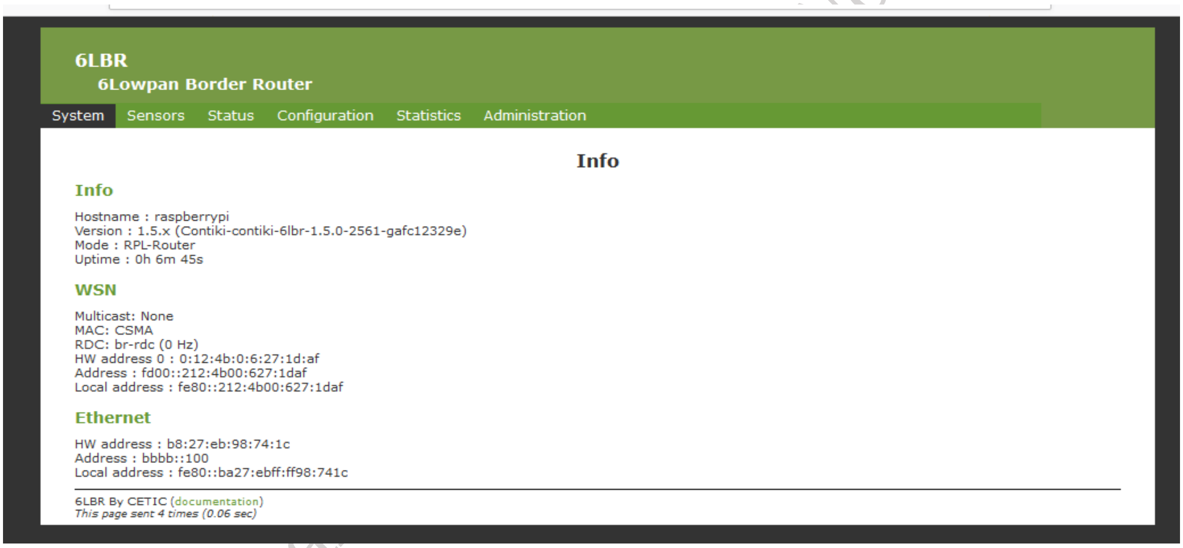
Practical Activity 1.3. Demonstrate to check the connection of the devices to the gateway.

Material required

Router, computer, Ethernet cable, sensor device

Procedure

Step 1. Launch the IoT device software installed on the laptop or desktop and open the default web server page. Figure 1.27 (a) and (b) show the screenshot of the 6lowPAN Border router details along with the system information, sensors connected, network status, and so on:



6LBR

6Lowpan Border Router

Info

Info

Hostname : raspberrypi
Version : 1.5.x (Contiki-contiki-6lbr-1.5.0-2561-gafc12329e)
Mode : RPL-Router
Uptime : 0h 6m 45s

WSN

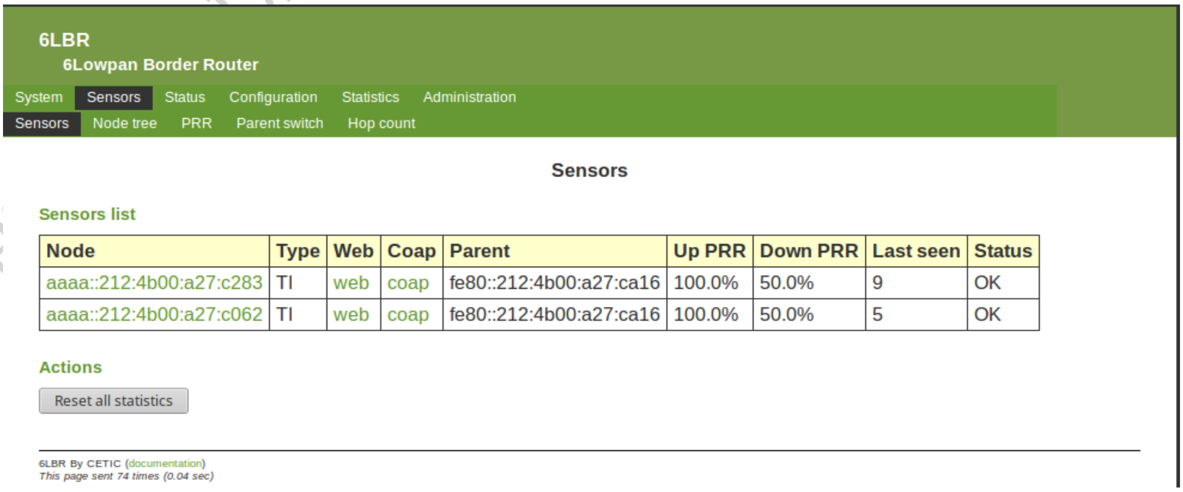
Multicast: None
MAC: CSMA
RDC: br-rdc (0 Hz)
HW address 0 : 0:12:4b:0:6:27:1d:af
Address : fd00::212:4b00:627:1daf
Local address : fe80::212:4b00:627:1daf

Ethernet

HW address : b8:27:eb:98:74:1c
Address : bbbb::100
Local address : fe80::ba27:ebff:ff98:741c

6LBR By CETIC (documentation)
This page sent 4 times (0.06 sec)

Fig. 1.27 (a): Internet settings



6LBR

6Lowpan Border Router

Sensors

Sensors list

Node	Type	Web	Coap	Parent	Up PRR	Down PRR	Last seen	Status
aaaa::212:4b00:a27:c283	TI	web	coap	fe80::212:4b00:a27:ca16	100.0%	50.0%	9	OK
aaaa::212:4b00:a27:c062	TI	web	coap	fe80::212:4b00:a27:ca16	100.0%	50.0%	5	OK

Actions

6LBR By CETIC (documentation)
This page sent 74 times (0.04 sec)

Fig. 1.27 (b): List of sensors connected

Step 2. Check that the status of each device and sensor is "OK". This means that the devices are connected to the gateway or the router.

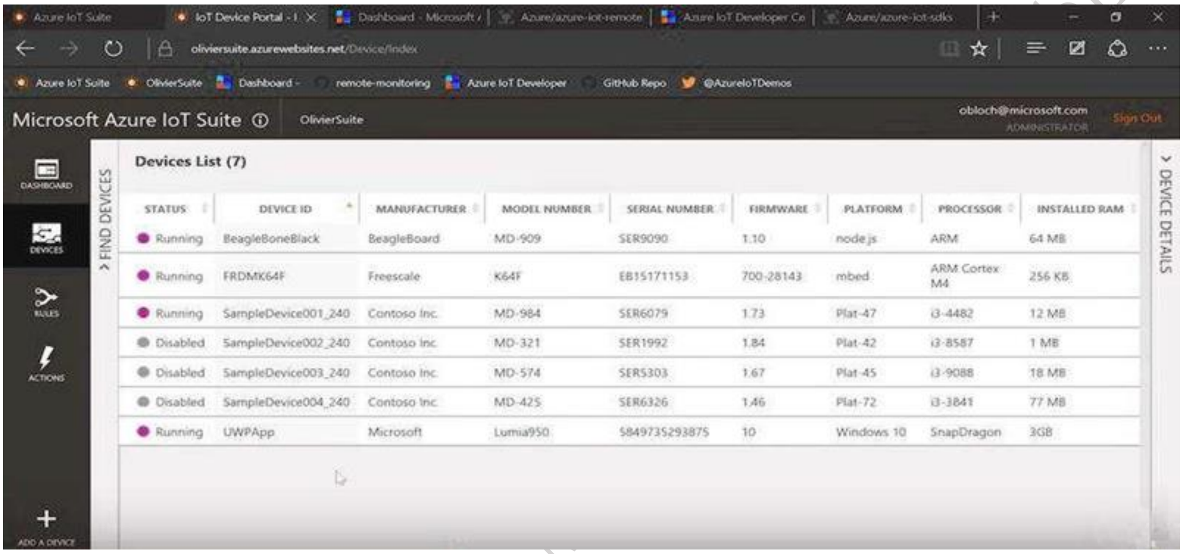
Practical Activity 1.4. Demonstrate to connect a physical device to the gateway and to test the connectivity

Material required

Microsoft Azure suite installed computer, router, Ethernet cable, sensor device

Procedure

Step 1. To do so in the Microsoft Azure suite, click on the devices to check the device parameters. Figure 1.28 shows the connected devices in the Microsoft Azure window.

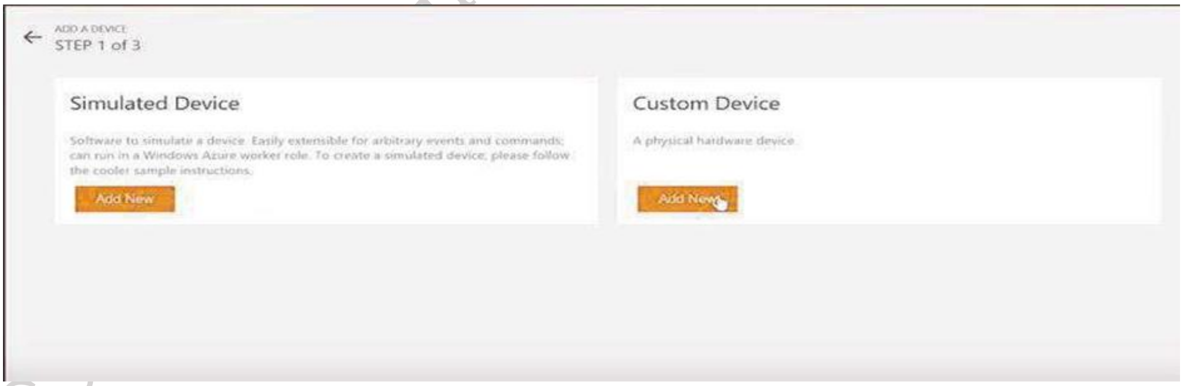


Devices List (7)

STATUS	DEVICE ID	MANUFACTURER	MODEL NUMBER	SERIAL NUMBER	FIRMWARE	PLATFORM	PROCESSOR	INSTALLED RAM
● Running	BeagleBoneBlack	BeagleBoard	MD-909	SER9090	1.10	node.js	ARM	64 MB
● Running	FRDMK64F	Freescale	K64F	EB15171153	700-28143	mbed	ARM Cortex M4	256 KB
● Running	SampleDevice001_240	Contoso Inc.	MD-984	SER6079	1.73	Plat-47	i3-4482	12 MB
● Disabled	SampleDevice002_240	Contoso Inc.	MD-321	SER1992	1.84	Plat-42	i3-8587	1 MB
● Disabled	SampleDevice003_240	Contoso Inc.	MD-574	SER5303	1.67	Plat-45	i3-9088	18 MB
● Disabled	SampleDevice004_240	Contoso Inc.	MD-425	SER6326	1.46	Plat-72	i3-3841	77 MB
● Running	UWPApp	Microsoft	Lumia950	5849735293875	10	Windows 10	SnapDragon	3GB

Fig. 1.28: Microsoft Azure window

Step 2. Click on "Add New" as shown in Figure 1.29.



ADD A DEVICE
STEP 1 of 3

Simulated Device

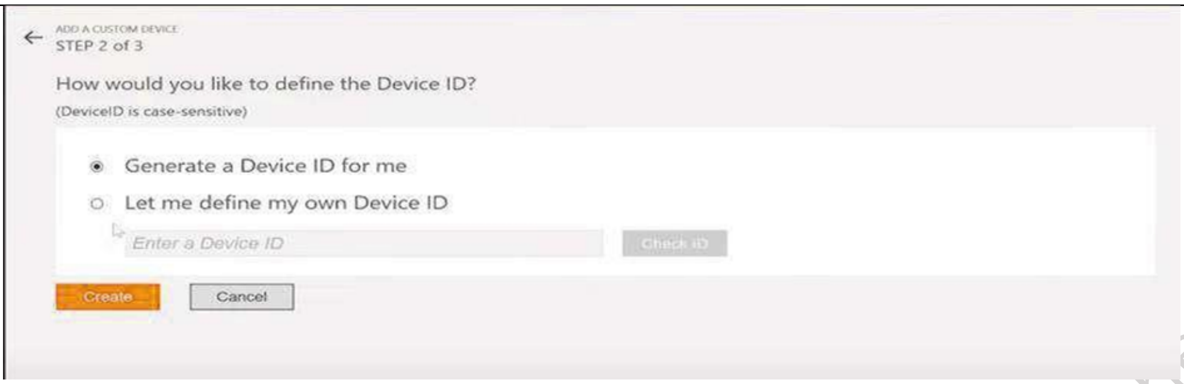
Software to simulate a device. Easily extensible for arbitrary events and commands; can run in a Windows Azure worker role. To create a simulated device, please follow the cooler sample instructions.

Custom Device

A physical hardware device

Fig. 1.29: Add new device

Step 3. Define the device ID as shown in Figure 1.30.



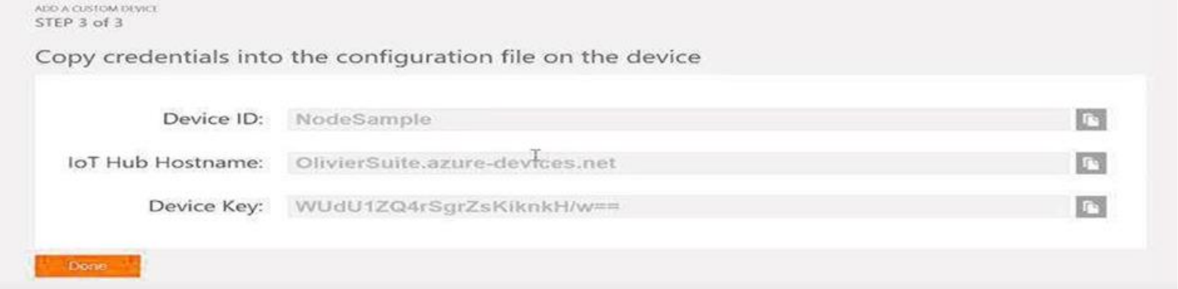
ADD A CUSTOM DEVICE
STEP 2 of 3

How would you like to define the Device ID?
(DeviceID is case-sensitive)

● Generate a Device ID for me
○ Let me define my own Device ID

Fig. 1.30: Defining device ID

Step 4. Configure the device ID and IoT hub name as shown in Figure 1.31.



ADD A CUSTOM DEVICE
STEP 3 of 3

Copy credentials into the configuration file on the device

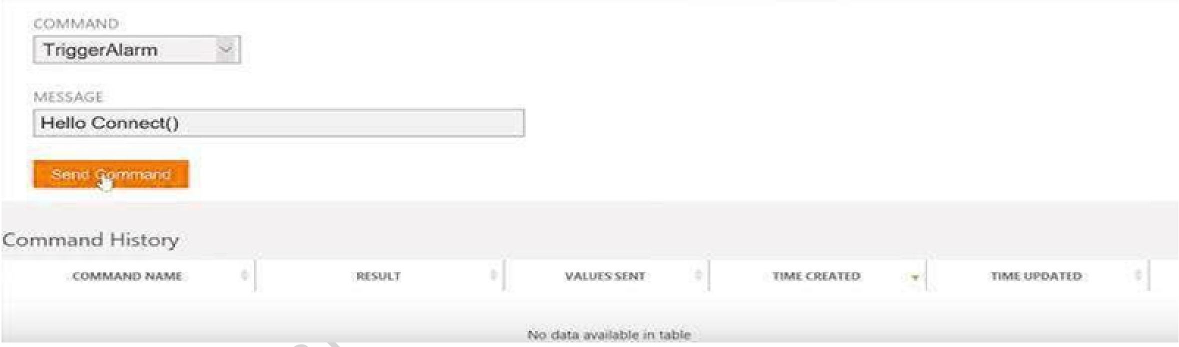
Device ID: NodeSample

IoT Hub Hostname: OlivierSuite.azure-devices.net

Device Key: WUdU1ZQ4rSgrZsKiknkH/w==

Fig. 1.31: Configuring the device ID and IoT hub name

Step 5. Set the command for the device as shown in Figure 1.31.



COMMAND: TriggerAlarm

MESSAGE: Hello Connect()

Command History

COMMAND NAME	RESULT	VALUES SENT	TIME CREATED	TIME UPDATED
No data available in table				

Fig. 1.32: Setting command for the device

Step 6. Check whether the device is functioning according to the command as shown in Figure 1.31.

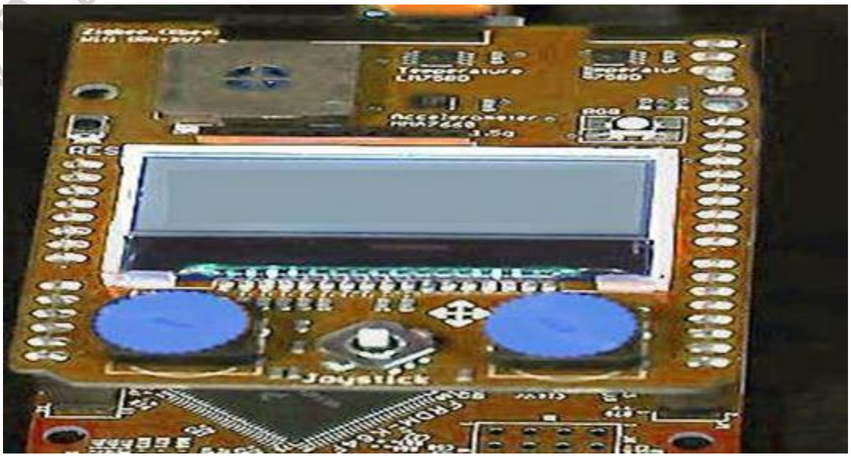


Fig. 1.33: Checking whether the device is functioning according to the command

1.3 Software Execution

The software is executed after the node devices and gateway (routers) have been initialized. The software is run in the final step, after which the device is joined to the communication channel.

Consider an IoT camera device that requires a connection to a ZigBee communication channel.

The following steps should be performed for connecting the device and executing the software

Step 1. Connect a USB cable to the ZigBee coordinator on the camera device and the computer system. Figure 1.34 shows the connection:

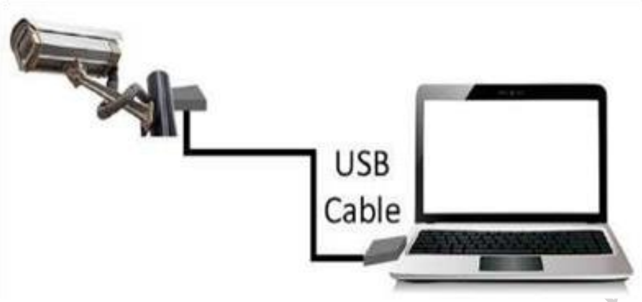


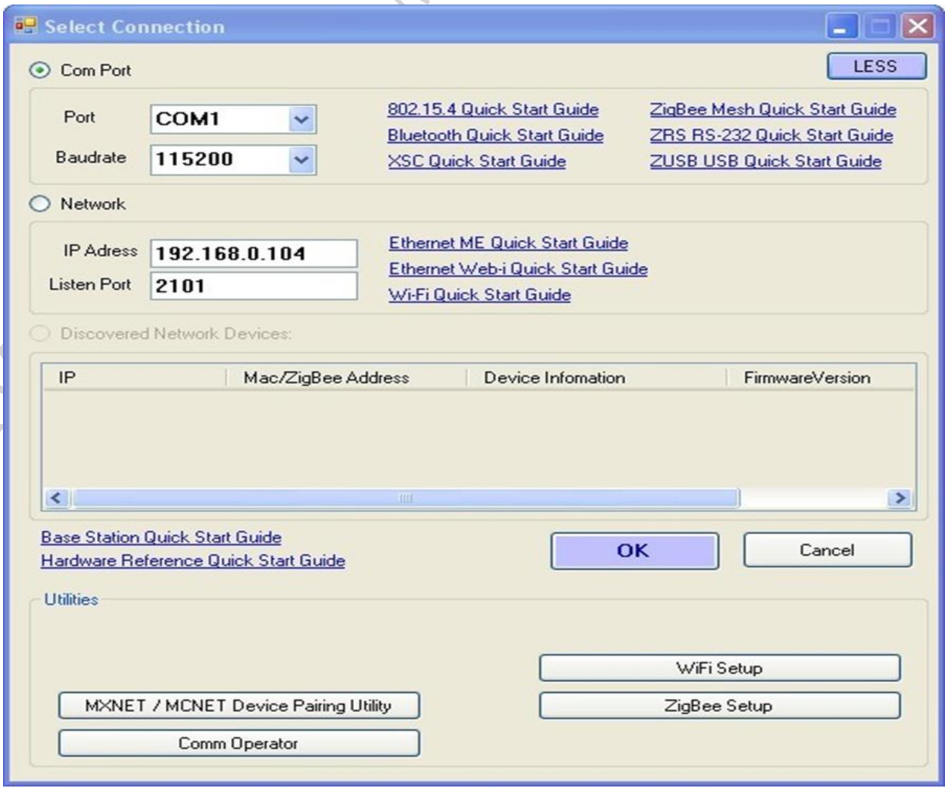
Fig. 1.34: Connection between camera and laptop with a USB cable

Step 1. Virtual COM port drivers are required for the ZigBee Mesh module; which can be downloaded through the link for Windows:

http://www.ftdichip.com/Drivers/VCP.htm

Step 1. Download the National Control Device (NCD) Base Station software to access the module; which will help to test devices and access them. The link for the software is given as: http://ncd-base-station.software.informer.com/

Step 4. Run the Base Station software for setting up the device. Figure 1.35 shows the selection window for setting up Base Station.



Select Connection

● Com Port

Port: COM1

Baudrate: 115200

○ Network

IP Adress: 192.168.0.104

Listen Port: 2101

○ Discovered Network Devices:

IP	Mac/ZigBee Address	Device Infomation	FirmwareVersion

LESS
802.15.4 Quick Start Guide
Bluetooth Quick Start Guide
XSC Quick Start Guide
ZigBee Mesh Quick Start Guide
ZRS RS-232 Quick Start Guide
ZUSB USB Quick Start Guide
Ethernet ME Quick Start Guide
Ethernet Web-i Quick Start Guide
Wi-Fi Quick Start Guide
Base Station Quick Start Guide
Hardware Reference Quick Start Guide
OK
Cancel
Utilities
WiFi Setup
ZigBee Setup
MXNET / MCNET Device Pairing Utility
Comm Operator

Fig. 1.35: Selection window for setting up Base Station

- Run Base Station.
- Select appropriate Com Port for ZigMo (ZigBee Coordinator).
- Click ZigBee Setup.
- Click Refresh.
- The progress bar will show for searching the device status.

Select the device in the list. Figure 1.36 shows the device selection window.

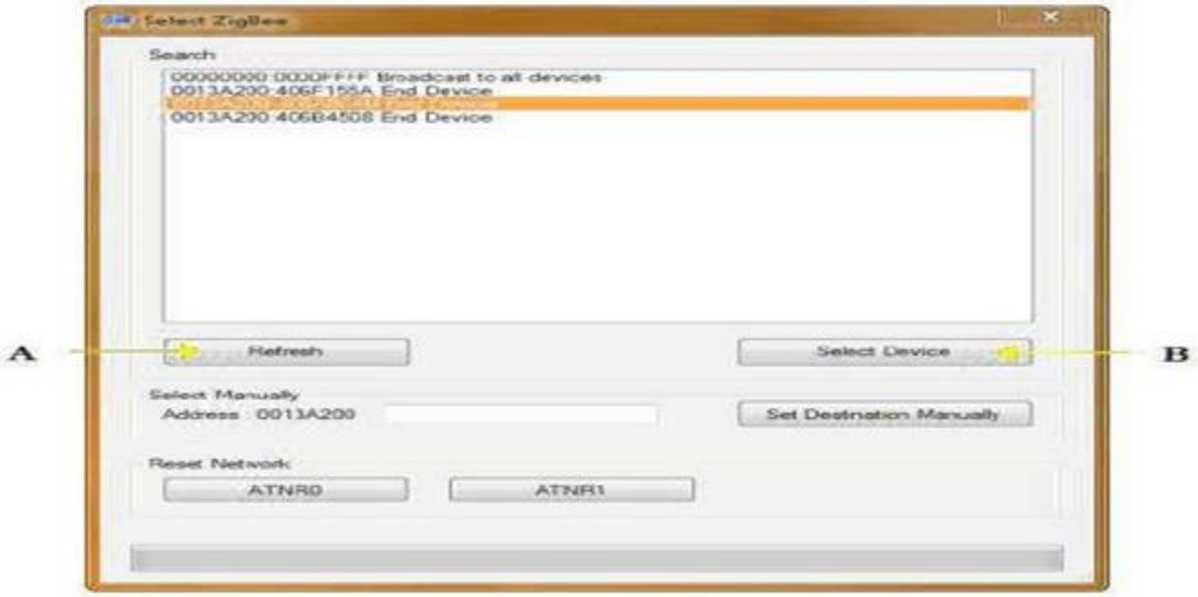
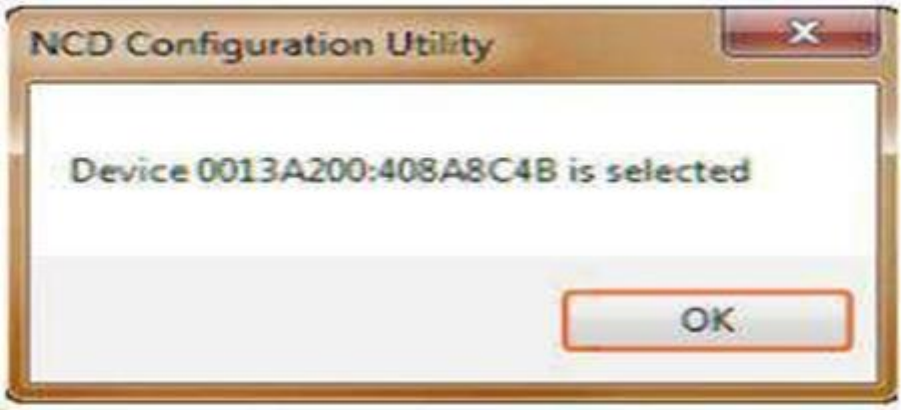


Fig. 1.36: Device selection window

- Click select device which is marked as (B) in the above screenshot.
- Progress bar will indicate that the device is loading.
- Click ‘OK’ in the alert box which appears.
- Close the Base Station window after the device is ready to use. Figure 1.37 shows the NCD configuration window.



Device 0013A200:408A8C4B is selected

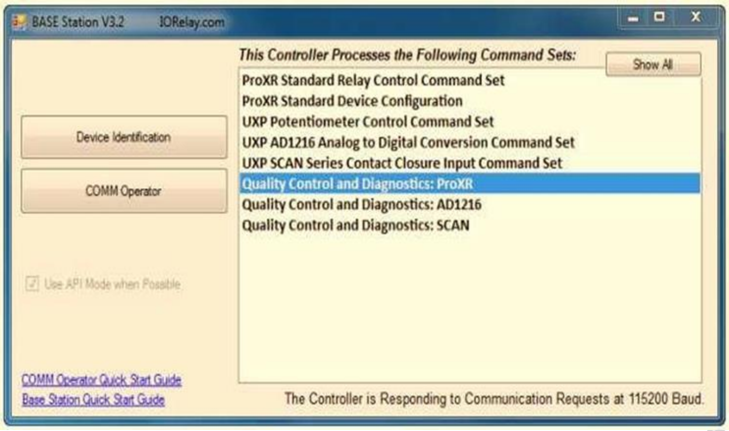
Fig. 1.37: NCD configuration window

5. Run the Base Station software to control the relays, read the A/D inputs, or start communicating with the remote device as follows:

- Run the Base Station software
- Now, select the appropriate Com Port on the opening **‘Select Connection’** window
- Click **OK**

6. Then, the Base Station software will generate a list of commands which the controller can process.

7. Now, select the command and use the device. Figure 1.38 shows the command option window.


BASE Station V3.2 IORelay.com
Show All
Device Identification
COMM Operator
☑ Use API Mode when Possible
COMM Operator Quick Start Guide
Base Station Quick Start Guide

This Controller Processes the Following Command Sets:

- ProXR Standard Relay Control Command Set
- ProXR Standard Device Configuration
- UXP Potentiometer Control Command Set
- UXP AD1216 Analog to Digital Conversion Command Set
- UXP SCAN Series Contact Closure Input Command Set
- Quality Control and Diagnostics: ProXR
- Quality Control and Diagnostics: AD1216
- Quality Control and Diagnostics: SCAN

The Controller is Responding to Communication Requests at 115200 Baud.

Fig. 1.38: Command option window

Summary

- This chapter covers the essential steps for setting up and configuring nodes, gateways, and control edge appliances in an IoT system.
- It emphasizes the importance of proper prerequisites, such as having routers, IoT devices, and internet connections in place.
- The process of installing an IoT camera and initializing nodes and gateways is given in detailed form in this chapter.
- Additionally, it outlines how to test network connectivity and execute necessary software for devices.
- This chapter provides a comprehensive guide for establishing a strong foundation in an IoT network.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the first step in initializing a node or gateway in an IoT setup? (a) Setting up a username and password (b) Unpacking the device (c) Connecting the power supply (d) Configuring the Internet connection
2. Which tool is recommended for manually connecting the camera in case automatic connection fails? (a) EnViewer Finder (b) NCD Base Station (c) Genius Vision NVR (d) ZigBee Coordinator
3. What is the purpose of mounting the camera on a wall? (a) To improve Wi-Fi signal strength (b) To enhance video quality (c) To cover a specific surveillance area adequately (d) To reduce power consumption
4. How can a technician verify that a camera is positioned within the router's coverage area? (a) Check the camera's packaging (b) Press the WPS button on the camera (c) Use EnViewer Finder tool (d) Compare installation kit specifications
5. What is the function of the WPS (Wi-Fi Protected Setup) button during camera setup? (a) Connect the camera to the power supply (b) Establish a wireless Internet connection (c) Initialize the camera's hardware (d) Mount the camera on a wall

6. Which mode of network connection requires providing an IP address manually? (a) DHCP (b) Manual (c) PPPoE (d) WPS
7. What is the purpose of unpacking the router device? (a) Matching specifications with the camera (b) Connecting the Ethernet cable (c) Checking for accessories and damage (d) Configuring the Internet connection
8. How can a technician access the router settings for configuration? (a) Open a web browser and enter the router's IP address (b) Run the NCD Base Station software (c) Connect the router with an Ethernet cable (d) Insert the utility tool disc
9. What does node initialization involve in an IoT setup? (a) Configuring network settings and securing the network (b) Connecting the power supply and cable (c) Mounting the camera on a wall (d) Unpacking the router
10. Which step follows the initialization of a node device in the provided content? (a) Testing network connectivity (b) Unpacking the router device (c) Configuring the router device (d) Installing the router

B. Fill in the blanks

1. To finish the cable connection, join the power adaptor end to the power supply port on the camera's _________.
2. The IoT camera must be connected to the router in order for it to function over a wireless Internet connection using _________.
3. If the automatic connection fails, establish a manual connection using a utility program like _________ that was included on the CD that came with the IoT camera's packaging.
4. To configure the router, a technician can connect the router with a desktop/laptop through a LAN wire or with the help of the _________ address.
5. To establish an Internet connection between the network provider and the gateway, which is the router installed at the location, the gateway or router must first be _________.
6. The software is executed after the node devices and gateway (routers) have been initialized. The software is run in the final step, after which the device is joined to the _________ channel.
7. After completing the hardware setup of the IoT device and connecting it with the Internet, the final step is to initialise _________.
8. Unpack the NVR device and connect the device to the router using an _____.
9. Connect a USB cable to the ZigBee coordinator ______ and the computer system.
10. Consider an IoT camera device that requires a connection to a _________.

C. State true or False for the following

1. Setting up a username and password on routers and IoT devices is known as initializing a node and gateway.
2. Unpacking the IoT camera is the first step in the installation process.
3. Mounting the camera and the camera stand are part of the fundamental hardware setup.
4. The power adaptor typically included in the packaging has a power output of 12 V/1 A.
5. The IoT camera must be connected to the router for it to function over a wireless Internet connection using Wi-Fi.
6. If the automatic connection fails, a technician can establish a manual connection using a utility program like EnViewer.

7. Unpacking the router is not necessary if the technician receives it from the Internet service provider (ISP).
8. Connecting the power cable end to the back of the router and the adapter plug to a power socket is part of the router installation process.
9. To configure the router, a technician can connect it to a desktop/laptop through a LAN wire or with the help of the IP address.
10. The final step after initializing the node devices and gateways is to execute the software, after which the device is joined to the communication channel.

D. Short Answer Type Questions

1. What is the purpose of initializing a node or gateway in an IoT setup?
2. Describe the steps involved in setting up the basic hardware of an IoT camera.
3. How can a technician connect the IoT camera to a wireless Internet connection using Wi-Fi?
4. What should be done if the automatic connection of the camera to the router fails?
5. What are the steps involved in unpacking and setting up a router for a wireless Internet connection?
6. How can a technician access the router settings for configuration?
7. What is the importance of node initialization in an IoT setup?
8. How does the technician test the network connectivity after initializing the node devices and gateways?
9. Explain the process of executing the software after initializing the node devices and gateways.
10. How does a technician connect a USB cable to the ZigBee coordinator on the camera device for software execution?

Session 2. Establish Communication and Connectivity between devices

All devices have USB ports. USB is the standard and must-have interface.

2.1 Types of USB Data Transfer

Data transmission from one device to another is referred to as data transfer. There are four types of transfer modes or types which can be used for data transfer via USB as shown in Figure 2.1.

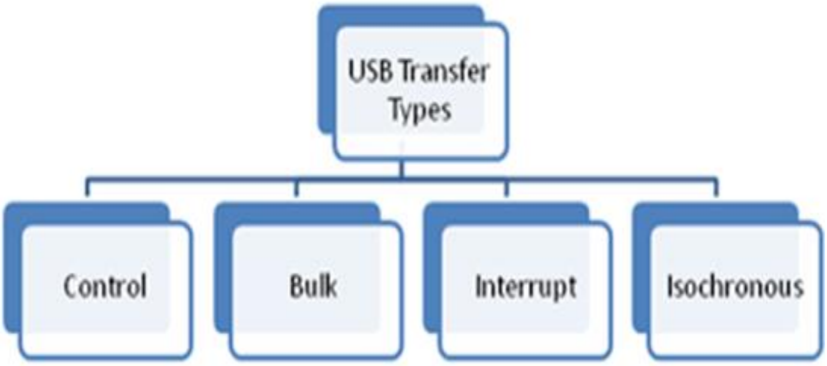


Fig. 2.1: Types of USB Data Transfer

Control Transfer

Control transfer is driven by rules about the content of the data to be transferred. It is used to allocate USB addresses, exchange device details and configure devices. All the devices use control transfer along with the other ones.

Bulk Transfer

Digital cameras, printers, scanners, and other image input, printing, and storage devices are necessary for the lossless transfer of large amounts of data.

Interrupt transfer

This is typically used by input devices like keyboards and mouse that are used as human interfaces. The input signals that are detected are treated as interrupt requests.

Isochronous Transfer

The audio and video devices require real-time data transfer. Such devices must be able to periodically transfer a certain amount of data. For the purpose of carrying out data transfers, USB divides time into frames. The main idea is to maintain a steady flow of time while transferring a fixed amount of data over each time interval. It is depicted with examples in Figure 2.1.

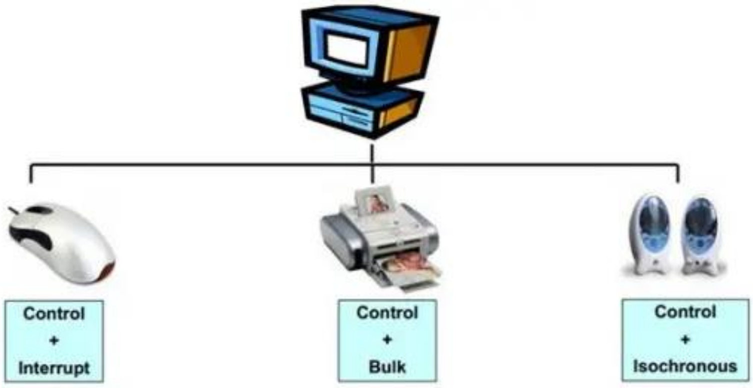


Fig.2.2: Example of USB Data Transfer

2.2 Data Transfer Modes

Communication technology deals with the mode of transfer of data. Mode refers to the direction of data flow over the network. There are three types of modes as follows:

2.1.1 Simplex

In simplex mode, the sender is able to send data but not receive it. It is a form of unidirectional communication in which only one direction is involved. Figure 2.3 shows direction of data transfer in simplex mode.

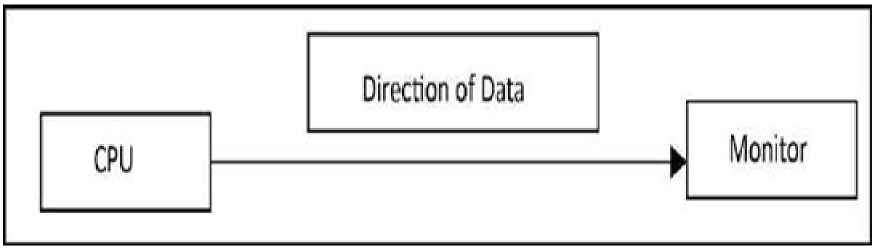


Fig. 2.3: Simplex mode

2.1.2 Half Duplex mode

The sender can send and receive data one at a time while in half-duplex mode. It is a form of two-way directional communication, but it can only be used by one person at once. Figure 2.4 shows direction of data transfer in half duplex mode.

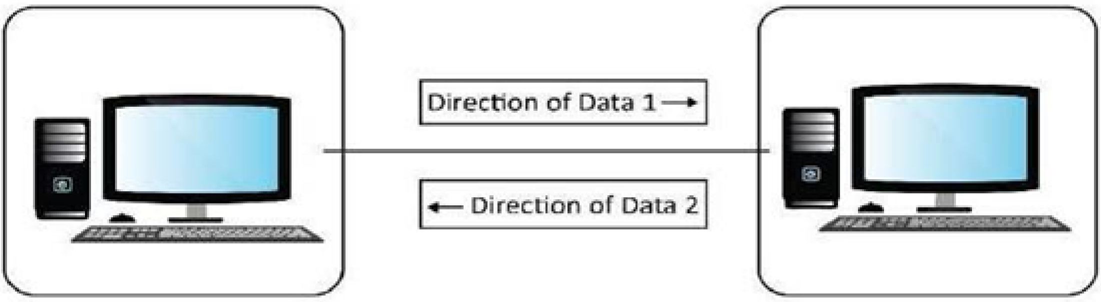


Fig. 2.4: Half duplex mode

2.1.3 Full Duplex Mode

In Full-duplex mode, the Sender can send the data and also receive the data simultaneously. It is two-way directional communication that can happen simultaneously. Figure 2.5 shows direction of data transfer in full duplex mode.

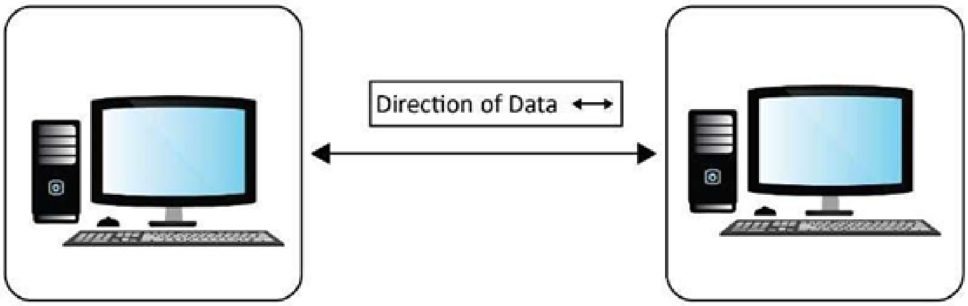


Fig. 2.5: Full Duplex Mode

2.3 Controlling the Data Transfer

Data transfer can be controlled by changing the baud rate of the Arduino or the Raspberry Pi. Figure 2.6 shows the baud rate of a setup.

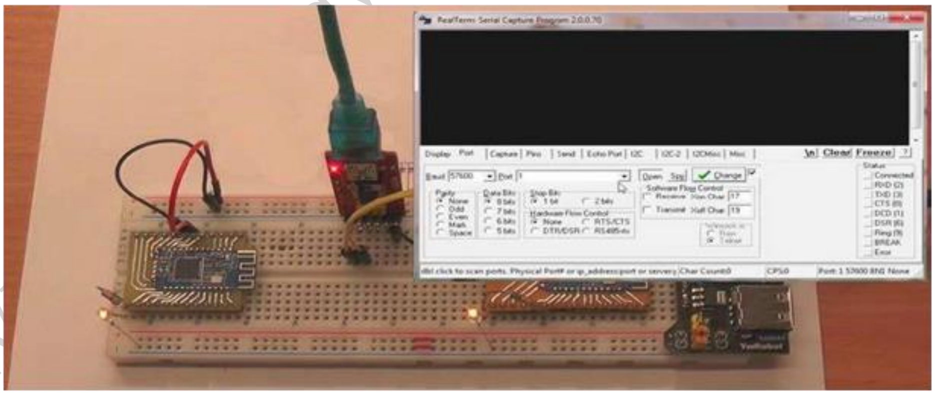
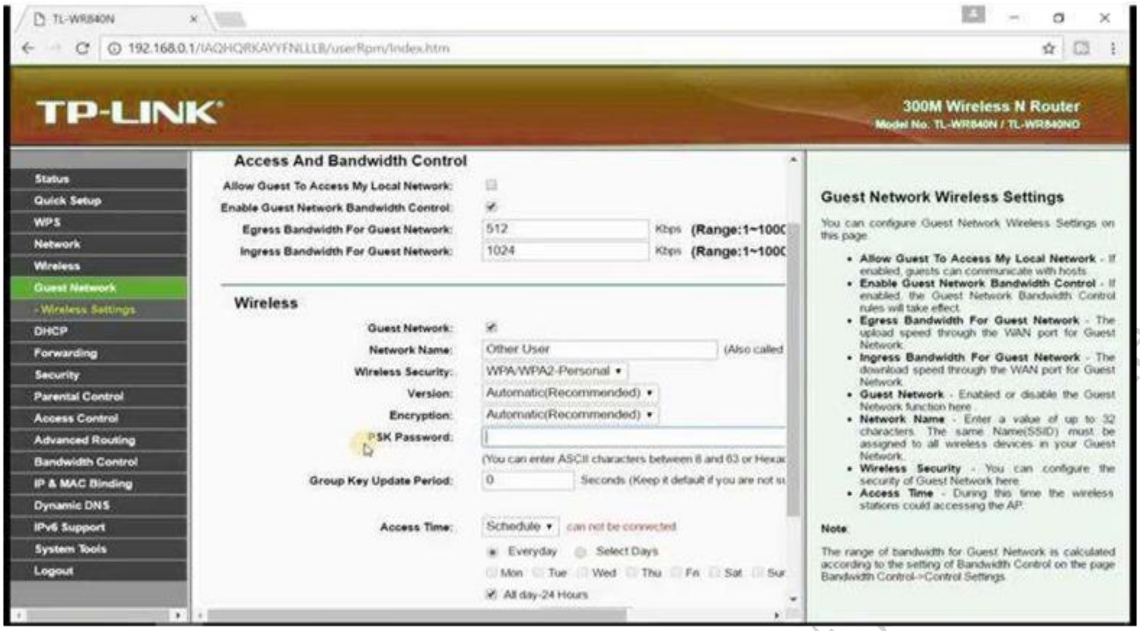


Fig. 2.6: Baud rate of a setup

To control the data transfer rate for a router, follows the steps:

Step 1. Open the router settings by entering the username and the password.

Step 2. Visit the “Guest Network” settings and enter the details. For controlling the transfer rate, the bandwidth needs to be set. Figure 2.7 shows the wireless settings for TP-Link.



Access And Bandwidth Control

Allow Guest To Access My Local Network: □

Enable Guest Network Bandwidth Control: ☑

Egress Bandwidth For Guest Network: 512 Kbps (Range:1~100C

Ingress Bandwidth For Guest Network: 1024 Kbps (Range:1~100C

Wireless

Guest Network: ☑

Network Name: Other User (Also called

Wireless Security: WPA/WPA2-Personal

Version: Automatic(Recommended)

Encryption: Automatic(Recommended)

PSK Password:

(You can enter ASCII characters between 8 and 63 or Hexac

Group Key Update Period: 0 Seconds (Keep it default if you are not su

Access Time: Schedule can not be connected

● Everyday ○ Select Days

□ Mon □ Tue □ Wed □ Thu □ Fri □ Sat □ Sur

☑ All day-24 Hours

Guest Network Wireless Settings

You can configure Guest Network Wireless Settings on this page.

- **Allow Guest To Access My Local Network** - If enabled, guests can communicate with hosts.
- **Enable Guest Network Bandwidth Control** - If enabled, the Guest Network Bandwidth Control rules will take effect.
- **Egress Bandwidth For Guest Network** - The upload speed through the WAN port for Guest Network.
- **Ingress Bandwidth For Guest Network** - The download speed through the WAN port for Guest Network.
- **Guest Network** - Enabled or disable the Guest Network function here .
- **Network Name** - Enter a value of up to 32 characters. The same Name(SSID) must be assigned to all wireless devices in your Guest Network.
- **Wireless Security** - You can configure the security of Guest Network here.
- **Access Time** - During this time the wireless stations could accessing the AP.

Note:

The range of bandwidth for Guest Network is calculated according to the setting of Bandwidth Control on the page Bandwidth Control->Control Settings.

Fig. 2.7: Wireless settings for TP-Link

2.4 Data Transfer Using the Indicators

The lights on devices, including routers, gateways, and other similar equipment, assist in determining the status of the equipment's operation. The various indicators on a device are listed in table 2.1.

Table 2.1 Different indicators on the device

	Solid	***Blinking***	***Off***
Battery	Battery is good	The battery is not good	No Battery
Wi-Fi	Wireless network enabled	Connection not stable due to traffic on the network	Network failure or disabled
Ethernet	Device connected to the Ethernet port	Data is being transmitted over Ethernet link	Device not connected to the Ethernet port
Online	Internet available	------	No Internet available
Upstream (US)	Yellow/ Green: Connected to the Internet	Not connected to the Internet	------
Downstream (DS)	Yellow / Green: Connected to the Internet	Not connected to the Internet	------
Power	AC power is available	------	There is no AC power

2.5 Comparison of data transfer techniques over various networks

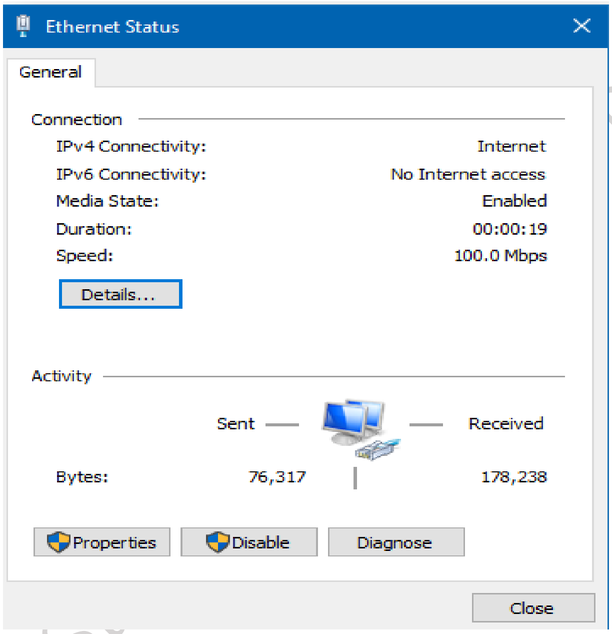
The mechanism and techniques of data transfer depend on the type of network. The table 2.2 lists the comparison between the data transfer over various networks:

Table 2.2 Comparison between the data transfer over various networks

	ZigBee	***Bluetooth LE***	***Z-Wave***	***NFC***	***Wi-Fi***
IEEE Specification	801.15.4	801.15.1	ITU -T	ISO 13157	801.11 a/b/g

Frequency Band	868/915 MHz; 1.4 GHz	1.4 – 1.5 GHz	908.42 MHz	13.56 MHz	1.4 GHz; 5 GHz
Network Type	WPAN	WPAN	WPAN	P2P	WPAN
Power Consumption (mA)	40	11.5	1.5	50	116
Nominal Range (m)	10	50	30	.05	100
Max. Signal Rate	250 kbps	305 kbps	40-100 kbps	424 kbps	54 Mbps

To check the network speed and data transfer rates, there are many tools available. By selecting "Ethernet" and then "Properties'' in Windows OS, it can be verified. An Ethernet network's status is displayed as shown in Figure 2.8.



Ethernet Status

General

Connection

IPv4 Connectivity: Internet

IPv6 Connectivity: No Internet access

Media State: Enabled

Duration: 00:00:19

Speed: 100.0 Mbps

Activity

	Sent	Received
Bytes:	76,317	178,238

Fig. 2.8: Network status

2.7 Connecting to the Network Remotely

An IoT framework must have external connectivity in order to give remote users access to the central site. A connectivity strategy that enables both site-to-site and remote client connectivity must be implemented for this. The gateway and the neighbourhood Wi-Fi router or 3G/4G connectivity options can be connected.

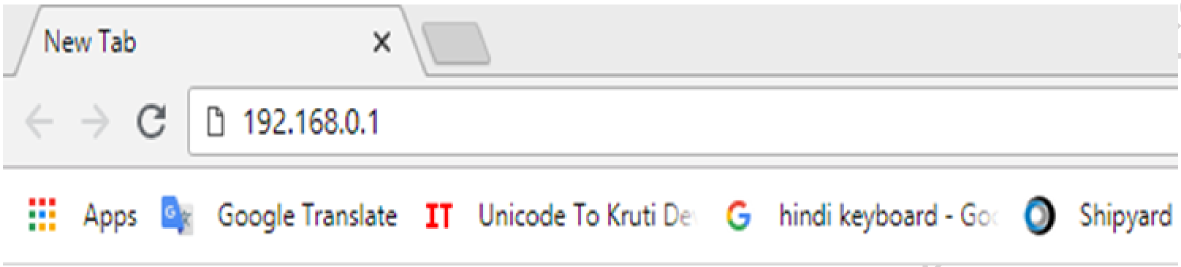
Practical Activity 2.1. Demonstrate to access a router or any device remotely.

Material Required

TP link wireless router, computer

Procedure

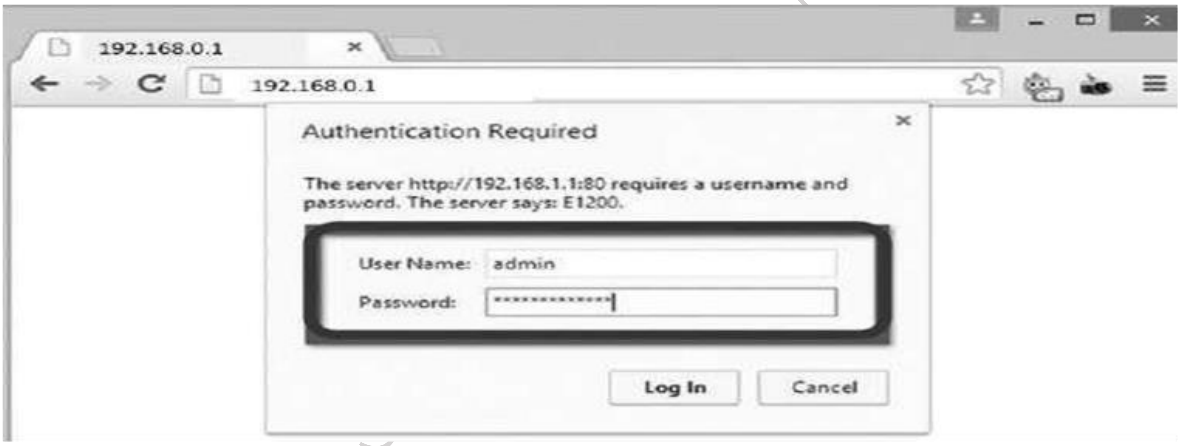
Step 1. Open the web browser and enter the router address. The default address is 191.168.0.1. For any device, such as a surveillance camera, enter the device's IP address. Figure 2.9 shows the default IP address at the address bar:



192.168.0.1

Fig. 2.9: IP address at address bar

Step 2. An authentication window will appear. Enter the user ID and the password in the window as shown Figure 2.10.



192.168.0.1

Authentication Required

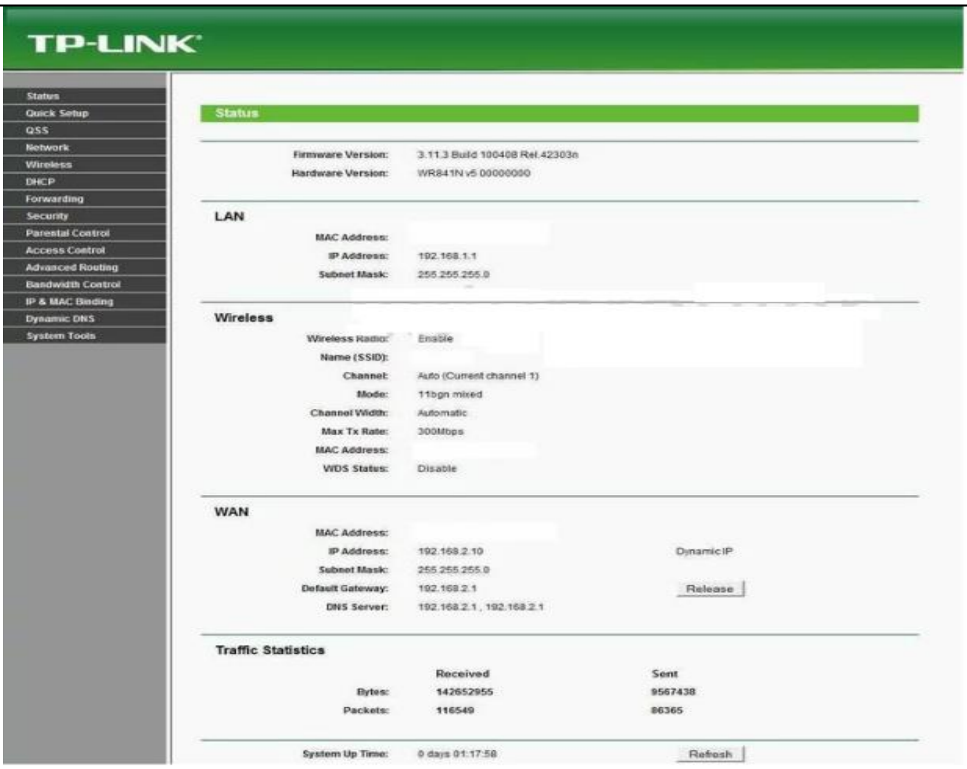
The server http://192.168.1.1:80 requires a username and password. The server says: E1200.

User Name: admin

Password: *************

Fig. 2.10: Authentication window

Step 3. Check the network status and the details on the window as shown Figure 2.11.



Status

Firmware Version: 3.11.3 Build 100408 Rel.42303n
Hardware Version: WR841N v5 00000000

LAN

MAC Address:
IP Address: 192.168.1.1
Subnet Mask: 255.255.255.0

Wireless

Wireless Radio: Enable
Name (SSID):
Channel: Auto (Current channel 1)
Mode: 11bgn mixed
Channel Width: Automatic
Max Tx Rate: 300Mbps
MAC Address:
WDS Status: Disable

WAN

MAC Address:
IP Address: 192.168.2.10 Dynamic IP
Subnet Mask: 255.255.255.0
Default Gateway: 192.168.2.1
DNS Server: 192.168.2.1 , 192.168.2.1

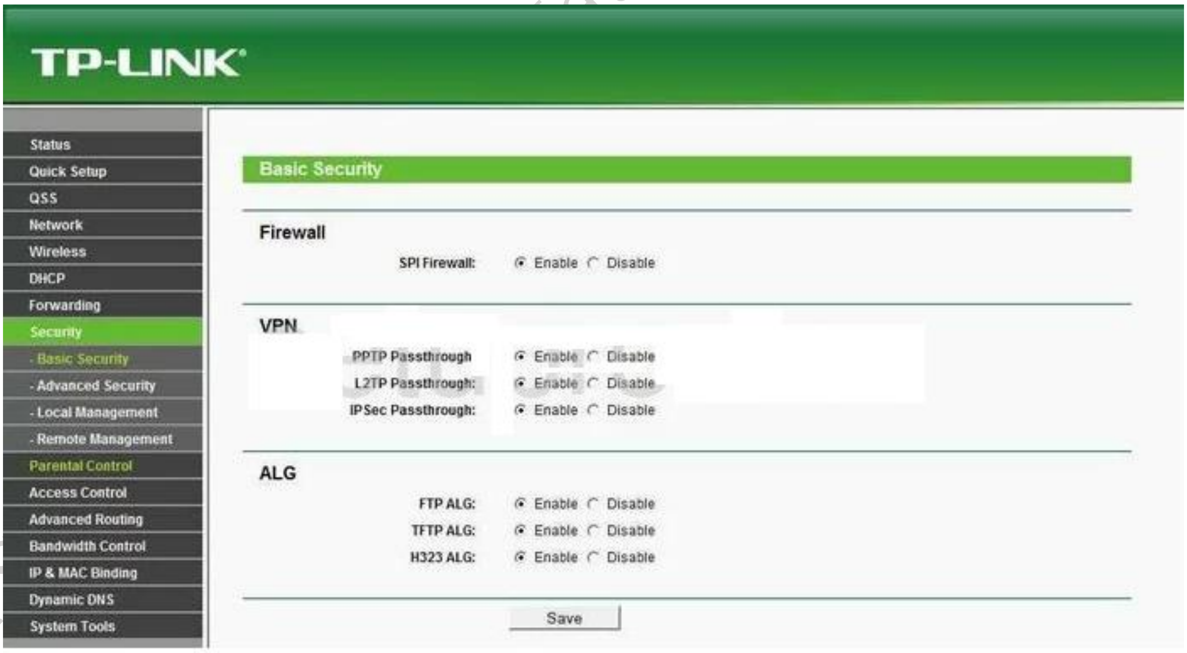
Traffic Statistics

	Received	Sent
Bytes:	142652955	9567438
Packets:	116549	86365

System Up Time: 0 days 01:17:58

Fig. 2.11: Network status window

Step 2. Enter the security settings details and enable the security option suitable, as shown in Figure 2.12.



Basic Security

Firewall

SPI Firewall: ● Enable ○ Disable

VPN

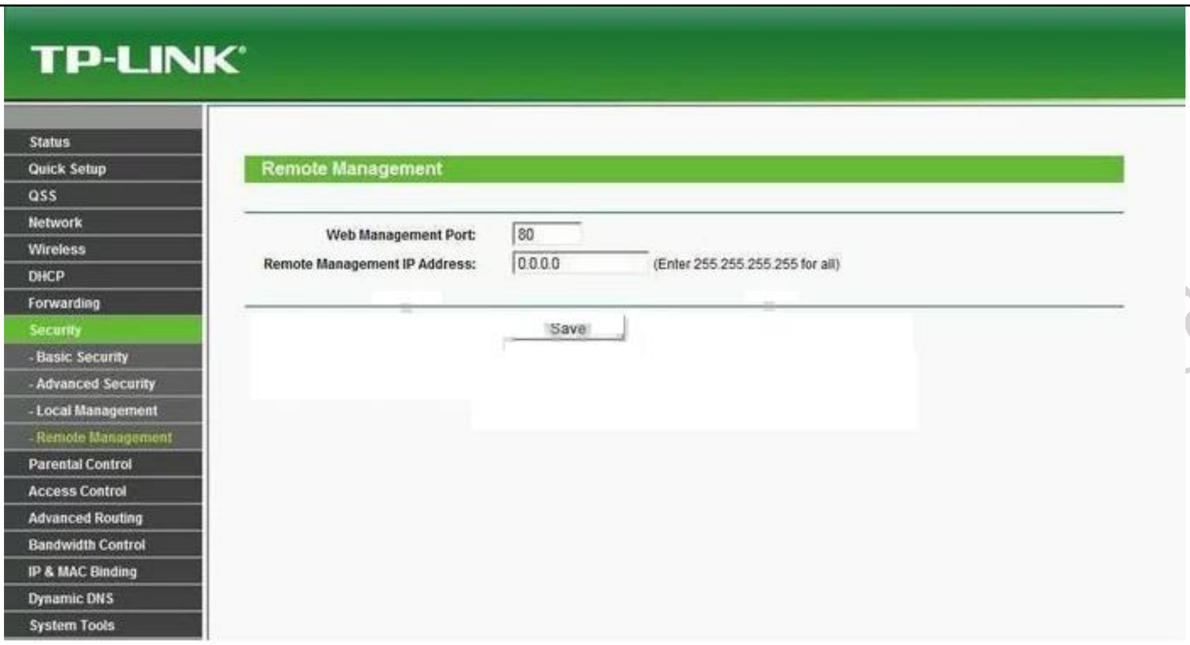
PPTP Passthrough: ● Enable ○ Disable
L2TP Passthrough: ● Enable ○ Disable
IPSec Passthrough: ● Enable ○ Disable

ALG

FTP ALG: ● Enable ○ Disable
TFTP ALG: ● Enable ○ Disable
H323 ALG: ● Enable ○ Disable

Fig. 2.12: Basic security settings

Step 5. Enter the details such as port and remote IP address in the *"Remote Management"* under security. The IP address will be 255.255.255.255 for the device to make it public as shown in Figure 2.13.



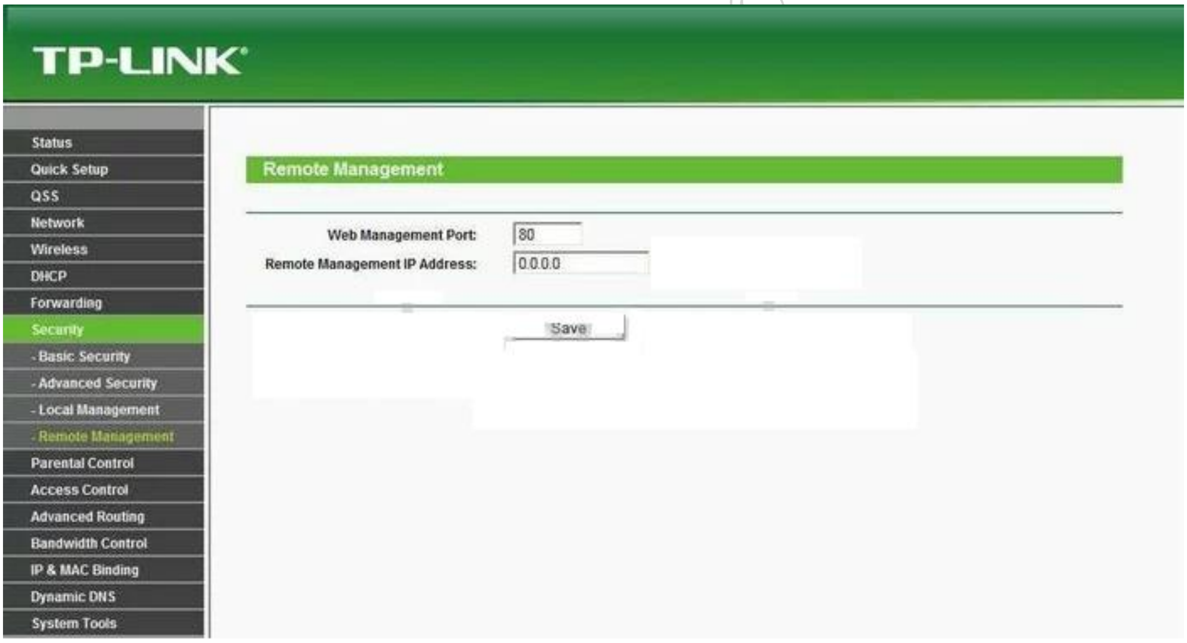
Remote Management

Web Management Port: 80

Remote Management IP Address: 0.0.0.0 (Enter 255.255.255.255 for all)

Fig. 2.13: Remote management settings for public access

Step 6. The IP address will be 0.0.0.0, for the device to deny any access, as shown in Figure 2.14.



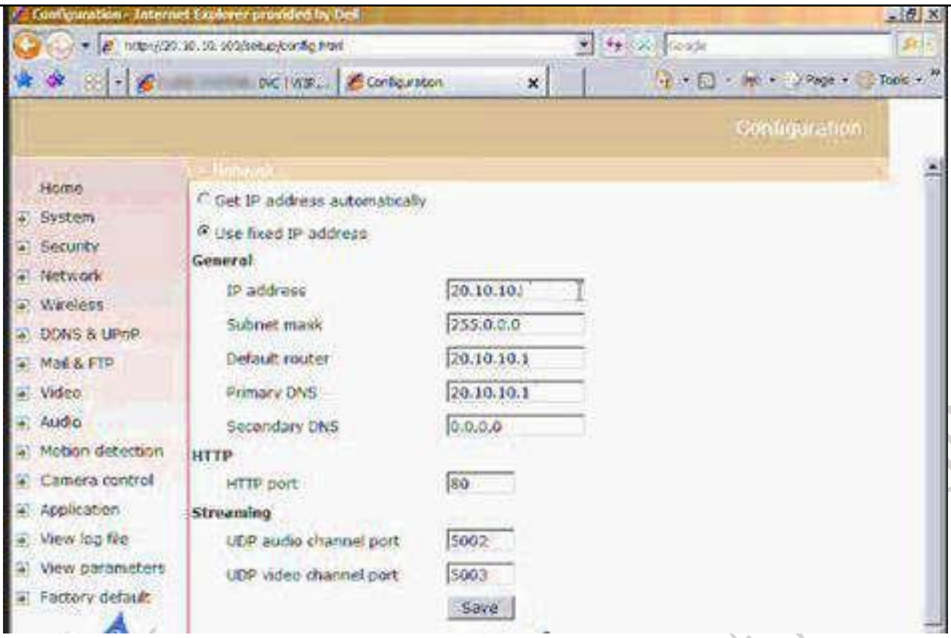
Remote Management

Web Management Port: 80

Remote Management IP Address: 0.0.0.0

Fig. 2.14: Remote management settings for denying any access

Step 7. For a surveillance camera, the IP address must be entered in the address bar. The configuration such as network details and port numbers can be assigned to the device remotely. Figure 2.15 shows accessing the camera remotely.



○ Get IP address automatically

● Use fixed IP address

General

IP address 20.10.10.

Subnet mask 255.0.0.0

Default router 20.10.10.1

Primary DNS 20.10.10.1

Secondary DNS 0.0.0.0

HTTP

HTTP port 80

Streaming

UDP audio channel port 5002

UDP video channel port 5003

Fig. 2.15: Accessing the camera remotely

2.8 Connecting to Different Short- Range Wireless Networks

The devices can be connected to different wireless networks within the range. The wireless network may be Bluetooth, NFC, wireless router, ZigBee and so on.

Practical Activity 2.2. Demonstrate to establish a Bluetooth connection with a computer using the USB Bluetooth device on Raspbian OS.

Material Required

Raspbian OS installed computer, Bluetooth device

Procedure

Step 1. Connect a Bluetooth module to the Raspberry Pi and open the interface for the Raspberry Pi in the system. Figure 2.16 shows the interface window.

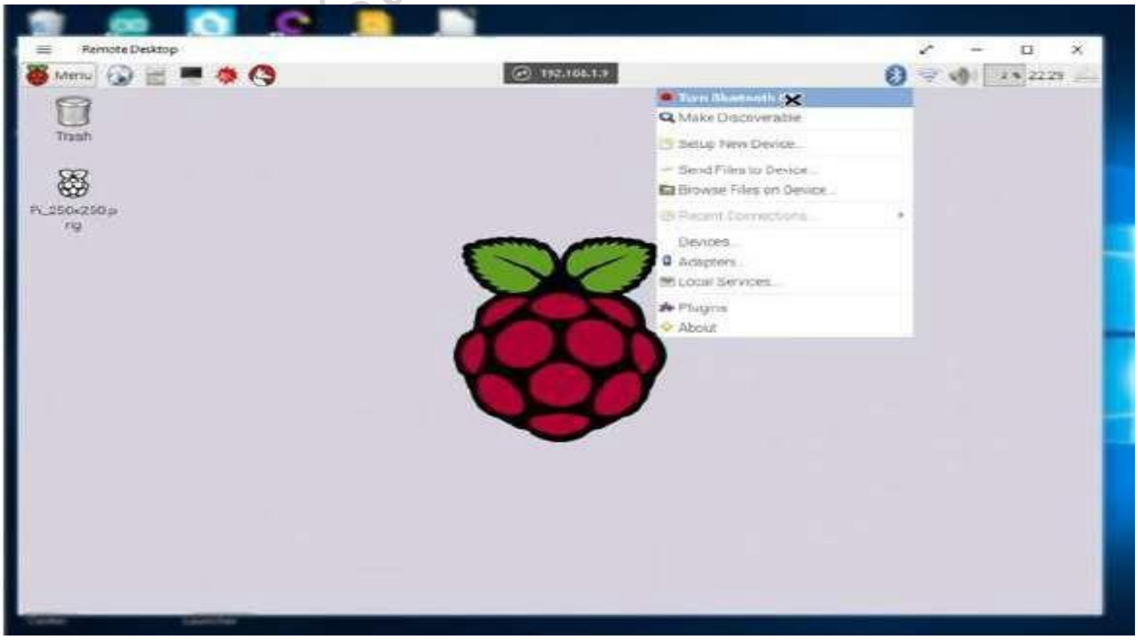


Fig. 2.16: Raspberry Pi interface window

Step 2. Open the Bluetooth in the system and turn it on. The Figure 2.17 shows turning the Bluetooth on:

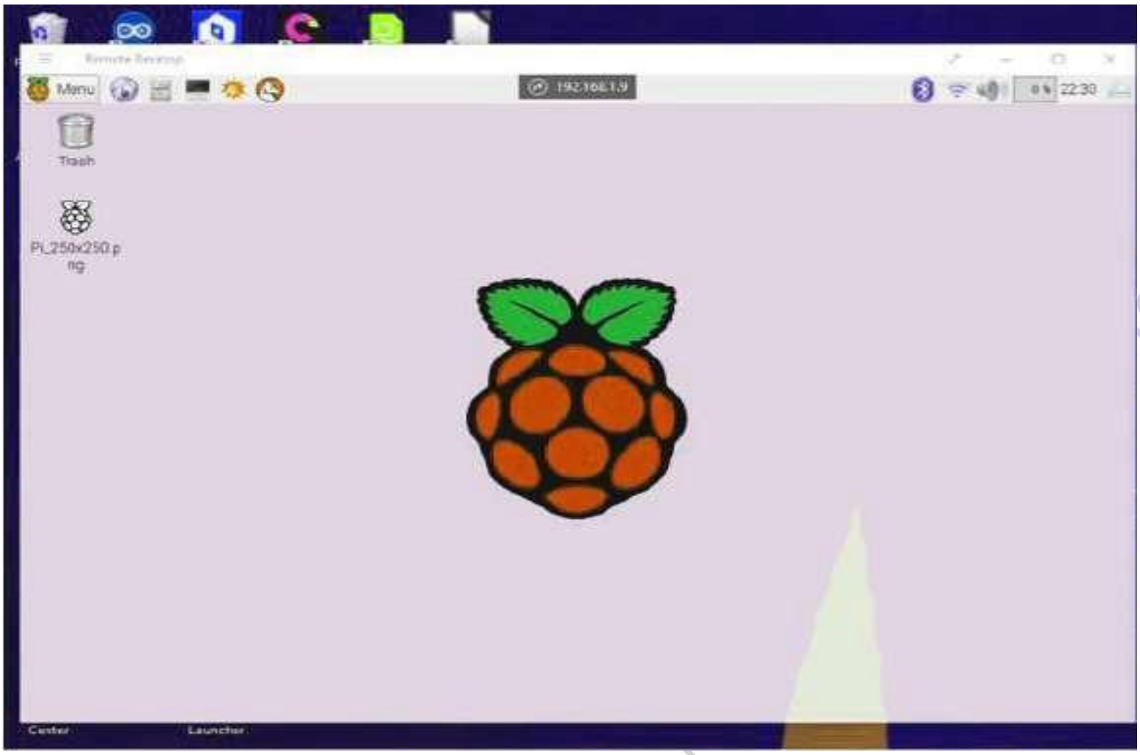
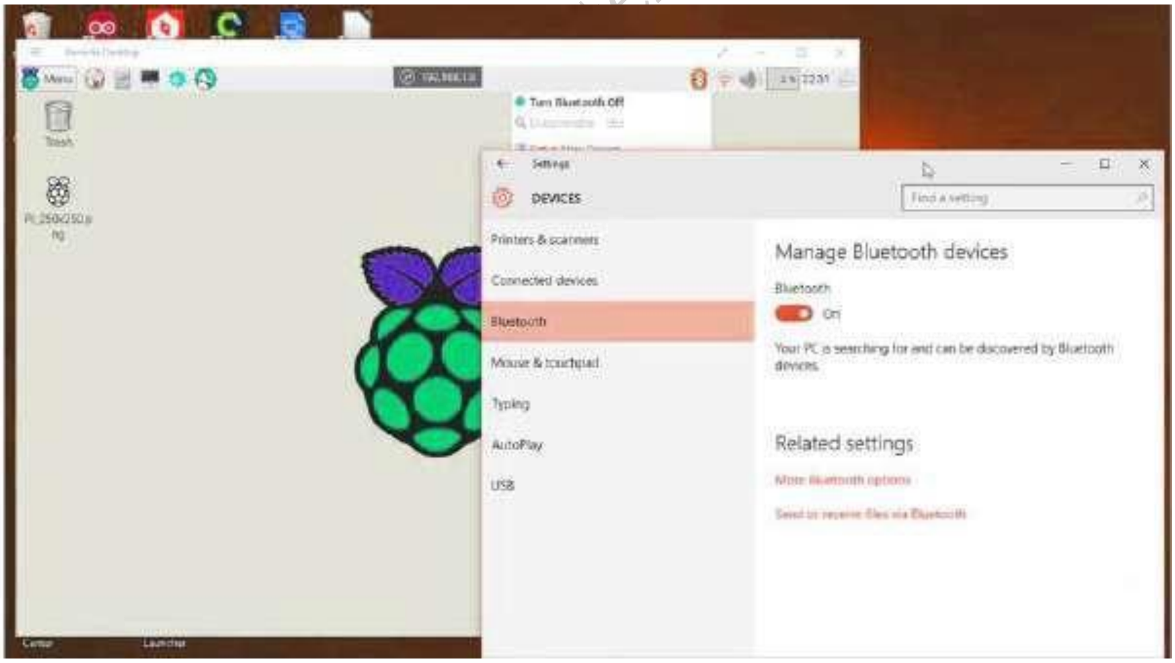


Fig. 2.17: Turning Bluetooth on

Step 3. Open the devices window and search for Bluetooth devices as shown in Figure 2.18.



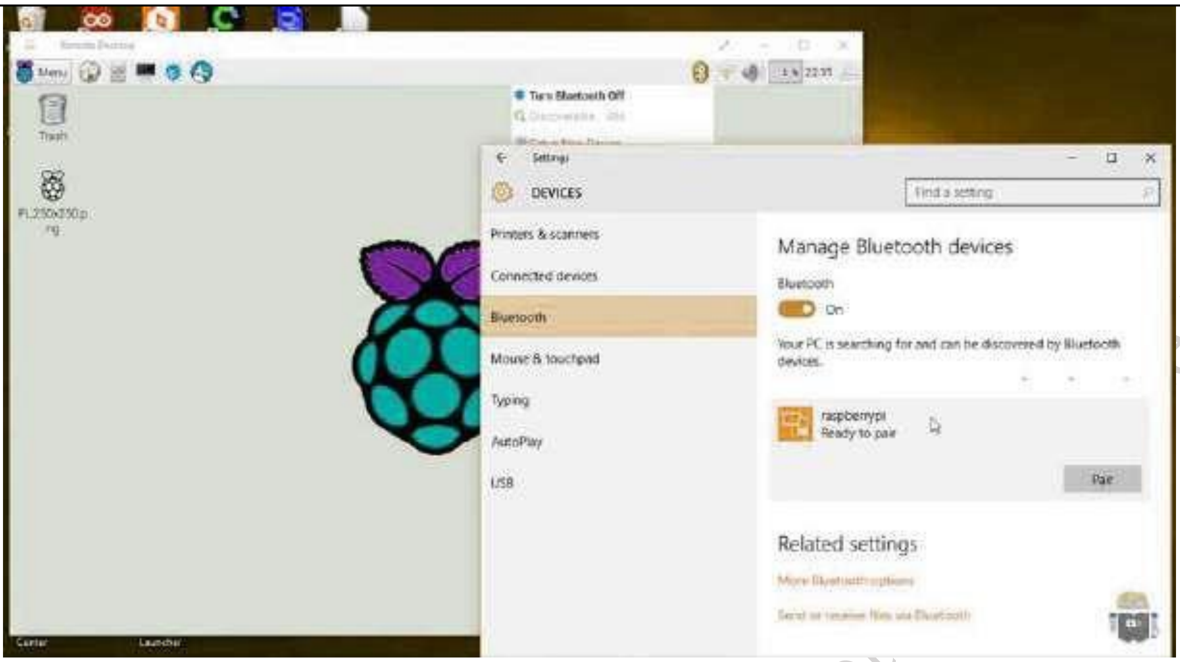
Manage Bluetooth devices

Bluetooth: On

Your PC is searching for and can be discovered by Bluetooth devices.

Fig. 2.18: Searching for Bluetooth devices

Step 4. Check for the Raspberry Pi and pair the devices as shown in Figure 2.19.



Manage Bluetooth devices

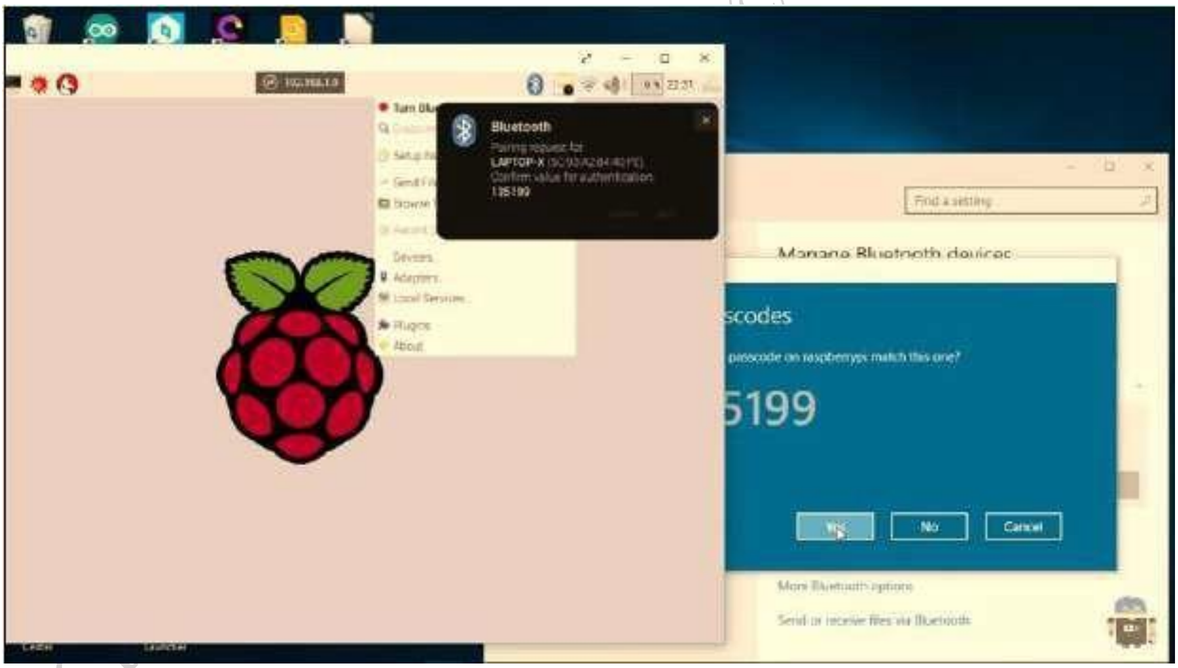
Bluetooth: On

Your PC is searching for and can be discovered by Bluetooth devices.

raspberrypi
Ready to pair

Fig. 2.19: Pairing the Bluetooth devices

Step 5. Check whether the passcodes are matching and confirm the pairing as shown in Figure 2.20.

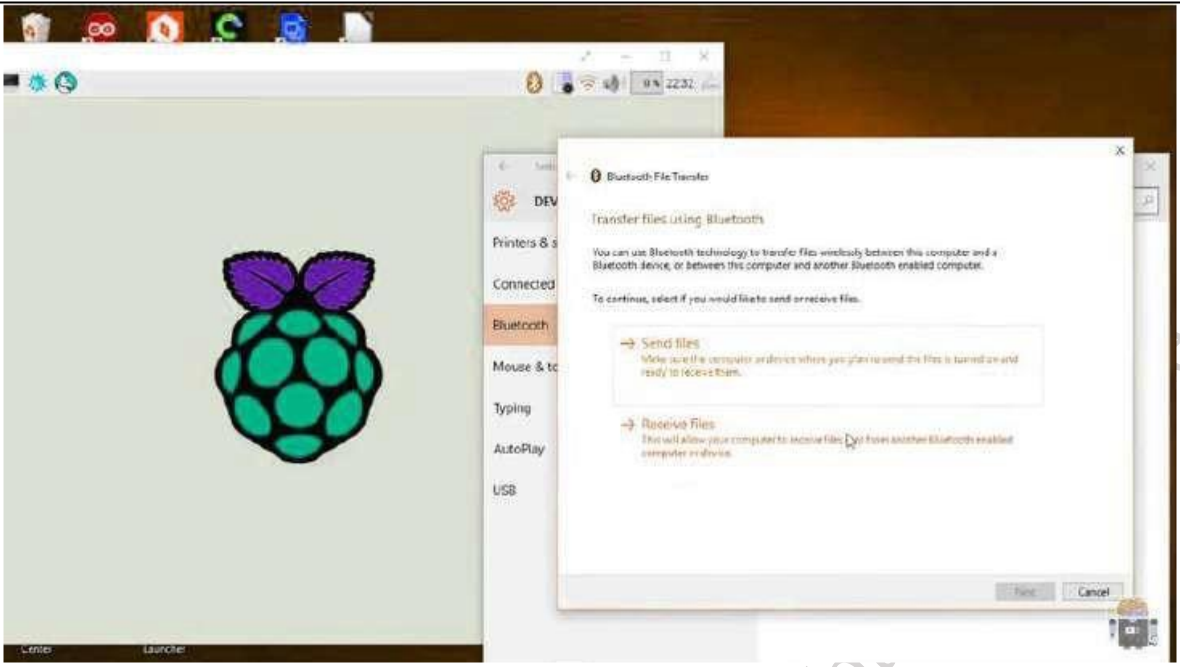


Bluetooth
Pairing request for
LAPTOP-X (5C:93:A2:84:40:FE)
Confirm value for authentication
135199

scodes
passcode on raspberrypi match this one?
5199

Fig. 2.20: Checking the passcodes

Step 6. Click on the *"Send/Receive files"* for file sharing as shown in Figure 2.21.



Bluetooth File Transfer

Transfer files using Bluetooth

You can use Bluetooth technology to transfer files wirelessly between this computer and a Bluetooth device, or between this computer and another Bluetooth enabled computer.

To continue, select if you would like to send or receive files.

→ Send files
Make sure that the computer or device where you plan to send the files is turned on and ready to receive them.

→ Receive Files
This will allow your computer to receive files from another Bluetooth enabled computer or device.

Fig. 2.21: Sharing the files

Practical Activity 2.3. Demonstrate the different data transfer modes and troubleshoot common data transfer issues.

Materials Required

Two laptops/desktops with Ethernet ports, Ethernet cables, Router

Step 1. Setting Up Devices:

a. Connect one laptop (Device A) to the router using an Ethernet cable and ensure it has internet access.

b. Connect the second laptop (Device B) to the router using another Ethernet cable.

Step 2. Exploring Data Transfer Modes:

Test Data Transfer Modes:

- Test Simplex Mode: Using Device A, send a file to Device B, but don't allow Device B to send anything back.
- Test Half Duplex Mode: Allow Device B to reply after receiving a file from Device A.
- Test Full Duplex Mode: Simultaneously send and receive files between Device A and Device B.

Step 3. Troubleshooting Data Transfer:

- Introduce common issues like loose Ethernet connections, outdated drivers, or interference for both wired and Bluetooth connections.
- Have participants troubleshoot and resolve these issues.

Step 4. Testing Remote Access:

- Access the router settings of Device A from Device B by entering the router's IP address in a web browser.
- Enable or disable remote management settings and observe the impact on access.

Summary

- This chapter covers data transfer types (Interrupt, Bulk, Isochronous, Control), modes (Simplex, Half Duplex, Full Duplex), and controlling transfer rates.
- It explains device indicators and troubleshooting.
- Additionally, it touches on remote network access and connecting via Bluetooth and ZigBee for IoT communication.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What type of data transfer is typically used by input devices like keyboards and mouse? (a) Bulk Transfer (b) Isochronous Transfer (c) Control Transfer (d) Interrupt Transfer
2. Which mode of data transfer allows the sender to send data and receive it one at a time? (a) Simplex (b) Half Duplex (c) Full Duplex (d) None of these
3. Which type of data transfer is used for audio and video devices requiring real-time data transfer? (a) Bulk Transfer (b) Isochronous Transfer (c) Control Transfer (d) Interrupt Transfer
4. What is the purpose of Control Transfer? (a) To transfer large amounts of data (b) To allocate USB addresses and configure devices (c) For lossless transfer of data (d) To periodically transfer a fixed amount of data
5. Which indicator on a device indicates that the battery is not good? (a) Solid (b) Blinking (c) Off (d) red
6. In which mode of transfer is communication simultaneous in both directions? (a) Simplex (b) Half Duplex (c) Full Duplex (d) Both b and c
7. What can cause data transfer failure due to bad network connection? (a) Faulty network hardware (b) Outdated firmware (c) Third-party applications (d) All of the above
8. How can an IoT framework provide remote user access to the central site? (a) Through gateway and neighbourhood Wi-Fi router (b) Through Ethernet connection (c) Through direct cable connection (d) …………………
9. What is the purpose of connecting ZigBee modules to Arduino? (a) To transfer large amounts of data (b) To establish short-range wireless communication (c) To control data transfer modes (d) …………………
10. Which network type is suitable for WPAN (Wireless Personal Area Network)? (a) ZigBee (d) Wi-Fi (c) NFC (d) All of the above

B. Fill in the blanks

1. Data transmission from one device to another is referred to as ___________.
2. Digital cameras, printers, scanners, and other image input, printing, and storage devices require ___________ for the lossless transfer of large amounts of data.
3. Control transfer is driven by rules about the content of the data to be transferred and is used to allocate ___________.
4. In simplex mode, the sender is able to ___________ data but not receive it.
5. In half-duplex mode, the sender can send and receive data ___________ at a time.
6. In full-duplex mode, the sender can send and receive data ___________.

7. The mechanism and techniques of data transfer depend on the __________ of the network.
8. Data transfer failure can occur due to bad network connection or improper connection and configuration. One common cause is the absence of a __________.
9. The devices can be connected to different wireless networks within the range, such as __________.
10. Control transfer is driven by rules about the ____________to be transferred.

C. State true or False for the following

1. Simplex mode allows data to be sent in both directions simultaneously.
2. Full Duplex mode allows simultaneous two-way communication.
3. Baud rate is a crucial factor in controlling data transfer for Arduino and Raspberry Pi.
4. Data transfer over 1.4 and 5 GHz Wi-Fi bands is generally faster than wired Ethernet.
5. Backup functions do not impact CPU, memory, and disk access resources during data transfer.
6. An IoT framework must have external connectivity to provide remote user access.
7. To access a router remotely, the user must enter the default address 191.168.0.1 in the web browser.
8. Bluetooth can be used to connect a Raspberry Pi to another system.
9. ZigBee modules need to be connected to an Arduino to establish a ZigBee network.
10. Port parameters play a crucial role in connecting ZigBee modules.

D. Short Answer Type Questions

1. What are the four types of data transfer?
2. Which types of devices typically use Interrupt Transfer for data transmission?
3. What kind of devices benefit from Bulk Transfer for data transfer?
4. Why is Isochronous Transfer important for audio and video devices?
5. Provide an example of a device that operates in Full Duplex mode.
6. How can the data transfer rate for a router be controlled?
7. What is the significance of the baud rate in controlling data transfer?
8. What are the steps involved in accessing a router or device remotely?
9. How can a Raspberry Pi be connected to another system via Bluetooth?
10. What is the purpose of installing ZigBee module software in the system?

Session 3. Authentication and Authorization Mechanism in IoT

3.1 Authenticating the Edge Devices

The Figure 3.1 shows the procedure of authenticating edge devices in IoT.

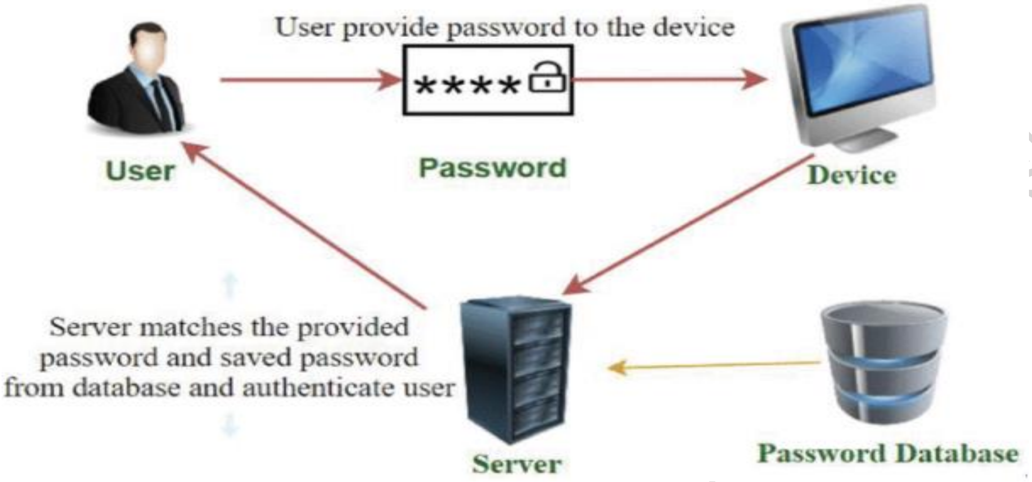

User provide password to the device
****
User
Password
Device
Server matches the provided password and saved password from database and authenticate user
Server
Password Database

Fig. 3.1: Procedure for authenticating edge devices in IoT

Authenticating each device poses a significant challenge. Authentication is the process of confirming the identity of users and devices before granting access to a network or information system. Radio Frequency Identification (RFID) is a valuable tool for entity identification, using electromagnetic induction and wave propagation to distinguish objects. Various security mechanisms have been proposed, including cryptographic, password-based, biometric, token-based, and multi-factor authentication.

3.1.1 Password-based authentication

It is commonly used for device or user verification. Users create a unique ID and password, stored in a database, and only with a matching ID and password can access be granted as shown in Figure 3.1.

3.1.2 Token-based authentication

It involves generating a token to identify a user or device. In soft token-based authentication, a one-time password (OTP) is sent to the registered device or user and stored in the database for matching. In hard token-based authentication, a physical card or device with verification information is created. It is illustrated in Figure 3.2.

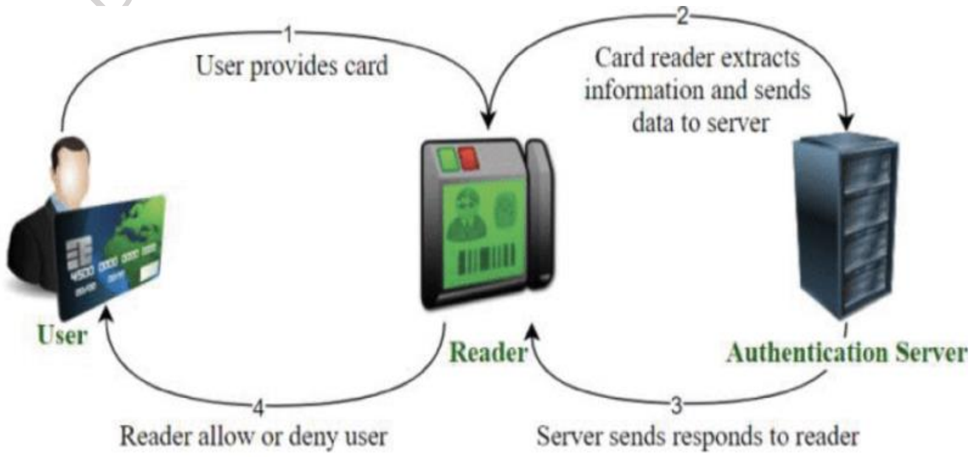

1
User provides card
2
Card reader extracts information and sends data to server
User
Reader
Authentication Server
4
Reader allow or deny user
3
Server sends responds to reader

Fig. 3.2: Token-based authentication

3.1.3 Biometric authentication

It relies on human biological features. A scanner collects unique biological data from a user, comparing it with previously collected data in the database. This method can use fingerprint, face, iris, retina, hand, voice authentication, or a combination of these to maintain data uniqueness. It is shown in Figure 3.3.

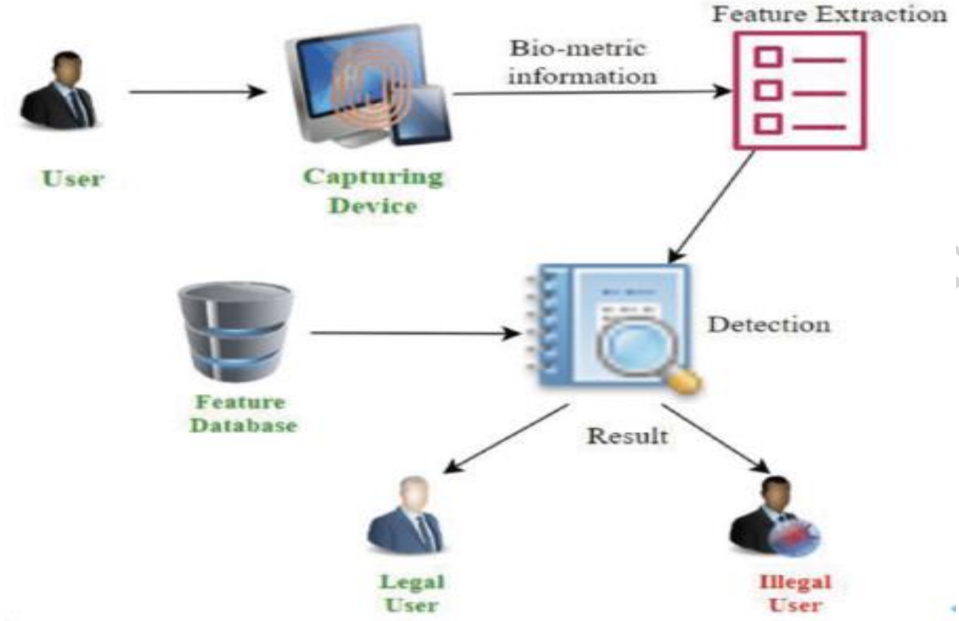


Fig. 3.3: Biometric authentication

3.1.4 Multi-factor authentication

It combines two or more ways to identify the user or device identity.

3.4 Authorization of the Edge Devices

The control software is used as the entire controller framework. Dual control can be configured via a mobile app for mobile devices notifications can be received in real time. Figure 3.4 shows a mobile app connected to a home alarm system.

Fig. 3.4: A mobile app connected to a home alarm system

Each authorized mobile device must use its own unique IP address for acquisition access to the main controller to operate the security system. Also, the main server has a unique IP address to establish communication among access control system components.

3.5 Installation of Access Control System

Managing an access control system can be a complex task. To install the system the technician must know the following tasks:

- Addition of a new base station to the control system

- Keep the system secure
- Identification of users and devices
- Solve installation problems
- Ensures servers are up to date
- Make sure proper firewalls and the latest security patches are installed

3.6 Access Control System Architecture for IoT

Access control for IoT can be implemented in two ways as follows:

3.6.1 Distributed Architecture

In a distributed architecture, the control server offers access tokens to the users, so that they can have direct access to the IoT devices. These tokens serve as digital credentials, allowing users direct access to IoT devices. The tokens contain user identity and permissions, ensuring secure interaction while managing access throughout their lifecycle. Figure 3.5 shows the distributed architecture.

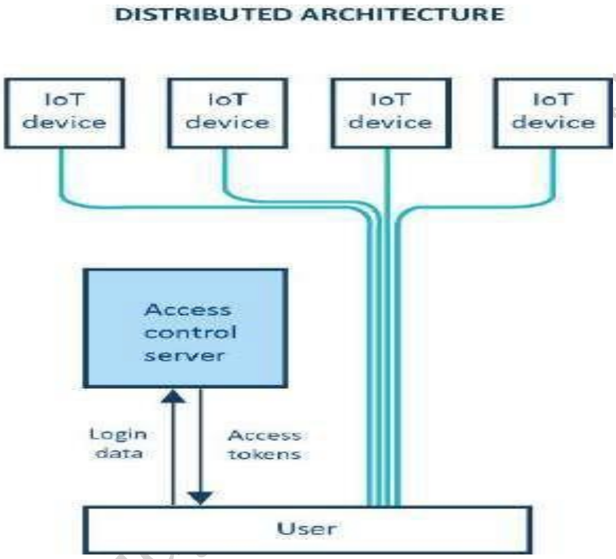


Fig. 3.5: Distributed architecture

3.6.2 Centralized Architecture

In a centralized architecture, users access cloud-based servers to interact with IoT devices. These servers authorize user requests and relay data between users and devices. They also handle data processing, scalability, security, and management, offering a centralized solution for IoT communication. Figure 3.6 shows the centralized architecture.

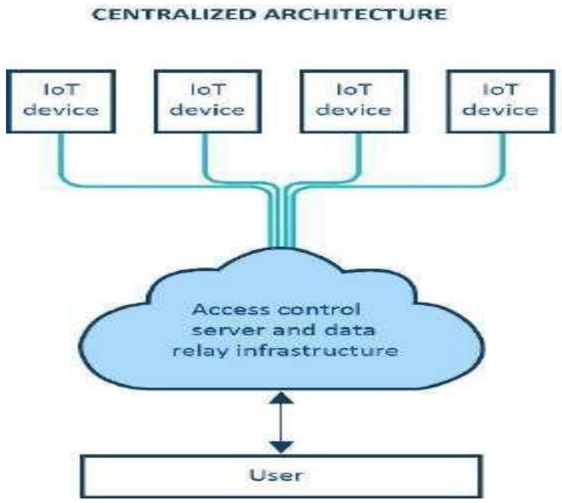


Fig. 3.6: Centralized architecture

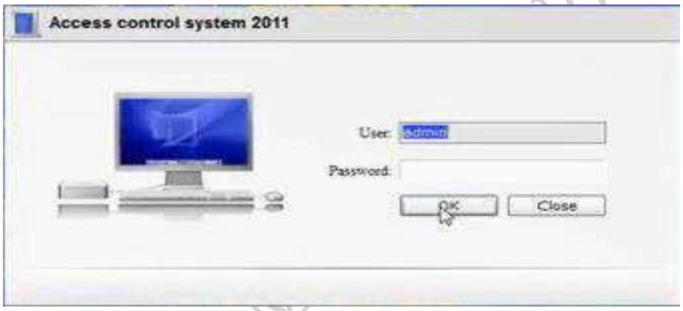
3.7 Control Access Using Security

The access control system provides security to the organisation by offering access only to the authorised people. Figure 3.7(a) and (b) shows two examples of granting and denying access to a person.

Fig. 3.7 (a): Access granted

To set up the software interface, the following steps should be followed:

Step 1. Install the software and open it. Enter the login details as shown in Figure 3.8.



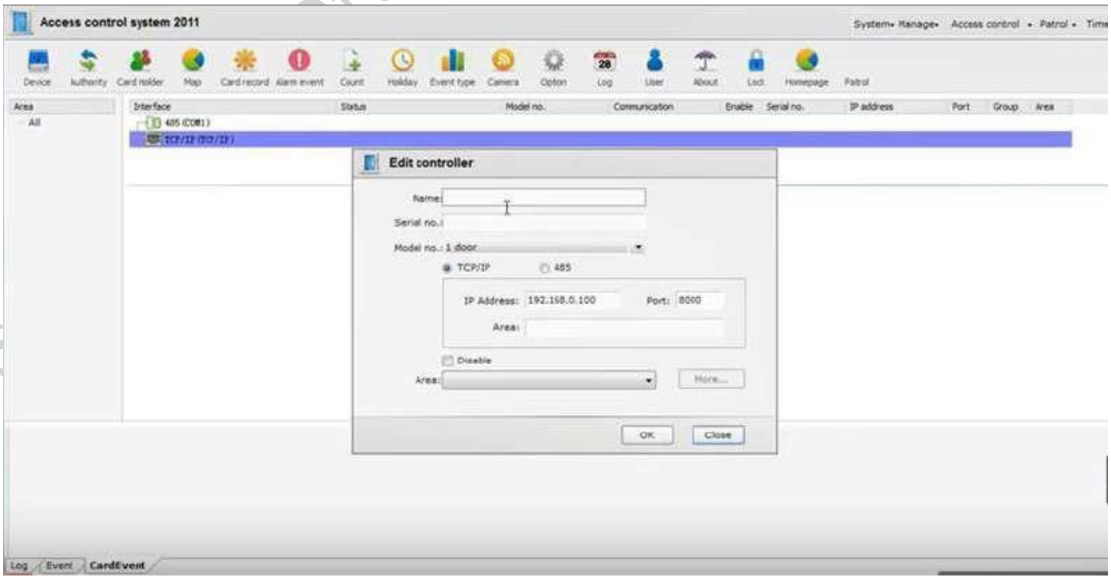
Access control system 2011

User: admin

Password:

Fig. 3.8: Software login window

Step 1. Edit the controller settings by entering the network details and product details. Figure 3.9 shows the edit controller window.



Access control system 2011

Edit controller

Name:

Serial no.:

Model no.: 1 door

● TCP/IP ○ 485

IP Address: 192.168.0.100 Port: 8000

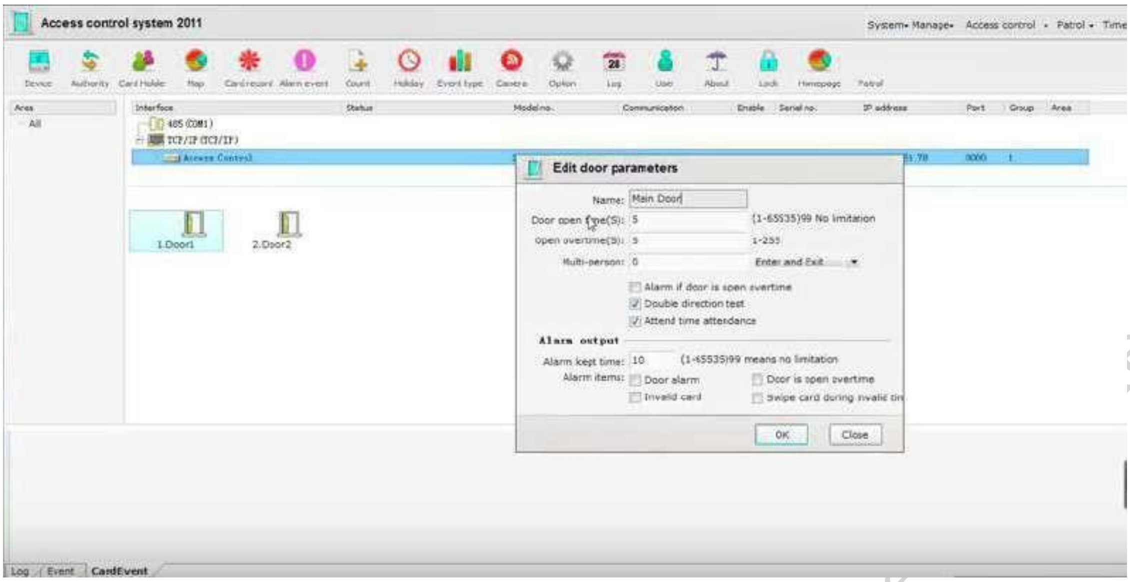
Area:

□ Disable

Area:

Fig. 3.9: Edit controller window

Step 3. Edit the device or machine settings. Figure 3.10 shows the device settings window.


Access control system 2011

Edit door parameters

Name: Main Door

Door open time(S): 5 (1-65535)99 No limitation

Open overtime(S): 5 1-255

Multi-person: 0 Enter and Exit

□ Alarm if door is open overtime

☑ Double direction test

☑ Attend time attendance

Alarm output

Alarm kept time: 10 (1-65535)99 means no limitation

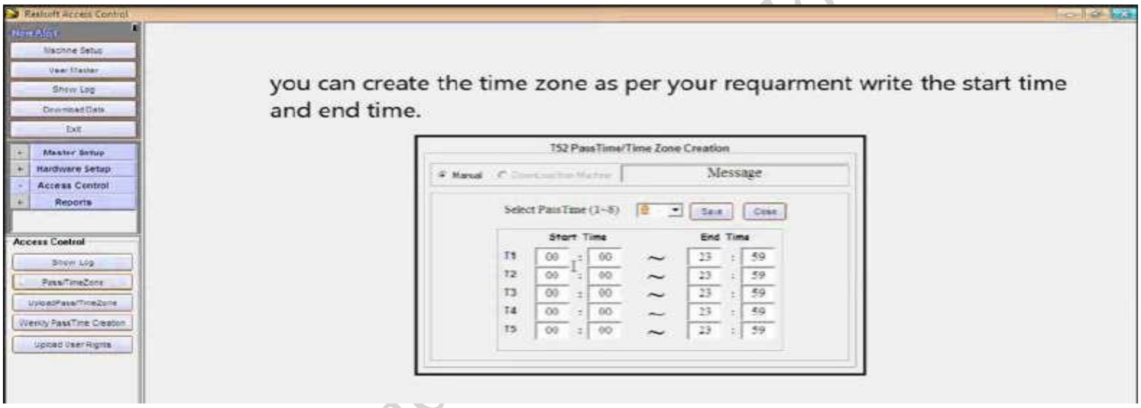
Alarm items: □ Door alarm □ Door is open overtime

□ Invalid card □ Swipe card during invalid tim

OK Close

Fig. 3.10: Device settings window

Step 4. Create the time zone settings as per requirement. Figure 3.11 shows the time settings window.


you can create the time zone as per your requarment write the start time and end time.

T52 PassTime/Time Zone Creation

● Manual ○ Download from Machine

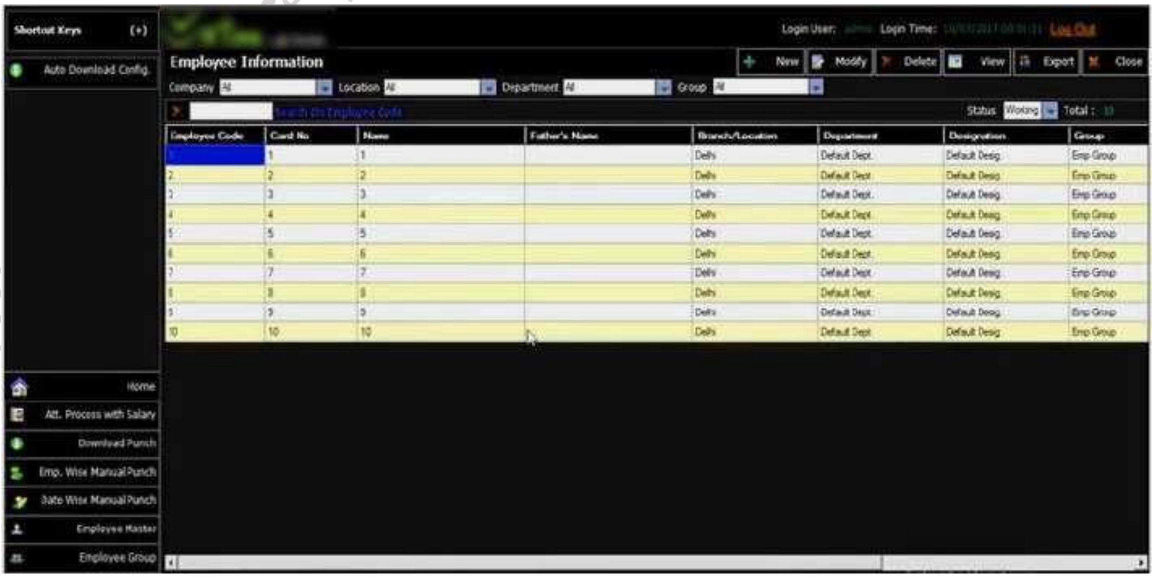
Message

Select PassTime (1~8) Save Close

	Start Time			End Time	
T1	00	00	~	23	59
T2	00	00	~	23	59
T3	00	00	~	23	59
T4	00	00	~	23	59
T5	00	00	~	23	59

Fig. 3.11: Time settings window

Step 3. Fill the employee records. Figure 3.12 shows the employee records window.


Employee Information

Company All Location All Department All Group All

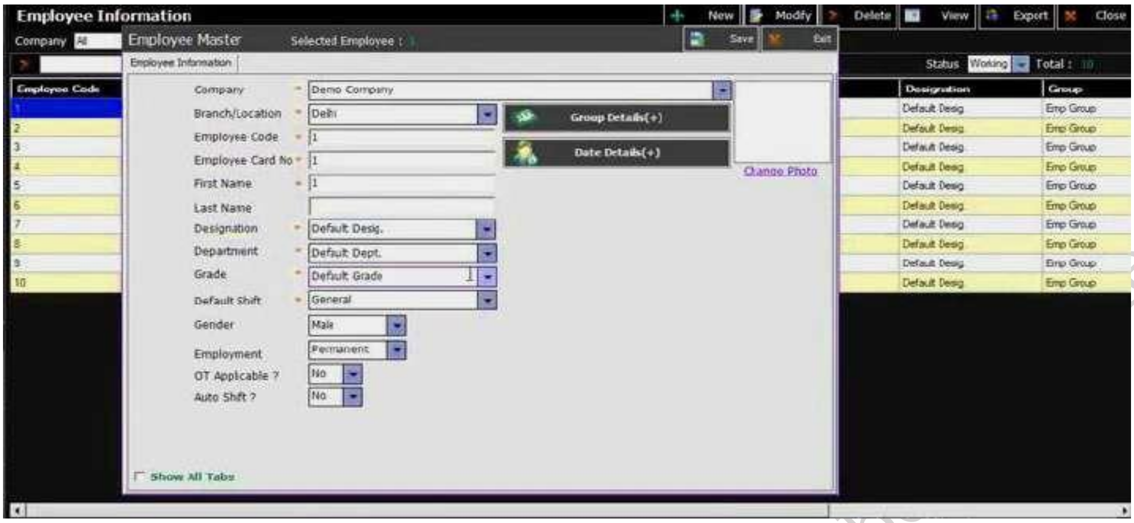
Search On Employee Code

Status Working Total : 10

Employee Code	Card No	Name	Father's Name	Branch/Location	Department	Designation	Group
1	1	1		Delhi	Default Dept.	Default Desig	Emp Group
2	2	2		Delhi	Default Dept	Default Desig	Emp Group
3	3	3		Delhi	Default Dept.	Default Desig	Emp Group
4	4	4		Delhi	Default Dept	Default Desig	Emp Group
5	5	5		Delhi	Default Dept.	Default Desig	Emp Group
6	6	6		Delhi	Default Dept.	Default Desig	Emp Group
7	7	7		Delhi	Default Dept	Default Desig	Emp Group
8	8	8		Delhi	Default Dept	Default Desig	Emp Group
9	9	9		Delhi	Default Dept	Default Desig	Emp Group
10	10	10		Delhi	Default Dept	Default Desig	Emp Group

Fig. 3.12: Employee details window

Step 6. Click on a row to create or update the employee details. Figure 3.13 shows editing the employee records window.

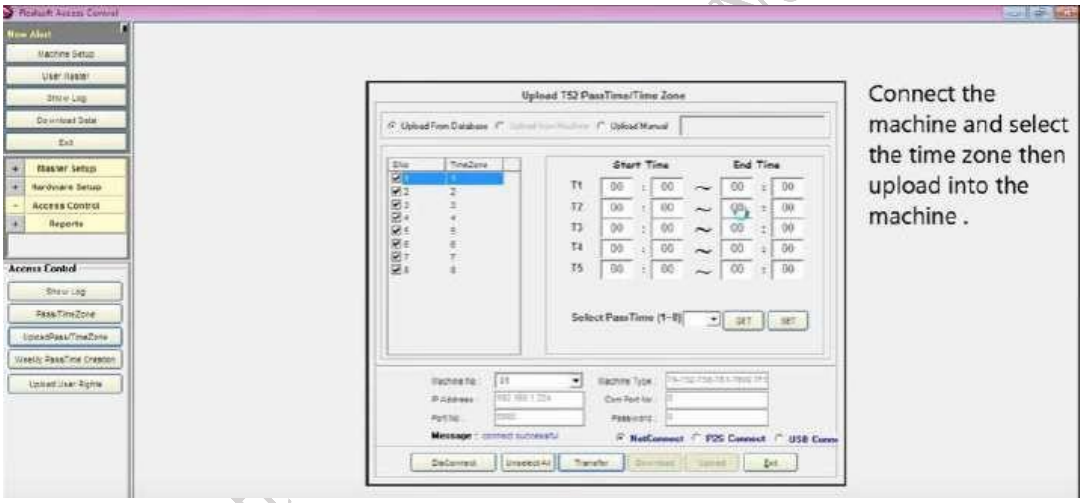


Employee Information

- Company: Demo Company
- Branch/Location: Delhi
- Employee Code: 1
- Employee Card No: 1
- First Name: 1
- Last Name:
- Designation: Default Desig.
- Department: Default Dept.
- Grade: Default Grade
- Default Shift: General
- Gender: Male
- Employment: Permanent
- OT Applicable ?: No
- Auto Shift ?: No

Fig. 3.13: Editing employee records window

Step 7. Connect the device and select the time zone and upload it to the machine as shown in Figure 3.14.



● Upload From Database ○ Upload from Machine ○ Upload Manual

Sno	TimeZone
☑ 1	1
☑ 2	2
☑ 3	3
☑ 4	4
☑ 5	5
☑ 6	6
☑ 7	7
☑ 8	8

	Start Time		End Time	
T1	00	00	00	00
T2	00	00	00	00
T3	00	00	00	00
T4	00	00	00	00
T5	00	00	00	00

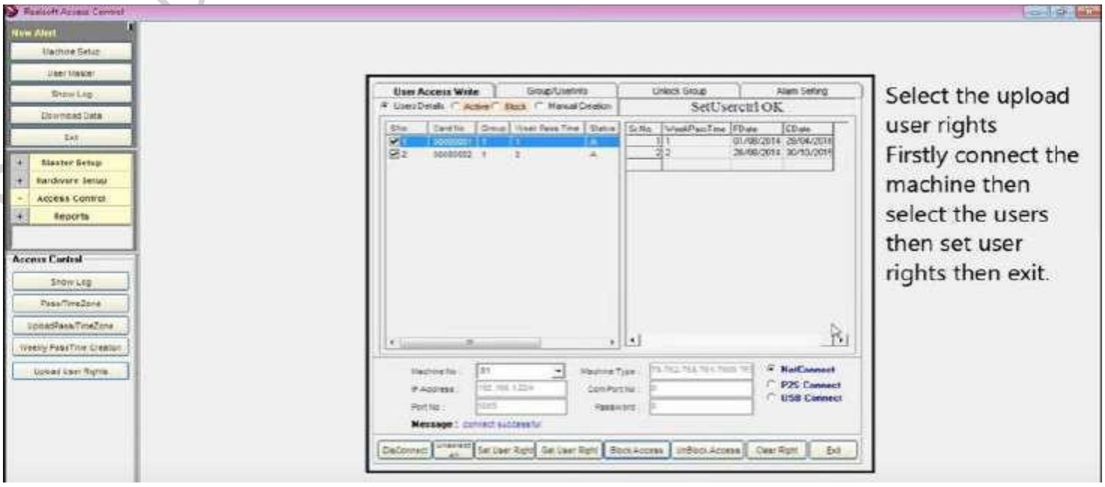
Message : connect successful

● NetConnect ○ P2S Connect ○ USB Conn

Connect the machine and select the time zone then upload into the machine .

Fig. 3.14: Uploading time zone to the device

Step 8. Upload the user rights to the device as shown in Figure 3.13.



● Users Details ○ Active ○ Block ○ Manual Creation

SetUserctrl OK

Sno	Card No	Group	Week Pass Time	Status
☑ 1	00000001	1	1	A
☑ 2	00000002	1	2	A

Sr.No.	WeekPassTime	FDate	CDate
1	1	01/08/2014	29/04/2018
2	2	26/08/2014	30/10/2019

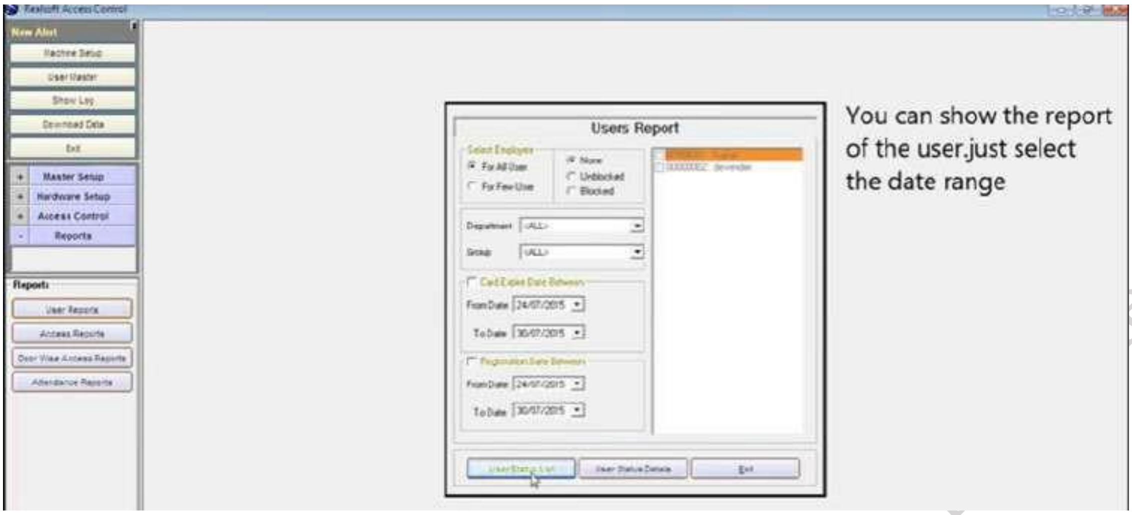
Message : connect successful

● NetConnect
○ P2S Connect
○ USB Connect

Select the upload user rights
Firstly connect the machine then select the users then set user rights then exit.

Fig. 3.15: Uploading user rights to the device

Step 9. Generate report as shown in Figure 3.16.



Users Report

Select Employee: ● For All User ○ For Few User; ● None ○ Unblocked ○ Blocked

Department: <ALL>

Group: <ALL>

□ Card Expiry Date Between: From Date 24/07/2015, To Date 30/07/2015

□ Registration Date Between: From Date 24/07/2015, To Date 30/07/2015

You can show the report of the user.just select the date range

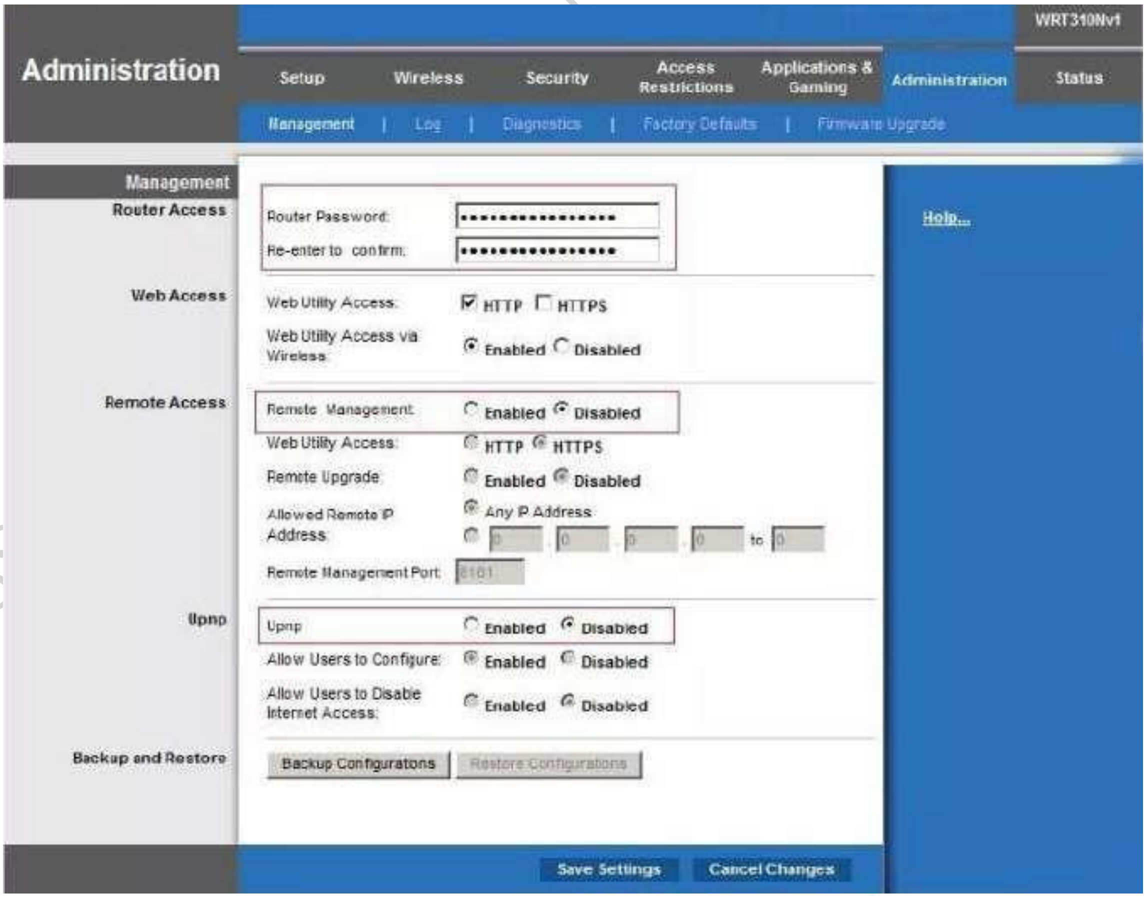
Fig. 3.16: Generating report

3.8 Securing Wireless Connection

Securing the network connection is very important. There are some ways to secure the wireless connection. The following default settings of the router must be changed:

1. Router password must be changed
2. IP address and the subnet mask should be updated
3. Remote management should be disabled

Figure 3.17 shows changing the default settings.



Management

Router Access

Router Password: ••••••••••••••••

Re-enter to confirm: ••••••••••••••••

Web Access

Web Utility Access: ☑ HTTP □ HTTPS

Web Utility Access via Wireless: ● Enabled ○ Disabled

Remote Access

Remote Management: ○ Enabled ● Disabled

Web Utility Access: ○ HTTP ● HTTPS

Remote Upgrade: ○ Enabled ● Disabled

Allowed Remote IP Address: ● Any IP Address ○ 0 . 0 . 0 . 0 to 0

Remote Management Port: 8181

Upnp

Upnp: ○ Enabled ● Disabled

Allow Users to Configure: ● Enabled ○ Disabled

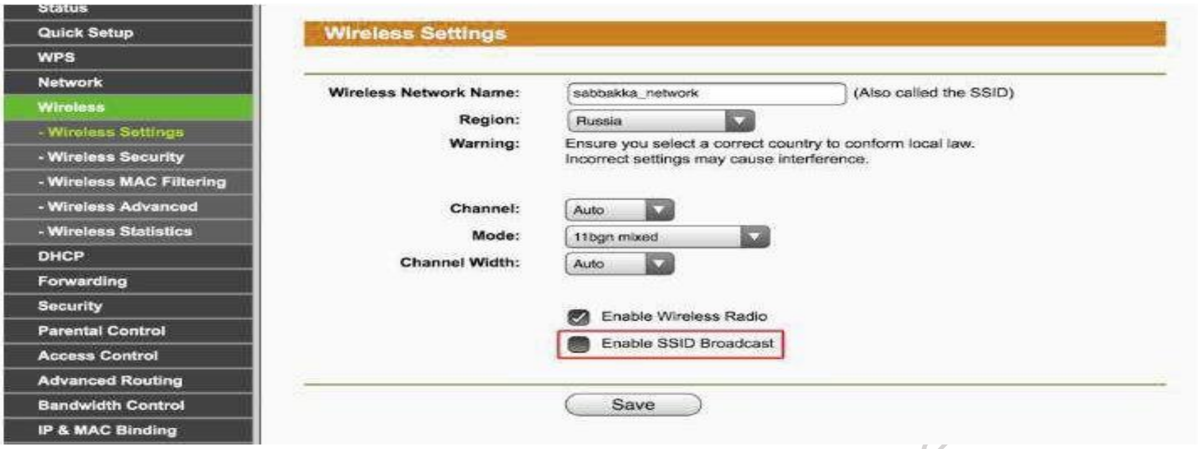
Allow Users to Disable Internet Access: ○ Enabled ● Disabled

Backup and Restore

Backup Configurations | Restore Configurations

Fig. 3.17: Changing the router default settings

The default Service Set Identifier (SSID), which denotes the name of the network, must be changed and the broadcasting name option should be disabled. Figure 3.18 shows changing the wireless settings.



Wireless Settings

Wireless Network Name: sabbakka_network (Also called the SSID)

Region: Russia

Warning: Ensure you select a correct country to conform local law. Incorrect settings may cause interference.

Channel: Auto

Mode: 11bgn mixed

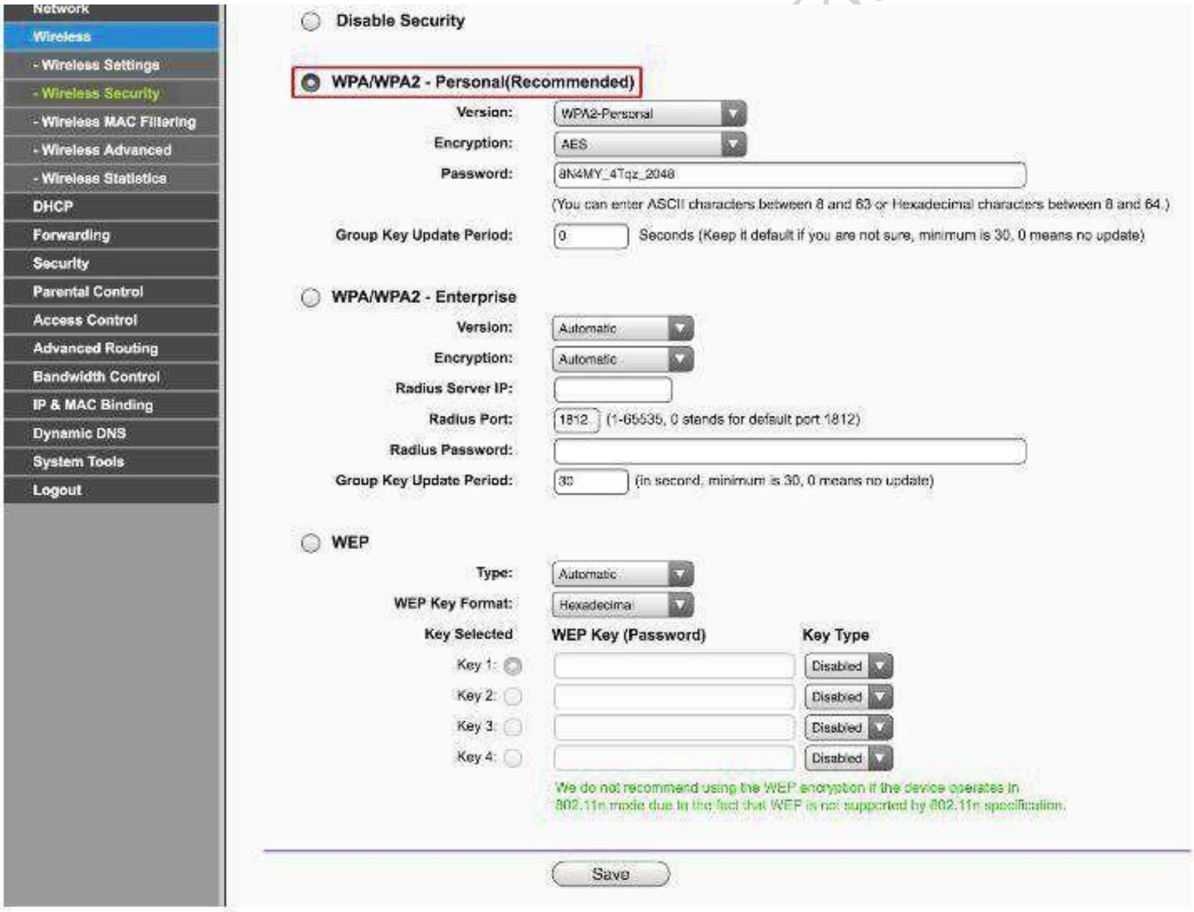
Channel Width: Auto

☑ Enable Wireless Radio

☐ Enable SSID Broadcast

Fig. 3.18: Changing the wireless settings

Reliable encryption standard must be selected. Figure 3.19 shows the WAP2 selected as encryption method.



○ Disable Security

● WPA/WPA2 - Personal(Recommended)

Version: WPA2-Personal

Encryption: AES

Password: 8N4MY_4Tqz_2048

(You can enter ASCII characters between 8 and 63 or Hexadecimal characters between 8 and 64.)

Group Key Update Period: 0 Seconds (Keep it default if you are not sure, minimum is 30, 0 means no update)

○ WPA/WPA2 - Enterprise

Version: Automatic

Encryption: Automatic

Radius Server IP:

Radius Port: 1812 (1-65535, 0 stands for default port 1812)

Radius Password:

Group Key Update Period: 30 (in second, minimum is 30, 0 means no update)

○ WEP

Type: Automatic

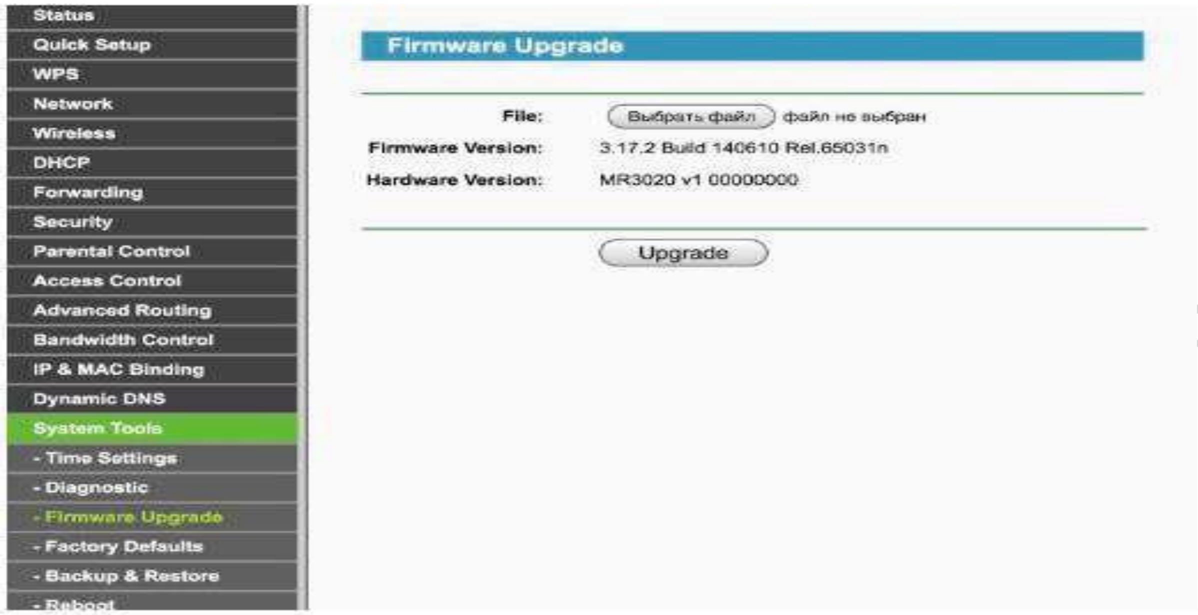
WEP Key Format: Hexadecimal

Key Selected	WEP Key (Password)	Key Type
Key 1: ●		Disabled
Key 2: ○		Disabled
Key 3: ○		Disabled
Key 4: ○		Disabled

We do not recommend using the WEP encryption if the device operates in 802.11n mode due to the fact that WEP is not supported by 802.11n specification.

Fig. 3.19: WAP2 selected as encryption method

Router firewall must be enabled and the firmware must be updated. Figure 3.20 shows the upgrading of firmware.



File: файл не выбран

Firmware Version: 3.17.2 Build 140610 Rel.65031n

Hardware Version: MR3020 v1 00000000

Fig. 3.20: Upgrading of firmware

3.8 Verifying Network Connectivity

Verifying network connectivity requires identifying and diagnosing problems with active directories. This leads to the diagnosis of different network problems as well as recommendations. To identify the issue with network functioning, the following areas are investigated:

3.8.1 Event Viewer

It is the most helpful tool for determining directory services issues, networking issues, and problem solutions. Additionally, it groups the errors for simple analysis. Examine the event log to determine whether there are any instances of potential future issues with the directory service. Examine the system log folder and note the kind of error warning lists that are present. To see the description and the data returned for each error warning, visit the event properties page. In the Data box, click the words to convert the hexadecimal code to decimal. Use the net help msg command to obtain the error's description if the error code has a number in the event column.

Example

If the starting four digits of the error code is “8007”, this means a network error is there. To solve this, a helpmsg command is used to decode the error code. Type the following code in the command prompt:

nethelpmsg <message number in decimal>

If the “access denied” or “bad password” error code appears, then the problem is in the security. The “No logon servers” error code indicates that the user is not able to find the domain controller.

3.8.2 Hardware components

The cables, devices, and other components in the hardware network hub are tested for functionality. For instance, the network cable is disconnected if the connection icon in the control panel's network dial-up connection property has a red "X" on it. To verify hardware functionality, consult the server operation manual. Use the control panel to verify that the network adapters and drivers are operating properly. You can also use the hardware wizard located on the hardware tab of the control panel's system properties. Choose the device from the device box to see if it is operating correctly. When you click **finish,** the Add/Remove hardware wizard closes and the trouble shooter opens. Double-clicking the device icon allows you to view each property of the device. Each device's tab status is typically shown. If there are any issues with the device's operation, click the trouble shooter.

3.8.3 Local Connectivity

To confirm network connectivity, first check the physical connectivity of the devices with the network. It is is properly conneted, test the network connectivity using the network commands. Following network commands are used to test the connectivity of the devices with in the network.

Ipconfig command

Ipconfig is used to view and configure the network settings on a Windows computer. It is also used to troubleshoot network issues, like connectivity problems or incorrect IP addresses. Issuing this command displays the IP addresses assigned to their network adapters as well as the default gateway and DNS servers. The sample output of the ipconfig command is shown below.

Ethernet adapter Ethernet

IP address: 191.168.1.100

Subnet mask: 255.255.255.0

Default gateway: 191.168.1.1

Ping command

The ping command is used to verify that a computer can communicate with another computer or network device. The command works by sending a signal – an Internet Control Message Protocol (ICMP) echo request to a host server to check for two things: if the target host is available, and, if so, how long the response takes. Response times are important because they indicate the reliability of the Internet connection between your server and websites, as well as upload speeds and download speeds for server. Essentially, the commands see how your network performs.

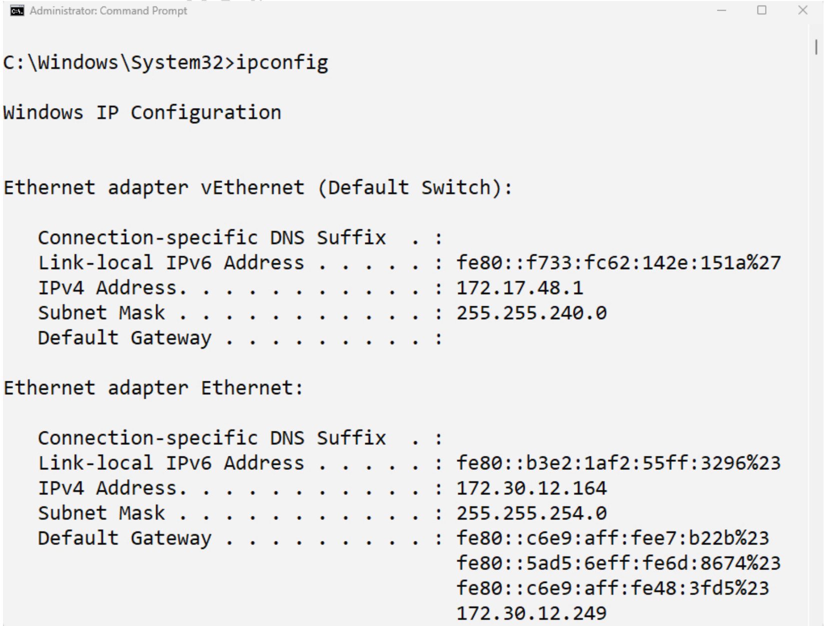
A) The steps to configure IP details are as follows:

Step 1. Open the command prompt, type ipconfig and press ENTER.

Step 1. In the output look for the following:

- IP address
- Default gateway
- DHCP server

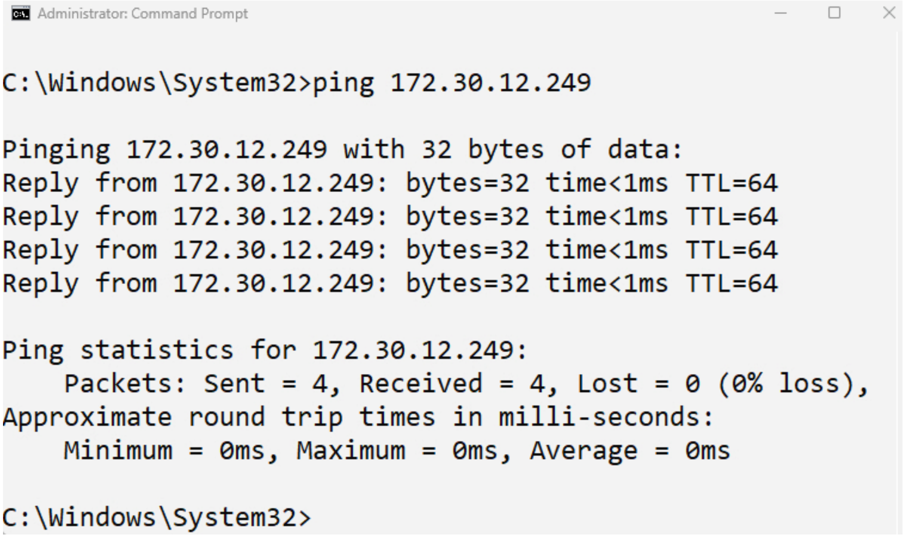
It is illustrated in the screenshot given in Figure 3.20.



```
C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f733:fc62:142e:151a%27
   IPv4 Address. . . . . . . . . . . : 172.17.48.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b3e2:1af2:55ff:3296%23
   IPv4 Address. . . . . . . . . . . : 172.30.12.164
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::c6e9:aff:fee7:b22b%23
                                       fe80::5ad5:6eff:fe6d:8674%23
                                       fe80::c6e9:aff:fe48:3fd5%23
                                       172.30.12.249
```

Fig. 3.20: Finding IP details of computer

Step 3. Use ping tool to get the network connectivity between default gateway and DHCP server as shown in Figure 3.21.

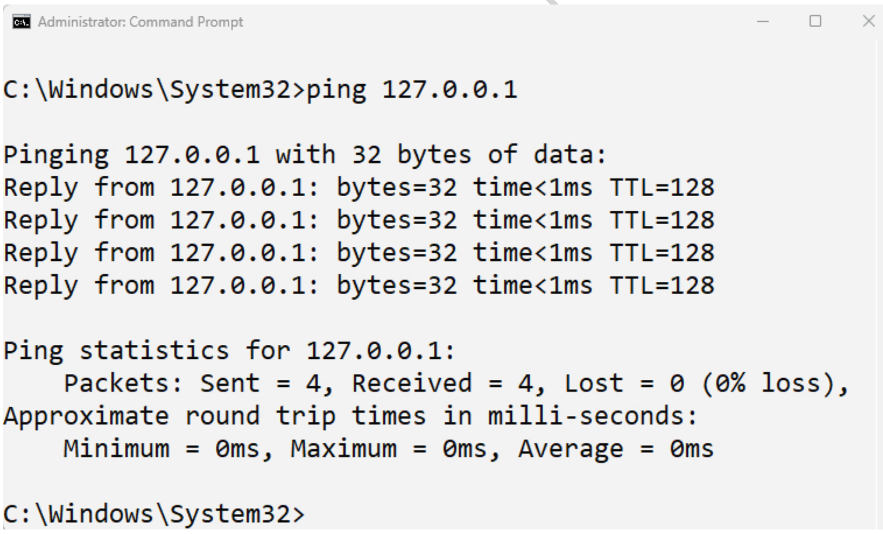


```
C:\Windows\System32>ping 172.30.12.249

Pinging 172.30.12.249 with 32 bytes of data:
Reply from 172.30.12.249: bytes=32 time<1ms TTL=64
Reply from 172.30.12.249: bytes=32 time<1ms TTL=64
Reply from 172.30.12.249: bytes=32 time<1ms TTL=64
Reply from 172.30.12.249: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.12.249:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>
```

Fig. 3.21: Checking network connectivity using ping command

B) The steps to test TCP/IP connectivity by using the ping command are as follows:

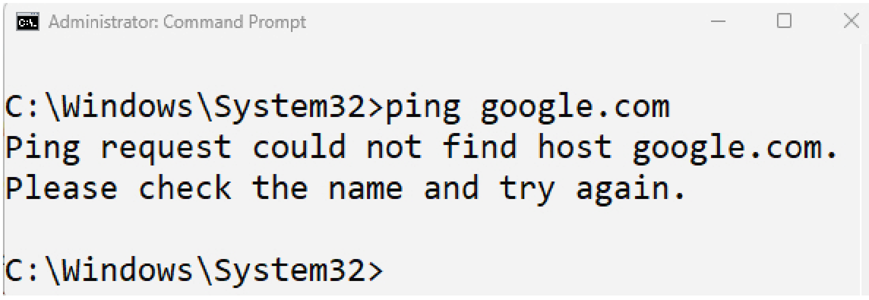
Step 1. Open the command prompt and issue the ping command to ping the loopback address, as shown in Figure 3.21.



```
C:\Windows\System32>ping 127.0.0.1

Pinging 127.0.0.1 with 32 bytes of data:
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128
Reply from 127.0.0.1: bytes=32 time<1ms TTL=128

Ping statistics for 127.0.0.1:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>
```

Fig. 3.22: Testing TCP/IP connectivity using ping command

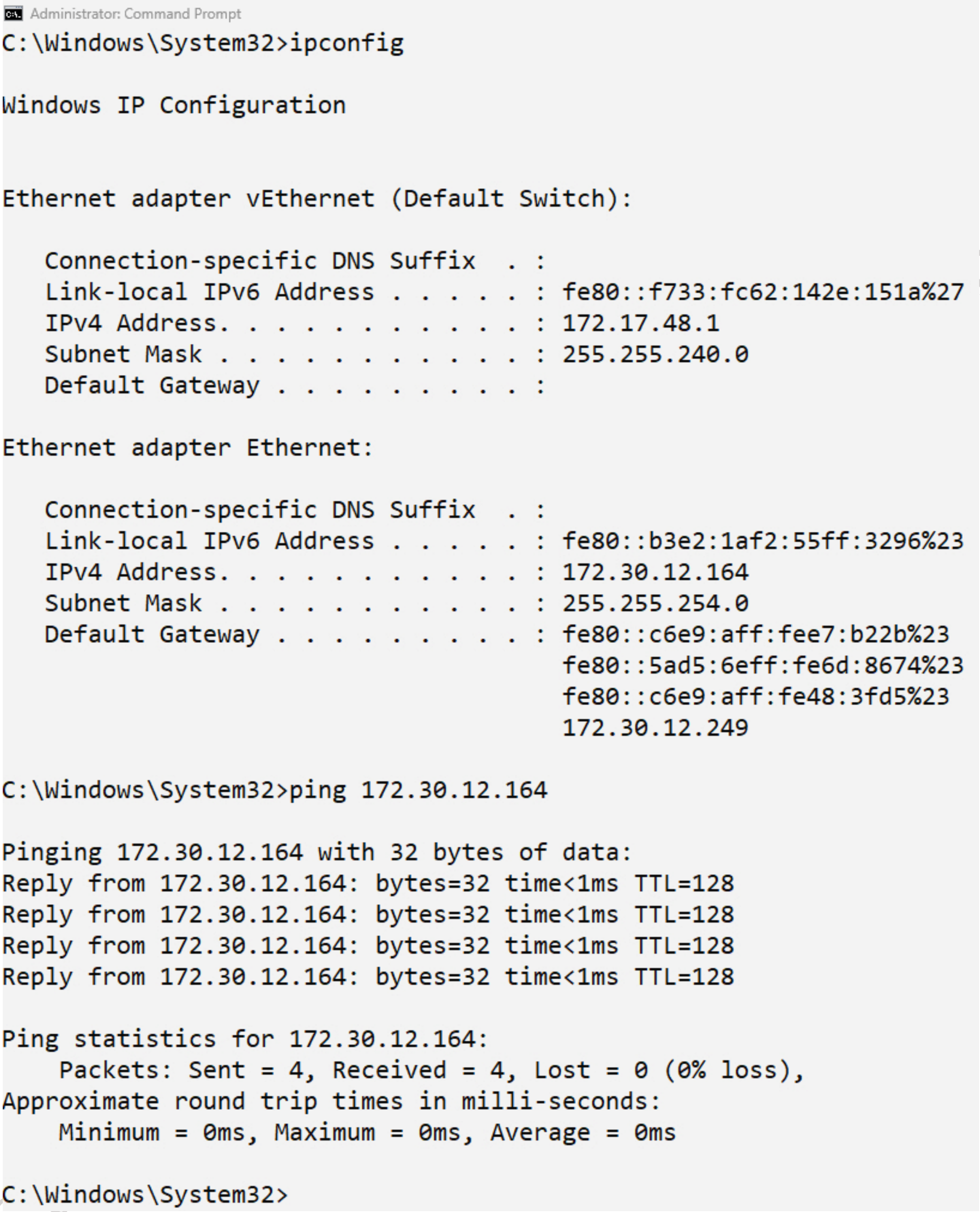
If it fails, then verify that the computer was restricted, after TCP/IP was installed and configured as shown in screenshot given in Figure 3.23.



```
C:\Windows\System32>ping google.com
Ping request could not find host google.com.
Please check the name and try again.

C:\Windows\System32>
```

Fig. 3.23: Result of failure of connectivity

Step 1. Ping the IP address of the computer. It gives the Default Gateway as 171.30.11.249. Ping the IP address of default gateway as shown in Figure 3.24.

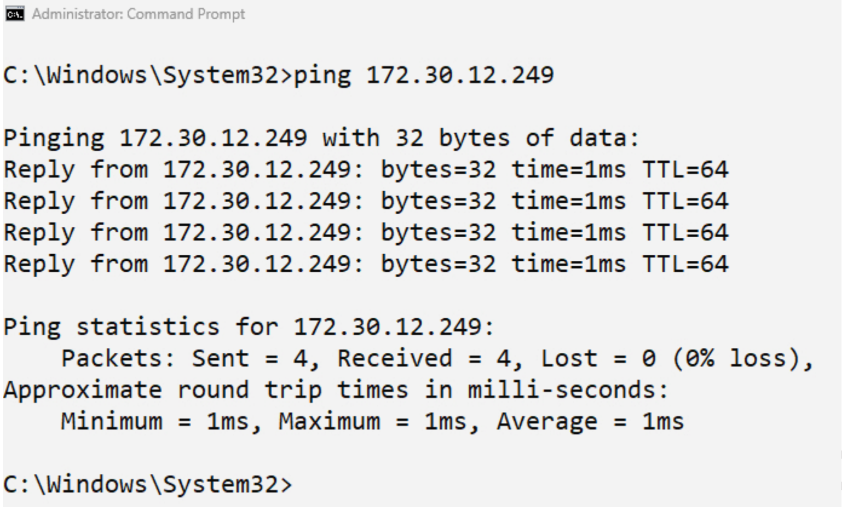


```
C:\Windows\System32>ipconfig

Windows IP Configuration


Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::f733:fc62:142e:151a%27
   IPv4 Address. . . . . . . . . . . : 172.17.48.1
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :

Ethernet adapter Ethernet:

   Connection-specific DNS Suffix  . :
   Link-local IPv6 Address . . . . . : fe80::b3e2:1af2:55ff:3296%23
   IPv4 Address. . . . . . . . . . . : 172.30.12.164
   Subnet Mask . . . . . . . . . . . : 255.255.254.0
   Default Gateway . . . . . . . . . : fe80::c6e9:aff:fee7:b22b%23
                                       fe80::5ad5:6eff:fe6d:8674%23
                                       fe80::c6e9:aff:fe48:3fd5%23
                                       172.30.12.249

C:\Windows\System32>ping 172.30.12.164

Pinging 172.30.12.164 with 32 bytes of data:
Reply from 172.30.12.164: bytes=32 time<1ms TTL=128
Reply from 172.30.12.164: bytes=32 time<1ms TTL=128
Reply from 172.30.12.164: bytes=32 time<1ms TTL=128
Reply from 172.30.12.164: bytes=32 time<1ms TTL=128

Ping statistics for 172.30.12.164:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 0ms, Average = 0ms

C:\Windows\System32>
```

Fig. 3.24: Finding IP address of computer and tesing connnectivity using ping command

If the ping command fails then restart the computer to check the computer with TCP/IP installed and configured.

Step 3. Ping the IP address of default gateway as shown in Figure 3.25.

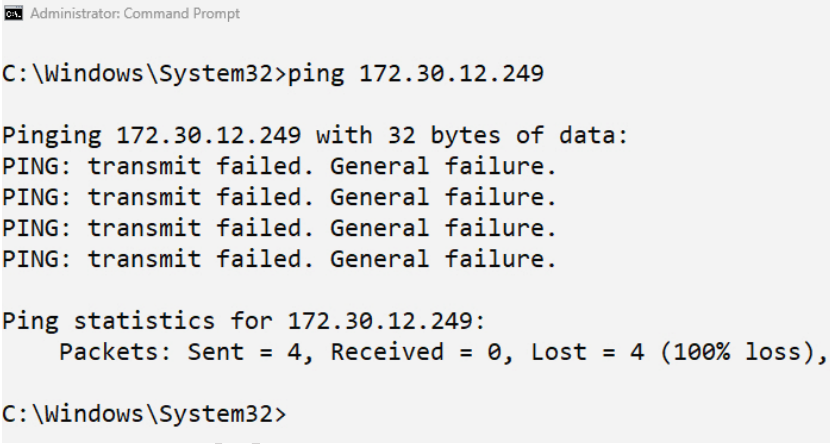


Administrator: Command Prompt

```
C:\Windows\System32>ping 172.30.12.249

Pinging 172.30.12.249 with 32 bytes of data:
Reply from 172.30.12.249: bytes=32 time=1ms TTL=64
Reply from 172.30.12.249: bytes=32 time=1ms TTL=64
Reply from 172.30.12.249: bytes=32 time=1ms TTL=64
Reply from 172.30.12.249: bytes=32 time=1ms TTL=64

Ping statistics for 172.30.12.249:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 1ms, Maximum = 1ms, Average = 1ms

C:\Windows\System32>
```

Fig. 3.25: **Ping the IP address of default gateway**

If the ping command fails, verify the default gateway IP and check the router for connectivity using ping command as shown in Figure 3.23.

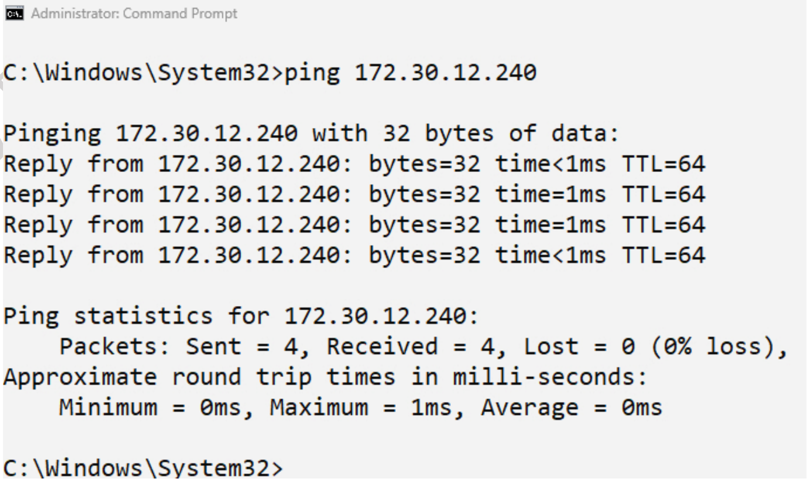


Administrator: Command Prompt

```
C:\Windows\System32>ping 172.30.12.249

Pinging 172.30.12.249 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 172.30.12.249:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\System32>
```

Fig. 3.26: Output of ping command when fail to connect the router

Step 4. Ping the IP address of the remote host as shown in screenshot of Figure 3.27.

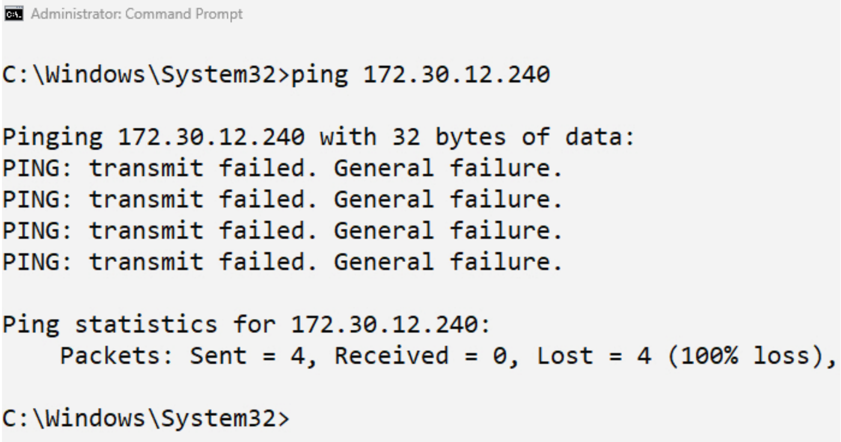


Administrator: Command Prompt

```
C:\Windows\System32>ping 172.30.12.240

Pinging 172.30.12.240 with 32 bytes of data:
Reply from 172.30.12.240: bytes=32 time<1ms TTL=64
Reply from 172.30.12.240: bytes=32 time=1ms TTL=64
Reply from 172.30.12.240: bytes=32 time=1ms TTL=64
Reply from 172.30.12.240: bytes=32 time<1ms TTL=64

Ping statistics for 172.30.12.240:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 0ms, Maximum = 1ms, Average = 0ms

C:\Windows\System32>
```

Fig. 3.27: **Ping the IP address of remote host**

If the ping fails, check the correctness of the remote host IP address; see that it is operational and the router between the host and the remote computer is operational as shown in Figure 3.28.

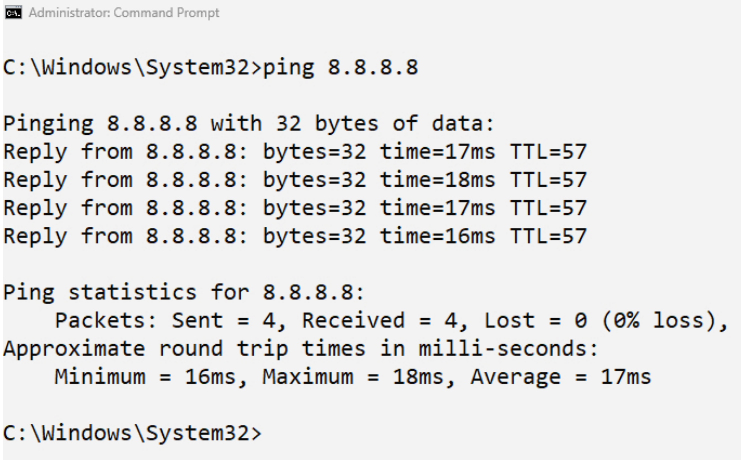


Administrator: Command Prompt

```
C:\Windows\System32>ping 172.30.12.240

Pinging 172.30.12.240 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 172.30.12.240:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\System32>
```

Fig. 3.28: Output of ping command when fail to connect the remote host

Step 5. Ping the IP address of the DNS server as shown in Figure 3.30.

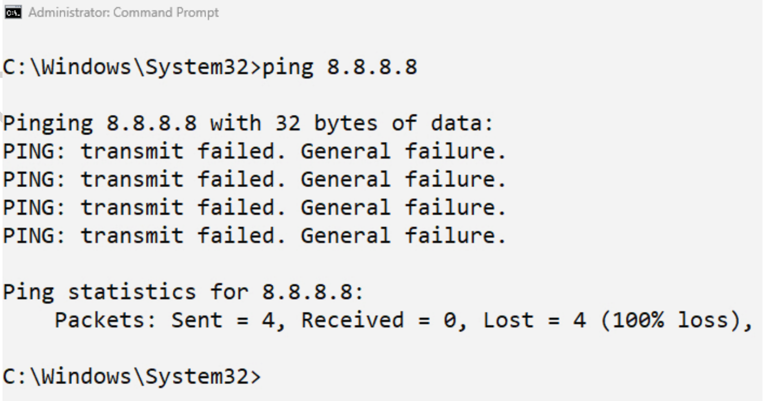


Administrator: Command Prompt

```
C:\Windows\System32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
Reply from 8.8.8.8: bytes=32 time=17ms TTL=57
Reply from 8.8.8.8: bytes=32 time=18ms TTL=57
Reply from 8.8.8.8: bytes=32 time=17ms TTL=57
Reply from 8.8.8.8: bytes=32 time=16ms TTL=57

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 16ms, Maximum = 18ms, Average = 17ms

C:\Windows\System32>
```

Fig. 3.29: Ping the IP address of the DNS server

If the command fails then verify the correctness of the DNS server's IP address; also check that the DNS server is operational and the router between the computer and the DNS server is operational as described in Figure 3.30.

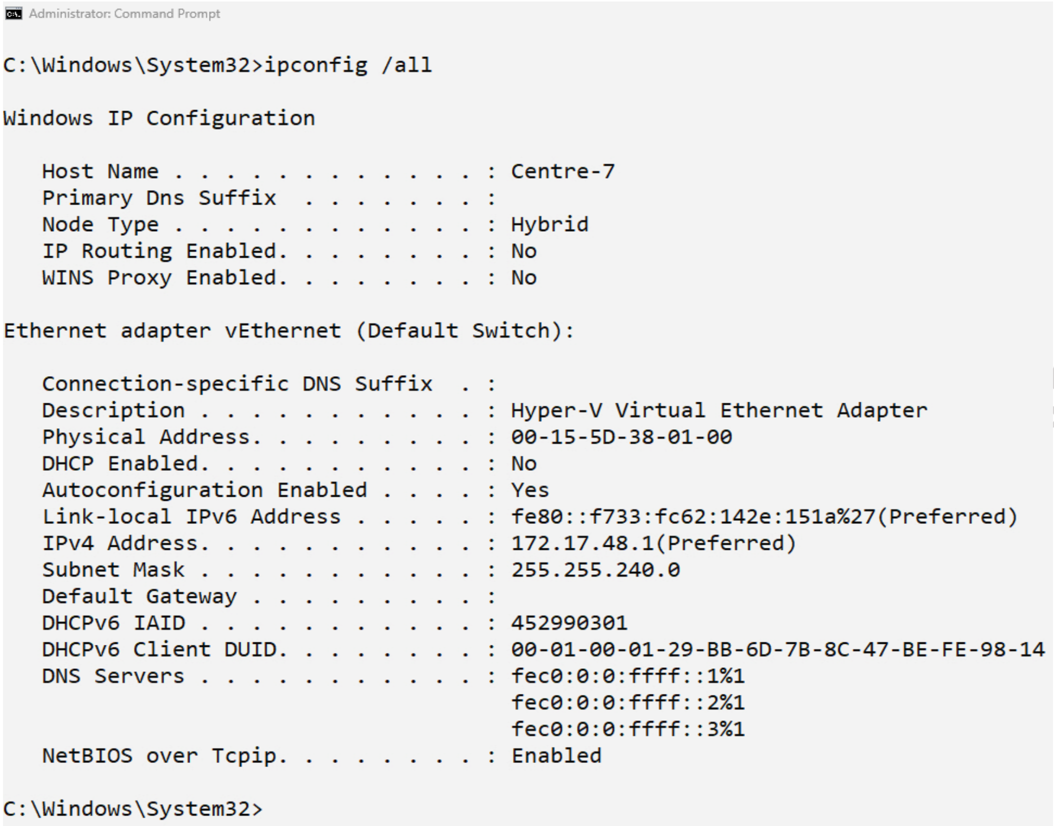


Administrator: Command Prompt

```
C:\Windows\System32>ping 8.8.8.8

Pinging 8.8.8.8 with 32 bytes of data:
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.
PING: transmit failed. General failure.

Ping statistics for 8.8.8.8:
    Packets: Sent = 4, Received = 0, Lost = 4 (100% loss),

C:\Windows\System32>
```

Fig. 3.30: Output of ping command when fail to connect DNS server

An example of an unsuccessful TCP/IP configuration for the local area network is given here. It can be seen that the disabled components are in bold text and the IP address is not displayed as the absence of IP address shows that the local area network is not properly connected. It is illustrated in the screenshot given below in Figure 3.31.



Administrator: Command Prompt

```
C:\Windows\System32>ipconfig /all

Windows IP Configuration

   Host Name . . . . . . . . . . . . : Centre-7
   Primary Dns Suffix  . . . . . . . :
   Node Type . . . . . . . . . . . . : Hybrid
   IP Routing Enabled. . . . . . . . : No
   WINS Proxy Enabled. . . . . . . . : No

Ethernet adapter vEthernet (Default Switch):

   Connection-specific DNS Suffix  . :
   Description . . . . . . . . . . . : Hyper-V Virtual Ethernet Adapter
   Physical Address. . . . . . . . . : 00-15-5D-38-01-00
   DHCP Enabled. . . . . . . . . . . : No
   Autoconfiguration Enabled . . . . : Yes
   Link-local IPv6 Address . . . . . : fe80::f733:fc62:142e:151a%27(Preferred)
   IPv4 Address. . . . . . . . . . . : 172.17.48.1(Preferred)
   Subnet Mask . . . . . . . . . . . : 255.255.240.0
   Default Gateway . . . . . . . . . :
   DHCPv6 IAID . . . . . . . . . . . : 452990301
   DHCPv6 Client DUID. . . . . . . . : 00-01-00-01-29-BB-6D-7B-8C-47-BE-FE-98-14
   DNS Servers . . . . . . . . . . . : fec0:0:0:ffff::1%1
                                       fec0:0:0:ffff::2%1
                                       fec0:0:0:ffff::3%1
   NetBIOS over Tcpip. . . . . . . . : Enabled

C:\Windows\System32>
```

Fig. 3.31: Output of unsuccessful TCP/IP configuration for the local area network

Practical Activity 3.4. Demonstrate to verify local network connectivity and identify any configuration issues.

Procedure

Provide participants with access to a computer or IoT device with networking capabilities.

Instruct participants to open the command prompt and type "ipconfig" to view network configuration details.

Ask participants to identify and note down the following information:

a. IP address

b. Subnet mask

c. Default gateway

d. DNS servers

Have participants use the "ping" command to test connectivity to the following addresses:

a. Loopback address (127.0.0.1)

b. IP address of the computer/device

c. Default gateway

d. External host (e.g., Google's public DNS - 8.8.8.8)

Instruct participants to analyse the results of the ping tests and identify any connectivity issues.

3.9 IoT connectivity

IoT connectivity is the method through which IoT devices, ranging from sensors to self-driving vehicles and encompassing applications like streetlights and robots, link to the cloud, other devices, and integration points such as IoT gateways.

This IoT module expands Internet connectivity to physical devices or common objects, utilizing technologies like embedded systems, wireless sensors, and automation. IoT device testing evaluates the communication strength between devices, applications, and users, ensuring seamless network connection and successful transmission of requested data. IoT connectivity is pivotal as it facilitates the "Internet" aspect of IoT, enabling devices to transmit data for action, service delivery, and revenue generation, thereby adding value to IoT implementations.

3.9.1 Requirements for good IoT Connectivity

For enterprises exploring IoT connectivity technology, three key technical requirements are coverage, energy efficiency, and data rate. Achieving excellence in all these areas simultaneously is challenging, as each radio technology involves trade-offs. Moreover, organizations must assess the geographic scope of their IoT offerings. For global IoT connectivity, opting for a technology available worldwide is essential.

Coverage

All IoT applications necessitate reliable coverage for device connectivity, with some targeting specific indoor zones while others demand extensive reach in rural or remote locales. Long-range technologies excel in connecting devices spread across vast areas.

For instance, traditional cellular technologies like 3G or 4G offer excellent outdoor radio range, particularly in urban settings. LPWA technologies enhance connectivity range further by employing robust coding schemes, making them well-suited for reaching remote areas and penetrating deep indoors. Conversely, short-range technologies like Wi-Fi and ZigBee are ideal for connecting numerous devices situated in close proximity.

Energy Efficiency

The energy efficiency of a connectivity technology greatly affects the lifespan of IoT devices powered by batteries or energy harvesting. Factors like range, topology, and complexity influence this efficiency. Short-range technologies like ZigBee use mesh topology, extending coverage but potentially draining batteries faster. Wide-area technologies like 2G use star topology, reducing power concerns. LPWA technologies like NB-IoT simplify signalling and minimize overhead for longer battery life.

Data rate (on up- and downlink)

Data rate needs for IoT applications vary widely, from hundreds of bps for metering to Mbps for video surveillance. Wi-Fi and LTE offer high data rates but may consume more power or have limited range. LPWA technologies like NB-IoT prioritize energy efficiency with lower data rates. Traditional cellular technologies like 4G and 5G excel in data rate and range, while short-range options like BLE focus on battery life.

Other technical features

In addition to the primary technical considerations mentioned earlier, certain other features are highly relevant for specific applications:

1. Mobility
2. Positioning
3. Latency
4. Device density

As the number of connected devices increases, the capability of a connectivity technology to manage numerous connections within a defined area becomes crucial. To get reliable connectivity while minimizing signal interference poses a significant challenge. Typically, device density within the context of massive IoT is measured in the number of devices per square kilometer.

3.9.2 Importance of Choosing the Right Connectivity Technology

Choosing the right way to connect IoT devices is super important. There are lots of options like cellular, Wi-Fi, Bluetooth, and more. For fast and reliable connections, 5G or 4G might be best, but they can be pricey and use more power. For simpler setups, slower connections can be used that don't need to be always ON. This can save money by using smaller batteries. It's a big decision that affects how well the IoT system works and how much it costs.

3.9.3 Connecting the Internet of Things – Trade-off Between Power Consumption, Range, and Bandwidth

The ideal network connectivity would use very little power, cover a large distance, and handle large data loads (high bandwidth). However, such perfect connectivity doesn't exist. Each connectivity option involves a trade-off between power usage, range, and bandwidth. This leads to a framework dividing connectivity options into three main groups.

A) High Power Consumption, High Range, High Bandwidth:

Sending large amounts of data wirelessly over long distances requires a lot of power. For instance, smartphones can transmit video over long distances, but they need frequent charging.

Connectivity options in this category include cellular and satellite. Cellular works when sensors/devices are within cell tower coverage, while satellites are necessary for remote locations like ships at sea.

B) Low Power Consumption, Low Range, High Bandwidth:

Reducing power usage while transmitting large data means sacrificing range. Wi-Fi, Bluetooth, and Ethernet are examples.

Ethernet, a wired connection, has a short range limited to cable length. Wi-Fi and Bluetooth, though wireless, have lower power consumption than cellular or satellite, yet their range is limited.

C) Low Power Consumption, High Range, Low Bandwidth:

To extend range while conserving power, data transmission must be reduced. This group features Low-Power Wide-Area Networks (LPWAN).

LPWANs send small data amounts, allowing for low-power operation with mile-range coverage. For instance, a moisture sensor in agriculture may only send moisture level readings every few hours, needing long battery life due to field placement. WiFi and Bluetooth lack the required range.

LPWANs are valuable for IoT, enabling numerous sensors to send data over wide areas for years on battery. Although data capacity is limited, most sensors don't need extensive transmission. LPWANs come in various types; some, like LoRa, use unlicensed bands, while others, like NB-IoT, utilize cellular infrastructure.

Summary

- The chapter explores authentication and authorization mechanisms in IoT, stressing the importance of securing edge devices and employing methods like password, token, biometric, and multi-factor authentication.
- It outlines security checklists, challenges, and measures for access control systems.
- The chapter provides the methods to secure wireless connections and detect malware and DDoS attacks.
- Overall, the chapter emphasized on the critical role of robust security practices in IoT environments.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the primary concern as IoT integrates into businesses? (a) Speed of data transmission (b) Security (c) Cost-effectiveness (d) Device compatibility

2. Which of the following is NOT considered an edge device? (a) Cell tower (b) Engine sensor (c) Cloud server (d) Smart thermostat
3. What is the purpose of authenticating edge devices in IoT? (a) To ensure efficient data transmission (b) To confirm the identity of users and devices (c) To regulate internet access (d) To prevent hardware malfunctions
4. Which authentication method relies on unique biological features? (a) Password-based authentication (b) Token-based authentication (c) Biometric authentication (d) Multi-factor authentication
5. What does RBAC stand for in the context of authorization? (a) Remote Biometric Access Control (b) Role-Based Access Control (c) Resource-Based Authorization Code (d) Restricted Biometric Access Center
6. Which architecture offers access tokens directly to users in IoT? (a) Distributed architecture (b) Centralized architecture (c) Decentralized architecture (d) Hybrid architecture
7. What is the primary purpose of securing wireless connections in IoT? (a) To increase data transmission speed (b) To reduce energy consumption (c) To prevent unauthorized access and attacks (d) To enhance device compatibility
8. What are common symptoms of malware-infected IoT devices? (a) Decreased internet speed (b) Unusual error messages (c) Reduced energy consumption (d) Improved device performance
9. What does DDoS stand for? (a) Distributed Denial of Service (b) Device Data Overload System (c) Digital Data Output Service (d) Directed Device Operation System
10. How can DDoS attacks be detected in Windows systems? (a) By running a malware scan (b) By deleting temporary files (c) By checking network connections using the NETSTAT command (d) By upgrading firmware and enabling firewalls

B. Fill in the blanks

1. Authenticating edge devices in IoT involves confirming the _______ of users and devices before granting access to a network or information system.
2. Multi-factor authentication combines two or more ways to identify the _______ or device identity.
3. Access control allows limited access to specific _______, people, or access levels to ensure easy and safe access to the site for users.
4. Securing the network connection is crucial in IoT, and changing the default settings of the router, such as updating the _______ and the subnet mask, is recommended.
5. Malware attacks on IoT devices can be identified through symptoms such as system _______ or crashes, unusual error messages, and increased internet traffic.
6. In token-based authentication, a one-time password (OTP) is sent to the registered device or user and stored in the database for _______.
7. Distributed architecture in access control for IoT involves the control server offering access tokens to users, allowing them to have direct access to _______.
8. _______ authentication relies on human biological features like fingerprint, face, iris, or voice authentication to confirm identity.
9. The steps for detecting DDoS attacks in Windows include using the NETSTAT command to display current TCP/IP network connections and protocol statistics, followed by checking for the total number of connections at port _______.
10. Access control systems provide security by offering access only to _______ individuals or devices.

C. State true or False for the following

1. In IoT settings, edge devices collect and transmit data to the data center or cloud for processing and analysis, enhancing real-time IoT analytics through edge computing.
2. Password-based authentication involves generating a token to identify a user or device.
3. Biometric authentication relies on human biological features such as fingerprint, face, iris, or voice authentication.
4. The centralized architecture in access control for IoT involves users having direct access to the IoT devices.
5. DDoS attacks involve flooding the incoming packets to a single target, causing denial of service for the users of the victim.
6. Multi-factor authentication combines two or more ways to identify the user or device identity.
7. Edge devices, such as engine sensors in the automotive sector, serve as edge devices that collect and transmit data in IoT settings.
8. In token-based authentication, a physical card or device with verification information is created for soft token-based authentication.
9. Access control allows unlimited access to specific groups, people, or access levels.
10. Malware attacks on IoT devices often target devices with advanced security features.

D. Short Answer Type Questions

1. How does RFID contribute to entity identification in IoT?
2. Describe the procedure for authenticating edge devices in IoT.
3. What is the importance of role-based access control (RBAC) in authorization mechanisms?
4. Explain the difference between distributed and centralized architecture in access control systems for IoT.
5. How does multi-factor authentication enhance security in IoT systems?
6. What are some security challenges faced in authenticating edge devices?
7. Describe the process of token-based authentication in IoT.
8. What are the key components of the security checklist for edge devices in IoT?
9. How can access control systems contribute to securing wireless connections in IoT environments?
10. What steps can be taken to detect and mitigate malware attacks in IoT devices?

Session 4. Communication Technologies and Protocols for IoT

Internet of Things (IoT) relies on robust internet connectivity, encompassing wired (e.g., Ethernet) and wireless options (Wi-Fi, Bluetooth, ZigBee, LPWAN). These connections enable seamless communication, empowering IoT devices to share information, synchronize actions, and make real-time decisions, enhancing overall efficiency across different domains.

4.1 Transmission control/Internet Protocol (TCP/IP)

The Internet is a global system of interconnected computer networks. It utilizes the Internet protocol suite to facilitate communication among the devices connected in these networks. Functioning as a network of networks, the internet comprises private or public domains, academic or business domains, and government networks. These networks are interconnected through wireless optical networking technology. The internet serves as a central repository for information and services, including hypertext documents linked through applications like the World Wide Web (WWW), electronic mail, internet telephony, and file sharing. The protocol plays a major role in encoding and decoding information that is transferred through the network.

The most commonly used protocol is TCP/IP. It is a collection of two protocols, namely, Transmission Control Protocol and Internet Protocol as shown in Figure 4.1. It is used to connect network devices in the world wide web.

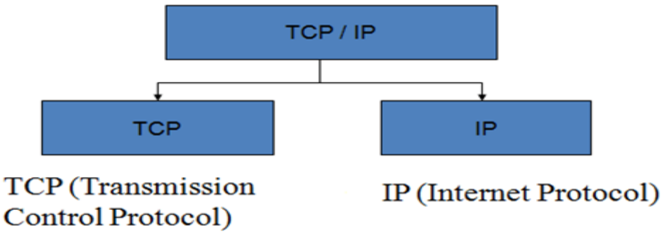


Fig.4.1: Transmission control/Internet Protocol (TCP/IP)

- TCP/IP defines how data is exchanged on the Internet. It delivers end to end communication that defines how data is divided into packets, addressed, transmitted and routed. At the destination data is received and reassembled.
- TCP/IP is a reliable protocol because it ensures data recovery automatically due to network failure or device failure.
- These two protocols serve specific purposes. TCP sets the standard applications on how they should establish a communication channel across the network. It also defines how the message is divided into different packets, packet header and footer and their order of transmission. At the destination it will be received and reassembled according to the header and footer information.
- The Internet Protocol is responsible for determining the address and route of each packet to make sure it reaches the right destination. Every computer on the network checks its IP address to determine the destination address.
- Subnet mask helps in identify email address and device ID to the network. Every IP address has two parts: the network ID and the host ID. Host ID and network ID are determined by network class.
- TCP/IP establishes a connection with the destination host before sending packages. This is called a handshake. Only when the connection is established, it starts sending data. it ensures that data is not lost and reaches the intended recipient.

TCP/IP protocol suite include the following:

- Hypertext Transfer Protocol (HTTP) handles the communication between a web server and a web browser.60
- HTTP Secure handles secure communication between a web server and a web browser.
- File Transfer Protocol handles transmission of files between computers.

TCP/IP is non-proprietary and, as a result, is not controlled by any single company. Therefore, the IP suite can be modified easily. It is compatible with all operating systems (OSes), so it can communicate with any other system. The IP suite is also compatible with all types of computer hardware and networks.

TCP/IP is a reliable, scalable and a routable protocol, it can determine the correct and short path through the network. It is widely used in current internet architecture.

4.2 TCP/IP layers

TCP/IP's most updated model includes the following four layers. All collaborate for the same purpose, the transmission of data.

Application Layer

The top layer serves as an interface for applications and network services to communicate. It defines participants in communication, access to network resources, and rules for application protocols and transport services interaction. Protocols at this layer include DNS, HTTP, SSH, FTP, SNMP, SMTP, DHCP, etc.

Transport Layer

Responsible for determining the data amount and rate for accurate data transport, this layer receives messages from the application layer. It breaks them into pieces, transports them, reconstructs them in the correct sequence, and addresses potential issues to ensure integrity and proper delivery. TCP operates within this layer.

Internet Layer

Also known as the IP or network layer (distinct from the network access layer), it handles packet transmission and ensures precise data transfer. Similar to a traffic controller, it manages traffic direction and pace. Additionally, it provides procedural steps and functionalities for data sequence transfer. Protocols at this layer include IPv4, IPv6, ICMP, and ARP.

Network Access Layer

Combining the OSI model's data link layer and physical layer, this layer outlines the process of actual data transfer over the network. It encompasses how hardware components interacting with a network, such as twisted-pair copper wire, optical fiber, and coaxial cable, transmit data via optical or electrical means. Positioned at the bottom, it is the TCP/IP model's lowest layer.

This is illustrated in Figure 4.1.

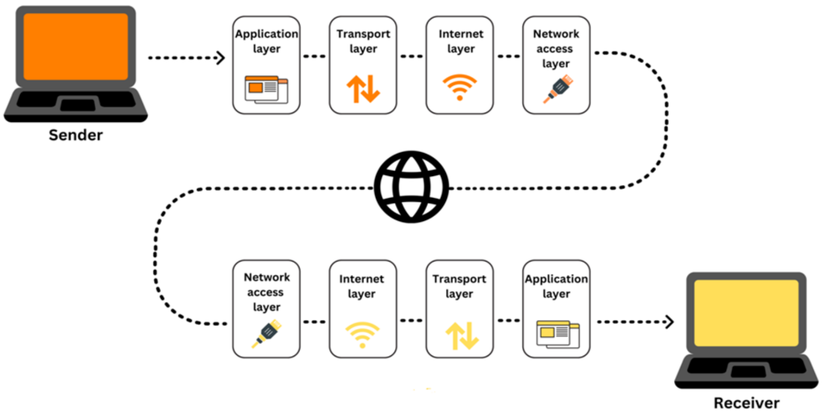


Fig.4.2: TCP/IP layers

4.3 IoT Device Connectivity

The Internet of Things (IoT) would not be possible without connectivity. A device within an IoT ecosystem will only function if it is connected to other devices and technologies, similar to how a sink is connected to a water line or a lamp plugged into an outlet.

Various categories of IoT devices collaborate to create communication pathways, ensuring seamless connectivity. Facilitating communication among diverse IoT devices forms the foundational framework of all IoT systems. These interconnected channels enable the sharing of information and the synchronization of actions, empowering devices to make real-time and proactive decisions in response to prevailing circumstances.

The fluidity of this communication elevates efficiency, expands the scalability of the IoT network, and broadens the possibilities for automation. It is imperative to consider the environmental context before establishing connections, as the network configuration may need to adapt to the specific ecosystem.

4.4 Types of IoT Device Connectivity

Wired – Wired connections deliver high-speed and reliable links across Ethernet and LAN networks, making them well-suited for industrial environments where connection stability is crucial for optimal performance.

Wireless – This category encompasses Wi-Fi and cellular networks, offering connectivity options with short, medium, and long ranges. Wireless connections are widely embraced in IoT networks, contributing to the development of smart homes and intelligent factories. These technologies are depicted in Figure 4.3.

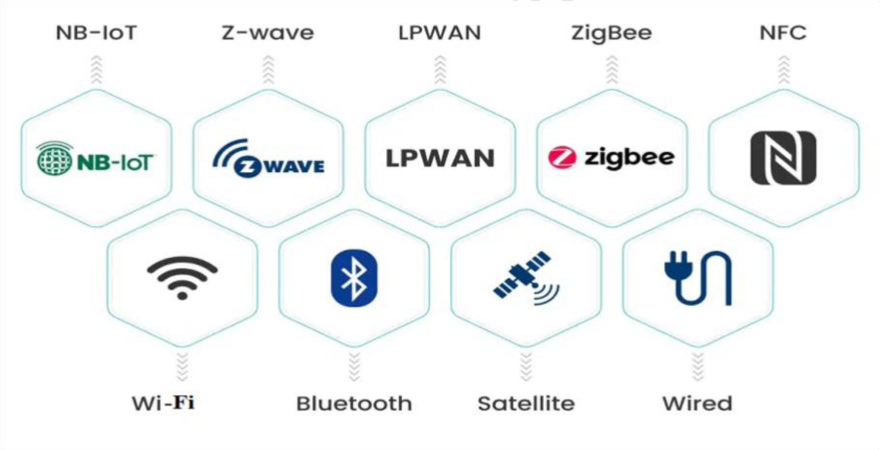


Fig. 4.3: Types of IoT device connectivity

4.4.1 Wired Connectivity

Wired connectivity involves high-capacity and high-speed networks, with Ethernet being a prime example for building IoT device connections. Ethernet offers various configurations, providing speeds ranging from 10 Mbps to 10 Gbps. Its significant advantage lies in high data throughput, crucial for industrial settings and high-capacity workstations. However, it has limitations, such as requiring a dedicated wire for each device, restricting mobility and introducing maintenance and operational challenges.

Applications areas of wired connectivity include Smart Grids, healthcare, transportation, industrial automation, security systems, and smart buildings.

4.4.2 Wireless Connectivity

Wireless connections operate without the need for physical wiring, leveraging Radio Frequency (RF) technology and radio wave propagation within the electromagnetic spectrum. This form of connectivity, extending across open spaces, enables IoT devices to connect and collaborate seamlessly within a network. The most popular wireless technologies used in IoT are discussed as follows:

A) LPWAN

Low-power wide-area Networks are used in environments where long-range wireless and reliable connectivity is required but in a low-power configuration. It is suitable for areas like environmental monitoring and asset tracking.

A popular IoT communication protocol is LoRaWAN, which is patented by Semtech Corporation. It is a Low Power Wide Area Network (LPWAN) protocol, making it an excellent choice for IoT applications due to its long-range connectivity, low power consumption, and low data rate.

B) Satellite

Satellite IoT connections are meant to build communication channels requiring global coverage. This type of connectivity is required for communication in isolated locations and maritime applications. It is shown in Figure 4.4.

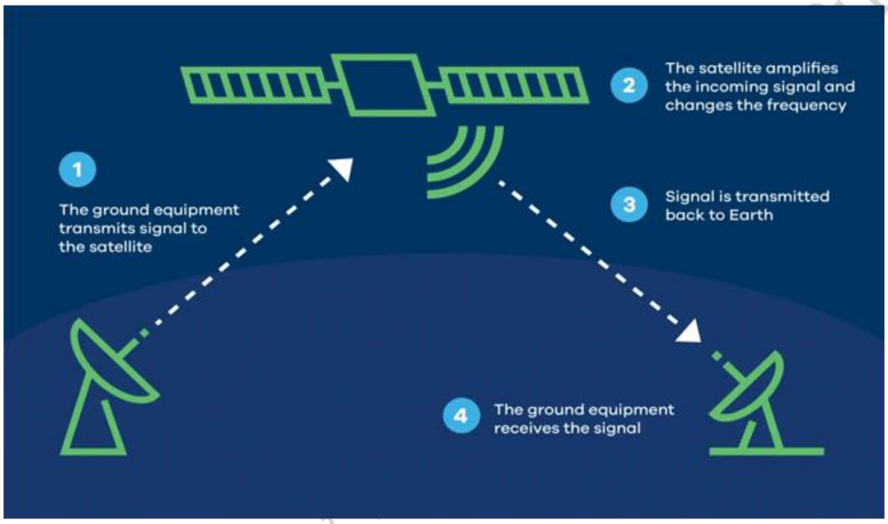

1 The ground equipment transmits signal to the satellite
2 The satellite amplifies the incoming signal and changes the frequency
3 Signal is transmitted back to Earth
4 The ground equipment receives the signal

Fig.4.4: Satellite Communication

C) Bluetooth

Bluetooth connectivity is a short-range wireless communication system used to transmit data at high speed via radio waves. This communication system requires proximity of 10 meters or less between two devices to achieve a data transfer speed of about 2 Mbps. It is designed especially for personal area network applications, operating in the 1.4GHz band. Its coverage range is very small, so it is more suitable for low-cost and low-power transmission for short distances e.g. indoor home applications. It can successfully connect different IoT devices, smart home gadgets, etc. Figure 4.5 shows the headset connected to the mobile phone via Bluetooth.

Fig.4.5: Bluetooth headphones connected to mobile phone

D) ZigBee

ZigBee is the latest wireless technology in the low-power wide area networks (LPWAN) segment technology based on IEEE 801.15.4 used to address the needs of low-power and low-cost IoT devices. ZigBee is designed specifically for mobile communication networks (M2M). It is used to create low-cost, low-power, low-data-rate wireless networks. It is easy to install, and implement and supports a large number of nodes to be connected. It can be used for short-range communications only. Zigbee connectivity is ideal for IoT devices over a mesh network. It is used in smart homes and factories while offering energy efficiency and reliable connectivity.

E) Wi-Fi

Wi-Fi is a short-range communication system that uses radio waves to enable two devices to communicate with each other and transfer data. It is used to connect Internet routers for devices such as computers, tablets, and phones. Wi-Fi is often taken for granted for technicians because it is used widely in-home environments as well as outside. This allows for fast transfer speeds and the ability to handle large quantities. Presently, the most common Wi-Fi standard used in homes and businesses is 801.11n which offers high throughput. It is appropriate for file transfers but highly power-consuming for IoT applications. The Figure 4.6 shows full-strength Wi-Fi in a mobile phone.

Fig.4.6: A mobile phone connected to full-strength Wi-Fi

F) Z-Wave

The Z-Wave connection is also meant to establish seamless connectivity in a home automation system over a secure wireless protocol.

G) Near-field communication

NFC (Near field Communication), is a communication technology that powers IoT devices in a close range and allows simple, secure, contactless data exchange between them. It is mainly used for contactless payments and access control systems for IoT applications. It is used for the identification of documents or objects. It is a protocol used for short-distance communication between devices. It is based on RFID technology but NFC allows information to be shared between two or more devices at a maximum distance of about 10 cm.

For example, NFC technology used in mobile communications allows one to pay for a product by waving the mobile phone at the payment device instead of swiping the card. NFC technology can be used in automated gate check-ins at public places. Figure 4.7 shows the applications of NFC technology.

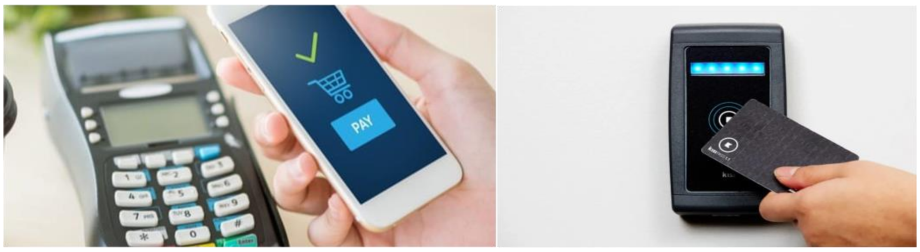


Fig. 4.7: NFC (a) transaction through a mobile phone(b) automated gate check-ins

H) NB-IoT

Narrowband IoT is a connectivity solution within the LPWAN technology that enables communication between different IoT devices.

It focuses specifically on indoor coverage, low cost, long battery life, and high connection density. It reduces the power consumption of connected devices while increasing system capacity and bandwidth efficiency, particularly in locations that aren't easily covered by traditional cellular technologies. NB-IoT-connected devices can have a battery life of more than 10 years for many use cases. It is depicted in Figure 4.9.

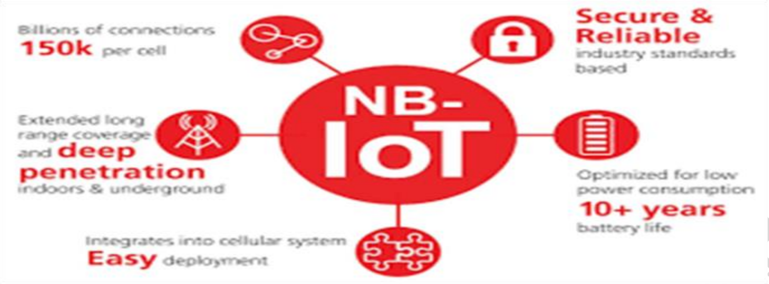


Fig. 4.9: NB-IoT

The comparison of these technologies based on data rate, power consumption and range are given in Figure 4.10.

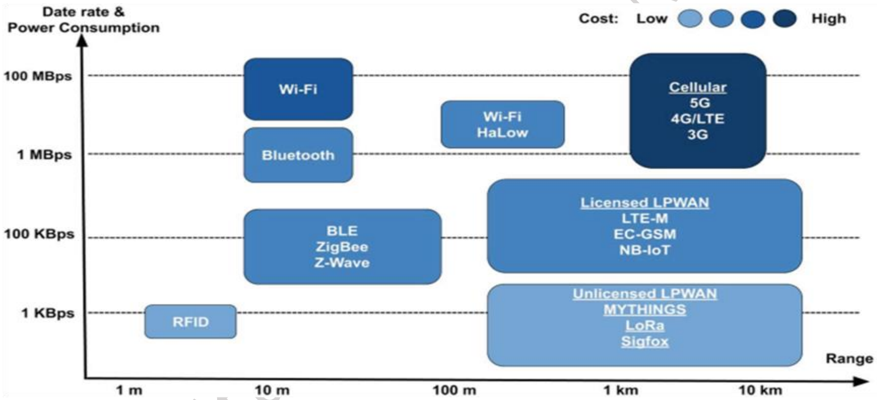


Fig. 4.10: Comparison of communication technologies

4.5 Factors affecting the communication

When selecting IoT connection devices and networks for communication, various factors must be considered. These factors are as follows:

A) Range

Evaluate the reach of the chosen connection solution. Ensure it can facilitate reliable communication among all devices without encountering issues such as lag, disconnection, or inconsistencies based on your specific requirements.

B) Data Rate

Understand the data throughput of the connectivity solution. Wired connections typically offer a data rate of 10 Gbps, while wireless connections vary between 1.4 GHz to 5 GHz bands. Cellular networks can achieve speeds up to 5 Gbps, and Bluetooth connections may reach up to 2 Mbps. Select the connection type that aligns with your data rate needs.

C)Power Consumption

Examine the power consumption of IoT devices. Higher power consumption in devices can lead to increased operational costs, so it's essential to choose devices that align with energy efficiency requirements.

D)Cost

Consider the overall cost of establishing the network, including both hardware and software expenses. Additionally, factor in ongoing costs for operation, maintenance, and potential device repairs.

E) Latency

Assess latency rates, which indicate the delay in data transmission. Wired connections and Bluetooth typically have lower latency, while LPWAN systems may exhibit higher latency. Choose a connection solution that meets your latency requirements based on the specific demands of your application. Some of the most popular wireless technologies include following characteristics:

Table 4.1: characteristics of wireless technologies

Parameters	***Wi-Fi***	***Bluetooth***	***ZIgBEE***	***Z-Wave***
Range	It can be set up in an area between 100 to 400 meters	It can be set up in an area up to 200 meters	When connected in a straight line of sight, the range is 300 meters. In an indoor environment, the range is 90 meters.	Up to 100 meters
Data Rate	Up to 1.3Gbps	Bluetooth's data rate is 350 kbps, & BLE's data rate is 3 Mbps	RE Zigbee connection's data rate is 250 Kbps, & serial Zigbee's data throughput is 1 Mbps.	Z-wave has a data rate of up to 100 kbps.
Power Consumption	When at idle-30 to 100 mA when working – 130 to 250 mA	BLE consumes 35 mA at idle, & Bluetooth devices consume 100 mA.	When at idle-15 to 20 mA when operational, - 45 to 130 mA.	When idle, -10 to 50 mA when running, -20 to 100 mA.
Compatibility	Wide range of consumer & commercial (industrial devices)	Suitable for consumer IoT devices requiring short-range & sensor networks, including smart homes.	These are mostly found in smart homes, connected healthcare, & smart factories.	Mostly employed in smart home applications IoT network setup.

4.6 Different types of IoT connections

Connection of different devices in an IoT network can be classified in three types as follows:

Consumer connected devices

This category covers smart home gadgets such as smart speakers, automated security systems, voice assistants, wearables, fitness trackers, and connected appliances.

Enterprises connected devices

These devices are employed in large-scale settings like smart factories and warehouses. Examples include smart security systems, energy management tools, asset and inventory trackers, mobility solutions, and more.

Industrial IoT

I IoT devices are utilized in large industrial setups, offering advantages like predictive maintenance, real-time monitoring, and automation. Industries leverage these systems for increased productivity, reduced downtime, and enhanced efficiency through data-driven insights.

4.7 IoT network

IoT networks are dynamic ecosystems where interconnected devices communicate and share data for collaborative functionality. Utilizing wired and wireless technologies like Wi-Fi and Bluetooth, these networks enable seamless interactions, supporting applications from smart homes to industrial setups. Emphasizing security and standardized protocols ensures efficient, reliable, and scalable IoT communication. Some common types of networks are cellular and Low-Power Wide-Area Network as discussed below:

4.7.1Cellular Network

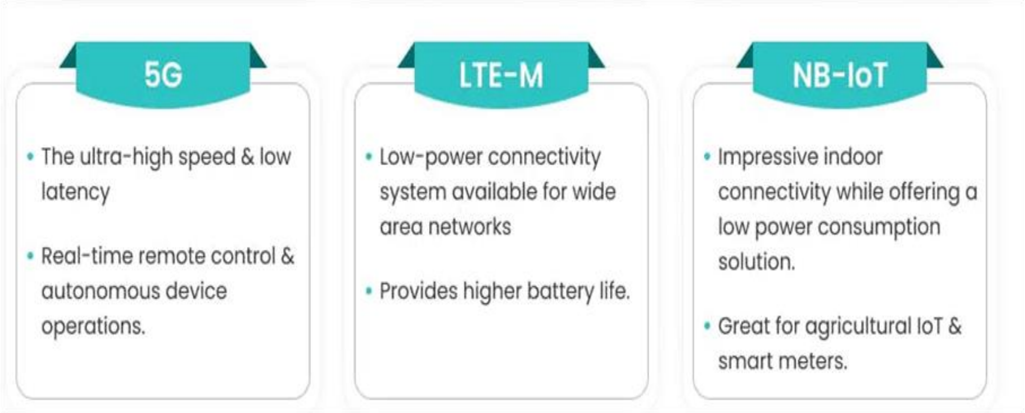
Cellular has become the most popular network connection system today, and the same applies to IoT networks. Establishing IoT connections with this system is easier with an already existing global cellular network. Different types of cellular networks are available, including;

5G – The ultra-high speed and low latency fifth-generation network provides capabilities like real-time remote control and autonomous device operations.

LTE-M – The LTE-Machine network is a low-power connectivity system available for wide area networks and can be used in IoT for its extended coverage. It also provides higher battery life.

NB-IoT – The Narrowband IoT network offers impressive indoor connectivity while offering a low power consumption solution. It's great for agricultural IoT and smart meters.

The characteristics of cellular network are shown in Figure 4.11.



5G

- The ultra-high speed & low latency
- Real-time remote control & autonomous device operations.

LTE-M

- Low-power connectivity system available for wide area networks
- Provides higher battery life.

NB-IoT

- Impressive indoor connectivity while offering a low power consumption solution.
- Great for agricultural IoT & smart meters.

Fig. 4.11: Cellular Network

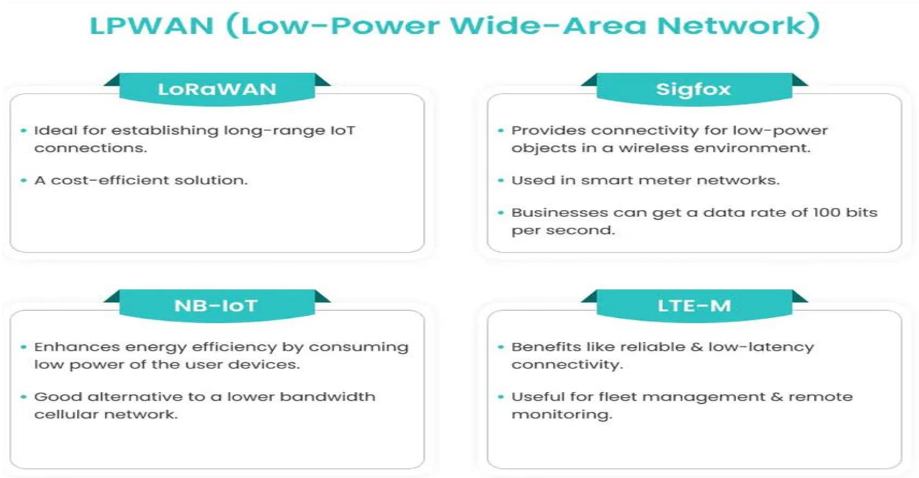
4.7.2 LPWAN (Low-Power Wide-Area Network)

LPWAN is a subset of the wireless communication systems and technologies specifically designed to build IoT networks. These connections provide communication channels for long-range coverage with benefits like low power consumption and cost efficiency.

Hence, LPWAN is ideal for battery power IoT connections, particularly in smart cities, agricultural settings, and environment monitoring. Different types of connections in LPWAN include:

LoRaWAN – LoRaWAN is ideal for establishing long-range IoT connections. Offering smart connectivity in agricultural settings and intelligent cities, LoRaWAN is a cost-efficient solution. However, entities using this network must set up their own infrastructure. Since this connection uses an unlicensed frequency, the businesses only have to pay for the infrastructure.

Sigfox – Sigfox is also specifically designed for to provide connectivity for low-power objects in a wireless environment. It is popularly used in intelligent meter networks. Currently, Sigfox has a 900 MHz band network in over 72 countries. Using this technology, businesses can get a data rate of 100 bits per second. It is shown in Figure 4.11.



LPWAN (Low-Power Wide-Area Network)

LoRaWAN

- Ideal for establishing long-range IoT connections.
- A cost-efficient solution.

Sigfox

- Provides connectivity for low-power objects in a wireless environment.
- Used in smart meter networks.
- Businesses can get a data rate of 100 bits per second.

NB-IoT

- Enhances energy efficiency by consuming low power of the user devices.
- Good alternative to a lower bandwidth cellular network.

LTE-M

- Benefits like reliable & low-latency connectivity.
- Useful for fleet management & remote monitoring.

Fig. 4.12: LPWAN Network

4.8 Security and Privacy Considerations

The connectivity of devices in an IoT network raises concerns about security and privacy. Although there are various solutions to address these challenges, it's important to acknowledge the potential for malicious actors to exploit weak security systems.

Authentication and Authorization

Secure IoT networks implement authentication systems, such as digital certificates and secure APIs, to identify devices and allow authorized access. The authorization system regulates the level of access and actions permitted for devices.

Security & Privacy Measures

Data Encryption

Utilizing encryption protocols ensures the security of data in storage and transmission, preventing eavesdropping, data tampering, and leakage. This safeguards data privacy and integrity.

Quantum Encryption

IoT connections employ quantum-safe encryption to address security gaps posed by quantum computing. Quantum algorithms are used to protect the network from potential attacks originating from quantum computing systems.

Firmware Updates

Secure Over-The-Air (OTA) updates are sent to enhance firmware security and protect the network from vulnerabilities. Cryptographic signatures on the web enable the establishment of a system to verify the authenticity and security of updates.

DDoS Mitigation

Secure IoT networks incorporate DDoS mitigation systems, including traffic analysis, rate limiting, and anomaly detection, to prevent and mitigate Distributed Denial of Service attacks.

4.9 IoT protocols and Standards

Each IoT network adheres to specific communication protocols and standards established to enhance overall utility, security, and integrity.

Protocols serve as a set of rules governing the transmission of data between electronic devices, adhering to pre-established agreements on information structure and the procedures for sending and receiving data. Similarly, IoT protocols are standards designed to facilitate the exchange and transmission of data between the Internet and devices at the edge.

These IoT protocols fall into two primary categories: IoT network protocols and IoT data protocols. Data protocols primarily concern themselves with information exchange, whereas network protocols provide the means to connect IoT edge devices with other edge devices or the Internet. Each category encompasses several protocols, each with its distinct features.

4.9.1 IoT network Protocols

- Wi-Fi
- NB-IoT
- Bluetooth
- ZigBee
- LoRaWAN

These all have been discussed in the previous section.

4.9.2 IoT Data Protocols

MQTT (Message Queuing Telemetry Transport)

MQTT is a publish-subscribe protocol widely utilized in networks with low bandwidth and high latency. Its real-time data transmission capability makes it suitable for IoT networks with limited resources.

CoAP (Constrained Application Protocol)

Designed for networks with limited resources, CoAP uses HTTP to connect the network with web services. This protocol is tailored to operate efficiently in constrained environments.

HTTP (Hypertext Transfer Protocol)

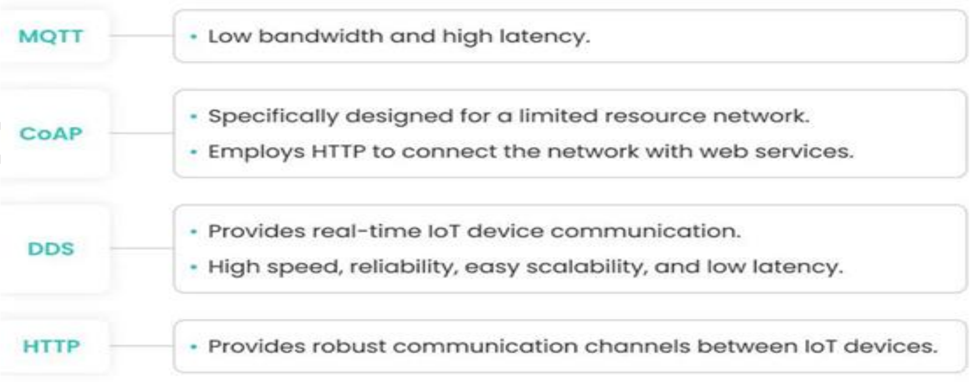
Widely employed for IoT device connectivity, HTTP is a globally recognized and implemented protocol that establishes robust and standardized communication channels among various IoT devices.

DDS (Data Distribution Service)

DDS is another publish-subscribe standard featuring a data-centric architecture. This protocol facilitates real-time communication among IoT devices, offering a channel characterized by high speed, reliability, easy scalability, and low latency. These standards can be effectively deployed in IoT systems, such as autonomous vehicles.

By utilizing these standards, a well-functioning IoT network can be constructed, operated, and managed, delivering assured benefits to end users.

This protocol is explained in Figure 4.13.



- Low bandwidth and high latency.
- Specifically designed for a limited resource network.
- Employs HTTP to connect the network with web services.
- Provides real-time IoT device communication.
- High speed, reliability, easy scalability, and low latency.
- Provides robust communication channels between IoT devices.

Fig. 4.13: IoT data protocols

4.10 IoT network topologies

The Internet of Things (IoT) is like a big network where devices talk to each other. Imagine all sorts of things like smart fridges, thermostats, and sensors sharing information. How they connect and chat with each other is IoT network topologies. These are the elements of wireless communication networks for the IoT. To decide which topology or connection is best for a specific smart application, it is required to know the advantages and disadvantages of each. Understanding the necessary communication network topology is crucial for an IoT application that shows compatibility with current technological norms. There are several types of IoT topologies for networking, the most common topologies are discussed here.

4.10.1 Point-to-Point Topology

A point-to-point network in a local area network is defined as an exclusive two-device communication channel or direct connection between two network nodes or devices. There is a dedicated link that exists between two endpoints, hence it is the simplest topology. The advantage of such a network is that all the available network bandwidth is dedicated to the two connected devices. The earpiece of the cell phone connected through a Bluetooth connection is the best illustration of a point-to-point network. This topology is illustrated in Figure 4.14.

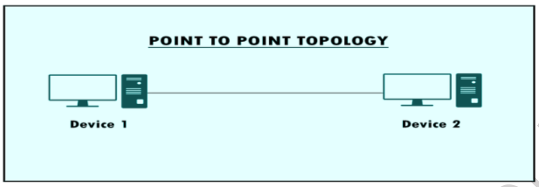


Fig. 4.14: Point-to-Point topology

For instance, the main benefits are simplicity of use and installation as well as low cost, whereas the biggest drawback is the lack of scalability beyond two devices because the relationship is one-to-one. One of the devices can function as a slave, with another serving as the master. Point-to-point networks are not very useful for IoT as it rarely makes sense in IoT to have a receiver talk to a single node instead of multiple nodes.

4.10.2 Star Topology

A star topology is a network configuration where each node or device links to a central hub or switch. This type of network layout is widely used for Local Area Networks (LANs) due to its simplicity in design and implementation. In this setup, the central hub acts as the server for the connected nodes or devices. All data traffic flows through the central hub, which is the essential criterion for classifying a network as a star topology. Interestingly, the physical arrangement of the network doesn't necessarily have to resemble a star. It is depicted in Figure 4.15.

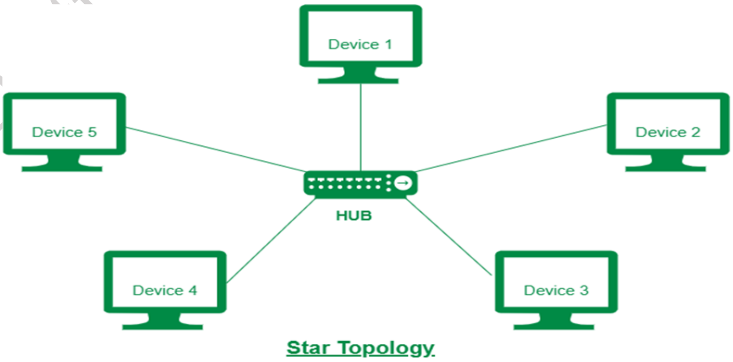


Fig. 4.15: Star Topology

The advantage of star topology is that all the complexity in the network is driven to a central node, so all the other nodes only need to communicate in their time or frequency slot. The primary disadvantage of star topology is that the radio link between the gateway and the end node or terminal can be very long, which means the further a node is away from the gateway, the more energy it has to expend relaying a message. A majority of low power wide-area network (LPWAN), Wi-Fi and cellular networks, use a star network topology.

4.10.3 Mesh Topology

A mesh topology is one in which the nodes connect directly and dynamically to many other nodes. It consists of an elaborate structure of point-to-point interconnections among the nodes. It is shown in Figure 4.14.

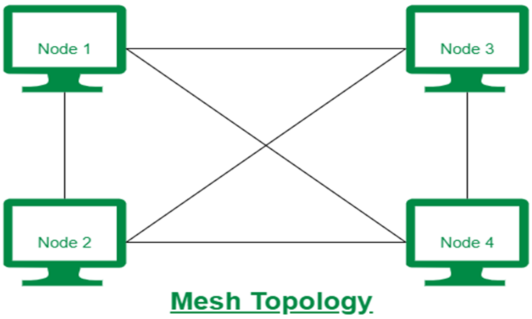


Fig. 4.16: Mesh Topology

Mesh topology is a type of networking where all nodes cooperate to distribute data in a network. This network consists of three types of nodes which are:

- For hub transmission
- Sensor nodes
- Sensor nodes with router/router function

A mesh network is quite similar to a combination of point-to-point and star networks; the nodes are arranged so that each node is in the transmission range of at least one other sensor/router node.

Broadcasting is done by multiple reachable sensor/router nodes. This topology is typically used for long-distance and wide-area applications such as home automation, smart buildings, energy management, industrial automation etc. The industry standards that rely on mesh network topology include Zigbee, Z-Wave, and Thread. The connection of devices in the IoT as discussed above are illustrated in Figure 4.17.

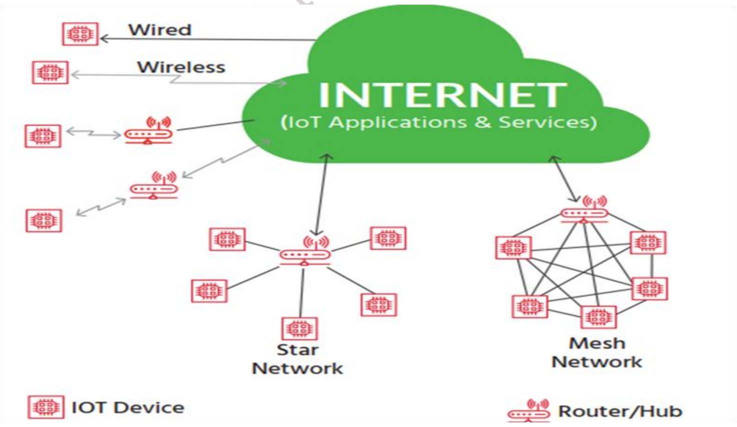


Fig. 4.17: IoT Network topologies

4.11 Multiprotocol IoT Environment

In today's world, it is hard to imagine a home without Wi-Fi and Bluetooth-compatible devices in the multi-protocol IoT environment. The more technological advances, the higher the expectations. The user wants to control the lighting and home technology at the push of a button which gave birth to smart hubs. The technology is used to protect against theft, burglary, smoke, and fire when not at home.

With the arrival of multi-protocol technology, and the introduction of new wireless sensors in the Internet of Things it is made possible. It is a combination of hardware and software to facilitate support of multiple wireless protocols (Bluetooth, ZigBee, and so on) in one device.

IoT infrastructure is built on legacy systems; the devices are made in a way that adding the latest wireless technologies to the old architecture is not difficult. This has been made possible with the help of small sensors embedded in the devices. It is explained in Figure 4.18.

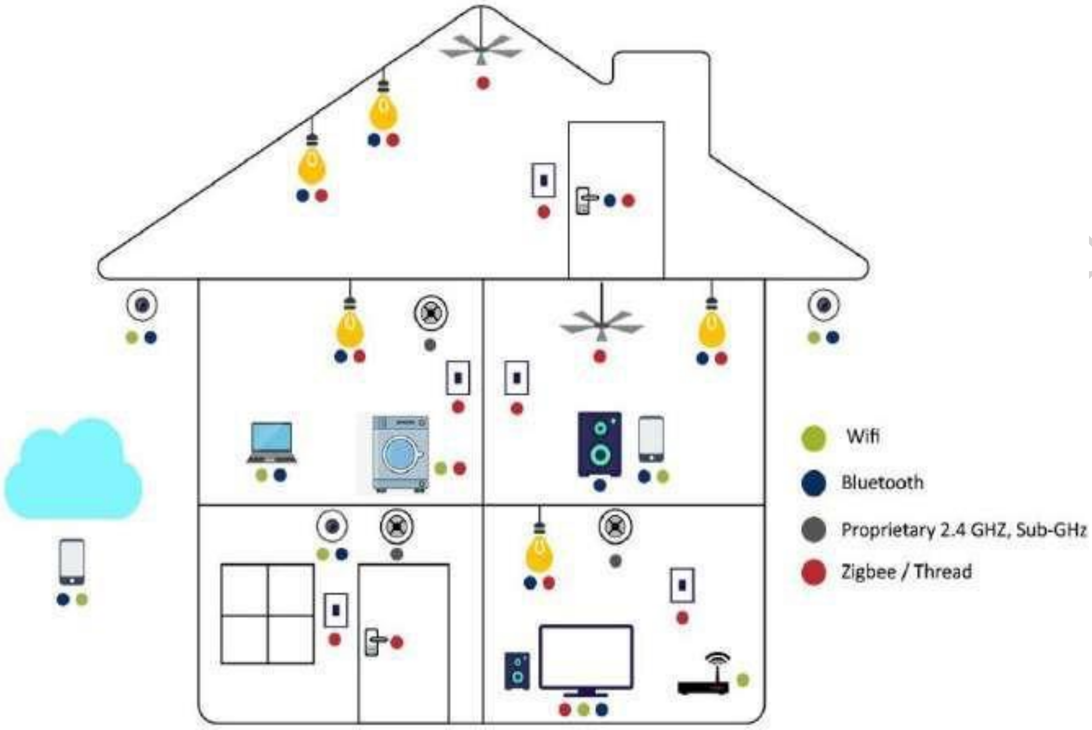


Fig.4.18: Multiprotocol IoT environment

Summary

- This chapter covers the basic knowledge of TCP/IP and IoT protocols.
- The content covers IoT communication technologies, like RFID, ZigBee, Bluetooth, Wi-Fi, Thread, NFC and LoRaWAN, SigFox, NB-IoT with their characteristics and operating range
- It explains network topologies like Point-to-Point, Star, and Mesh.
- Additionally, it introduces multi-protocol IoT environments for seamless integration of various wireless protocols in one device. This information is valuable for understanding and implementing IoT solutions

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. Which wireless communication technology is commonly used for short-range IoT devices? (a) ZigBee (b) LTE-M (c) LoRaWAN (d) NB-IoT
2. Which wireless communication technology is suitable for long-range, low-power IoT devices? (a) Wi-Fi (b) Bluetooth (c) LoRaWAN (d) ZigBee
3. Which of the following is a key feature of LoRaWAN technology? (a) High data rate (b) Long battery life (c) High power consumption (d) Short communication range
4. Which communication technology is commonly used for connecting IoT devices to the internet via a cellular network? (a) Wi-Fi (b) Ethernet (c) 4G/5G (d) Bluetooth

5. What does NFC (Near Field Communication) technology excel at in IoT applications? (a) Long-range communication (b) High data throughput (c) Secure short-range communication (d) Low-power communication
6. Which communication technology is known for its mesh networking capabilities in IoT applications? (a) ZigBee (b) LoRaWAN (c) NB-IoT (d) LTE-M
7. What was the range of Bluetooth? (a) More than 10m (b) Less than 10m (c) Only 10m (d) None of the above
8. The Bluetooth technology is used in ____ (a) Wireless mouse (b) Wireless keyboard (c) Headsets (d) All of the above
9. Mesh topology, has devices which are connected via (a) single and multiple links (b) Multipoint link (c) Point to point link (d) No Link
10. What does the acronym "NB" stand for in NB-IoT (Narrowband Internet of Things)? (a) Narrowband (b) National Bandwidth (c) Narrow Beam (d) Network-Based

B. Fill in the blanks

1. TCP/IP is a reliable protocol because it ensures ____automatically due to network failure or device failure.
2. A mesh network is quite similar to a combination of point-to-point and ____.
3. ZigBee is the latest wireless technology in the ______segment technology.
4. Wi-Fi is a short-range communication system that uses______ to enable two devices to communicate with each other and transfer data.
5. BLE is often used in wearable devices, healthcare, and fitness applications due to its low ________ consumption and ________ communication capabilities.
6. A star topology is a network configuration where each node or device links to a _____or switch.
7. SigFox is a cellular-style, _____________ wireless communication technology.
8. MQTT is _______widely utilized in networks with low bandwidth and high latency.
9. NFC allows information to be shared between two or more devices at a maximum distance of about ______.
10. ZigBee is the latest wireless technology in the low-power wide area networks (LPWAN) segment technology based on____________.

C. State True or false for the following

1. Bluetooth technology is a Wireless LAN technology.
2. LoRaWAN (Long Range Wide Area Network) is a low-power, long-range wireless communication technology suitable for IoT deployments with devices spread over a wide area.
3. Thread is a low-power, wireless communication protocol that is suitable for home automation and other IoT applications.
4. Mobile computing uses wireless as the mode of communication for transferring or exchanging data between various mobiles over a short range.
5. Star topology has a Multipoint connection.
6. Bluetooth is a commonly used wireless communication protocol in IoT.
7. Zigbee is a low-power, short-range wireless communication protocol suitable for battery-powered devices in IoT applications.

8. RFID (Radio-Frequency Identification) is a communication technology commonly used for tracking and identifying objects in IoT applications.
9. Thread is a low-power, wireless mesh networking protocol suitable for home automation and other IoT applications.
10. The term "LPWAN" stands for Long-Range, Low-Power Wide Area Network, which is a category of communication technologies suitable for IoT devices with long-range communication requirements.

D. Short answer type questions

1. Explain the difference between Wi-Fi and Bluetooth in the context of IoT communication.
2. How does LoRaWAN address the communication needs of IoT devices in terms of range and power consumption?
3. Describe a scenario where Zigbee would be a suitable communication technology for an IoT application.
4. Discuss the advantages of using a Low-Power Wide Area Network (LPWAN) for IoT communication.
5. Explain how NFC technology can be used in IoT applications, providing an example.
6. What are some key considerations when choosing a communication protocol for a specific IoT application?
7. Describe a situation where a hybrid communication approach (combining multiple communication technologies) would be beneficial in an IoT ecosystem.
8. Explain the concept of mesh networking and how it is relevant in IoT communication.
9. What are the key considerations in ensuring the security of communication in an IoT ecosystem?
10. What is the role of 5G technology in advancing IoT communication? Provide an example of an IoT application that benefits from 5G.

Session 5. Cloud Computing

IoT means connecting devices to the Internet to provide services they're designed for. This involves storing and processing data, which needs to be preserved. The term cloud refers to a network or the internet. It is a technology that uses remote servers on the internet to store, manage, and access data online rather than local drives. The data can be anything such as files, images, documents, audio, video, and more. Cloud storage helps keep data on the Internet, giving advantages by offering services online.

For example, if an employee and manager are in different places, a cloud service can solve the problem by using Internet-hosted applications. These applications manage data from a distance, and the cloud can be used for both temporary and permanent storage.

5.1 Concept of Cloud Computing

Cloud computing is the on-demand availability of computing resources (such as storage and infrastructure), as services over the internet. It eliminates the need for individuals and businesses to self-manage physical resources themselves, and only pay for what they use. Cloud computing enables the remote manipulation, configuration, and access of both hardware and software. Essentially, it involves accessing and storing files and databases over the internet rather than on your computer's hard drive.

This partnership also advances the Internet of Things. Working together, IoT and cloud tech enhance the development of control devices and the processing of sensor data. For instance, sensor data can be stored and retrieved from cloud storage, enabling the control of other smart devices. The goal is to achieve a more efficient and cost-effective solution. The cloud platform aids in data analysis, decision-making, and optimizing communication. The integration of IoT and the cloud addresses aspects like QoS, quality of experience (QoE), information security, privacy, and data reliability. Cloud services offer a utility-based model, allowing users to access information anytime, anywhere. The Figure 5.1 shows the concept of a cloud platform.

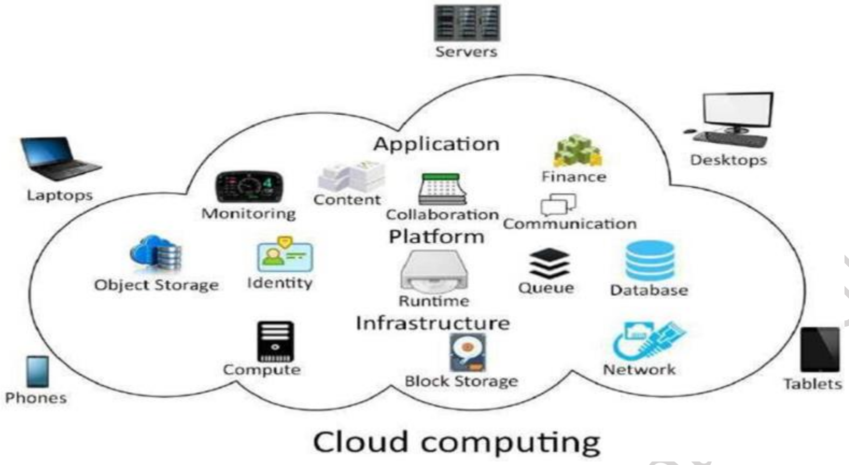


Fig. 5.1: Concept of cloud computing

5.2 Characteristics of Cloud Computing

There are a few characteristics of cloud computing which determine its working. The Figure 5.2 shows these characteristics.

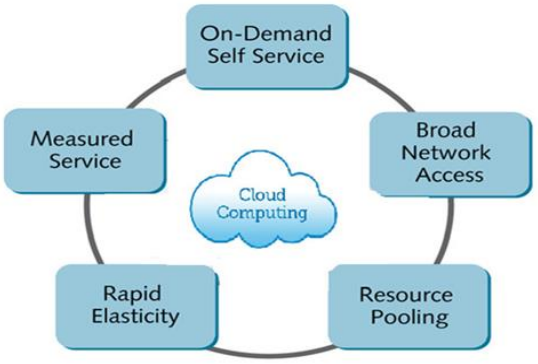


Fig. 5.2: Concept of cloud computing

These characteristics are explained as follows:

On-demand self-services – Cloud services do not require system administrators, but users themselves can provision, monitor and manage computing resources themselves as needed.

Broad network access – The Computing services are generally provided over standard networks and heterogeneous thin or thick client platforms (e.g., mobile phones, tablets, laptops, and workstations).

Resource pooling – IT resources (such as networks, servers, storage, applications and services) are shared between multiple applications and used on a non-committed basis. Multiple clients receive service from the same physical resource.

Rapid elasticity – IT services must have IT resources that can be scaled and scaled quickly as needed. When a user needs services, it is offered to them and scaled as soon as their demand is met.

Measured service – Resource usage is tracked for each application and user, giving both the user and the resource provider a report on what was used. This happens for a number of reasons, such as invoice tracking and efficient use of resources.

5.3 Basic Models of Cloud Computing

There are certain services and models to make cloud computing feasible and accessible to the end users such as *Deployment Models, Service Models.*

5.3.1 Deployment Models

Deployment models in cloud computing refer to the specific configurations and arrangements through which cloud services are made available to users. These models dictate how resources, applications, and services are deployed and managed in the cloud environment. The deployment of cloud services includes four deployment models: private cloud, public cloud, community cloud and hybrid cloud as shown in the Figure 5.3.

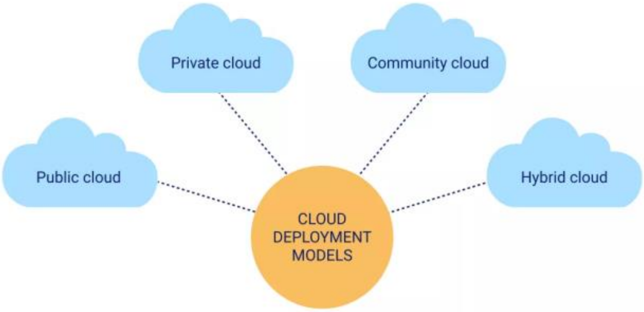


Fig. 5.3: Deployment Models in cloud computing

Public cloud – The public cloud is easily accessible to the general public and is operated by external providers. It offers cost-effectiveness as users only pay for the resources they use, eliminating wasted resources.

Private cloud – Contrarily, the private cloud is exclusive to an organization, providing control over the cloud environment. It is suitable for businesses with dynamic or unpredictable computing needs, ensuring a tailored and secure infrastructure.

Community clouds – In the community cloud model, resources are shared among multiple organizations, fostering collaboration on a shared platform. This setup enables companies to jointly utilize and benefit from shared resources.

Hybrid cloud – Combining elements of both private and public clouds, the hybrid cloud is ideal for managing heavy workloads. It offers flexibility by allowing organizations to leverage the benefits of both environments as needed.

5.3.2 Service Models

There are three service models as follows:

Infrastructure-as-a-Service (IaaS) – In IaaS, users manage data, applications, and runtime, while providers handle virtualization, servers, storage, and networking. Examples include Amazon Web Services (AWS) and Microsoft Azure.

Platform-as-a-Service (PaaS) – PaaS is tailored for development, allowing users to develop and customize applications easily. It simplifies the development, testing, and deployment of applications. An example is Apparenda.

Software-as-a-Service (SaaS) – SaaS delivers complete software to clients as a service, offering pre-configured hardware resources through a virtual interface. It does not include an Operating System and provides access to the software only. Examples include Google Apps, Salesforce, and Workday. It is depicted in Figure 5.4.

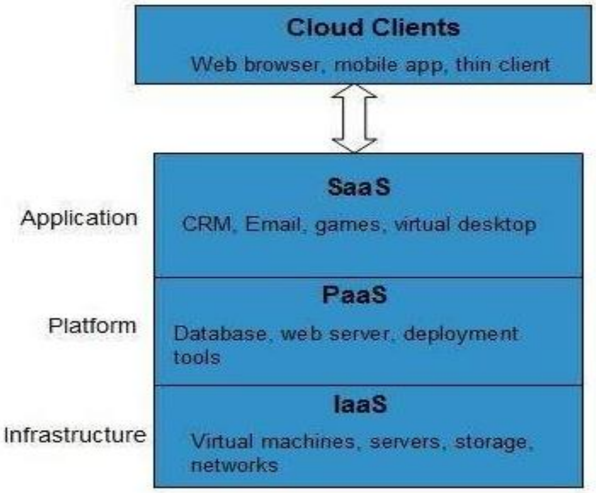

Cloud Clients
Web browser, mobile app, thin client
Application
SaaS
CRM, Email, games, virtual desktop
Platform
PaaS
Database, web server, deployment tools
Infrastructure
IaaS
Virtual machines, servers, storage, networks

Fig. 5.4: Service Models in cloud computing

5.4 Cloud Optimization and Business Analytics

All organizations must monitor their analytics, as data is crucial for them to collect, analyze, and interpret. However, with the rapid growth of technology, the volume and variety of data sources are increasing significantly. It becomes challenging to assess new data sources and identify valuable information without a flexible technology that can adapt to the evolving business needs and changing data landscape.

Enterprises have found a solution in the cloud—a versatile technology that can scale with the business and accommodate evolving requirements. Many businesses are reassessing their infrastructure to become more agile in comprehending the data they generate. Cloud technology provides the flexibility needed for businesses to move quickly and adapt to changes.

In the contemporary business landscape, organizations are shifting to the cloud for the analysis and interpretation of data in various domains, including HR, sales, marketing, and finance. This transition prompts the need to understand why the cloud is the optimal choice for business analytics. The characteristics that make cloud an ideal choice for business analytics are as follows:

Fast and flexible deployment

Ease of deployment is considered as one of the most important reasons to switch to cloud services.it is an even more influential factor than price. The cloud enables a quick start without need for additional hardware, configuration or installation. Host can share a panel and others can start with.

Highly Secure

It is another important reason why people are moving to the cloud. This is mainly because cloud service providers can monitor 24/8, make regular checks and threats assessments and a team that can deploy a new patch if needed. All these things would otherwise require additional expenses in the organization of the company's office setup.

Easy Mobile Access

The cloud solution can be accessed from anywhere without accessing the firewall; which means that business owners and their IT teams can access and benefit from a secure system and authentication management on the go.

Easy to sharing with customers and others outside the organization

Since there is no real requirement to access the firewall every time, the company can provide it third parties - including customers - can access and gain access to the cloud platform simply. For example, marketing companies use analytics to analyze campaign results and revenue in investments. This interpretation of the data is then used to make the right offers to customers and ensure that offers reach customers on time. Also, data analysis helps to predict what customers will react to next or in the near future.

5.5 Role of Cloud in IoT

IoT is incorporated into everyday items like consumer devices, vehicles, and buildings. It involves embedded software, sensors, electronics, and network connectivity, enabling these objects to exchange and gather data.

Despite its practicality, IoT poses a challenge by generating significant amounts of Big Data, putting strain on an organization's internet infrastructure. To handle the extensive data analysis needs, organizations turn to cloud computing. Cloud computing offers scalability in delivering enterprise applications and Software as a Service (SaaS). It is illustrated in Figure 5.5.

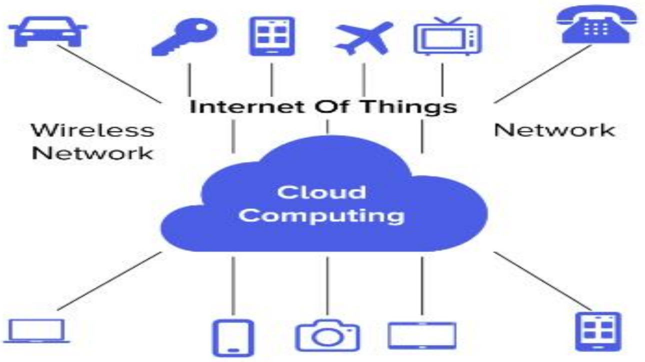


Fig.5.5: Integration of cloud computing in IoT

5.6 Advantages of Cloud in Internet of Things

Cloud computing involves accessing data and programs when needed from a centralized computing resource. On the other side, IoT (Internet of Things) connects various devices, beyond just computers, using software, sensors, and more. IoT enables cost-effective and intelligent device connections, facilitating real-time monitoring and control.

Despite their apparent differences, both IoT and cloud computing enhance efficiency in everyday tasks. They have a complementary relationship – while IoT generates vast amounts of Big Data, the cloud provides a pathway for that data. This makes it convenient for developers to access massive quantities of Big Data through the cloud. Cloud computing services typically follow a pay-per-use model, meaning businesses only pay for the resources they use. This approach helps IoT companies achieve economies of scale by minimizing overall infrastructure costs. Cloud computing also benefits IoT through improved data collaboration and user-friendliness. The cloud allows IoT developers to access and store data remotely or on the go, saving time and labor.

5.7 IoT Cloud Framework

The placement of connected devices, applications, storage, power, and intelligence is transitioning from traditional endpoints like desktop computers and laptops to cloud systems. Cloud-based services offer platforms for deploying and overseeing IoT applications, as well as gathering, storing, and analyzing data from smart, connected product endpoints. These platforms offer scalability and convenient access to third-party applications and services.

The IoT cloud serves as a platform capable of running applications and storing data on the Internet. It utilizes distinct technology; for instance, Microsoft's cloud platform operates Windows Azure instead of Windows Server. The Figure 5.6 shows the Azure framework.

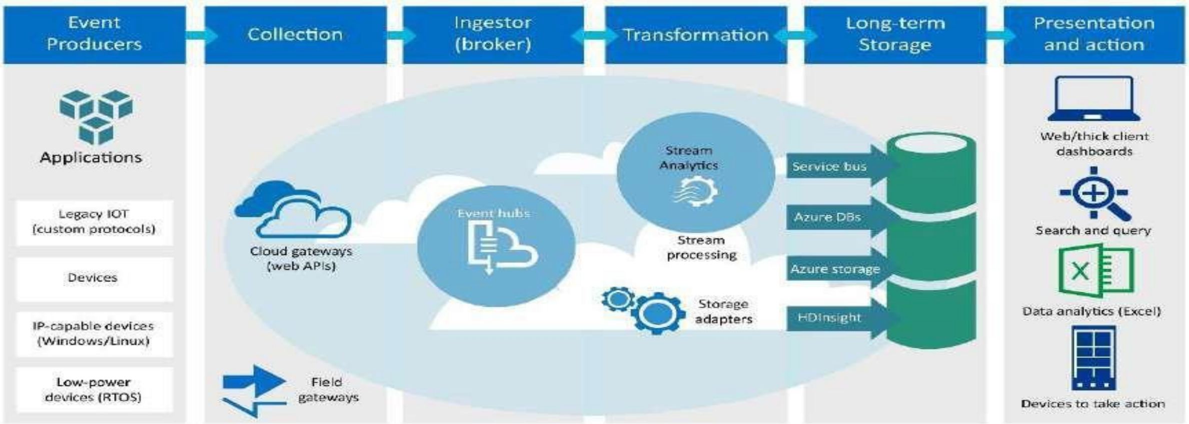


Fig. 5.6: Azure framework

Microsoft Azure Stream Analytics is a cloud service designed for processing data in real-time. It facilitates real-time computations on data streaming from diverse devices, applications, and sensors. With support for high-level languages like sequential query language (SQL), it simplifies the logic required for real-time actions. This service aids in monitoring and gaining analytical insights from a variety of devices, including mobile phones and connected cars.

Practical activity 5.1: To design GAS-level monitoring system using cloud.

Material Required: ESP32 board, MQ-2 gas sensor, Buzzer, LCD screen, I2C module, Breadboard, Jumper wires

Procedure:

Step 1. Collect all the components as given in the description.

Step 1. Connect the ESP32 board to the adapter. If adapter is not available, use two breadboards together. It is shown in Figure 5.5.

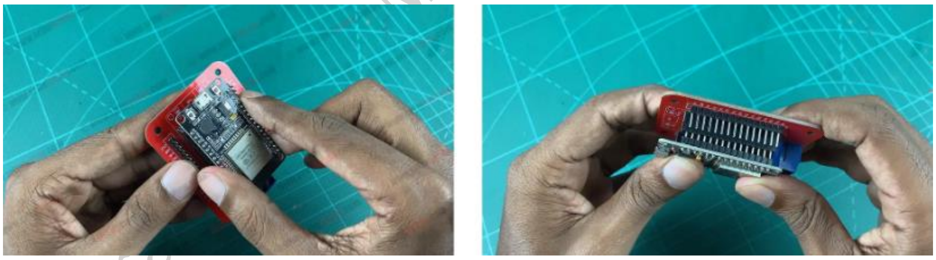


Fig. 5.7: ESP32 board to the adapter connection

Step 3. Now place the MQ-2 sensor and buzzer on the mini breadboard. And then, connect these components to the ESP32 board. For that, use the circuit diagram given in Figure 5.8.

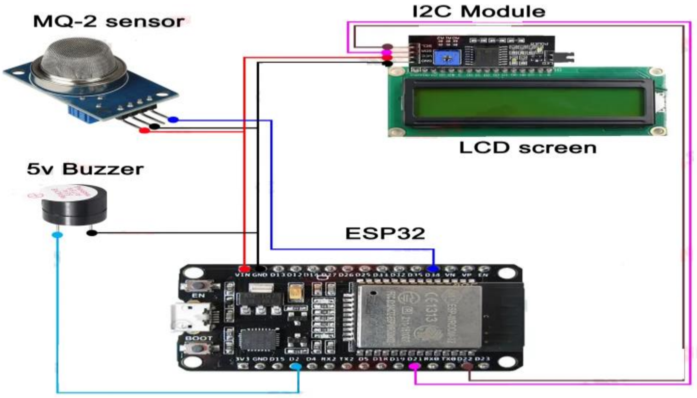


Fig.5.8: circuit diagram

These connections are shown in Figure 5.9.

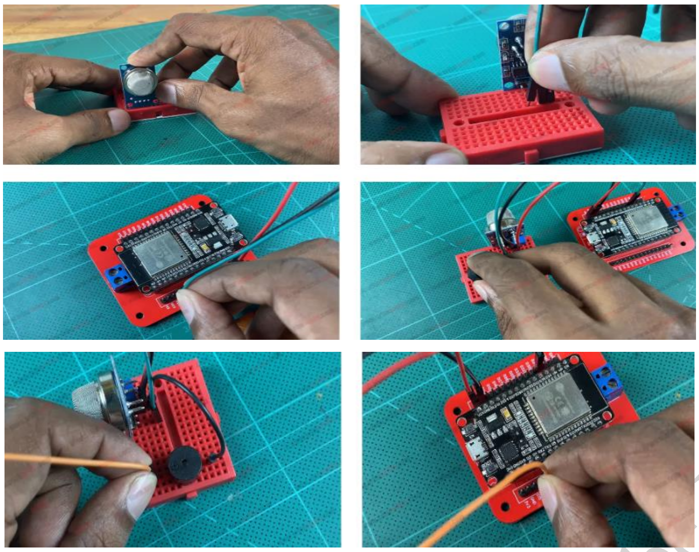


Fig.5.9 Connections of components

Step 4. Now connect the LCD screen to the ESP32 board as shown in Figure 5.10.

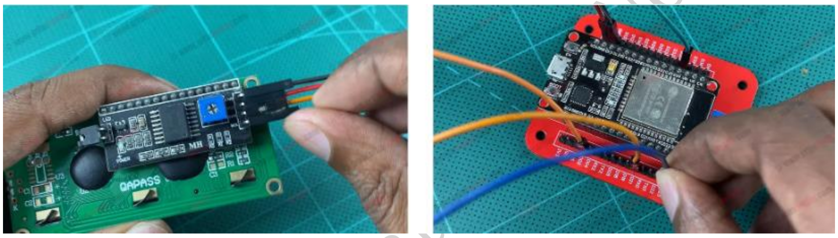
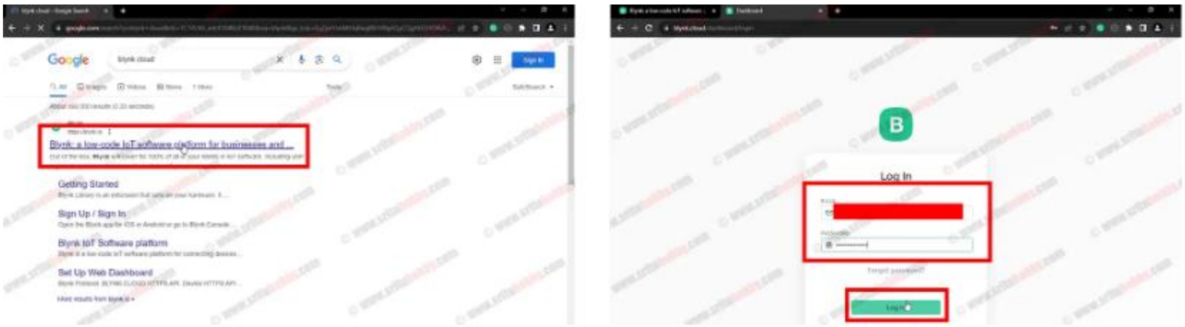


Fig.5.10: Connection of LCD screen to the ESP32 board

Step 5. Next, set up the Blynk web dashboard step by step. For that, follow the instructions below.

First, go to the Blynk official website and create a new account. Then, log in to your account as shown in screenshot in Figure 5.11.



Blynk: a low-code IoT software platform for businesses and ...

Getting Started

Sign Up / Sign In

Blynk IoT Software platform

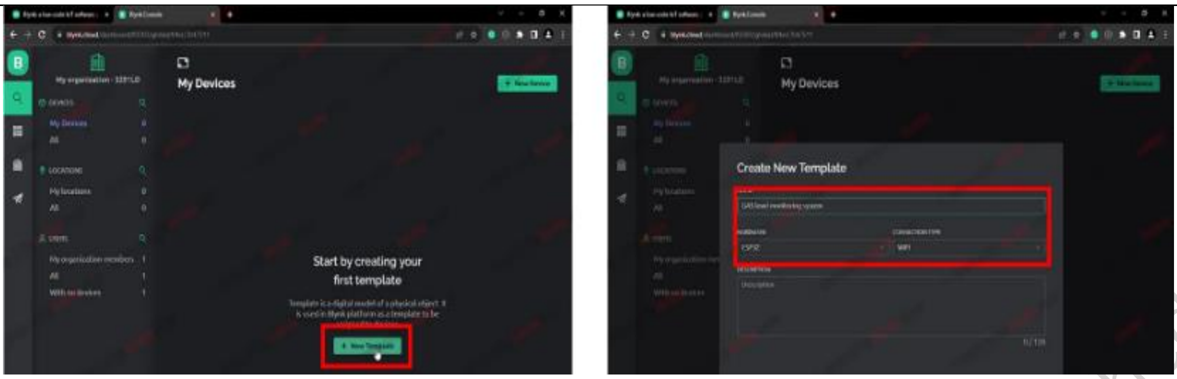
Set Up Web Dashboard

Log In

Forgot password?

Fig.5.11: Blynk web dashboard

Next, create a new template. For that, select the device as ESP32 and name it as you like. Here it is named as "GAS-level monitoring system" as shown in screenshot in Figure 5.11.



- **Fig.5.12: GAS-level monitoring system" Blynk web dashboard**

Now, click the data streams tab and create two virtual pins as shown in Figure 5.13.

Virtual Pin > Name – GAS Level / PIN – V0 / MIN – 0 / MAX – 100

Virtual Pin > Name – Warning LED / PIN – V1 / MIN – 0 / MAX – 1

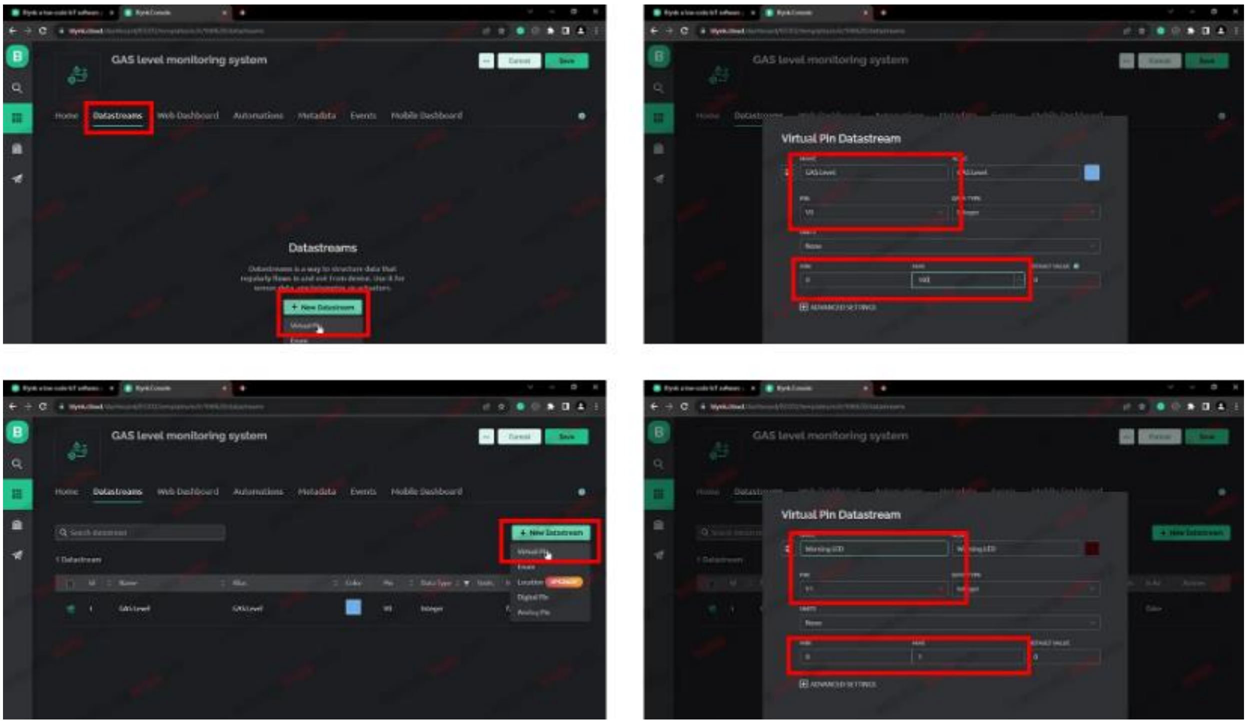
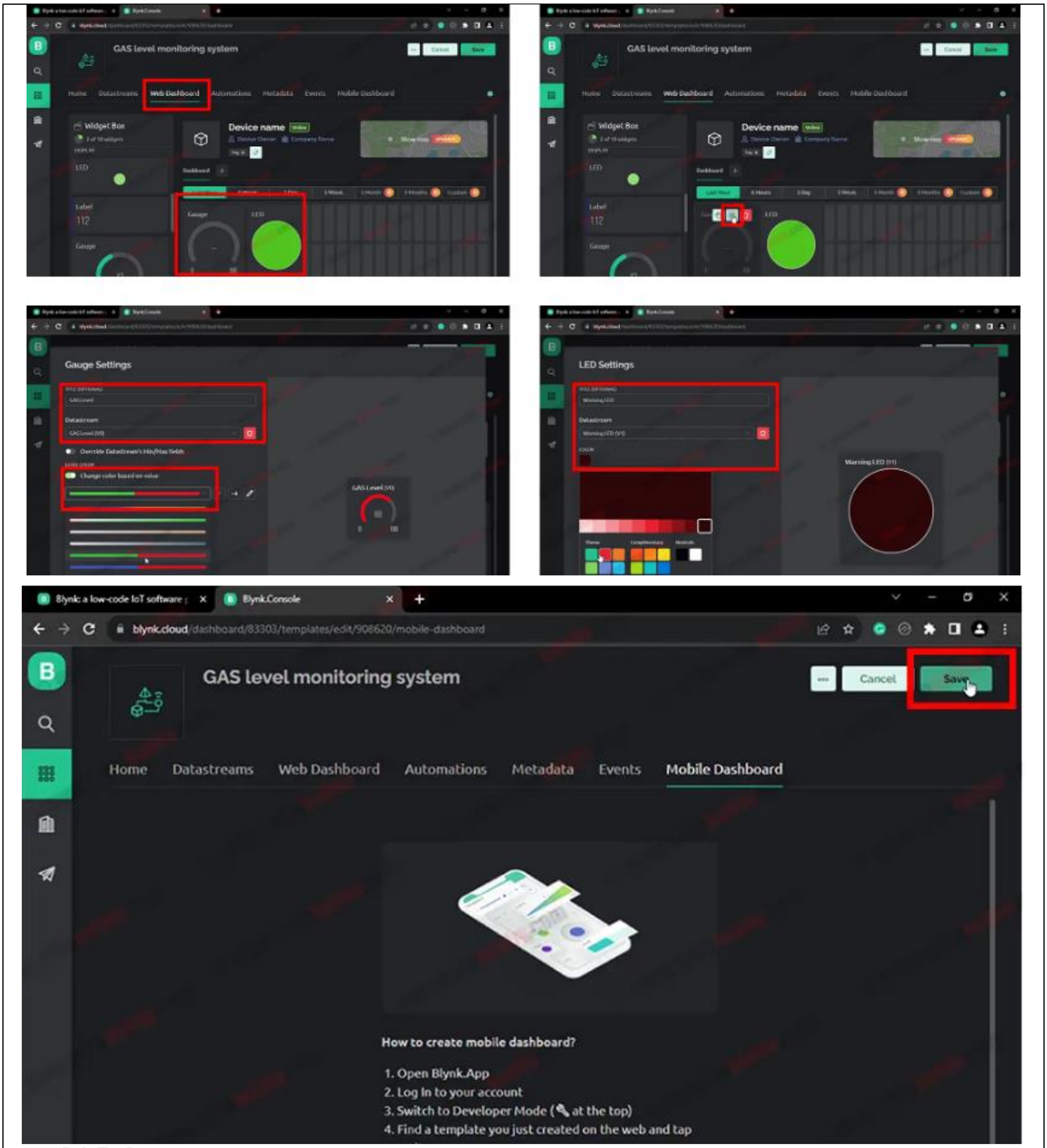


Fig.5.13: datastreams tabs on Blynk web dashboard

Next, click the Web dashboard tab and drag and drop one-gauge widget and one LED widget to the dashboard.

Then, click the one-by-one setting icons and select the Data Stream that is created earlier. Also, you can change colors as you like. It is shown in Figure 5.14.

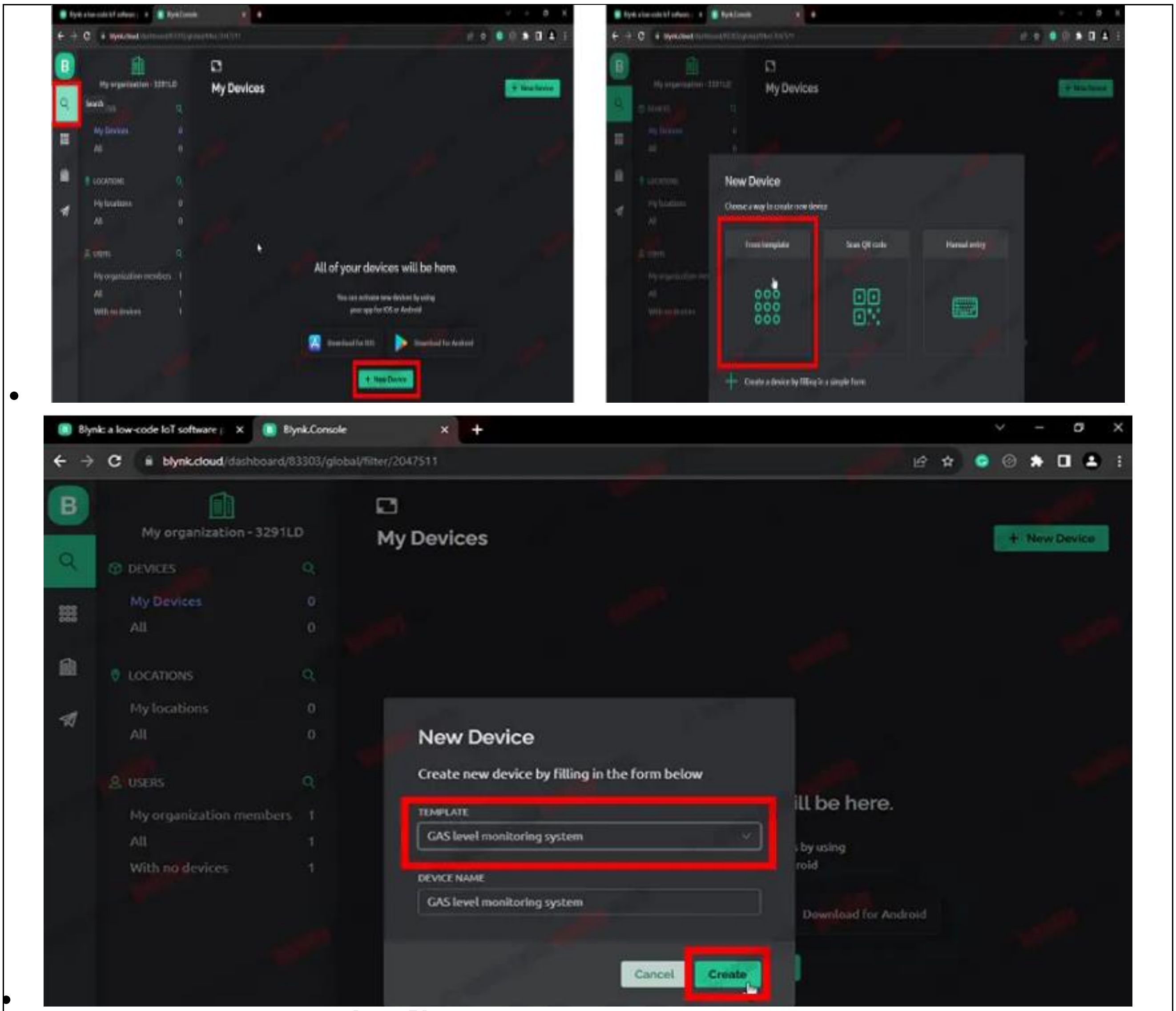


How to create mobile dashboard?

1. Open Blynk.App
2. Log In to your account
3. Switch to Developer Mode (🔧 at the top)
4. Find a template you just created on the web and tap

Fig.5.14: GAS-level monitoring system" Blynk web dashboard settings

Now, click the search icon button and create a new device. For that, select the template you created earlier. Then, you can see the Blynk auth token of this project. It is shown in Figure 5.15.



New Device

Create new device by filling in the form below

TEMPLATE: GAS level monitoring system

DEVICE NAME: GAS level monitoring system

Fig.5.15: Blynk dashboard ready to use.

Now, the Blynk dashboard is ready to use.

Step 6. Next, set up the Blynk mobile dashboard. For that, follow the instructions below.

First, download and install the Blynk app on your smartphone. Then, log in to your account using your email and password.

Next, click the template and add one gauge widget and one LED widget to the dashboard. Next, customize these widgets as you like.It is shown in Figure 5.16.

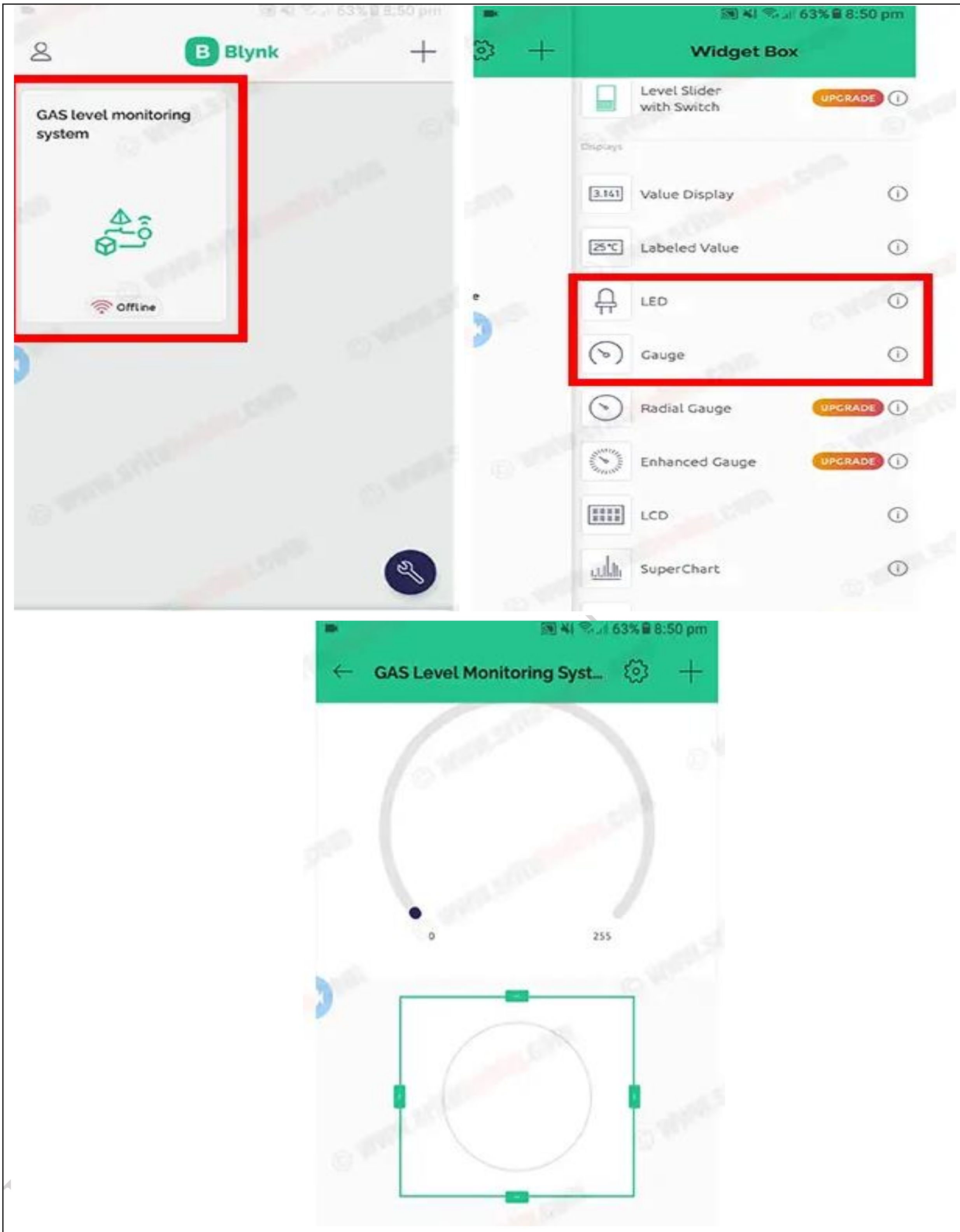
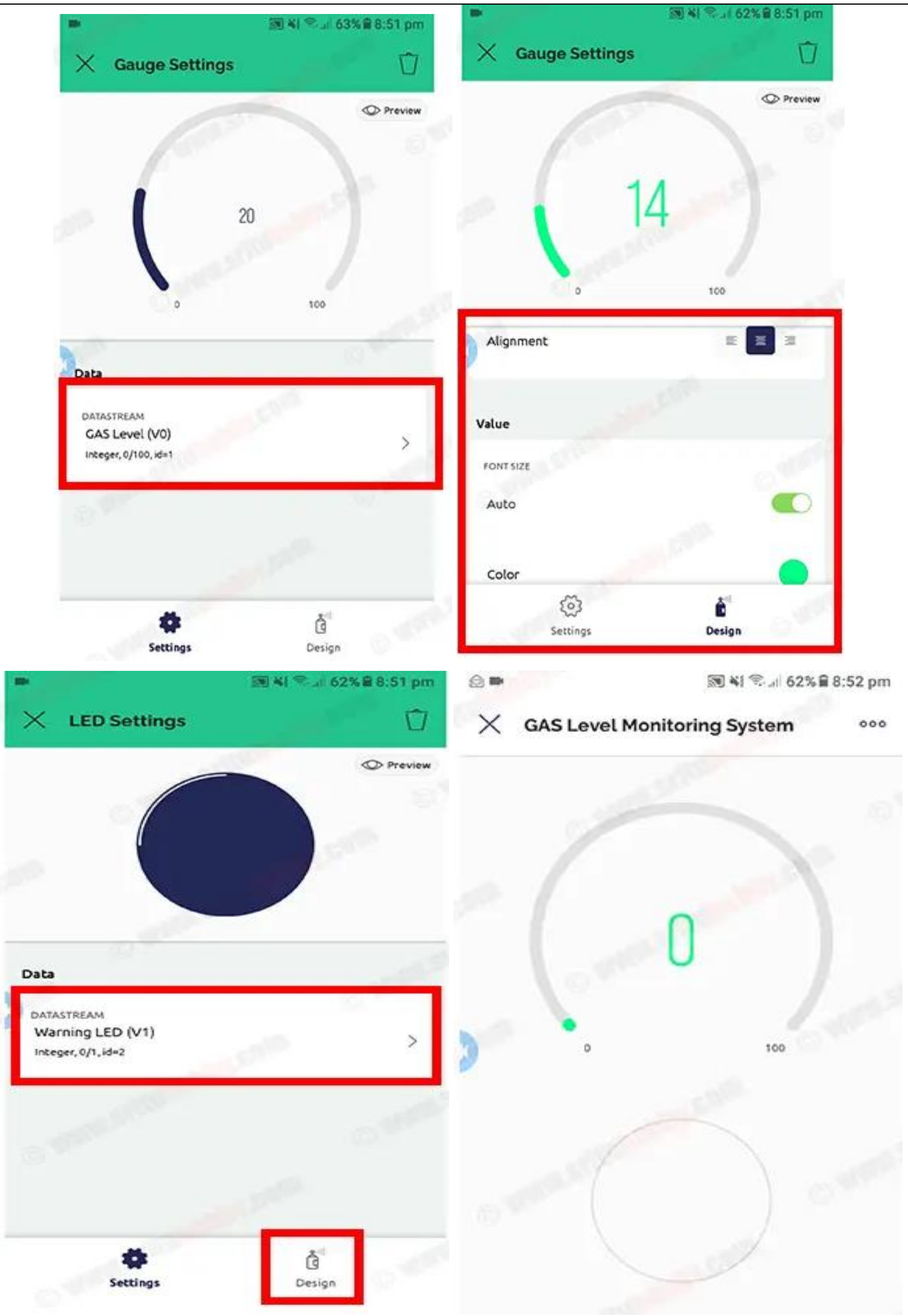


Fig.5.16: Blynk mobile dashboard

Then click one-by-one widget and select the data streams created on the web dashboard. Also, you can change the colors as you like as shown in Figure 5.15.



DATASTREAM
GAS Level (V0)
Integer, 0/100, id=1

DATASTREAM
Warning LED (V1)
Integer, 0/1, id=2

Fig.5.17: Blynk mobile dashboard

Now, Blynk mobile dashboard is ready to use.

Step 5. Now, set up the program for this project. For that, connect the ESP32 board to the computer as shown in Figure 5.18.

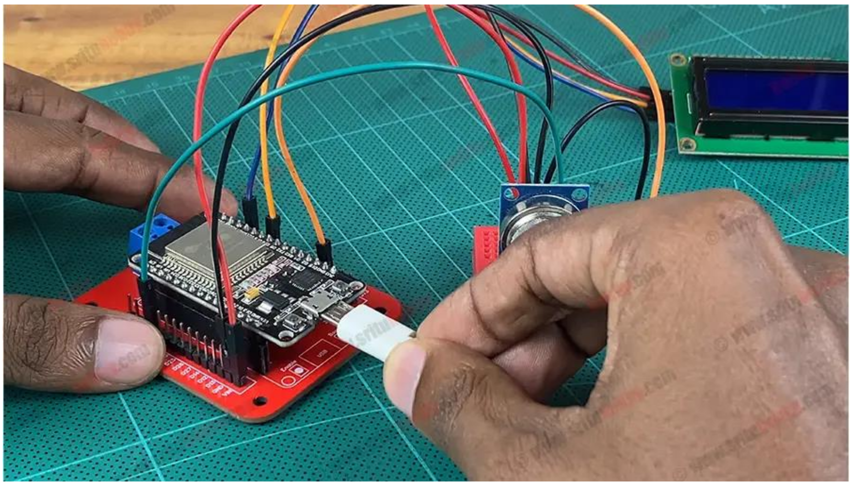
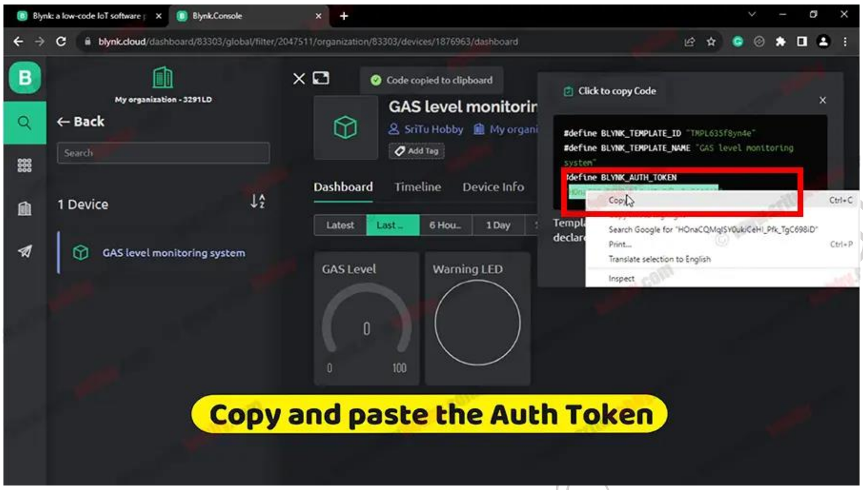


Fig.5.18: Connection of the ESP32 board to the computer

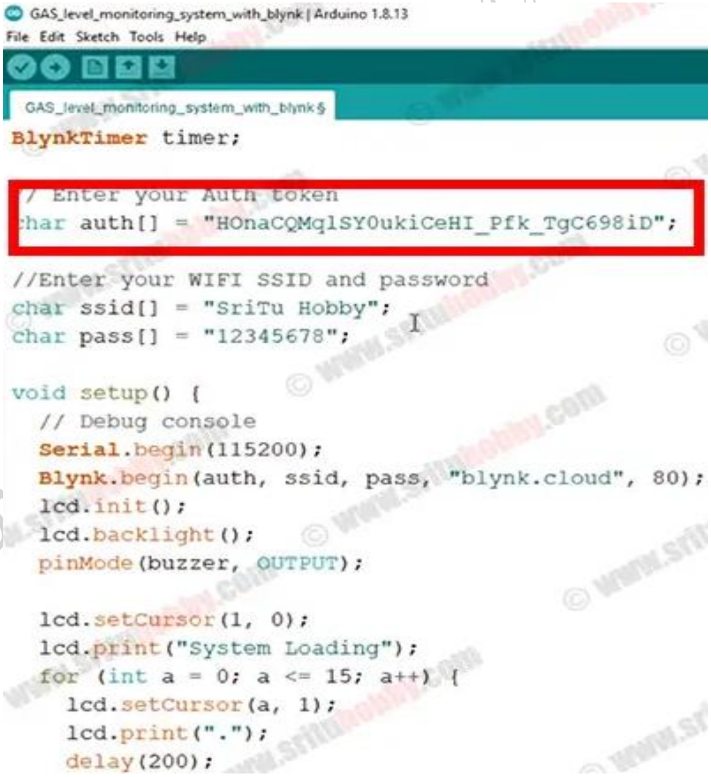
Step 8. Next copy and paste following program to the Arduino IDE.Then, install the I2C and Blynk libraries on the Arduino IDE.

```
//Include the library files
#include <LiquidCrystal_I2C.h>
#include <Wire.h>
#include <WiFiClient.h>
#include <BlynkSimpleEsp31.h>

#define sensor 34
#define buzzer 2

//Initialize the LCD display
LiquidCrystal_I2C lcd(0x27, 16, 2);

BlynkTimer timer;

// Enter your Auth token
char auth[] = "************";

//Enter your WIFI SSID and password
char ssid[] = "************";
char pass[] = "***********";

void setup() {
  // Debug console
  Serial.begin(115200);
  Blynk.begin(auth, ssid, pass, "blynk.cloud", 80);
  lcd.init();
  lcd.backlight();
  pinMode(buzzer, OUTPUT);

  lcd.setCursor(1, 0);
  lcd.print("System Loading");
  for (int a = 0; a <= 15; a++) {
    lcd.setCursor(a, 1);
    lcd.print(".");
    delay(200);
  }
  lcd.clear();
}
//Get the ultrasonic sensor values
void GASLevel() {
  int value = analogRead(sensor);
  value = map(value, 0, 4095, 0, 100);

  if (value >= 50) {
    digitalWrite(buzzer, HIGH);
    lcd.setCursor(0, 1);
    lcd.print("Warning!  ");
    WidgetLED LED(V1);
    LED.on();
  } else {
    digitalWrite(buzzer, LOW);
    lcd.setCursor(0, 1);
    lcd.print("Normal   ");
    WidgetLED LED(V1);
    LED.off();
  }

  Blynk.virtualWrite(V0, value);
  Serial.println(value);
  lcd.setCursor(0, 0);
  lcd.print("GAS Level :");
  lcd.print(value);
  lcd.print(" ");
}

void loop() {
  GASLevel();
  Blynk.run();//Run the Blynk library
  delay(200);
}
```

Step 9. Now copy and paste the Blynk Auth token into this program. It's included in the Blynk web dashboard. Then, enter your WIFI SSID and password as shown in Figure 5.19.

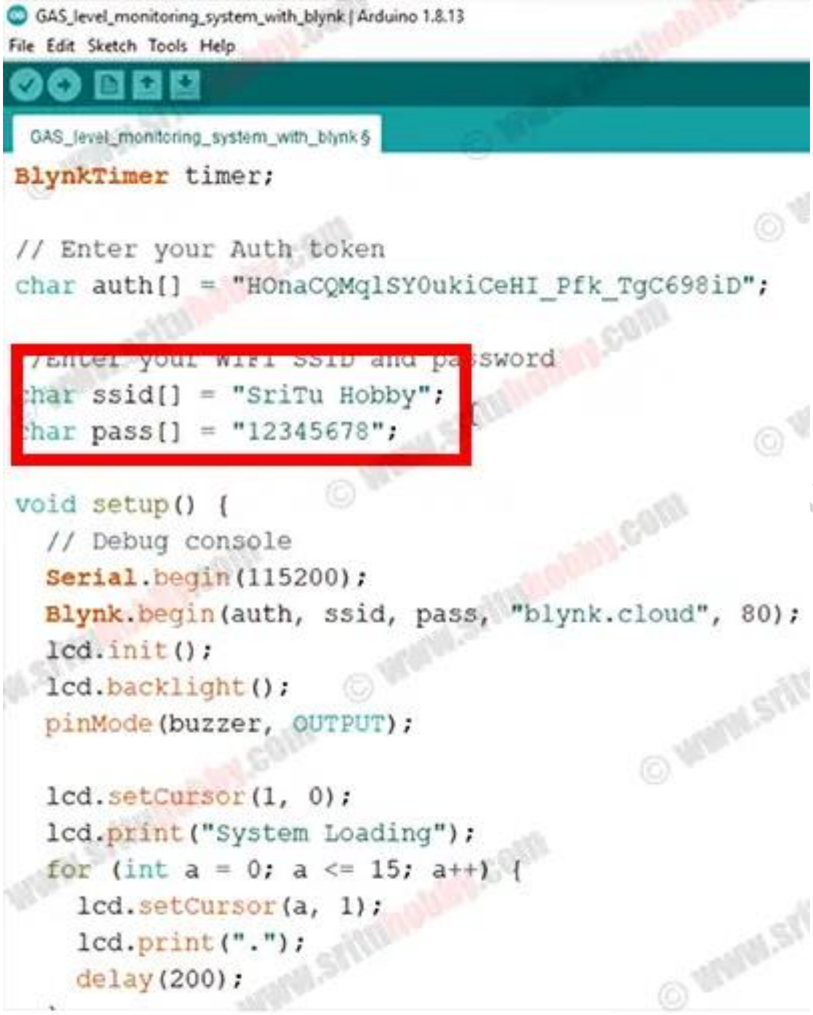


```
#define BLYNK_TEMPLATE_ID "TMPL635f8yn4e"
#define BLYNK_TEMPLATE_NAME "GAS level monitoring system"
#define BLYNK_AUTH_TOKEN
```



GAS_level_monitoring_system_with_blynk | Arduino 1.8.13
File Edit Sketch Tools Help
GAS_level_monitoring_system_with_blynk §

```
BlynkTimer timer;

// Enter your Auth token
char auth[] = "HOnaCQMqlSY0ukiCeHI_Pfk_TgC698iD";

//Enter your WIFI SSID and password
char ssid[] = "SriTu Hobby";
char pass[] = "12345678";

void setup() {
  // Debug console
  Serial.begin(115200);
  Blynk.begin(auth, ssid, pass, "blynk.cloud", 80);
  lcd.init();
  lcd.backlight();
  pinMode(buzzer, OUTPUT);

  lcd.setCursor(1, 0);
  lcd.print("System Loading");
  for (int a = 0; a <= 15; a++) {
    lcd.setCursor(a, 1);
    lcd.print(".");
    delay(200);
```



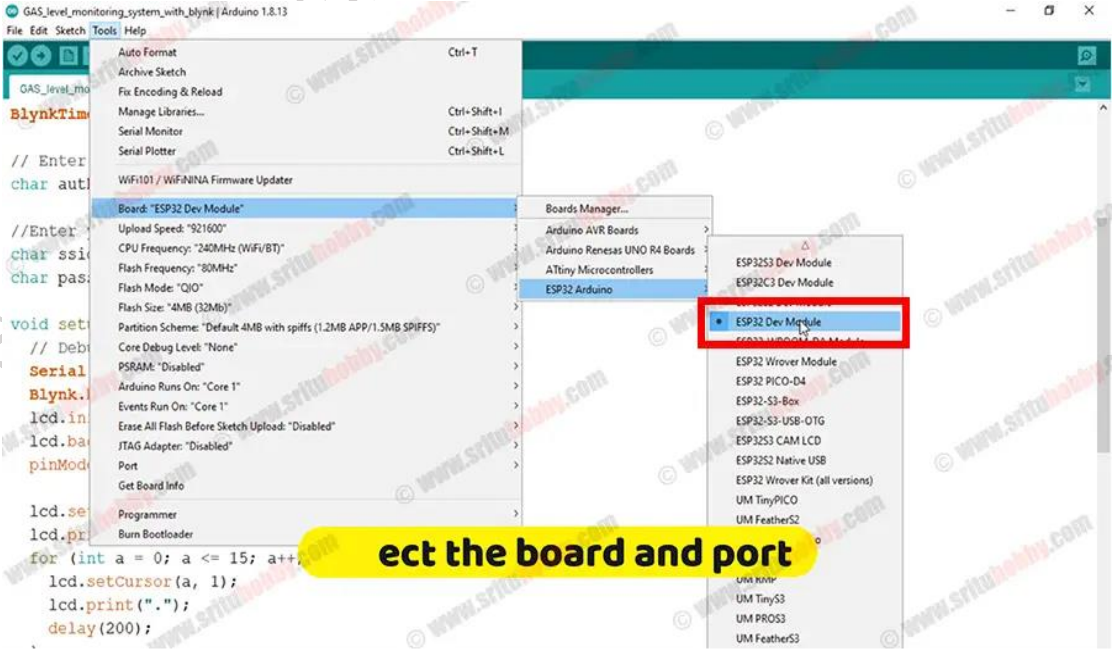
GAS_level_monitoring_system_with_blynk | Arduino 1.8.13

```
BlynkTimer timer;

// Enter your Auth token
char auth[] = "HOnaCQMqlSY0ukiCeHI_Pfk_TgC698iD";

/Enter your WiFi SSID and password
har ssid[] = "SriTu Hobby";
har pass[] = "12345678";

void setup() {
  // Debug console
  Serial.begin(115200);
  Blynk.begin(auth, ssid, pass, "blynk.cloud", 80);
  lcd.init();
  lcd.backlight();
  pinMode(buzzer, OUTPUT);

  lcd.setCursor(1, 0);
  lcd.print("System Loading");
  for (int a = 0; a <= 15; a++) {
    lcd.setCursor(a, 1);
    lcd.print(".");
    delay(200);
```

File Edit Sketch Tools Help
GAS_level_monitoring_system_with_blynk §

Fig.5.19: Blynk Auth token copied in program

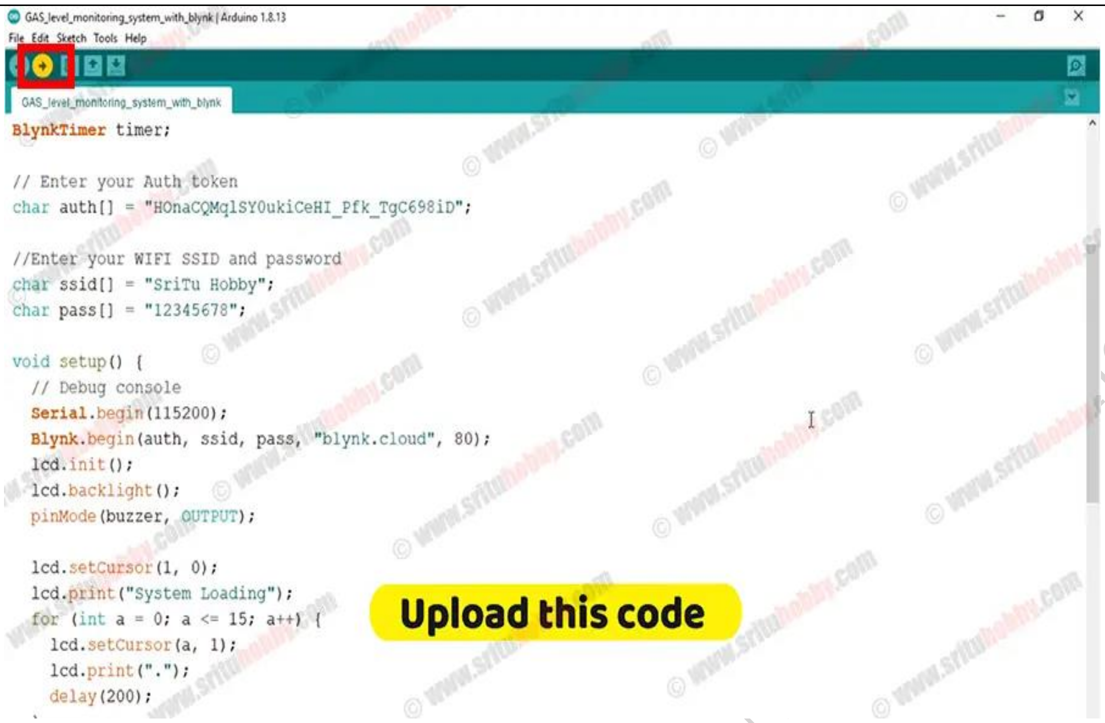
Step 10. Next, select the board and port. After, click the upload button as shown in Figure 5.20.



GAS_level_monitoring_system_with_blynk | Arduino 1.8.13

Board: "ESP32 Dev Module"
Upload Speed: "921600"
CPU Frequency: "240MHz (WiFi/BT)"
Flash Frequency: "80MHz"
Flash Mode: "QIO"
Flash Size: "4MB (32Mb)"
Partition Scheme: "Default 4MB with spiffs (1.2MB APP/1.5MB SPIFFS)"
Core Debug Level: "None"
PSRAM: "Disabled"
Arduino Runs On: "Core 1"
Events Run On: "Core 1"
Erase All Flash Before Sketch Upload: "Disabled"
JTAG Adapter: "Disabled"

```
BlynkTim
// Enter
char aut
//Enter
char ssi
char pas
void set
  // Deb
  Serial
  Blynk.
  lcd.in
  lcd.ba
  pinMod
  lcd.se
  lcd.pr
  for (int a = 0; a <= 15; a++
    lcd.setCursor(a, 1);
    lcd.print(".");
    delay(200);
```


GAS_level_monitoring_system_with_blynk | Arduino 1.8.13
File Edit Sketch Tools Help
GAS_level_monitoring_system_with_blynk
Upload this code

```
BlynkTimer timer;

// Enter your Auth token
char auth[] = "HOnaCQMqlSYOukiCeHI_Pfk_TgC698iD";

//Enter your WIFI SSID and password
char ssid[] = "SriTu Hobby";
char pass[] = "12345678";

void setup() {
  // Debug console
  Serial.begin(115200);
  Blynk.begin(auth, ssid, pass, "blynk.cloud", 80);
  lcd.init();
  lcd.backlight();
  pinMode(buzzer, OUTPUT);

  lcd.setCursor(1, 0);
  lcd.print("System Loading");
  for (int a = 0; a <= 15; a++) {
    lcd.setCursor(a, 1);
    lcd.print(".");
    delay(200);
```

Fig.5.20: select the board and port for uploading

Step 11. Now to test the circuit, power up this circuit and bring the GAS source close to the sensor. For example, a lighter can be used for testing it as shown in Figure 5.21.

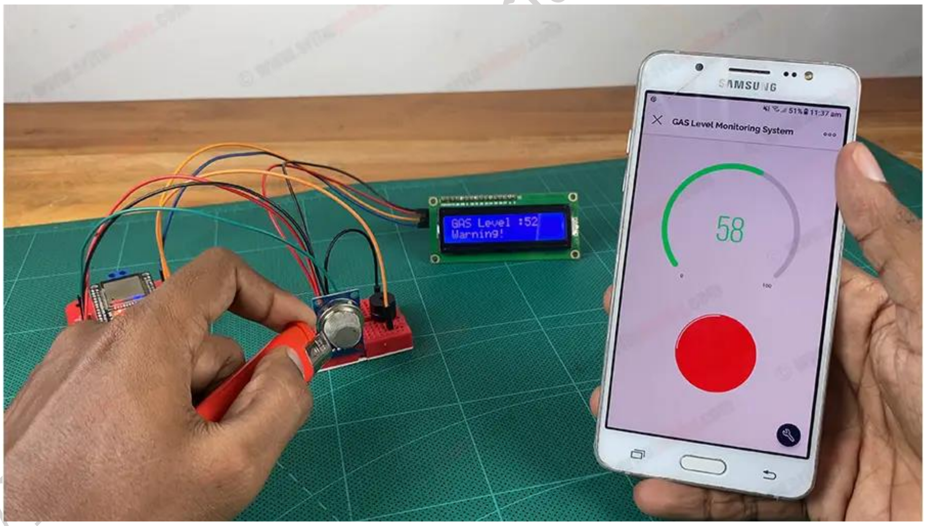


Fig.5.21: testing of the gas level monitoring circuit

Summary

- This chapter explores the collaboration between IoT and Cloud Computing, emphasizing how cloud services efficiently process and store data from connected devices.
- It covers key characteristics of cloud computing, deployment models, and highlights the advantages of cloud in IoT, including rapid deployment and enhanced security.
- This chapter also provide practical implementation of cloud for better understanding.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the primary purpose of IoT (Internet of Things)? (a) Connecting devices to the Internet for entertainment purposes (b) Connecting devices to the Internet to provide services they're designed for (c) Storing and managing data on local drives (d) Offline communication between devices
2. How is cloud computing related to IoT? (a) It has no relation to IoT (b) It hinders the development of control devices (c) Cloud computing handles local data processing for IoT (d) Cloud computing is not mentioned in the context of IoT
3. What does the term "cloud" refer to in cloud computing? (a) A visible mass of water droplets (b) A network or the internet (c) A physical data storage device (d) A computing device on the edge of the network
4. Which deployment model in cloud computing is suitable for businesses with dynamic or unpredictable computing needs? (a) Public cloud (b) Private cloud (c) Community cloud (d) Hybrid cloud
5. In cloud computing, what does IaaS (Infrastructure-as-a-Service) involve? (a) Delivering complete software to clients (b) On-demand availability of computing resources over the internet (c) Tailored development and customization of applications (d) Monitoring and interpreting data for business analytics
6. What is one of the advantages of cloud computing in the context of IoT? (a) Increased dependence on local storage (b) Higher infrastructure costs (c) Delayed data collaboration (d) Scalability and cost-effectiveness in handling Big Data generated by IoT
7. What does the IoT cloud framework involve? (a) Traditional endpoints like desktop computers (b) Cloud services with no role in IoT (c) Platforms for deploying and overseeing IoT applications (d) Storage of data only on local devices
8. Which cloud service is mentioned for processing real-time data in the provided content? (a) Google Apps (b) Microsoft Azure Stream Analytics (c) Salesforce (d) Apparenda
9. What is the characteristic of cloud computing that involves tracking resource usage for each application and user? (a) On-demand self-services (b) Broad network access (c) Rapid elasticity (d) Measured service
10. Why do businesses consider cloud technology for business analytics? (a) To increase infrastructure costs (b) To slow down data analysis (c) For fast and flexible deployment (d) To limit access to data for third parties

B. Fill in the blanks

1. In cloud computing, IT resources are shared between multiple applications and used on a __________ basis, known as resource pooling.
2. Rapid elasticity in cloud computing refers to IT resources that can be scaled quickly as __________.
3. The public cloud is easily accessible to the general public and is operated by __________ providers.
4. The hybrid cloud combines elements of both private and public clouds, ideal for managing __________ workloads.
5. Platform-as-a-Service (PaaS) is tailored for development, simplifying the development, testing, and deployment of __________.
6. Software-as-a-Service (SaaS) delivers complete software to clients as a service, offering pre-configured hardware resources through a __________ interface.

7. Highly secure cloud services involve continuous monitoring, regular checks, threat assessments, and a team that can deploy __________ if needed.
8. IoT involves embedding software, sensors, electronics, and network connectivity in everyday items to enable them to exchange and gather __________.
9. The IoT cloud framework involves transitioning from traditional endpoints like desktop computers to __________ systems.
10. Microsoft Azure Stream Analytics is a cloud service designed for processing data in __________, simplifying the logic required for real-time actions.

C. State True or false for the following

1. IoT stands for connecting devices to the Internet to provide services they are designed for, involving storing and processing data.
2. Cloud computing uses local servers on the internet to store, manage, and access data online.
3. Cloud storage helps keep data offline, offering advantages by providing services locally.
4. Broad network access in cloud computing involves providing computing services over specific networks and client platforms.
5. Measured service in cloud computing involves tracking resource usage for each application but not for users.
6. The private cloud is easily accessible to the general public and is operated by external providers.
7. In the community cloud model, resources are not shared among multiple organizations, preventing collaboration.
8. Software-as-a-Service (SaaS) delivers complete software to clients, including an Operating System.
9. Fast and flexible deployment is considered less important than price when switching to cloud services.
10. Cloud computing involves accessing data and programs locally from a decentralized computing resource.

D. Short answer type questions

1. What does IoT stand for, and what is its primary purpose in the context of connecting devices to the Internet?
2. Define the concept of "On-demand self-services" in cloud computing.
3. How does cloud computing achieve "Broad network access," and what platforms can be used for accessing computing services?
4. How does the private cloud differ from the public cloud, and for what type of organizations is it suitable?
5. What is the community cloud model, and how does it foster collaboration among organizations?
6. Differentiate between Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS), and Software-as-a-Service (SaaS).
7. Discuss the importance of the highly secure nature of cloud services, particularly in terms of monitoring and threat assessments.
8. What components are involved in IoT, and how do they enable devices to exchange and gather data?
9. How does cloud computing assist in handling the extensive data analysis needs generated by IoT?
10. How does cloud computing benefit IoT through a pay-per-use model, and what does it help IoT companies achieve?

Module 3 Installation of IoT Devices

Module Overview

This Module explores the foundational aspects of implementing Internet of Things (IoT) solutions. In this Module, the intricacies of setting up the hardware components that form the backbone of an IoT ecosystem are discussed. The Module explores key topics such as the Framework for Internet of Things, establishing communication between nodes, gateways, and servers, pre-installation preparation of IoT devices, mounting devices at desired locations, and performing checks and connections to ensure a seamless and robust deployment.

It encompasses the establishment of a robust IoT framework, emphasizing the criticality of communication between nodes, gateways, and servers. Through this Module, students will gain proficiency in undertaking pre-installation preparations for IoT devices, a crucial step in ensuring the smooth deployment of IoT solutions. This foundational knowledge provides the necessary groundwork for successful hardware installations in various IoT applications.

Moreover, students will learn the art of strategically mounting IoT devices at desired locations, by considering factors like accessibility, environmental conditions, and security. The Module also presents a comprehensive understanding of the essential checks and connections that need to be performed to guarantee the optimal functionality of the installed hardware.

These skills are instrumental in enabling students to contribute effectively to the deployment of IoT solutions across a range of industries and applications. Overall, this Module lays a solid foundation for the practical implementation of IoT hardware installations.

Learning Outcomes

After completing this module, you will be able to:

- Understand the framework and architecture of Internet of Things (IoT) systems.
- Establish effective communication between nodes, gateways, and servers.
- Perform necessary pre-installation preparations for setting up IoT devices.
- Mount IoT devices accurately at specified or desired locations.
- Carry out proper checks and make reliable connections of IoT devices.

Module Structure

Session 1. Framework for Internet of Things

Framework for the Internet of Things serves as a structured and organized approach to building, deploying, and managing IoT solutions. This framework provides a comprehensive structure for connecting and coordinating a multitude of devices, sensors, and platforms, ensuring they work harmoniously to collect, process, and communicate data. In essence, it acts as a blueprint, empowering developers and organizations to navigate the complexities of the IoT ecosystem with greater efficiency and effectiveness.

1.1 Basic Steps for Installing the IoT Framework

A technician needs to understand the requirements of the site by analysing the framework in order to create a functional IoT framework. The IoT framework includes many parameters like the type of IoT device, gateways, nodes, types of connection between IoT devices, communication channels, and database management. The Figure 1.1 shows the basic hardware installation steps:

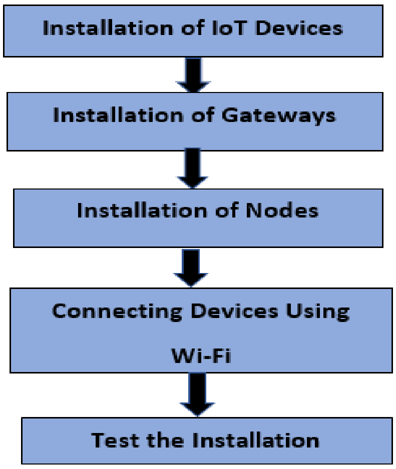


Fig. 1.1: IoT Installation Framework

1.2 Installation of IoT Devices

Motion sensor is one of the sensors which is used to implement IoT devices. It is used in an alarm system. The sensor activates when it detects an object or someone nearby. The Figure 1.2 depicted the motion sensor.

Fig. 1.2: Motion sensor

The following are the basic steps for installing a framework for a sensor:

1. Identify the suitable points or locations
2. Mount the sensor
3. Connect the sensor to the power source
4. Connect the sensor to the system
5. Configure and install the sensor

1.1.1 Identification of Suitable Points or Locations

It is very important to find a suitable location for the access points of the sensors. The access points must be located in places where they are not easily accessible and not easy to damage and covers maximum of the target area. In general, to keep an IoT system secure the criteria to be taken into consideration are as shown below:

1. The sensor devices should be installed in such locations that their operational requirements such as temperature fluctuations, humidity, or static electricity are met.
2. Proper protection of the sensor devices from weather elements, incidental damage, and theft must be considered.
3. The process to be monitored must be considered and compatibility of the sensor material with the environment must be verified. It is illustrated in Figure 1.3.

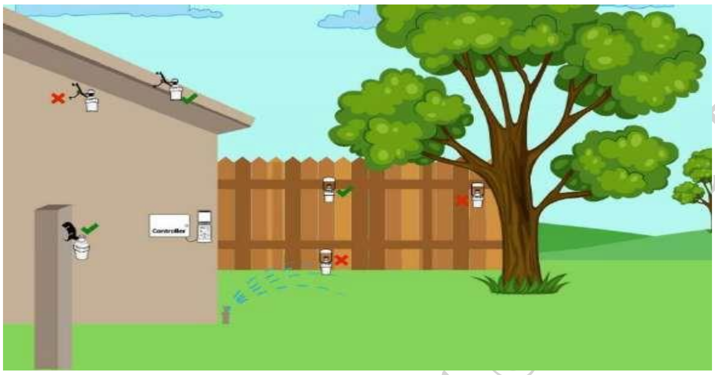


Fig. 1.3: Suitable location for outdoor sensors

1.1.2 Mount the Sensor

A sensible area for the scope of the motion sensor must be considered for mounting a sensor on a wall or ceiling as shown in Figure 1.4.

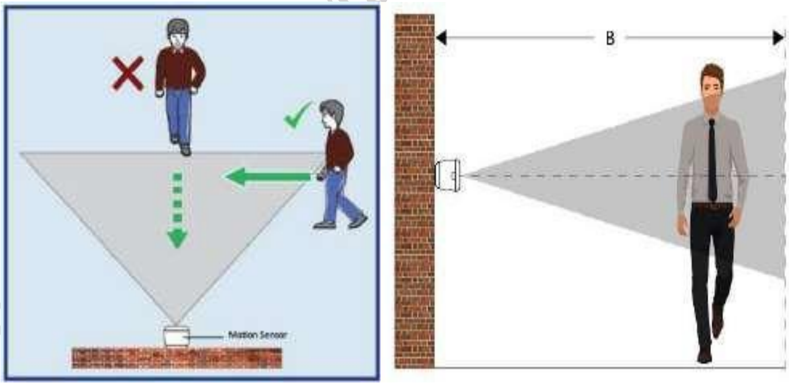


Fig.1.4: Scope of a motion sensor

The mounting can be done using an adhesive or using the knockout holes on the unit's base.

Steps for mounting a sensor

Step 1. Remove the cover by unscrewing the cover.

Step 1. Open any recessed knockout hole.

Step 3. Fix the base on the wall.

Step 4. Place the cover and tighten it with a screw.

Some key points that should be kept in mind while installation are as follows:

- The sensor must be attached to a stable surface that can support the weight.
- The sensor should not be attached to soft material as it may fall, break and cause injury.

- The motion sensor should not be attached to any of the surfaces as shown in the following Figure 1.5.

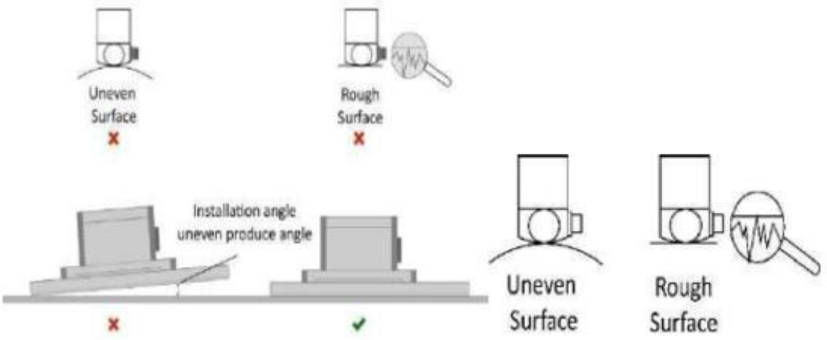


Fig. 1.5: Suitable and unsuitable surfaces for mounting

1.1.3 Connect the Sensor to the Power Source

The adapter that is already attached to the motion sensor should be plugged into a power source.

If the sensor is battery-controlled, then the steps to be adhered to are as follows:

Open the battery cover by using a flathead screwdriver as shown in the Figure 1.6.

Fig.1.6: Opening the battery cover

Install the battery according to the indicated polarity as shown in the Figure 1.7.

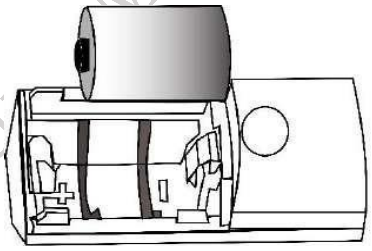


Fig.1.7: Installing the battery

The sensors can be connected to the mains or to the utility using cables also. The Figure 1.8 shows the connection of multiple sensors to the power supply.

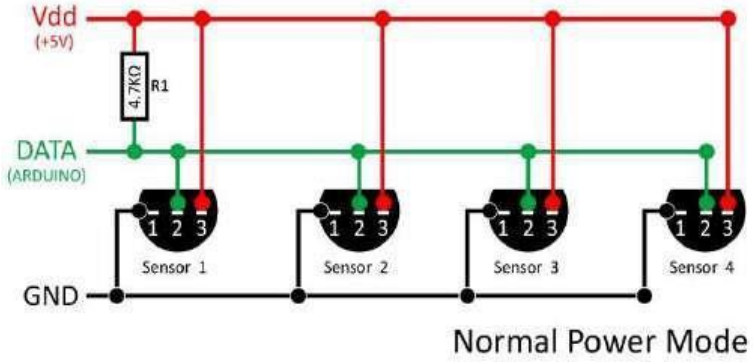


Fig.1.8: Schematic diagram of sensor connectivity to the power supply

1.1.4 Connect the Sensor to the System

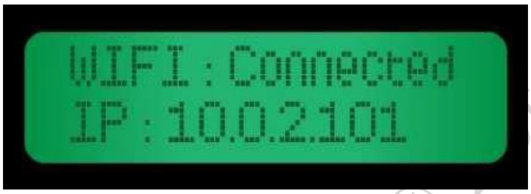
The motion sensors come with a speaker cable. The other end of the cable must be attached to the switch port of the alarm system. The sensors can be connected to the alarm system wirelessly via Wi-Fi or Bluetooth network.

1.1.5 Configure and Install the Sensor

The motion sensor needs to be joined to the network. This can be done by configuring the sensor by referring to the instructions given on the computer software of the system, the web portal, or a smartphone application.

The technician needs to ensure that all the sensors are connected before the power is on. Then, he/she should:

- Switch on the power supply.
- Check that the power is detected in the sensor.
- Check the network status shown on the display as shown in the Figure 1.9.



```
WIFI : Connected
IP : 10.0.2.101
```

Fig. 1.9: Network detected and displayed

1.1.6 Input Parameters Captured by Sensors

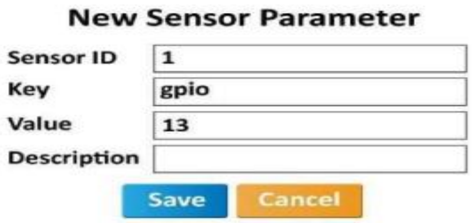
A sensor detects and responds to the inputs from the physical environment. The inputs may be heat, light, pressure, motion, moisture, or any other environmental phenomena. The parameter is a property of a sensor. The device specification should be checked to know the available parameters and what they measure.

To configure the sensor, a combination of the fields as shown in the table 1.1 must be added.

Table 1.1 Sensor Configuration Fields

Name	Name of the Sensor
Sensor ID	This includes the ID number of the sensor node. When a sensor is connected to the unit, the ID is automatically detected. The colour of the sensor ID indicates the status of the sensor. **Green:** Properly connected and configured **Yellow:** Connected but not configured **Red:** Not detected
Sensor Description	Description of the sensor can be used to define the quality to be monitored and the location of the node. It helps to resolve any problem regarding the sensor easily.
Alarm Notification	It helps to define the notifications for which alarms will be raised.
Worker ID	This includes the IF of the worker to which the sensor is attached.

Most of the sensors require some additional input. The parameters may have a key, value, and description that needs to be added by accessing the sensor control panel or adding the information in the sensor through a computer. These descriptions are shown in the screenshot of a sensor control system shown in Figure 1.10.


New Sensor Parameter

Sensor ID	1
Key	gpio
Value	13
Description	

Fig. 1.10: Input parameters of sensors

1.1.7 Collating Installation Points and Collecting Data

An IoT system requires multiple devices to be installed at different locations. These mounting points must be collated at one point so that the obtained information can be analysed. So, all devices are connected to a host device which is used as a hub or master device as shown in the Figure 1.11.

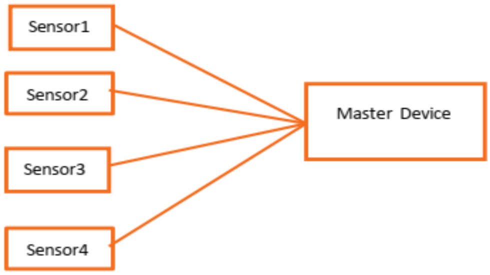


Fig. 1.11: Collating installation points

1.1.8 Calibrating User Data

To make a meaningful measurement, it is always required to measure the sensor's output in response to the known input. A device can be calibrated by applying several known physical inputs and recording the response of the system. The outputs of the sensors are tested and matched with the previous records to know whether the outputs are as per the user's requirements.

Practical Activity 1.1. To install and configure a motion sensor in a controlled environment.

Materials Required

Motion Sensor, Power Source (Adapter/Battery), Wall Mounting Accessories (Screws, Adhesive), Jumper Wires (if applicable)

Step 1. Choose suitable locations for motion sensor installation -identify and mark suitable locations within the classroom or designated area.

Step 1. Mounting the Sensor -securely mount the motion sensor using screws or adhesive. Emphasize stability and proper alignment for accurate detection.

Step 3. Connecting the Sensor-connect the sensor to a power source (adapter or battery).

Step 4. Configuring the Sensor -configure the sensor using a computer or smartphone application.

Step 5. Testing the Sensor-Conduct a functionality test by triggering the motion sensor.

1.3 Installation of Gateways

A sensor, an IoT module, and a smart device all are connected to the cloud by an IoT gateway, which can be either a real-world or virtual platform. Gateways act as a wireless access point to connect Internet-connected devices. Sensors produce large amounts of data per second. Data is pre-processed locally at the edge before being sent to the cloud. The gateway is the point where local processing takes place.

IoT is a set of multiple interconnected sensors, actuators, and processors. Embedded chips have reliable communication capabilities and are becoming cheaper and more sophisticated. The first important task for installing the gateway is selecting a proper location for it. The following are the installation steps of a gateway:

- Choose location
- Connect power source
- Connect to the Internet

1.3.1 Choose location – IoT gateways must be placed at the intersection of edge nodes, which are devices, controllers, sensors, and the cloud. The gate must be installed in a place raised to a certain height, which is not easily accessible, so as not to disturb the position. The gateway must be visible to all nodes. For example, a gateway installed for a building or house wi-fi network should be installed approximately 6 feet above the maximum height of surrounding buildings for clear visibility. The Figure 1.12 shows the position of an IoT gateway as discussed in the example.

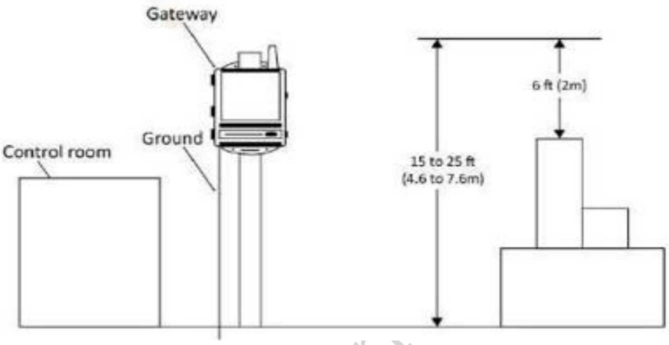


Fig.1.12: Position of IoT gateway

When choosing the location of the gateway, the practices that should be kept in mind are as follows:

- Ensure the gateway is within the range of the nodes. Typically, it needs to be located within the perimeter of the node perimeter.
- Ensure it is at least three feet away from wireless devices such as cellular transmitters, Wi-Fi access points, and cordless phones.
- Ensure it is installed in a discrete and locked location to restrict physical access to the device.
- Ensure that the gateway is installed at least 4 feet off the ground. It helps in maximizing reception distance.
- Make sure that the gateway is not placed inside any metal or behind large metal objects.
- The gateway must be near an Ethernet port or a Wi -fi interface, so that connectivity is not an issue.

The Figure 1.13 shows a metal enclosure for the gateway.

Fig. 1.13: A metal enclosure for the gateway

1.3.2 Connect Power Source – Power is required to manage the gateway's functions, including embedded processing, multiple sensor interfaces, and Internet connectivity. Therefore, devices must be plugged or charged frequently. Choosing the right power supply should be based on several considerations, such as the following:

- Availability of electricity points on the site
- Sensor type
- Number of sensors and other modules connected to the IoT framework
- The type of current, DC or AC, that the device supports
- Power supply suitable for installing the IoT framework
- Use of sensor and other modules

After considering these factors, the technician must select a power supply/supply for the sensors and other modules. The technician can refer to the installation documentation to verify the proper power supply for any module. Most edge nodes requires rechargeable batteries. Usually, a Li-Ion battery is used. The power source must be specified. The gateway can be powered by a 5V DC wall adapter. It can also be connected with a wired connector. If the power source is mains power, the input device must be installed close to the plug to use the cable as little as possible.

Connecting the Power Adapter

Use of the wall adapter requires that the adapter is connected to an approved plug behind the lock body. The technician must perform the following steps:

- Open the housing by removing the screws. The important task is to make sure that there is no static charge in the internal electronics.
- Connect the right end of the AC adapter cable to the power port of the outlet.
- Insert the removed wires into the corresponding connection terminals on the printed circuit board.
- Fit the housing around the circuit board and wire, then fasten the housing together with screws.
- Connect the power cord to the outlet.
- Check that the power indicator blinks green and then stays green.

The Figure 1.14 shows a gateway connected to a power outlet.

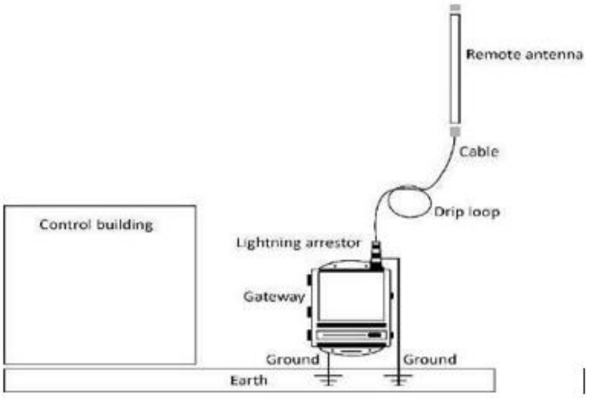


Fig. 1.14: A gateway connected to a power outlet

1.3.3 Connect to Internet – Typically, gateways are connected to the Internet via Wi-Fi, Ethernet, or GPS. Some ports are connected to a local area network (LAN). It is necessary to understand the data information collected by the gateway which messages to send over GPS networks and which can be saved to the device for offline processing. Gateway software is responsible for collecting messages from sensors and properly storing them until they can be pre-processed and sent to the data centre.

Among wireless technologies such as Bluetooth, Wi-Fi, and ZigBee. ZigBee is the most popular protocol in terms of cost and efficiency of IoT devices. A technician should complete the following steps:

- Connect the other end of the digital subscriber line (DSL) cable to the DSL port on the gateway.
- Connect the other end to the network.
- The connection can also be done via a WAN Ethernet port as follows:
- Connect the Ethernet cable to the WAN Ethernet port of the gateway.
- Connect the other end to the WAN Ethernet port.

The Figure 1.15 shows the overview of cabling a gateway.

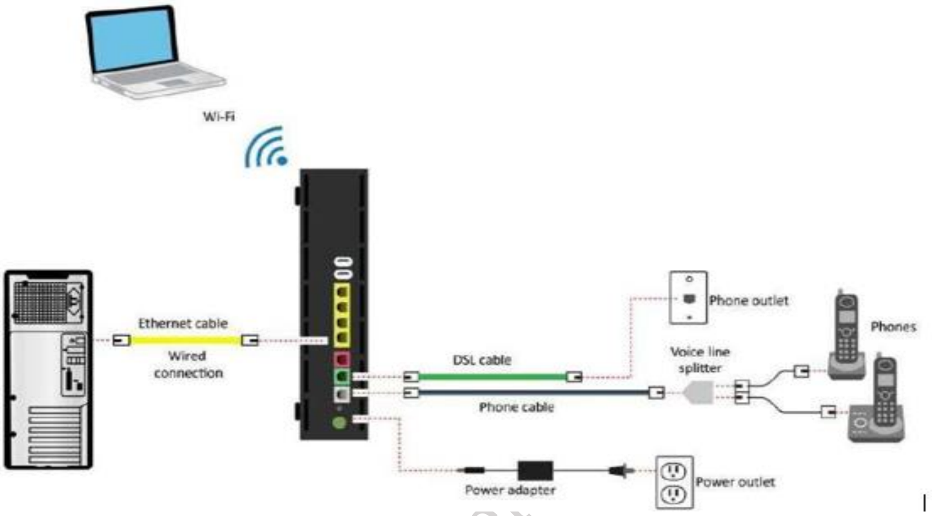


Fig. 1.15: Overview of cabling a gateway

Practical Activity 1.1. To install and connect an IoT gateway for data aggregation.

Materials Required: IoT Gateway, Power Source (Adapter), Ethernet Cable (if applicable)

Step 1. Selecting a Suitable Location.

Select an appropriate location for the gateway (proximity to nodes, accessibility, visibility).

Step 1. Connecting the Gateway.

Connect the gateway to a power source using an adapter.

Connect the gateway to the internet via Ethernet or Wi-Fi (if applicable).

Step 3. Verifying Connectivity.

Conduct a connectivity test to ensure the gateway is successfully connected to the internet. Perform any troubleshooting steps if needed.

1.4 Installation of Nodes

The nodes should be installed in the locations after considering all of the elements such as reachability, strength requirements, Internet connectivity, etc. The best practices are:

- The nodes should be established within the range of each other. The user interface settings need to be checked to confirm that every node is connected properly.
- The nodes should be established within the range of the gateway in order that the gateway can communicate with all nodes.
- The nodes should be established at 0.5-1.0 meters off the ground.
- When the location to be sensed is surrounded with the aid of using walls, the nodes should be installed on the interior side of the walls. For example, to locate any motion in a room, the sensors should be

established in a vicinity from which it is able to cover the maximum of the location. The best place is to install it on a roof.

- It is important to test the node locations when hardwiring and installing DC nodes.
- The nodes should not be installed near windows as the alarm systems are sensitive to outside motion.
- The nodes should not be placed near microwave ovens.

The Figure 1.16 shows possible sensor locations in a room to detect movement in a surrounding area.

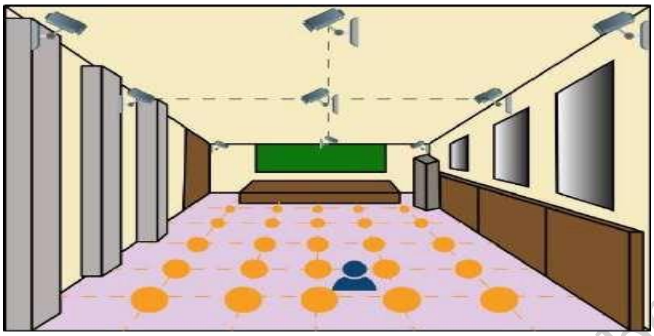


Fig. 1.16: Sensor locations in a surrounding area

1.5 Connection of the Nodes

The IoT devices are connected to the power source and the gateway after the IoT nodes and gateways have been installed. For instance, for an IoT framework for motion detection with IR-illuminated sensors in order to work, the nodes need to be connected to a power supply unit. A sample schematic diagram for the connection between the nodes in the same case is shown in the Figure 1.17.

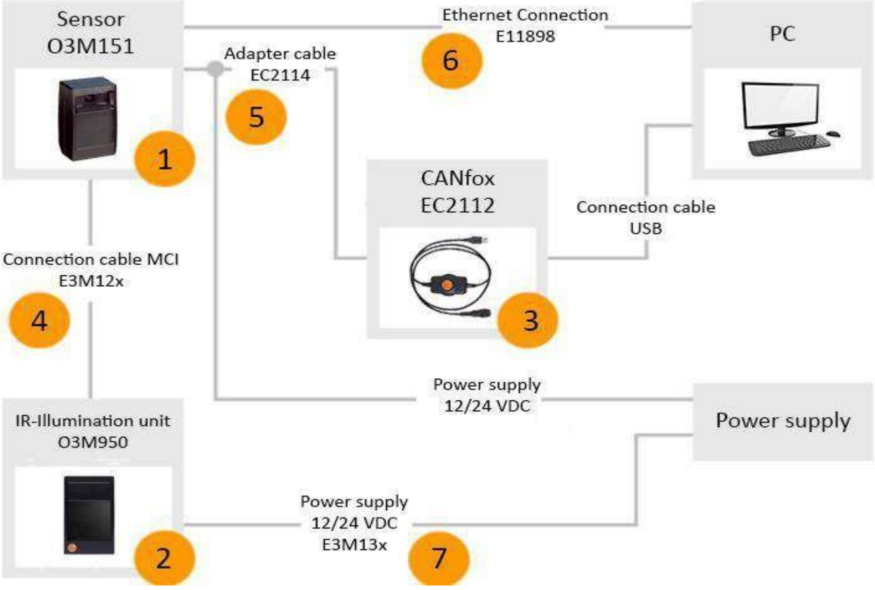


Fig. 1.17: Connection of IoT node

1.6 Installation of Home IoT system

1.6.1 Block Diagram

Home IoT system block diagram is shown in Figure 1.11.

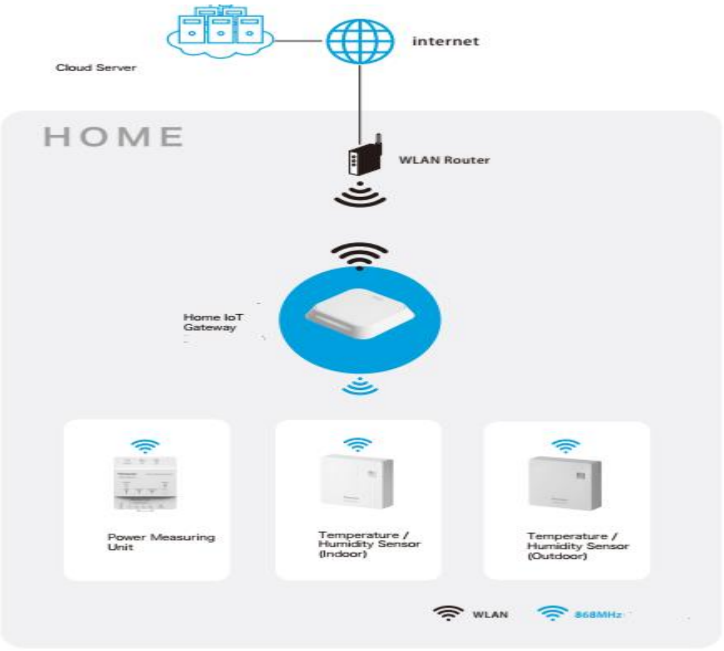


Fig. 1.18: block diagram of home IoT system

1.6.2 Components of Home IoT System

1) Home IoT Gateway

2) Power Measuring Unit

3) Temperature/Humidity Sensor

4) Adapter

These components are shown in Figure 1.19 and 1.20.

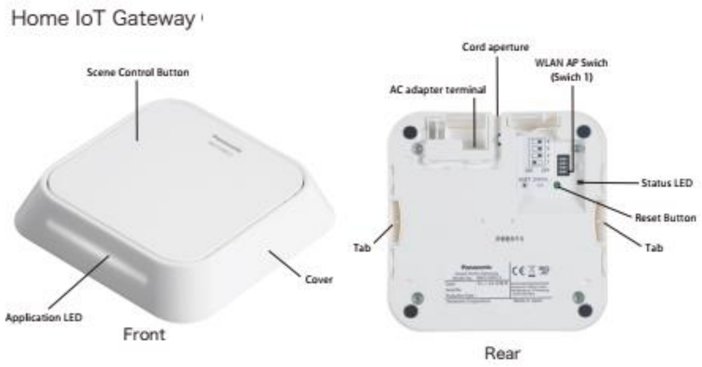


Fig. 1.19: Home IoT Gateway a) Front b) Rear

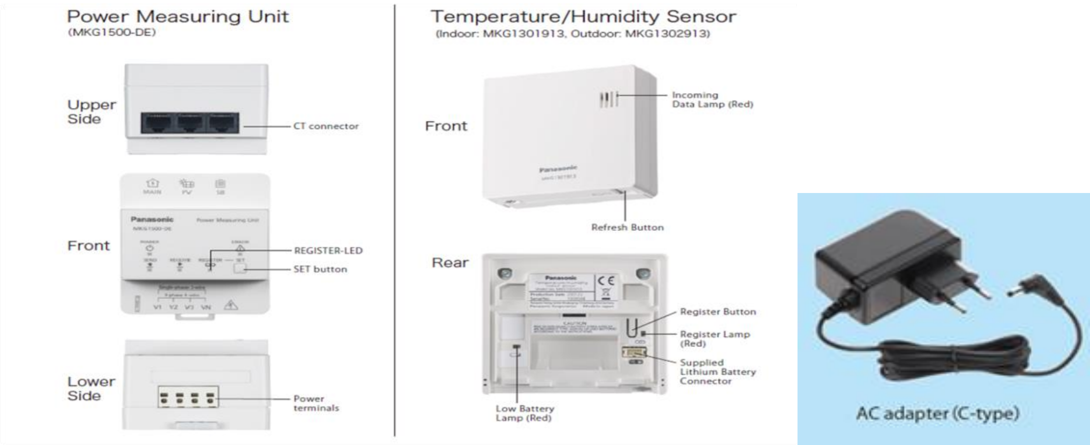


Fig. 1.20: Power Measuring Unit Temperature/Humidity Sensor and Adapter

1.6.3 Installation flow

The flow of the installation and setup process is given below in step wise:

A. Installation and App Setup by Installer

Preparation: Download the HOME IoT App

Step 1. Connect the HOME IoT App to the Home IoT Gateway

1. Remove the cover using the tabs on the rear of the cover as shown in Figure 1.21.

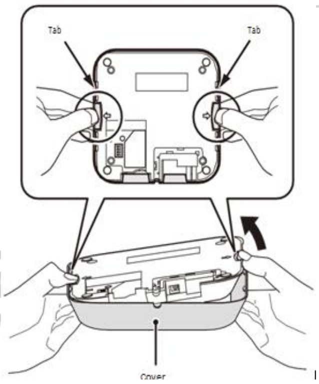


Fig. 1.21: Remove the cover using the tabs on the rear of the cover

1. Plug in the AC adapter, passing the cord through the cord stops as shown in Figure 1.21.

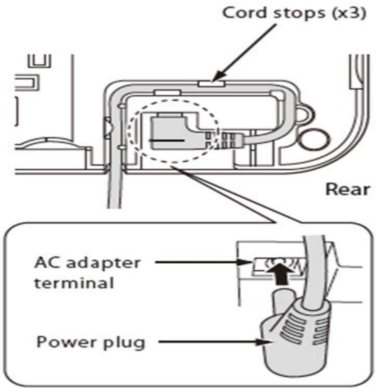


Fig. 1.22: Plug in the AC adapter, passing the cord through the cord stops

3. Reattach the cover by aligning the cover and body so that the cord passes through the cord aperture as shown in Figure 1.23.

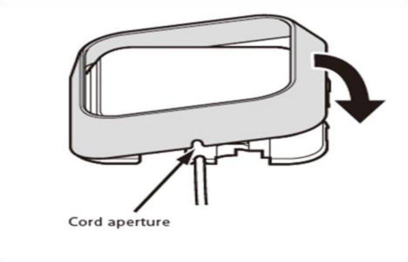


Fig. 1.23: Reattach the cover

4. Plug the AC adapter into the wall socket. Check that the Status LED on the rear of the Gateway double flashes in green. It will take around 1 minute to start up after plugging the AC adapter into the wall socket. It is depicted in Figure 1.24.

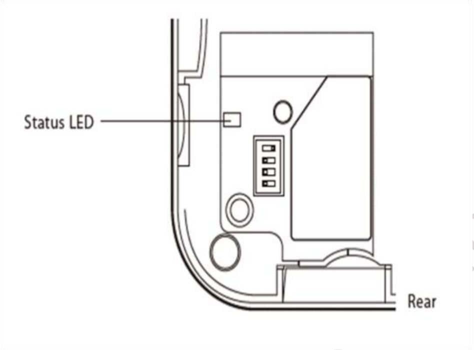
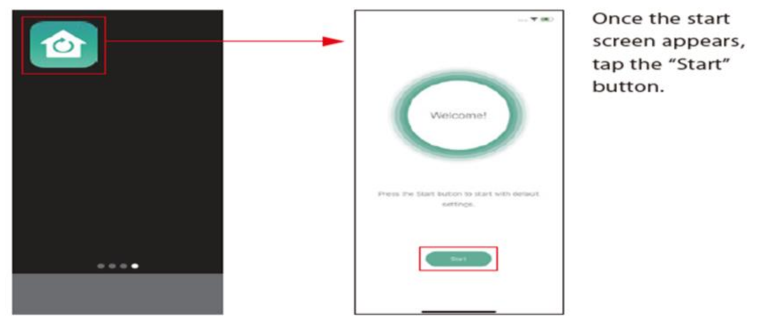


Fig. 1.24: Plug the AC adapter and check the status of LED

5. Tap to open the downloaded HOME IoT App on your smartphone as shown in Figure 1.25.

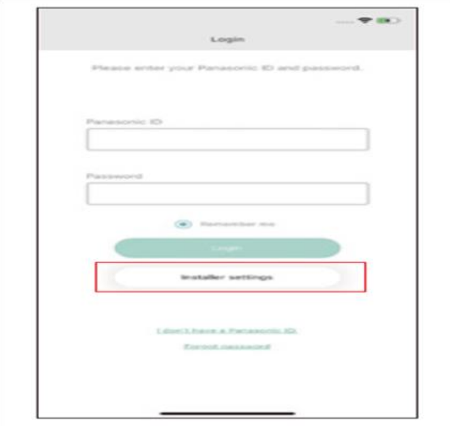

Once the start screen appears, tap the "Start" button.

Welcome!

Press the Start button to start with default settings.

Fig. 1.25: HOME IoT App on smartphone

6. Tap the "Installer settings" button as shown in Figure 1.26.


Login

Please enter your Panasonic ID and password.

Panasonic ID

Password

○ Remember me

Fig. 1.26: "Installer settings" button

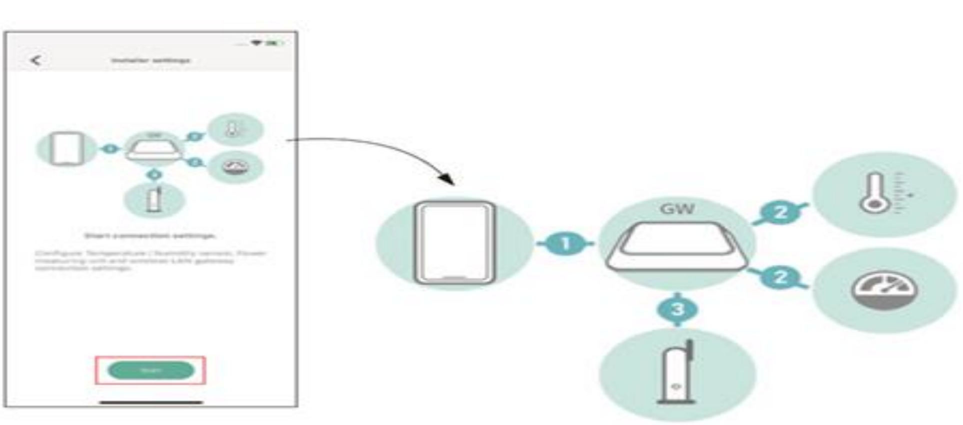
7. Next, proceed according to the instructions in the HOME IoT App. The install procedure is displayed. Check the details and tap the “Start” button. Installation follows the following process.

1. Connect your smartphone to the Gateway.

1. Register the Power Measuring Unit and sensors to the Gateway

3. Connect the Gateway to the internet.

4. The install procedure is displayed. Check the details and tap the “Start” button. It is illustrated in Figure 1.27.



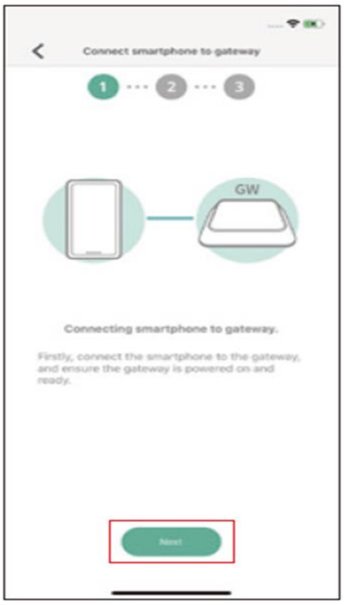
Installer settings

Start connection settings.

Configure Temperature / Humidity sensor, Power measuring unit and wireless LAN gateway connection settings.

Fig. 1.27: Installation procedure

1. First, make the initial connection from the smartphone to the Gateway. The Gateway and check that the power is on. Tap the “Next” button as shown in Figure 1.21.



Connect smartphone to gateway

Connecting smartphone to gateway.

Firstly, connect the smartphone to the gateway, and ensure the gateway is powered on and ready.

Fig. 1.28: initial connection from the smartphone to the Gateway

9.Switch the connection mode to “ON”.

Check that the Status LED on the rear of the Gateway is either lit or double or triple flashing, and set WLAN AP switch 1 to the on position. The Gateway will immediately enter AP mode. Once in AP mode, the Application LED on the front of the Gateway will flash in orange. If there are no problems, tap the “Next” button. The Gateway may take around 1 minute to boot after powering on. It is depicted in Figure 1.29.

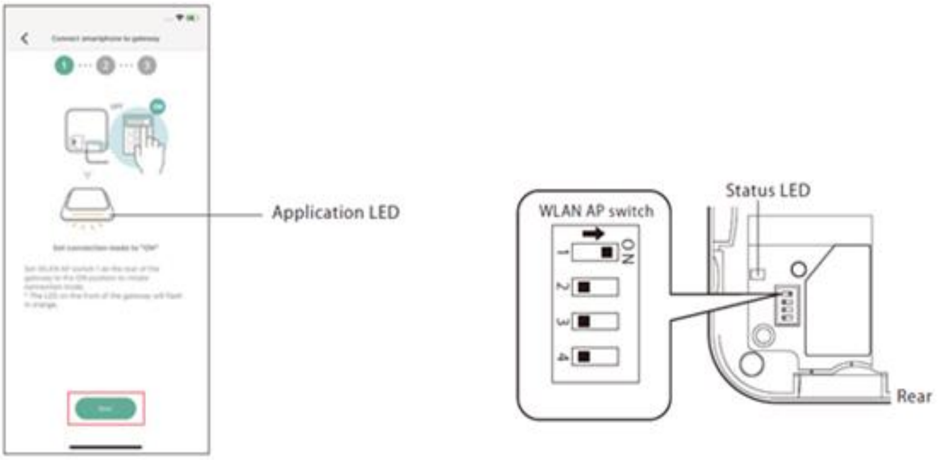


Fig. 1.29: Gateway in ON mode

10. Select and connect to the Gateway's SSID using the Wi-Fi Settings on your smartphone. The configuration process differs for Android and iOS smartphones.

Android

1. Tap the "Go to Wi-Fi Settings" button to open the Wi-Fi Settings on your smartphone.

1. Select the Gateways SSID.

3. Once the selected SSID has a check next to it indicating, it is connected, tap the Back button on your smartphone navigation bar to return to the HOME IoT App. It is shown in Figure 1.30.

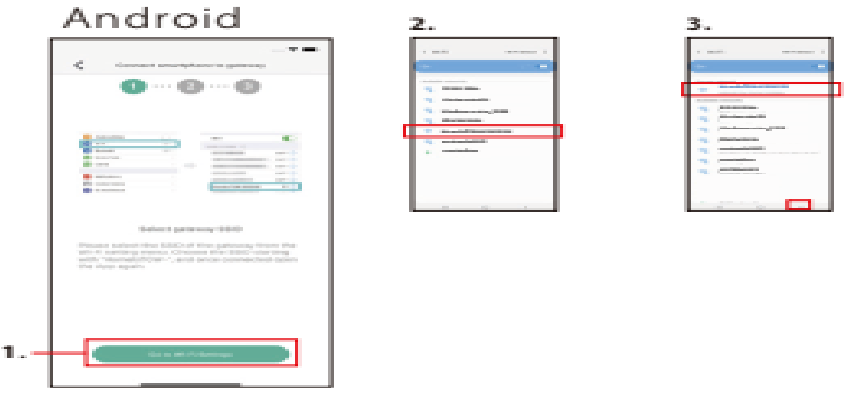


Fig. 1.30: Configuration process for Android

iOS

1. Before tapping the "Push here after Wi-Fi Settings" button on the guidance screen, tap your smartphones Home button to return to your home screen.

1. Tap the Settings icon to open the settings screen.

3. Under Wi-Fi Settings, select the Gate ways SSID.

4. Once the selected SSID has a check next to it indicating it is connected, tap the Home button to return to your Home screen. Now tap the app icon again to return to the HOME IoT App.

5. Tap the "Push here after Wi-Fi Settings" button on the guidance screen.

6. The Home IoT Gateway SSID is displayed as shown in Figure 1.31.

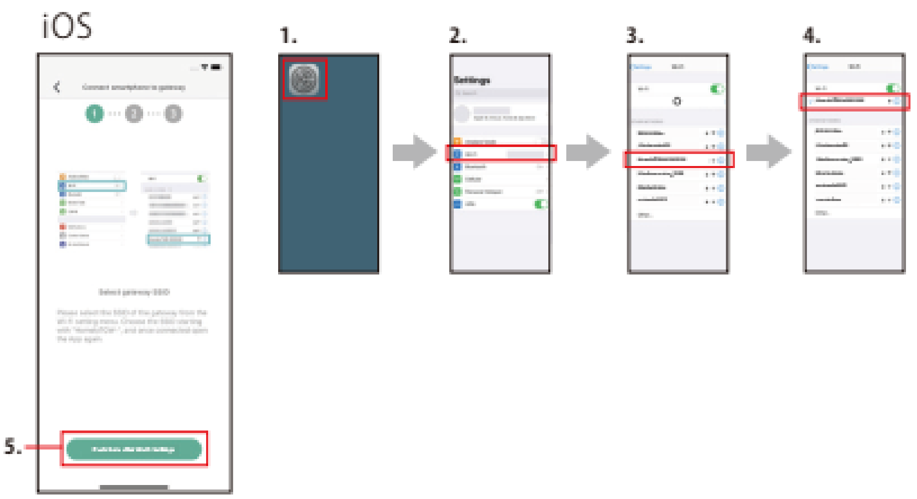
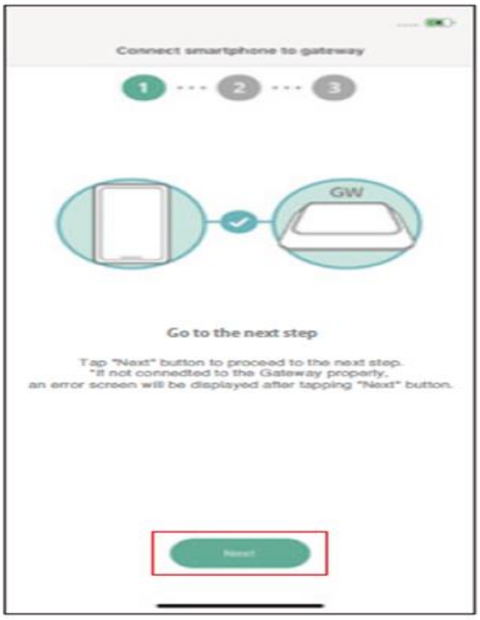


Fig. 1.31: Configuration process for iOS

7. “Home IoT GW-XXXXXX” where XXXXXX indicates the number.

11.The smart phone is successfully connected to the Gateway. Tap the Next button to move to the next step as shown in Figure 1.31.



Go to the next step

Tap "Next" button to proceed to the next step.
*If not connected to the Gateway properly,
an error screen will be displayed after tapping "Next" button.

Fig. 1.32: Smartphone connected to the Gateway

Step 1. Setup the Power Measuring Unit

The Power Measuring Unit includes the following products:

1. Power Measuring Unit
2. CT cable
3. CT sensor

These are shown in Figure 1.33.

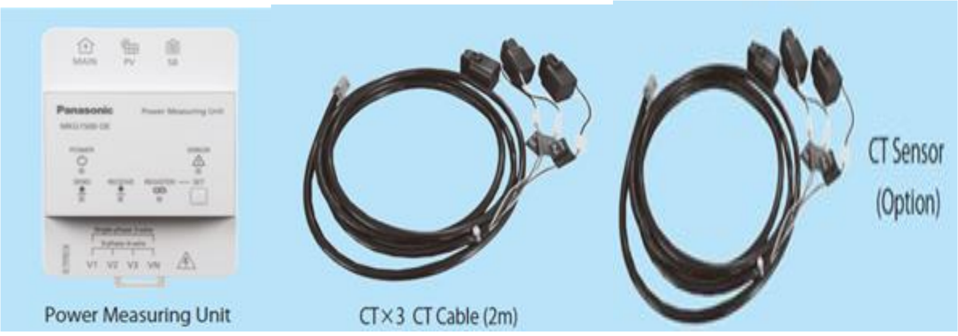
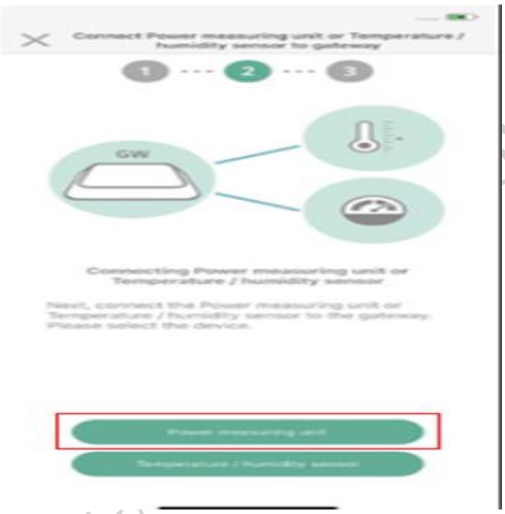


Fig. 1.33: Power Measuring Unit

1. Follow the instructions in the HOME IoT App to install and register the Power Measuring Unit.

Tapping the “Next” button on the final screen of **STEP1** brings up the screen to the following screen shown in Figure 1.34.



Connect Power measuring unit or Temperature / humidity sensor to gateway

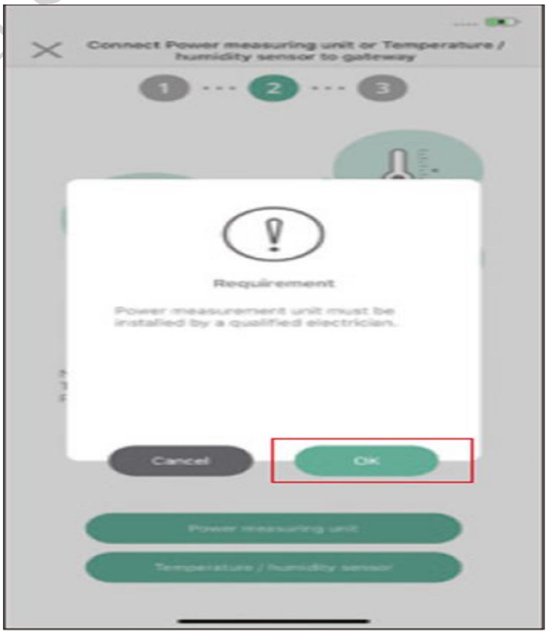
Connecting Power measuring unit or Temperature / humidity sensor

Next, connect the Power measuring unit or Temperature / humidity sensor to the gateway. Please select the device.

Fig. 1.34: install and register the Power Measuring Unit

Tap the “Power measuring Unit” button to start registration.

1. Installation must be carried out by a competent person. It is shown in figure 1.35.



Connect Power measuring unit or Temperature / humidity sensor to gateway

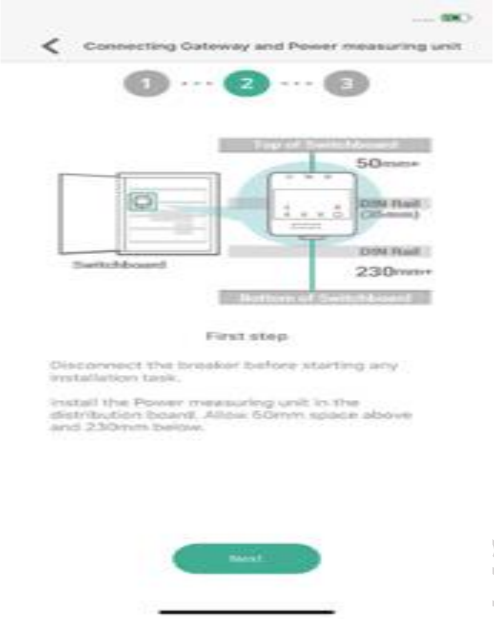
Requirement

Power measurement unit must be installed by a qualified electrician.

Fig. 1.35: Power Measuring Unit Registration

Tap the “OK” button to continue.

3. First, determine the installation position of the Power Measuring Unit as depicted in Figure 1.36.



Connecting Gateway and Power measuring unit

First step

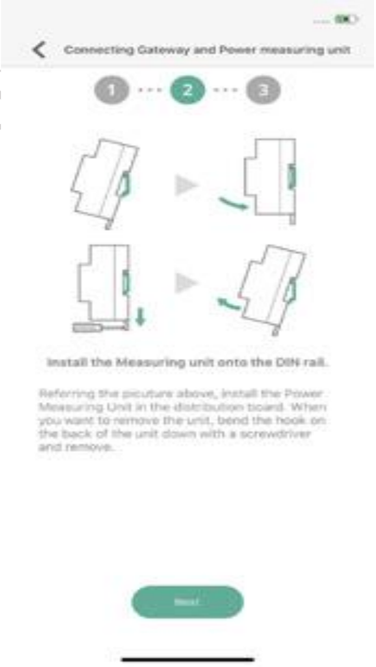
Disconnect the breaker before starting any installation task.

Install the Power measuring unit in the distribution board. Allow 50mm space above and 230mm below.

Fig. 1.36: installation position of the Power Measuring Unit

If the Power Measuring Unit is to be positioned in a consumer unit ensure that at least 50 mm of space is provided above the unit and 230mm below the unit. After determining the position, tap the “Next” button. Ensure the main breaker is opened before starting the task.

4. Attach the Power Measuring Unit to a rail within the consumer unit. Refer to the diagram for the installation of the Power Measuring Unit. To remove, use a flat-head screwdriver to lower the tab before pulling out. After installation, tap the “Next” button. It is shown in Figure 1.37.



Connecting Gateway and Power measuring unit

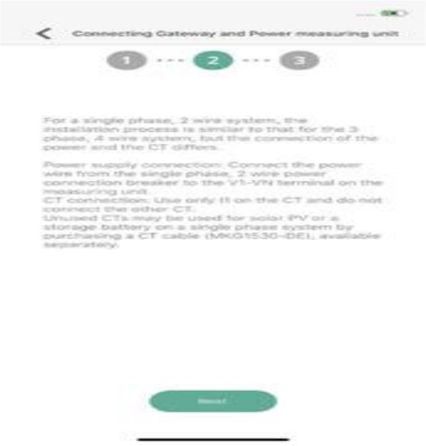
Install the Measuring unit onto the DIN rail.

Referring the picuture above, install the Power Measuring Unit in the distribution board. When you want to remove the unit, bend the hook on the back of the unit down with a screwdriver and remove.

Fig. 1.37: installation of Power Measuring Unit

5. Connection method for a single phase, 2-wire system

For a single phase,2-wire system, connect the wires to terminals V1-VN on the Power Measuring Unit. Use only I1 on the CT and do not connect the other CT as shown in Figure 1.31.



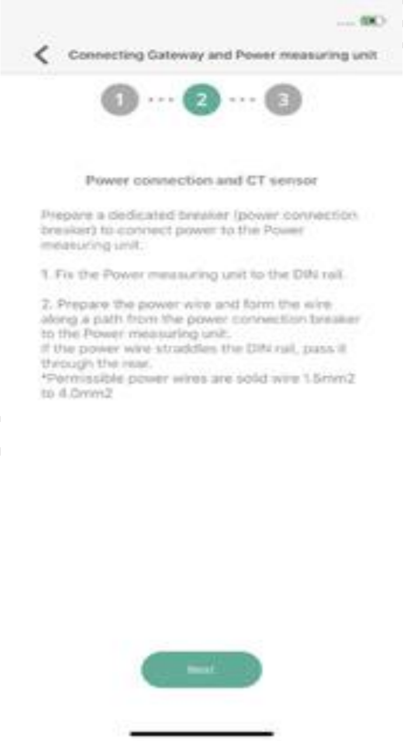
For a single phase, 2 wire system, the installation process is similar to that for the 3 phase, 4 wire system, but the connection of the power and the CT differs.

Power supply connection: Connect the power wire from the single phase, 2 wire power connection breaker to the V1-VN terminal on the measuring unit.
CT connection: Use only I1 on the CT and do not connect the other CT.
Unused CTs may be used for solar PV or a storage battery on a single phase system by purchasing a CT cable (MKG1530-DE), available separately.

Fig. 1.38: Connection method for a single phase, 2-wire system

Once connect, tap the “Next” button

6. Connection method for power and CT. It is depicted in Figure 1.39.



Power connection and CT sensor

Prepare a dedicated breaker (power connection breaker) to connect power to the Power measuring unit.

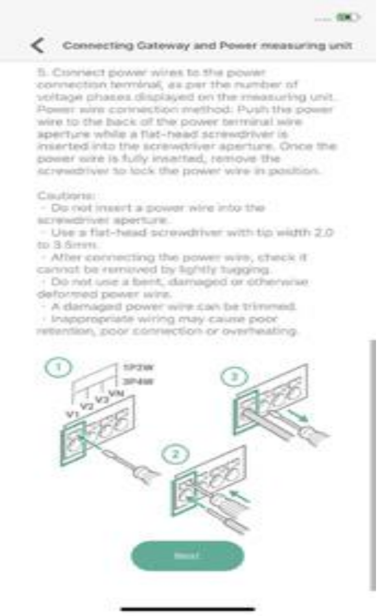
1. Fix the Power measuring unit to the DIN rail.

2. Prepare the power wire and form the wire along a path from the power connection breaker to the Power measuring unit.
If the power wire straddles the DIN rail, pass it through the rear.
*Permissible power wires are solid wire 1.5mm2 to 4.0mm2

Fig. 1.39: Connection method for power and CT

1. Prepare the power wire and form the wire along a path from the dedicated circuit breaker to the Power Measuring Unit.

1. Prepare the dedicated circuit breaker end of the power wire and connect it to the dedicated circuit breaker as shown in Figure 1.40.



Connecting Gateway and Power measuring unit

5. Connect power wires to the power connection terminal, as per the number of voltage phases displayed on the measuring unit. Power wire connection method: Push the power wire to the back of the power terminal wire aperture while a flat-head screwdriver is inserted into the screwdriver aperture. Once the power wire is fully inserted, remove the screwdriver to lock the power wire in position.

Cautions:
- Do not insert a power wire into the screwdriver aperture.
- Use a flat-head screwdriver with tip width 2.0 to 3.5mm.
- After connecting the power wire, check it cannot be removed by lightly tugging.
- Do not use a bent, damaged or otherwise deformed power wire.
- A damaged power wire can be trimmed.
- Inappropriate wiring may cause poor retention, poor connection or overheating.

Fig. 1.40: Connection of Power Measuring Unit

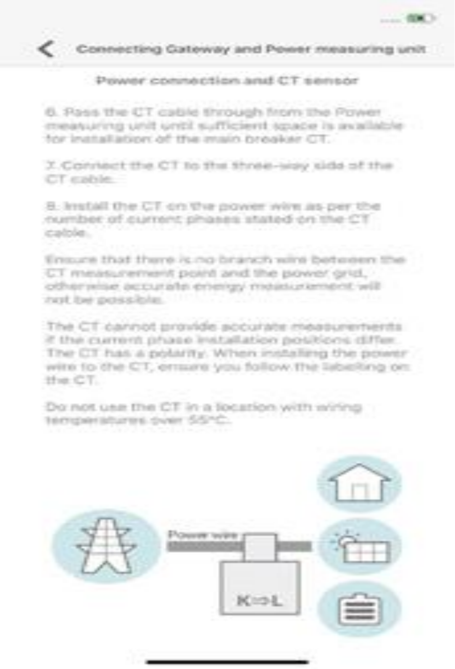
3. Remove 10 mm of insulation from the Power Measuring Unit side of the power wire to match the unit's strip gauge. (Power wires must be solid core and sized at 1.5mm^2)

4. Connect power wires to the power connection terminals, as per the number of voltage phases stated on the Power Measuring Unit. Power wire connection method: Push the power wire to the back of the power terminal wire aperture while a flat-head screwdriver is inserted into the screwdriver aperture. Once the power wire is fully inserted, remove the screwdriver to lock the power wire in position.

5. Pass the CT Cable through from the Power Measuring Unit until sufficient space is available for installation of the main breaker CT.

6. Connect the CT to the three-way split side of the CT Cable.

7. Clamp the CT on the power wire as per the number of current phases stated on the CT Cable. It is shown in Figure 1.41.



Connecting Gateway and Power measuring unit

Power connection and CT sensor

6. Pass the CT cable through from the Power measuring unit until sufficient space is available for installation of the main breaker CT.

7. Connect the CT to the three-way side of the CT cable.

8. Install the CT on the power wire as per the number of current phases stated on the CT cable.

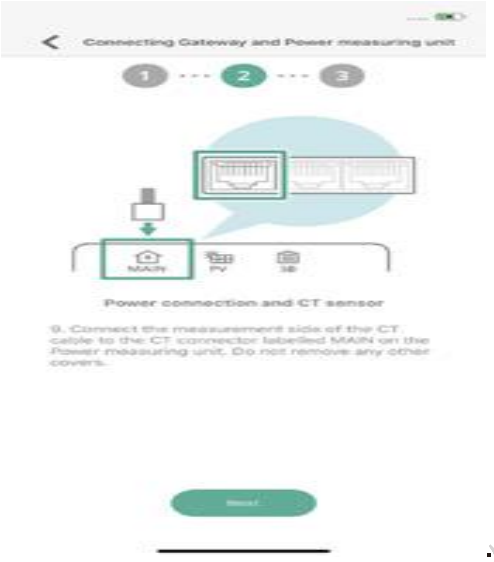
Ensure that there is no branch wire between the CT measurement point and the power grid, otherwise accurate energy measurement will not be possible.

The CT cannot provide accurate measurements if the current phase installation positions differ. The CT has a polarity. When installing the power wire to the CT, ensure you follow the labeling on the CT.

Do not use the CT in a location with wiring temperatures over 55°C.

Fig. 1.41: Connection of Power Measuring Unit

1. Connect the Power Measuring Unit side of the CT Cable to the CT connector labelled MAIN on the Power Measuring Unit. It is given in Figure 1.41.



Connecting Gateway and Power measuring unit

Power connection and CT sensor

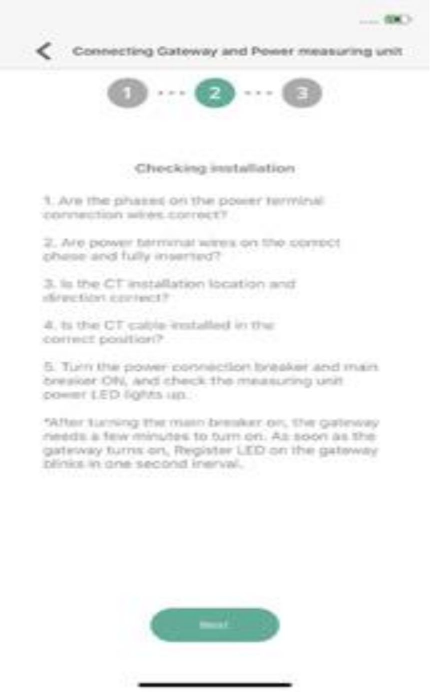
9. Connect the measurement side of the CT cable to the CT connector labelled MAIN on the Power measuring unit. Do not remove any other covers.

.

Fig. 1.42: Connection of Power Measuring Unit

Once connect, tap the “Next” button.

9. Checking the connection of the Power Measuring Unit to the Gateway as shown in Figure 1.43.



Connecting Gateway and Power measuring unit

Checking installation

1. Are the phases on the power terminal connection wires correct?

2. Are power terminal wires on the correct phase and fully inserted?

3. Is the CT installation location and direction correct?

4. Is the CT cable installed in the correct position?

5. Turn the power connection breaker and main breaker ON, and check the measuring unit power LED lights up.

*After turning the main breaker on, the gateway needs a few minutes to turn on. As soon as the gateway turns on, Register LED on the gateway blinks in one second inerval.

Fig. 1.43: Connection of Power Measuring Unit to Gateway

1. Are the phases on the power terminal connection wires correct?

1. Are power terminal wires in the correct position and fully inserted?

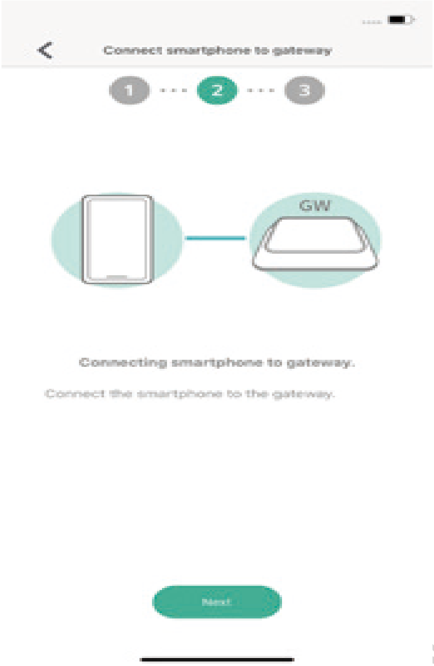
3. Is the CT installation position and direction correct?

4. Is the CT Cable installed in the correct location?

5. Turn the dedicated power connection breaker and main breaker on, and check the Power Measuring Unit power LED lights up.

Once checks are complete, tap the "Next" button.

10. Connect the smartphone to the Gateway as shown in Figure 1.44.



Connect smartphone to gateway

Connecting smartphone to gateway.

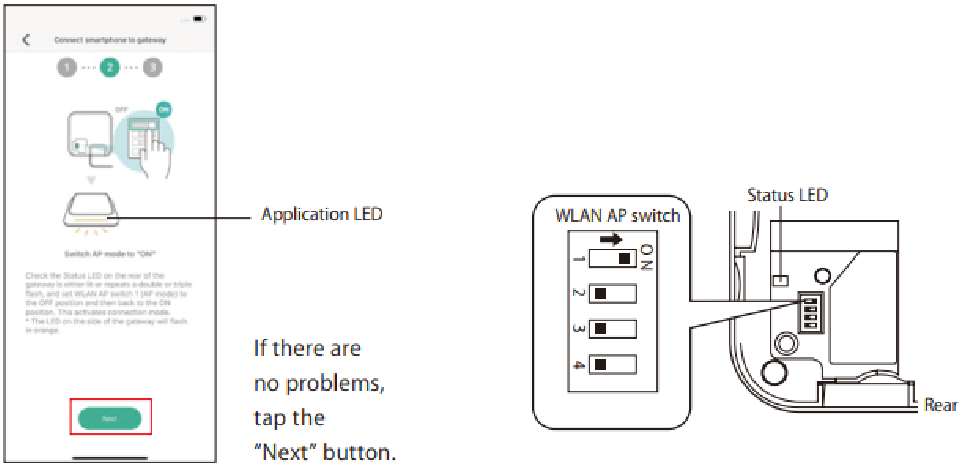
Connect the smartphone to the gateway.

Fig. 1.44: Connection of smartphone to the Gateway

Tap the “Next” button.

11. Switch the Gateway’s WLAN AP switch to the ON position.

Check the Status LED on the rear of the Gateway is either lit or repeats a double or triple flash, and set WLAN AP switch 1 to the OFF position, and the back to the ON position. The Gateway will immediately enter AP mode. Once in AP mode, the Application LED on the front of the Gateway will flash in orange. It is illustrated in Figure 1.45.



Connect smartphone to gateway

Switch AP mode to "ON"

Check the Status LED on the rear of the gateway is either lit or repeats a double or triple flash, and set WLAN AP switch 1 (AP mode) to the OFF position and then back to the ON position. This activates connection mode.
* The LED on the side of the gateway will flash in orange.

If there are no problems, tap the “Next” button.

Fig. 1.45: Gateway’s WLAN AP switch to the ON position

11. Select and connect to the Gateway’s SSID using the Wi-Fi Settings on your smartphone. The configuration process differs for Android and iOS smartphones.

Android

1. Tap the “Go to Wi-Fi Settings” button to open the Wi-Fi Settings on your smartphone.

1. Select the Gateway’s SSID.

3. Once the selected SSID has a check next to it indicating it is connected, tap the Back button on your smartphone's navigation bar to return to the HOME IoT App as shown in Figure 1.46.

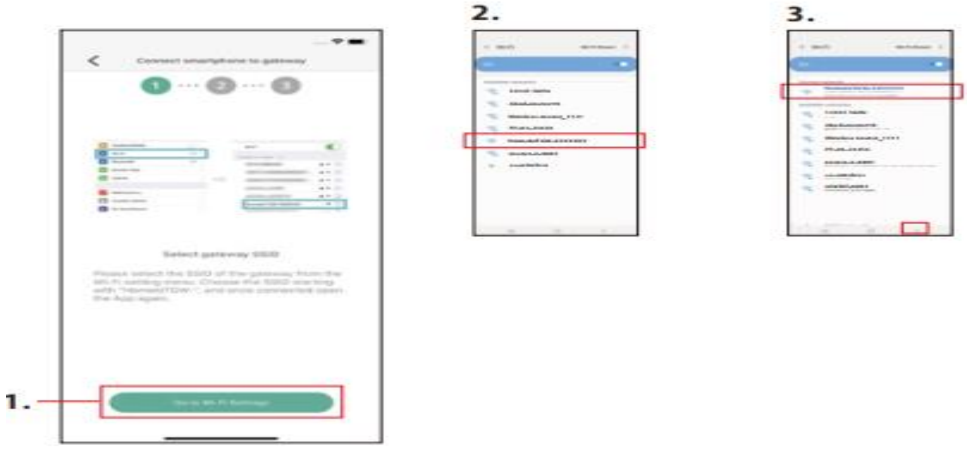


Fig. 1.46: Configuration process for Android

iOS

1. Before tapping the "Push here after Wi-Fi Settings" button on the guidance screen, tap your smartphone's Home button to return to your home screen.

1. Tap the Settings icon to open the settings screen.

3. Under Wi-Fi Settings, select the Gateway's SSID.

4. Once the selected SSID has a check next to it indicating it is connected, tap the Home button to return to your Home screen. Now tap the app icon again to return to the Panasonic HOME IoT App.

5. Tap the "Push here after Wi-Fi Settings" button on the guidance screen. It is illustrated in Figure 1.47.

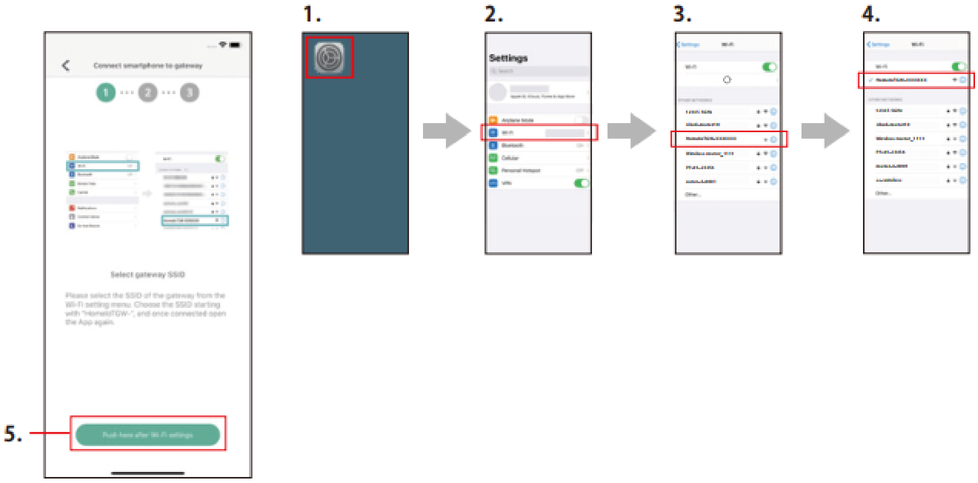
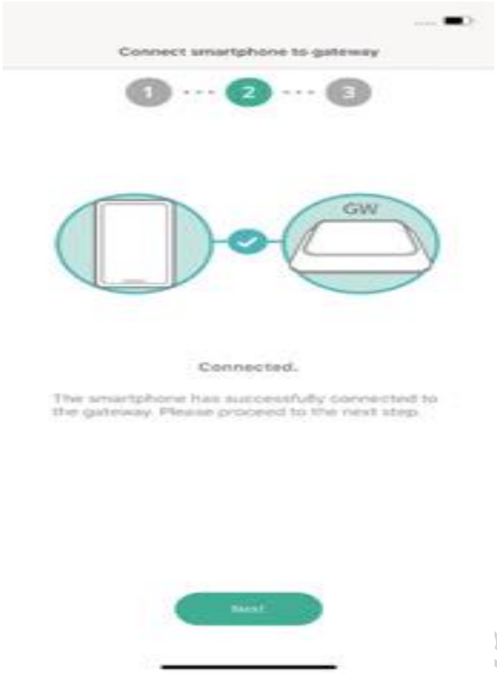

1.
2.
3.
4.
5.
Connect smartphone to gateway
Select gateway SSID
Please select the SSID of the gateway from the Wi-Fi setting menu. Choose the SSID starting with "HomeIoTGW-", and once connected open the App again.
Push here after Wi-Fi settings
Settings
Wi-Fi

Fig. 1.47: Configuration process for iOS

13. The smartphone is successfully connected to the Gateway as shown in Figure 1.41.



Connect smartphone to gateway

Connected.

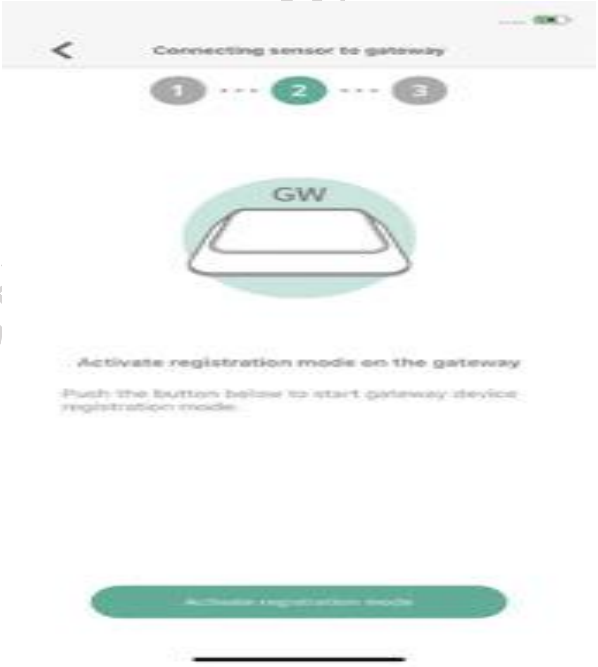
The smartphone has successfully connected to the gateway. Please proceed to the next step.

Fig. 1.48: Smartphone connected to the Gateway

Tap the “Next” button to move to the next step.

14. Put the Gateway into registration mode

Check that the Application LED is flashing in orange. Tap the “Activate Registration Mode” at the bottom of the screen to enter the Gateway’s device registration mode as shown in Figure 1.49.



Connecting sensor to gateway

Activate registration mode on the gateway

Push the button below to start gateway device registration mode

Fig. 1.49: Smartphone connected to the Gateway

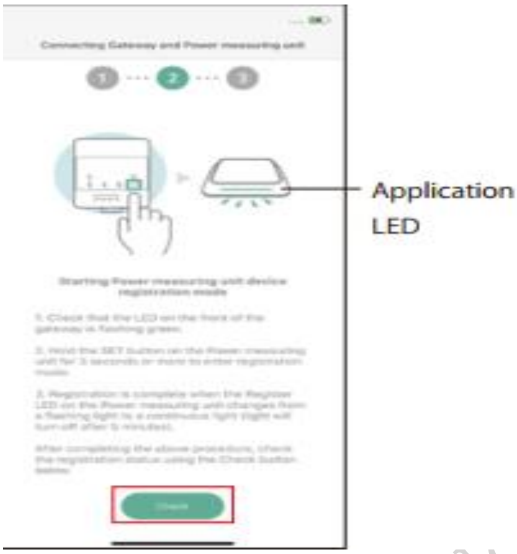
15. Put the Power Measuring Unit into registration mode.

1. Once the Gateway is in registration mode, the Application LED on the front of the Gateway will flash in green.

1. Hold the SET button on the Power Measuring Unit for at least 3 seconds to put it into registration mode.

3. Once the REGISTER LED on the Power Measuring Unit changes from flashing to permanently on, registration is complete (the LED will turn off after 5 minutes).

After completing the above process, tap the “Check” button to confirm registration as shown in Figure 1.50.



Connecting Gateway and Power measuring unit

1 ··· 2 ··· 3

Starting Power measuring unit device registration mode

1. Check that the LED on the front of the gateway is flashing green.

2. Hold the SET button on the Power measuring unit for 3 seconds or more to enter registration mode.

3. Registration is complete when the Register LED on the Power measuring unit changes from a flashing light to a continuous light (light will turn off after 5 minutes).

After completing the above procedure, check the registration status using the Check button below.

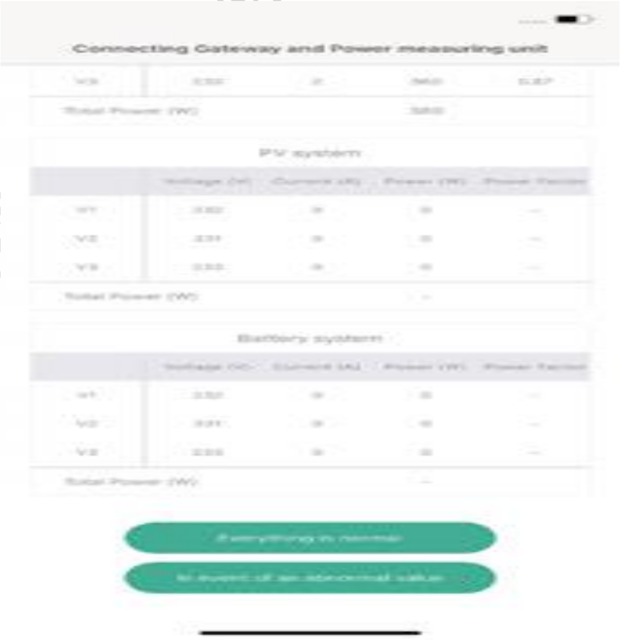
Check

Fig. 1.50: Power Measuring Unit in registration mode

16.Power Measuring Unit registration complete.

1. Here we confirm that the measurements being taken look correct. If an abnormal value is shown, tap the “In event of an abnormal value” button to restart the process for Step. If PV is installed, negative value is displayed while generating.

1. A storage battery will display as a positive number while charging and negative while discharging. It is shown in Figure 1.51.



Connecting Gateway and Power measuring unit

PV system

Battery system

Everything is normal

In event of an abnormal value

Fig. 1.51: Power Measuring Unit registration complete

If displayed figures are OK then Tap the “Everything is normal” button.

B. Installation and App Setup by Installer

Step 3. Setup the Temperature / Humidity Sensor

The Temperature / Humidity Sensor contains the following products as shown in Figure 1.51.

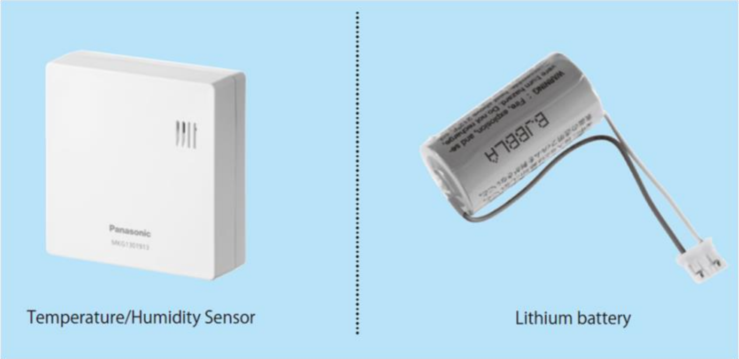
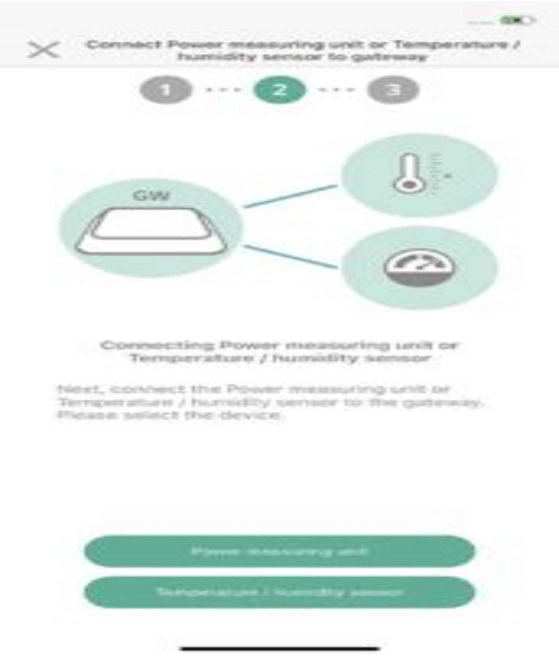


Fig. 1.52: Temperature / Humidity Sensor

1.Tap the “Temperature /Humidity Sensor” button to start registration.

Tapping the “Next” button on the final page of step 1 displays this screen as shown in Figure 1.53.


Connect Power measuring unit or Temperature / humidity sensor to gateway

Connecting Power measuring unit or Temperature / humidity sensor

Next, connect the Power measuring unit or Temperature / humidity sensor to the gateway. Please select the device.

Fig. 1.53: Temperature / Humidity Sensor registration

1.Insert the lithium battery into the Temperature /Humidity Sensor

1. Check that the Gateway’s Application LED is flashing in green.

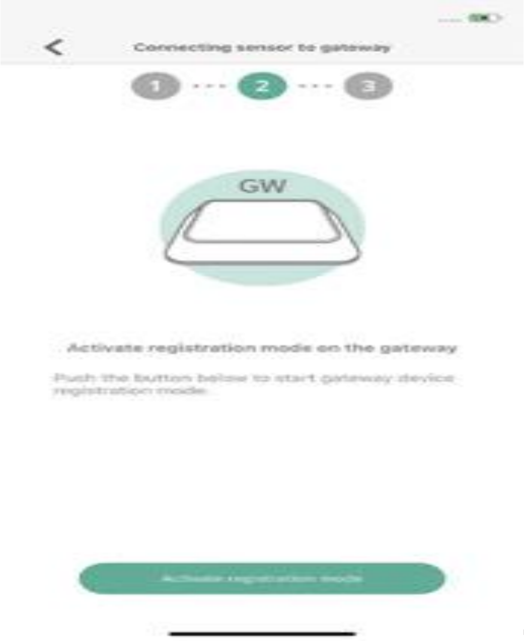
1. Hold the Register Button inside the battery cover of the Temperature /Humidity Sensor for at least 2 seconds to enter registration mode.

3. Once the Temperature / Humidity Sensor’s Register Lamp changes from a flashing red to a permanent red, registration is complete (the LED will turn off after 5 seconds).

4. Tap the “Check” button to move on.

3. Put the Gateway into registration mode.

Tap the “Activate registration mode” button to start the Gateway’s device registration mode. It is shown in Figure 1.54.



Connecting sensor to gateway

Activate registration mode on the gateway

Push the button below to start gateway device registration mode.

Fig. 1.54: Connection of sensor to Gateway

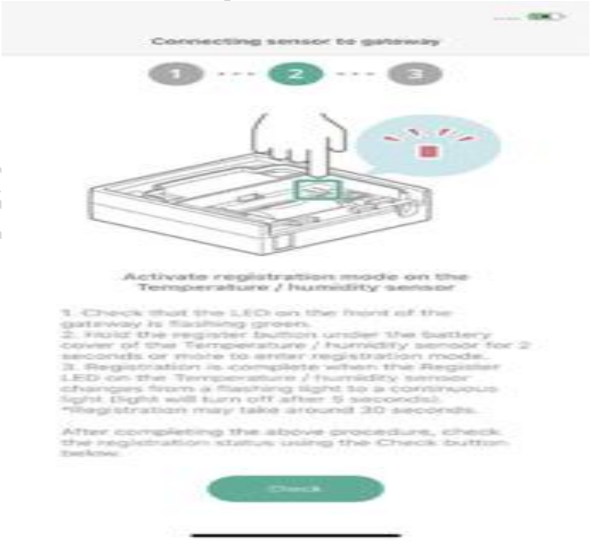
4. Press the Register Button on the Temperature / Humidity Sensor and register it to the Gateway

1. Check that the Gateway's Application LED is flashing in green.

1. Hold the Register Button inside the battery cover of the Temperature / Humidity Sensor for at least 2 seconds to enter registration mode.

3. Once the Temperature / Humidity Sensor's Resistor Lamp changes from a flashing red to a permanent red, registration is complete (the LED will turn off after 5 seconds).

4. Tap the "Check" button to move on.It is depicted in Figure 1.55.



Connecting sensor to gateway

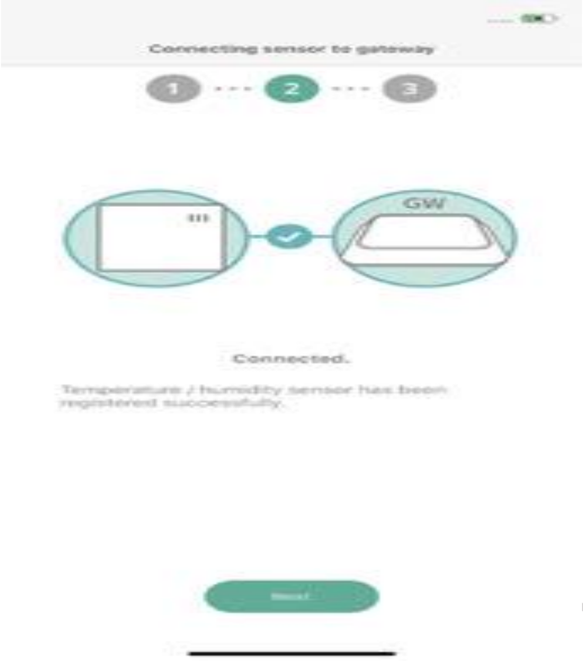
Activate registration mode on the Temperature / humidity sensor

1. Check that the LED on the front of the gateway is flashing green.
2. Hold the register button under the battery cover of the Temperature / humidity sensor for 2 seconds or more to enter registration mode.
3. Registration is complete when the Register LED on the Temperature / humidity sensor changes from a flashing light to a continuous light (light will turn off after 5 seconds).
*Registration may take around 30 seconds.

After completing the above procedure, check the registration status using the Check button below.

Fig. 1.55: Temperature / Humidity Sensor registration

5. Registration is complete.Once this screen is displayed, registration is complete. Tap the "Next" button as shown in Figure 1.56.

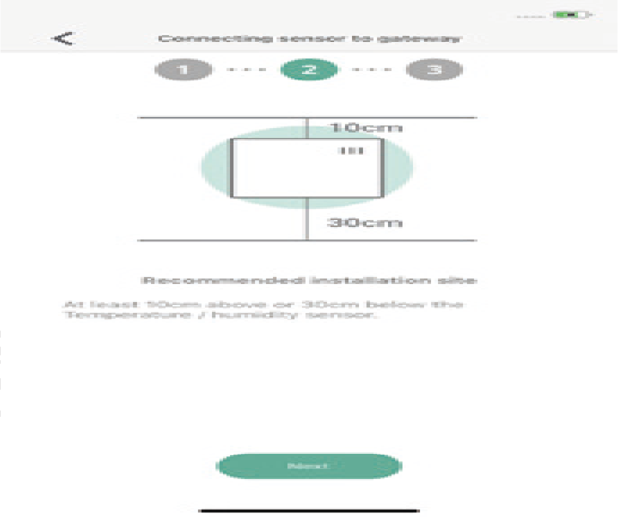

Connecting sensor to gateway

Connected.

Temperature / humidity sensor has been registered successfully.

Fig. 1.56: Temperature / Humidity Sensor registration

6. Install the device in the location where temperature and humidity measurements are to be taken. Installation should allow 10cm above and 30cm below the device. Once installed, tap the “Next” button as shown in Figure 1.57.


Connecting sensor to gateway

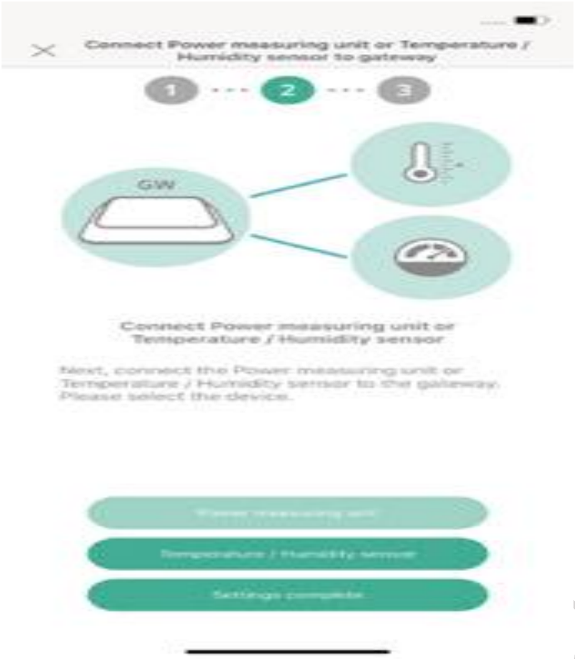
Recommended installation site

At least 10cm above or 30cm below the Temperature / humidity sensor.

Fig. 1.57: Temperature / Humidity Sensor installation

Step 4. Check the wireless signal strength to the Home IoT Gateway

1. Once all devices are installed, tap the “Settings Complete” button on the screen below. Tapping the “Next” button on the final screen of displays the screen to the left. Tap the “Settings Complete” button to continue. It is shown in Figure 1.51.



Connect Power measuring unit or Temperature / Humidity sensor to gateway

Connect Power measuring unit or Temperature / Humidity sensor

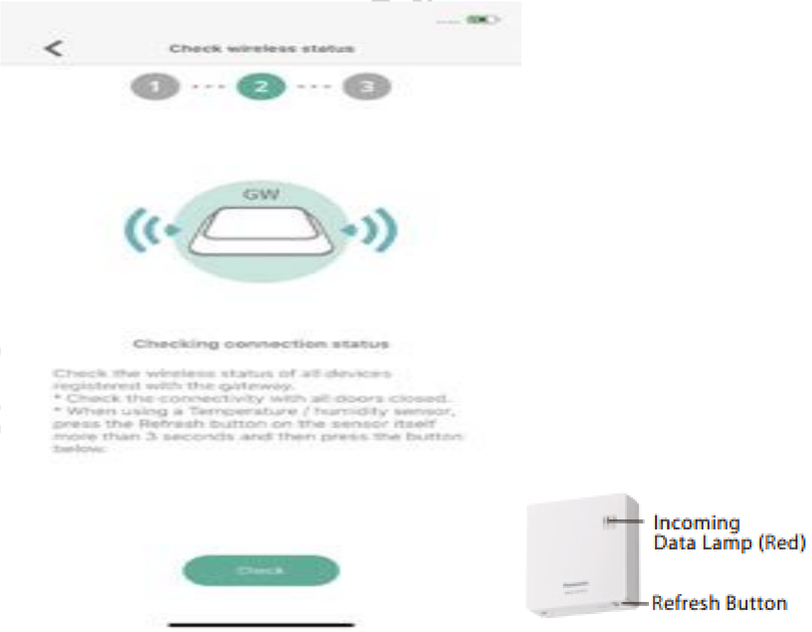
Next, connect the Power measuring unit or Temperature / Humidity sensor to the gateway. Please select the device.

Fig. 1.58: Temperature / Humidity Sensor installation

1. Check the connection signal strength for devices connected to the Gateway.

If a Power Measuring Unit is installed, check the signal with the consumer unit cover closed.

If a Temperature /Humidity Sensor is installed, hold the Refresh Button on the base of the sensor for at least 3 seconds and check that the Incoming Data Lamp lights in red. Once the above checks are complete, tap the “Check” button at the bottom of the screen as shown in Figure 1.59.



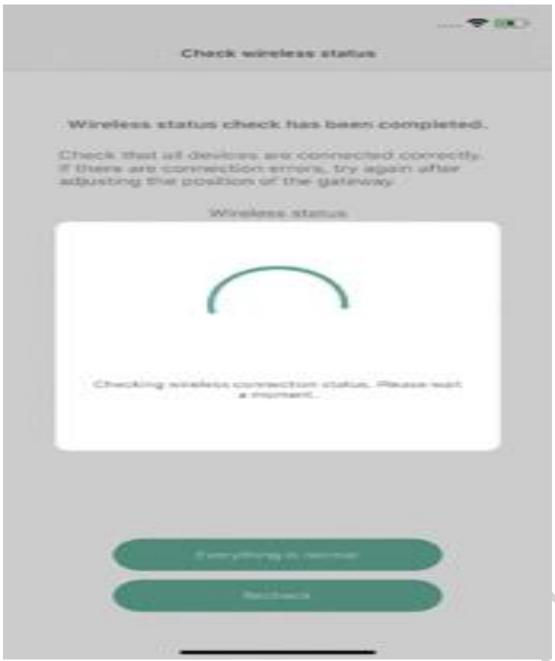
Check wireless status

Checking connection status

Check the wireless status of all devices registered with the gateway.
* Check the connectivity with all doors closed.
* When using a Temperature / humidity sensor, press the Refresh button on the sensor itself more than 3 seconds and then press the button below.

Fig. 1.59: Check the connection signal strength for devices connected to the Gateway.

3. Check the signal strength to the Gateway. Please be patient as the checking process takes several minutes. It is shown in Figure 1.60.



Check wireless status

Wireless status check has been completed.

Check that all devices are connected correctly. If there are connection errors, try again after adjusting the position of the gateway.

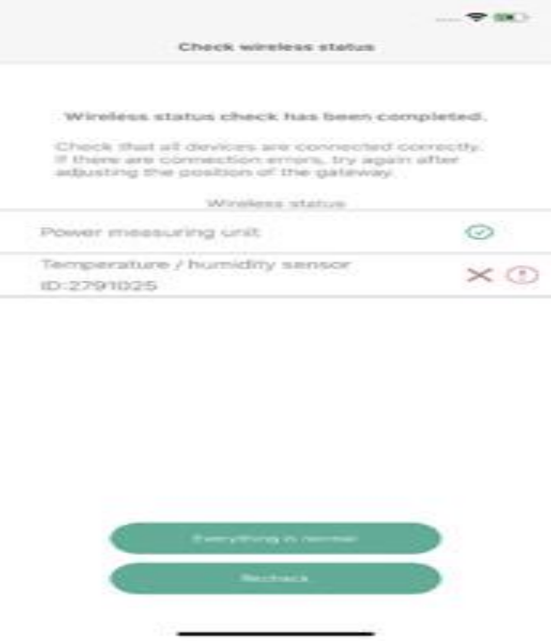
Wireless status

Checking wireless connection status. Please wait a moment...

Fig. 1.60: Check the connection signal strength for devices connected to the Gateway.

4. Once checks are complete, tap the "Everything is normal" button.

Confirm the output on the screen to the left. If there are no problems, tap the "Everything is normal" button as shown in Figure 1.61.



Check wireless status

Wireless status check has been completed.

Check that all devices are connected correctly. If there are connection errors, try again after adjusting the position of the gateway.

Wireless status

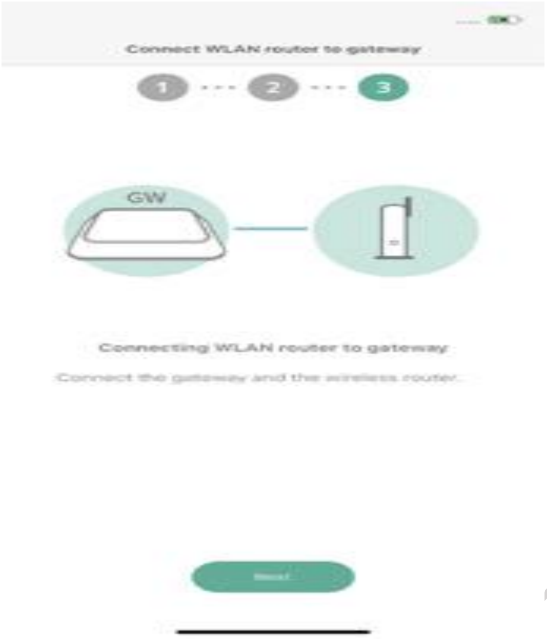
Power measuring unit ✓

Temperature / humidity sensor ID:2791025 ✕ ⓘ

Fig. 1.61: "Everything is normal"

Step 5. Connect the Home IoT Gateway to the internet

1. Connect the WLAN Router to the Gateway as shown in Figure 1.61.



Connect WLAN router to gateway

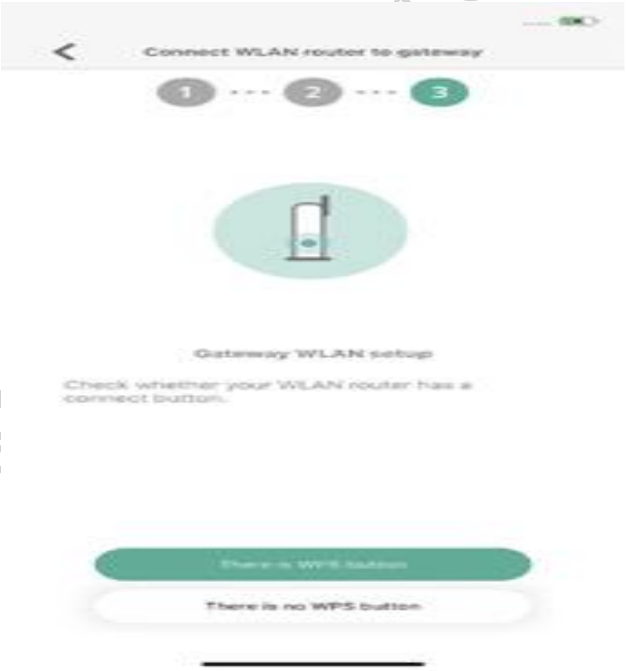
Connecting WLAN router to gateway

Connect the gateway and the wireless router.

Fig. 1.62: Connection of WLAN Router to Gateway

Tap the “Next” button.

1. Check whether your WLAN Router has a WPS button as shown in Figure 1.63.



Connect WLAN router to gateway

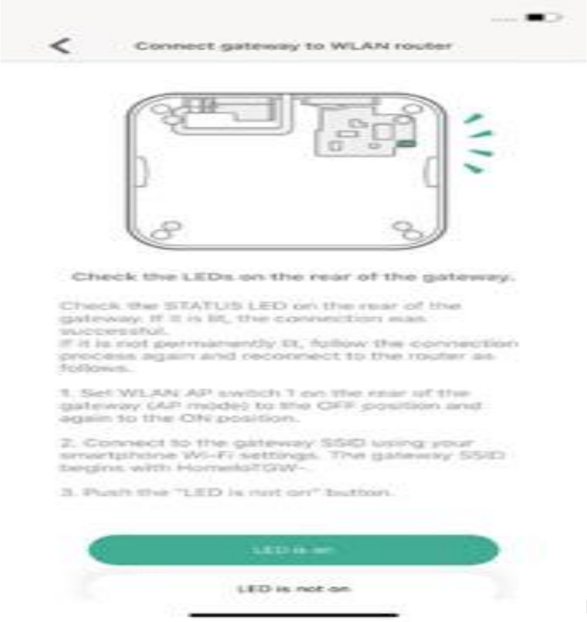
Gateway WLAN setup

Check whether your WLAN router has a connect button.

Fig. 1.63: check for WPS button

If it has a WPS button, tap “There is a WPS button”. If there is no WPS button, tap “There is no WPS button”.

3. After around 2 minutes, check the Status LED. Check the Status LED on the rear of the Gateway after 2 minutes. If the Status LED is lit, the Gateway is successfully connected to the WLAN Router. Tap the “LED is on” button to complete WLAN setup as shown in Figure 1.64.



Connect gateway to WLAN router

Check the LEDs on the rear of the gateway.

Check the STATUS LED on the rear of the gateway. If it is lit, the connection was successful.
If it is not permanently lit, follow the connection process again and reconnect to the router as follows.

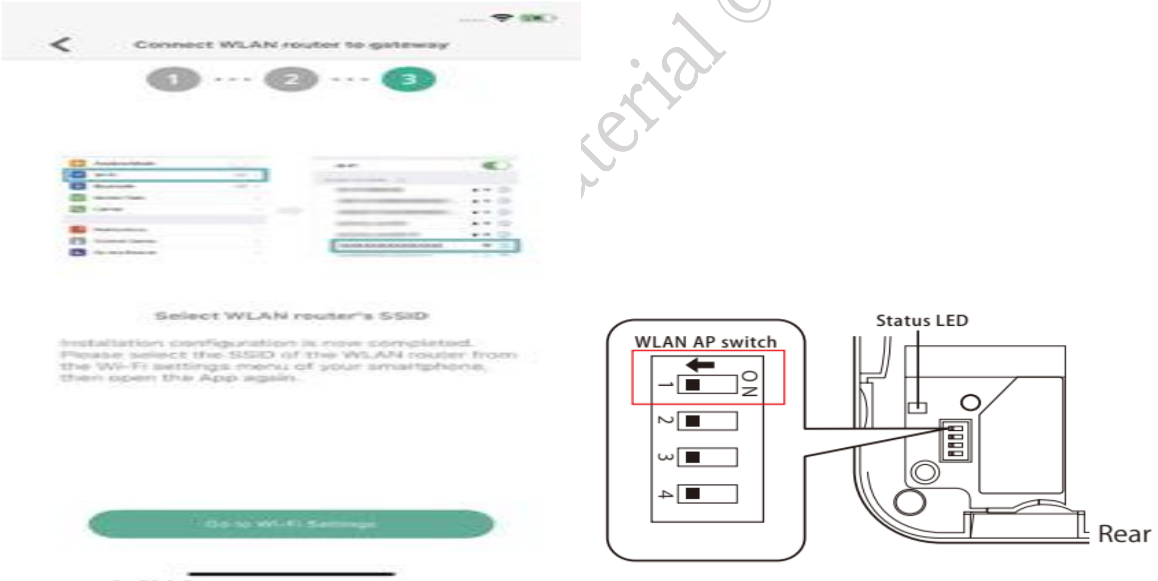
1. Set WLAN AP switch 1 on the rear of the gateway (AP mode) to the OFF position and again to the ON position.

2. Connect to the gateway SSID using your smartphone Wi-Fi settings. The gateway SSID begins with HomeIoTGW-.

3. Push the "LED is not on" button.

Fig. 1.64: Gateway connected to the WLAN Router

4. Installation is complete. Select the SSID of the WLAN Router from your smartphone's Wi-Fi Settings. Then, set the Gateway's WLAN AP switch (switch 1) to OFF. It is shown in Figure 1.65.



Connect WLAN router to gateway

Select WLAN router's SSID

Installation configuration is now completed. Please select the SSID of the WLAN router from the Wi-Fi settings menu of your smartphone, then open the App again.

Fig. 1.65: Gateway connected to the WLAN Router

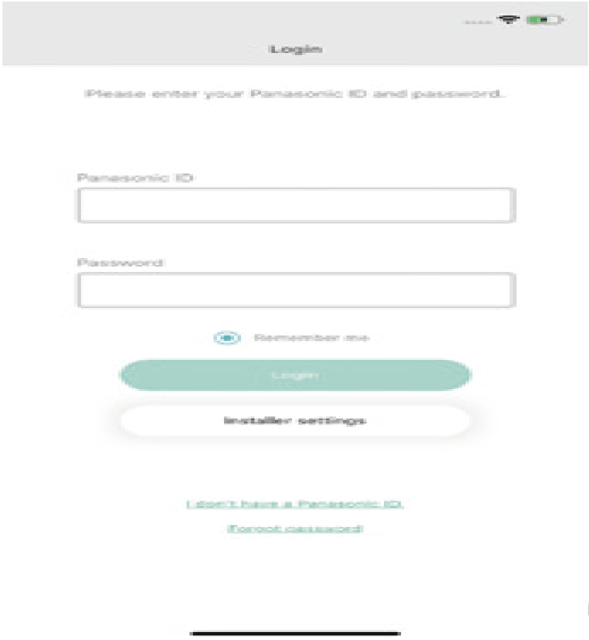
App Setup by User

Step 1. Create an ID

- Open the App on your smartphone.
- Tap the "Start" button.
- If you have an there is no need to create a new ID. Simply enter your existing ID and password to login.

Step 1. Initial registration to use the App

- Login with your ID and password
- Open the App and enter the ID and password from to login. It is shown in Figure 1.66.



Login

Please enter your Panasonic ID and password.

Panasonic ID

Password

● Remember me

Login

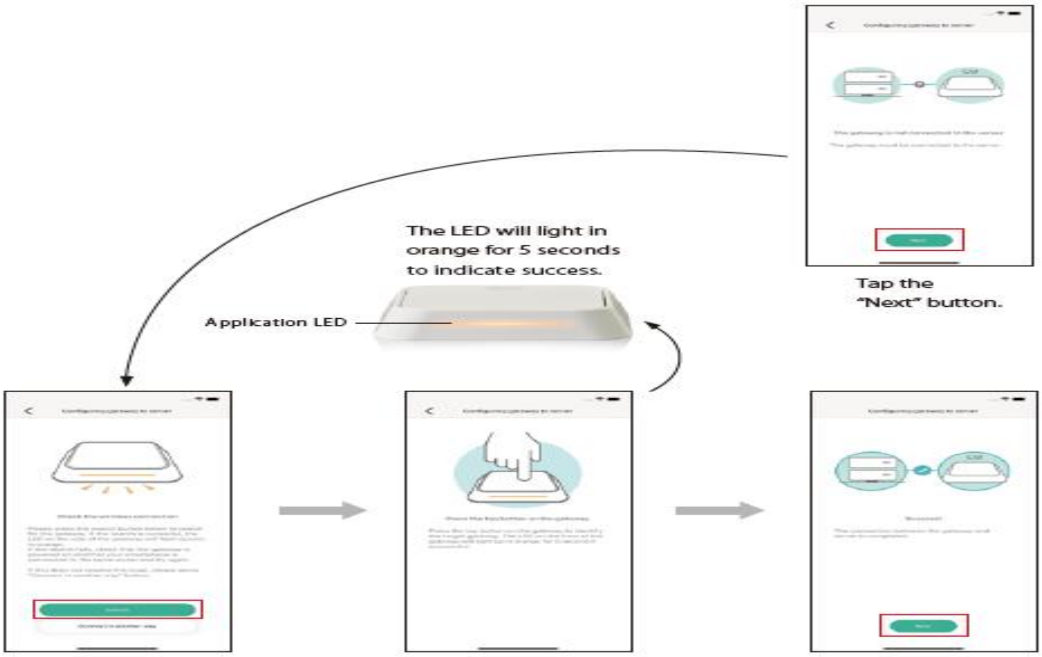
Installer settings

I don't have a Panasonic ID.

Forgot password!

Fig. 1.66: Initial registration on the App

- Agree to the Terms of Use by tapping the “Agree” button.
- Confirm the Privacy Notice.
- Read the privacy notice and tap the “Understood” button to continue.
- Registering the Gateway with the Server.
- Follow the on-screen instructions to complete server registration. It is depicted in Figure 1.67.



The LED will light in orange for 5 seconds to indicate success.
Application LED

Tap the “Next” button.

Tap the “Search” button.

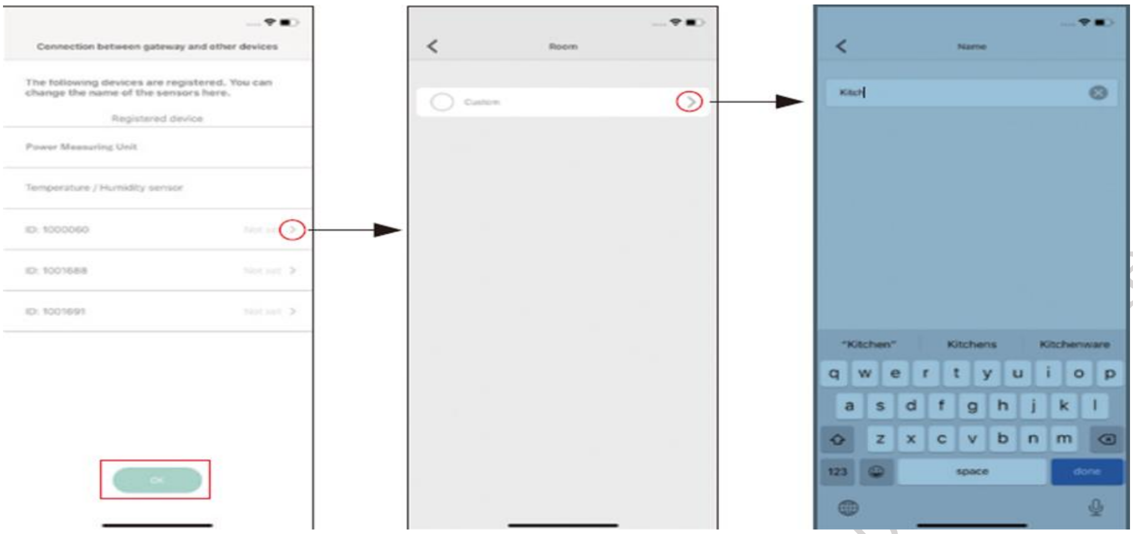
Check that the Gateway’s Application LED flashes in orange, and tap the Scene Control Button on top of the Gateway. The LED will light in orange for 5 seconds to indicate success.

Once registration is complete, tap the “Next” button.

Fig. 1.67: Server registration on the App

Confirm the list of devices registered with the Gateway.

If a Temperature /Humidity Sensor is listed in the registered devices, select its installed location. After selecting the location, tap the “OK” button on the list screen to move on as shown in Figure 1.61.



Connection between gateway and other devices

The following devices are registered. You can change the name of the sensors here.

Registered device

Power Measuring Unit

Temperature / Humidity sensor

ID: 1000060 Not set >

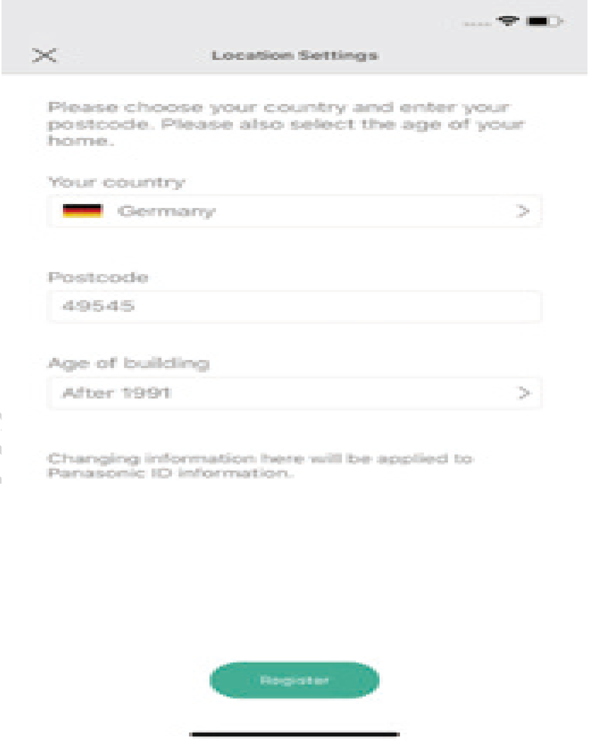
ID: 1001688 Not set >

ID: 1001691 Not set >

Fig. 1.68: Confirm the list of devices

Enter your country, postcode and the age of your home

It is depicted in Figure 1.69 given below.



Location Settings

Please choose your country and enter your postcode. Please also select the age of your home.

Your country: Germany

Postcode: 49545

Age of building: After 1991

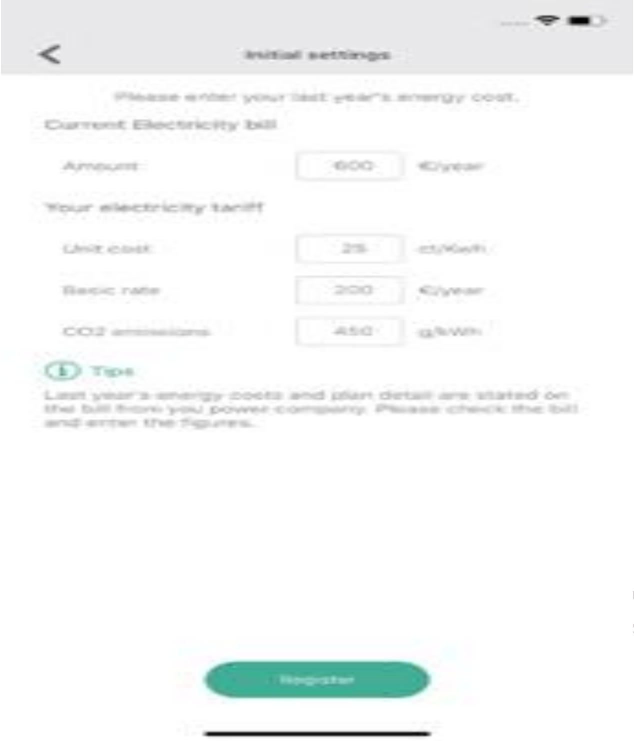
Changing information here will be applied to Panasonic ID information.

Fig. 1.69: Location settings

Tap the “Register” button.

Enter details on your electricity usage.

It is shown below in Figure 1.70.



Initial settings

Please enter your last year's energy cost.

Current Electricity bill

Amount	600	€/year

Your electricity tariff

Unit cost	25	ct/Kwh
Basic rate	200	€/year
CO2 emissions	450	g/kWh

Tips

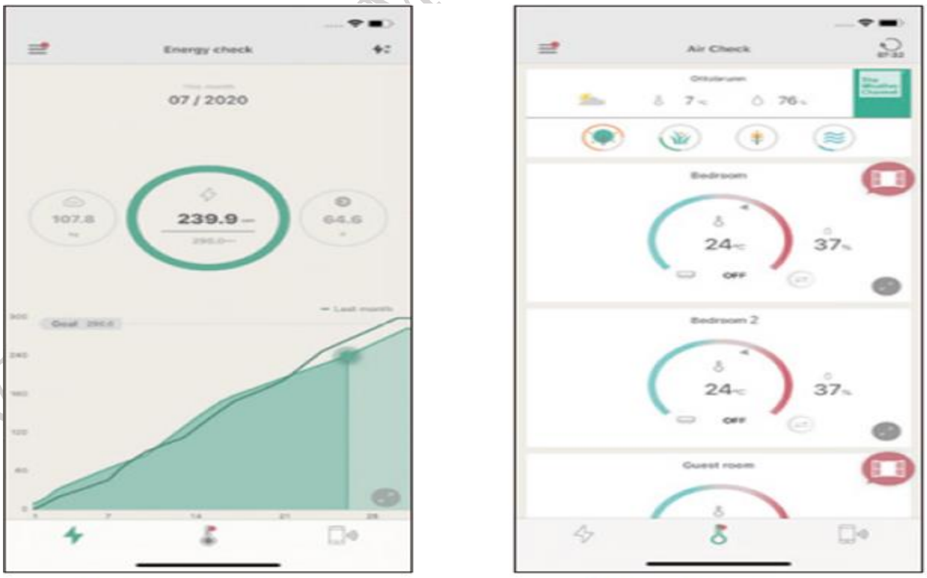
Last year's energy costs and plan detail are stated on the bill from you power company. Please check the bill and enter the figures.

Fig. 1.70: Details of electricity usage

Enter the electricity bill and energy plan for the previous year. Tap the "Register" button.

Initial setup complete

The above initial setup is complete. If a Power Measuring Unit is installed, the Energy screen will be displayed. Otherwise, the air quality screen will be displayed. It is shown in Figure 1.71.



Energy screen

Air quality screen

Fig. 1.71: Initial set up complete window

1.7 Test the Installation

It is necessary to test the nodes by turning them on and off repeatedly to see if they are functional. To check that all the connections are made properly, the devices, such as a lamp, can be plugged in and the switch is connected to an electrical socket. The technician needs to make sure of the following:

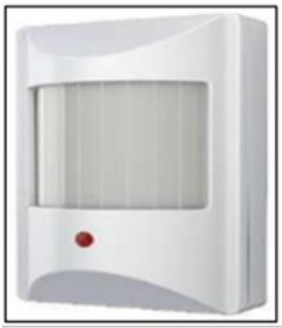
1. Every wireless connectivity and power metric work flawlessly.

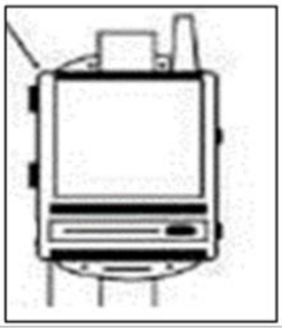
2. The nodes are positioned correctly based on the plan.
3. No external motion will result in a false trigger.

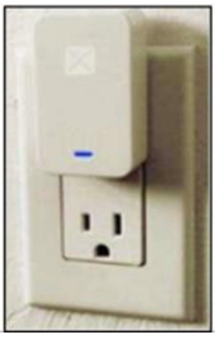
Practical activity 1.1: Demonstrate the steps of installation of the Home IoT system on personal mobile.

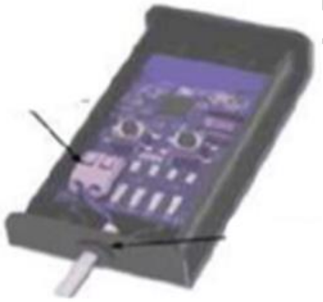
Practical activity 1.2

Identify and name the components given in following images.









Summary

- This chapter guides through setting up an Internet of Things (IoT) framework.
- It covers installing IoT devices like motion sensors, focusing on location selection, mounting, power connection, and system integration.
- The chapter also addresses gateway installation, emphasizing placement and connectivity.
- Node installation tips include proximity, elevation, and interference avoidance. Efficient node connections, both wired and wireless, are crucial. Thorough testing ensures system functionality.
- This chapter offers practical experience in deploying IoT systems effectively, reinforcing theoretical knowledge with hands-on application of Home IoT system.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. Which of the following is a key step in installing an IoT device? (a) Connecting to a Wi-Fi network (b) Plugging it into a power source (c) Inserting batteries (d) All of the above
2. In IoT device installation, what is the function of a gateway? (a) It provides power to the device (b) It connects the device to the internet (c) It collects data from the environment (d) It processes and analyses data
3. Which type of communication is commonly used for IoT devices to connect to the internet? (a) Bluetooth (b) Zigbee (c) Wi-Fi (d) NFC
4. Which of the following is an example of a sensor commonly used in IoT devices? (a) Motor (b) Camera (c) Temperature sensor (d) Speaker
5. Which of the following is an example of an edge device in an IoT installation? (a) Smart thermostat (b) Cloud server (c) Wi-Fi router (d) Internet browser
6. Which component of an IoT device is responsible for collecting data from the environment? (a) Microcontroller (b) Sensor (c) Actuator (d) Gateway

7. Which of the following is NOT a consideration for optimal placement of IoT devices? (a) Proximity to a power source (b) Signal strength for connectivity (c) Exposure to extreme temperatures or weather conditions (d) Nearness to water sources
8. Which of the following is a crucial consideration for placing sensors in an IoT system? (a) Close proximity to the gateway (b) Optimal location for accurate data collection (c) Near a power source (d) None of the above
9. What is the purpose of connecting IoT devices to a cloud platform? (a) To provide power to the devices (b) To analyse and store data remotely (c) To control the functions of the devices (d) To establish communication protocols
10. What is the purpose of a power source in IoT device installation? (a) To connect to the internet (b) To provide energy for the device's operation (c) To store data in the cloud (d) To establish communication protocols

B. Fill in the blanks

1. The gateway is responsible for storing data and providing power to an IoT ________.
2. Sensors are crucial for IoT devices as they collect ______ from the environment.
3. The ______ is a component of an IoT device that may perform actions such as turning on a motor or a light.
4. The sensor devices should be installed in such locations that their operational requirements such as _________are met.
5. A sensor detects and __________from the physical environment.
6. All devices are connected to a host device which is used as a ________.
7. The nodes should be established at ____________off the ground.
8. The IoT devices are connected to the _________after the IoT nodes and gateways have been installed.
9. Gateway software is responsible for___________and properly storing them.
10. ZigBee is the most popular protocol in terms of ___________of IoT devices.

C. State true or False for the following

1. A technician needs to understand the site requirements before creating a functional IoT framework.
2. The IoT framework includes parameters like the type of IoT device, gateways, nodes, and communication channels.
3. Motion sensor is an example of an IoT device used in an alarm system.
4. The sensor activates when it detects an object or someone nearby.
5. A parameter is a property of a sensor.
6. The device specification provides information about available parameters and what they measure.
7. All devices in an IoT system are connected to a host device used as a hub.
8. Calibrating user data involves measuring the sensor's output in response to known inputs.
9. A gateway is a wireless access point connecting Internet-connected devices.
10. Wired (DC) nodes need to be connected to the gateway.

D. Short Answer Type Questions

1. What are the basic steps involved in installing an IoT framework?

2. Explain the significance of identifying suitable points or locations for sensor installation.
3. Describe the steps involved in mounting a motion sensor on a wall or ceiling.
4. How is a motion sensor connected to the power source? What are the alternative methods for powering a sensor?
5. Briefly explain the process of configuring and installing a motion sensor.
6. What are the considerations for installing nodes in an IoT system?
7. What parameters should be considered when choosing a location for placing an IoT gateway?
8. What steps should be followed to connect devices to a gateway using Wi-Fi?
9. What are the different ways in which a gateway can be connected to the internet?
10. Why is it important to test the installation of nodes after they have been placed in their respective locations?

Session 2. Establish Communication between Nodes, Gateway and Servers

Establishing communication between nodes, gateways, and servers is a fundamental process that requires careful planning and implementation.

Nodes – These endpoints, such as sensors and devices, form the foundation of the network.

Gateway – Serving as an intermediary, the gateway connects nodes to the server, collecting and relaying data.

Servers – These systems store, process, and analyse data received from nodes via the gateway.

2.1 Different types of Communication and their applications

A) Point-to-Point – In this type of communication a single sender transmits data to a single receiver. It is shown in Figure 2.1.

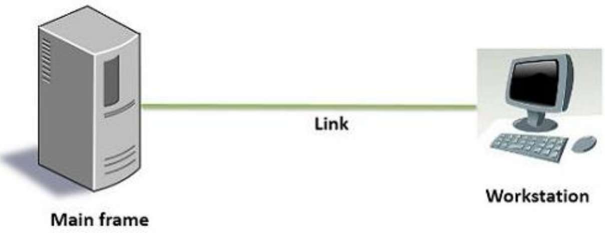


Fig. 2.1: Point-to-Point Communication

B) Point-to-Multipoint – Here a single sender transmits multiple signals to different nodes. It is depicted in the Figure 2.1.

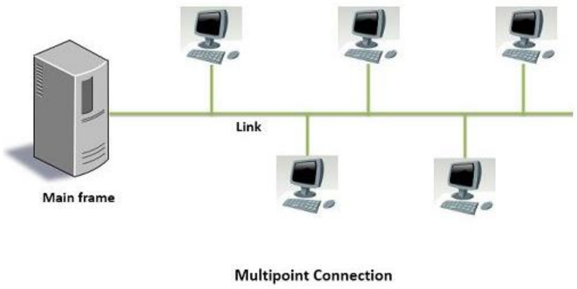


Fig. 2.2: Point-to-MultiPoint Communication

C) Multiple Access Techniques – This technique allows multiple senders to transmit signals to one or several nodes over a shared medium. It is illustrated in the Figure 2.3.

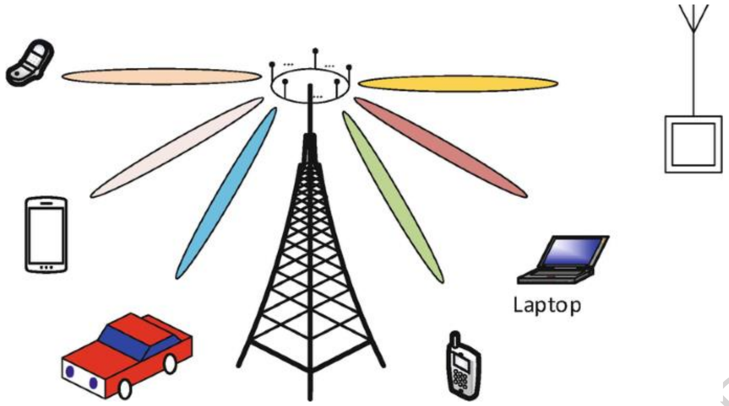


Fig. 2.3: Multiple Access Techniques

D) Relay – One or multiple intermediate nodes cooperate with a sender to transmit a signal to the receiver node in a relay network. The intermediate nodes are called repeater, relay, or gap filler nodes. It is shown in Figure 2.4.

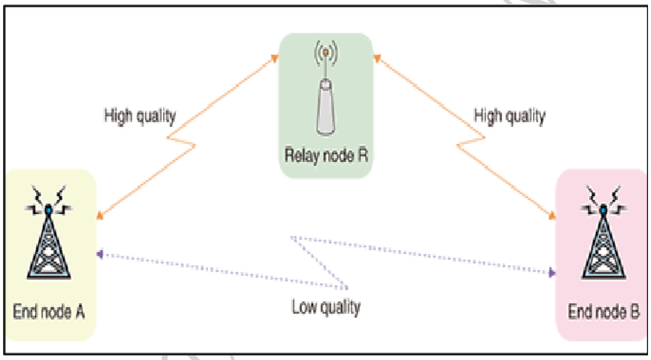


Fig.2.4: Relay Network

E) Unicast – In this type of communication, the transmitter sends data addressed to a specific user. An established phone is an example. It is depicted in Figure 2.5.

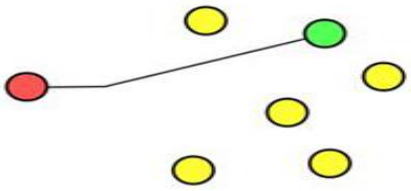


Fig. 2.5: Unicast Communication

F) Broadcast – Broadcasting means to send the data addressing all the users in the network. Radio and television are examples of broadcast mode of communication. It is given in Figure 2.6.

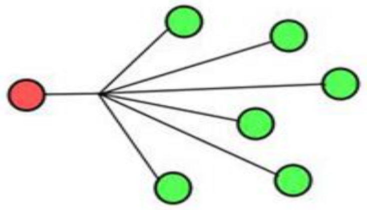


Fig. 2.6: Broadcast Communication

G) Multicast – In this type if communication, transmitter sends data addressed to a group of subscribing users. Multicasting refers to a single source of communication with simultaneous multiple receivers. Multimedia and streaming applications, such as web TV, web radio, and real time video/audio conferencing are example of this type of communication. It is given in Figure 2.7.

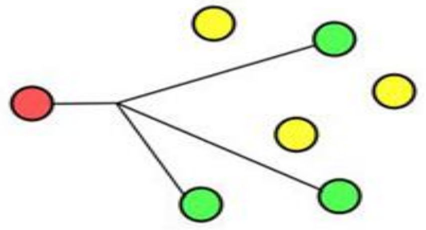


Fig. 2.7: Multicast Communication

2.2 Transmission Media

Transmission media is a communication channel that carries information from the sender to the receiver.

2.1.1 Types of Transmission Media

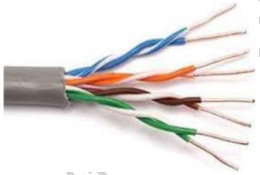
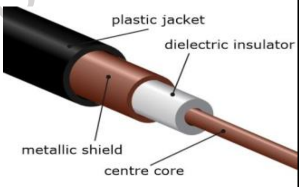
The transmission media can be of two types:

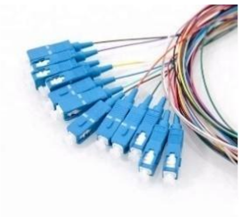
Physical Media – Consists of wires and cables

Wireless Media – Consists of air and wireless technologies such as wireless LAN (WLAN), Bluetooth, and Zigbee

Transmission channels are made of different types of communication wires and cables such as twisted-pair cable, coaxial cable, and optical fibre cable. The following table 2.1 lists different types of cables used in networking.

Table 2.1 Types of cables in networking

Type of Cable	Image	Description
Twisted pair		These have two conductor that are twisted together to cancel out the electromagnetic interference that may come from external sources. This type of cable is almost the same as a paired cable. The difference is in the two twined inner wires which are insulated, unlike in the paired cable. These are used for transmission of data over networks such as LAN.
Coaxial/ Helix cable	 plastic jacket dielectric insulator metallic shield centre core	This has a thin conducting wire inside a tubular conducting shield, which is protected by a tubular insulating jacket. It is used to connect video equipment and carry television signals.
Optical fibre cable		This contains one or more optical fibres for carrying light. The optical fibres are coated with plastic layers and secured in a protective tube. This is used for long distance communication.

Optical fibre cable (single mode)		This has small sized diametral core and permits a single mode of light to propagate through it. As a result, it reduces the number of light reflections when the light passes through the centre. This decreases the attenuation and enables the signal to travel further. This is used for a long-distance coverage with a very high bandwidth requirement.
Optical fibre cable (multimode)		This has big diametrical core and permits several modes of light to propagate through it. The number of light reflections formed when the light passes through the centre are more. This enables larger quantity of data to pass through at a given time. The strength of the signal decrease over long distance because of the increased dispersion and attenuation. This is used for backbone applications in building because of the reliability and high capacity.
Cross over cable		This connects computing devices, often of the same type as two switches.

Wireless Transmission Media

Wireless communication, using radio and microwaves, allows information to travel without needing physical cables. Radio waves are used in everyday things like radios and mobile phones for talking and broadcasting. They can also be handy in emergencies. Microwaves, which have shorter waves, are used for connecting things over longer distances, like in microwave links and satellites for TV and internet. These technologies help us stay connected without the need for wires, making communication easier and more accessible in our daily lives.

A wireless network uses wireless connections between two network nodes. Wireless networking helps to avoid the costly process of setting up cable connections in a building. Examples of wireless networks are WLAN, Bluetooth, cellular network, and so on.

2.3 Characteristics of Ethernet

A fundamentally wired or wireless network connection is needed to establish a network connection in an IoT framework. Ethernet cable connectivity is necessary for a wired connection. Ethernet is a network protocol that establishes a common method for wired (LAN) connections between computers on a network. Currently, Ethernet is the LAN technology that is used the most frequently.

The following are the characteristics of Ethernet:

- Ethernet transmits data at up to 10 megabits per second (10 Mbps).
- It is widely accepted in the computer marketplace.
- Its Cost is relatively low.
- It is generally resistant to noise.
- It has good data transfer quality.
- Speed is high.
- It is reliable.
- It provides data security.

2.4 Types of Ethernet and standards

The Figure 2.1 shows the types of Ethernet.

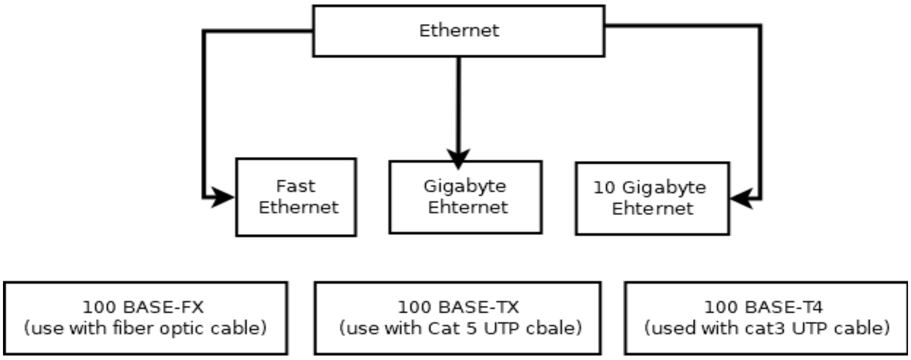

Ethernet
Fast Ethernet
Gigabyte Ehternet
10 Gigabyte Ehternet
100 BASE-FX (use with fiber optic cable)
100 BASE-TX (use with Cat 5 UTP cbale)
100 BASE-T4 (used with cat3 UTP cable)

Fig.2.8: Types of Ethernet

2.4.1 WLAN Standards

Institute of Electrical and Electronics Engineers (IEEE) has created some standards for WLAN. Wi-Fi is known by the number 801.11. Different frequency and speed bands are denominated by the letters mentioned afterwards. It is illustrated in table 2.1.

Table 2.2 WLAN Standards

Standard	Frequency	Maximum Speed
801.11	1.4 GHz	2 Mbps
801.11a	5 GHz	54 Mbps
801.11b	1.4 GHz	11 Mbps
801.11g	1.4 GHz	54 Mbps
801.11n	1.4 GHz and 5 GHz	600 Mbps

2.5 Connecting IoT Devices to the Network

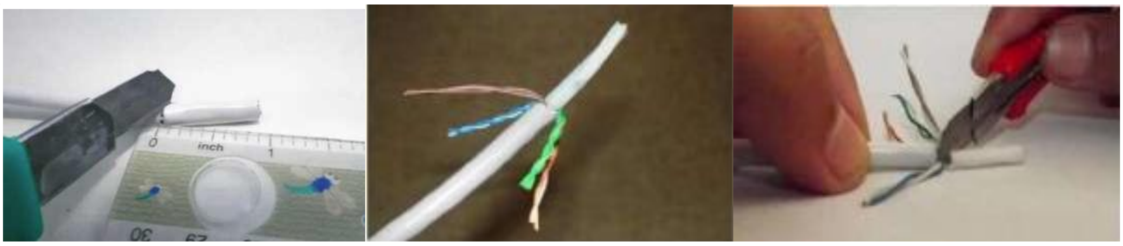
Cables need to be ready in order to connect the devices to a wired network. RJ-45 cables are typically needed for Ethernet ports. For this reason, the cables and connectors must be crimped.

2.5.1 Crimping

It is the process of joining two metal objects—typically a wire and a connector—by deforming one of them so that it can hold the other. A crimp is the resulting deformity. Crimping an RJ-45 connector onto an Ethernet cable involves several steps. The steps for crimping an RJ45 cable are as follows:

Step1. Gather Materials – Collect the necessary materials, including an RJ-45 connector, a crimping tool, and a properly measured Ethernet cable.

Step 1. Prepare the Cable – Use a cable stripper to remove about 2 inches of the outer insulation from the end of the Ethernet cable as shown in Figure 2.2.



(a) Stripping the cable (b) Pull wires backward (c) Cut the core

Fig. 2.9: Preparation of the Cable

Step 3. Arrange Wires According to Standard – Follow either the T568A or T568B color-coding standard for arranging the wires. The standard that is chosen should be consistent across the entire network.

Colour coding for Crimping RJ45 Cable

For crimping an RJ45 cable, the colour code of the internal wires is to be adhered as follows:

- To make a straight cable, the colour code is listed in the Figure 2.10.

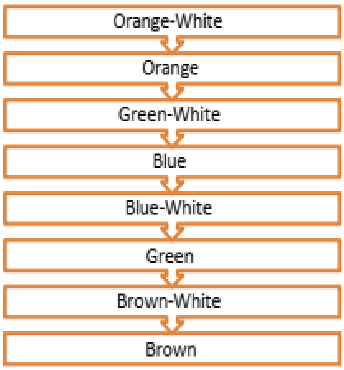


Fig.2.10: Colour code for crimping RJ45 straight cable

- To make a crossover cable, the colour code is listed in the Figure 2.11.

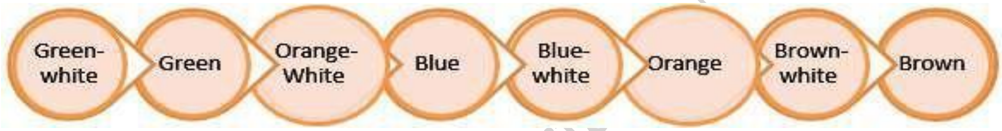
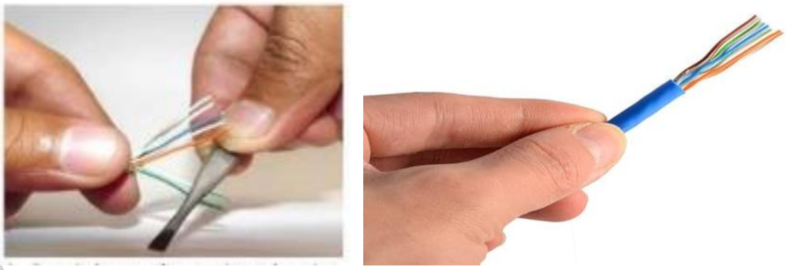


Fig. 2.11: Colour code for crimping RJ45 crossover cable

Step 4. Untwist and Straighten Wires – Untwist and straighten the individual wire pairs inside the cable. Ensure that the wires are flat and separated from each other. Make the twisted wires straight using tweezers and keep them arranged in a row based on T568A or T568B color-coding standard as shown in the Figure 2.11.



1. Straighten the twisted pairs 1. Arrange the wires in a row

Fig. 2.12: Straightening and arranging the wires

Step 5. Trim Excess Wires – Trim any excess length of the wires to ensure they fit snugly into the RJ-45 connector. Place the untwisted wires in a position from right to left according to the colour code of the wires and then trim the wires up to a suitable length as depicted in the image given in Figure 2.13.

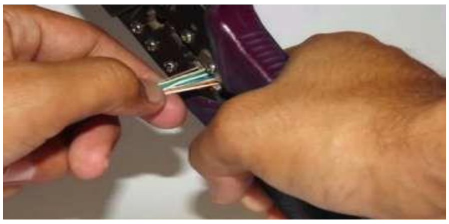


Fig.2.13: Trimming of wires

Step 6. Insert Wires into RJ-45 Connector **–** Carefully insert the arranged wires into the RJ-45 connector, ensuring they reach the end of the connector and contact the metal contacts. It is depicted in the Figure 2.14.

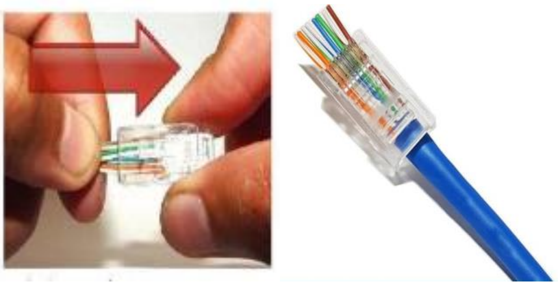


Fig.2.14: Insert Wires into RJ-45 Connector

Step 7. Check Alignment **–** The wires are to be inserted into an RJ-45 connector. Check that the wires are in the correct order and properly aligned within the connector. Any misalignment can affect the connection.

Step 8. Crimp the Connector using Crimping Tool **–** The RJ45 connector must be crimped to the cable using a crimping tool by compressing the jacket as well as the cable into the connector. This must be done in such a way that the wedge at the base of the connector is pushed into the jacket as illustrated in the Figure 2.15.

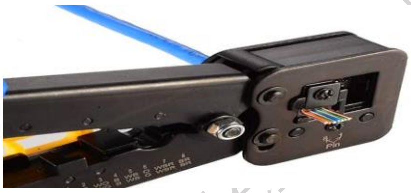


Fig. 2.15: Crimping of Connector using Crimping Tool

Step 10. Inspect the Crimp **–** After crimping, visually inspect the connector to ensure all wires are fully seated and there are no visible issues as shown in Figure 2.16.

Fig.2.16: Inspection of Connector after Crimping

Step 11. Test the Cable **–** Use a cable tester to verify that the crimped cable has been properly terminated and is capable of transmitting data without issues.

2.5.2 Connecting Devices Using Wired Ethernet

The gateway has Ethernet ports that are used to connect wired devices. The technician should perform the following steps:

1. Connect one end of the Ethernet cable to the Ethernet port as shown in the Figure 2.17.

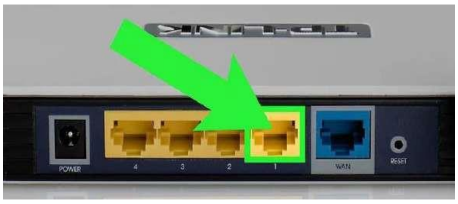


Fig.2.17: Ethernet ports

1. Connect to the WAN or Internet, if it is a modem. Otherwise, the LAN ports are connected for a router.

3. Connect the other end to the port on the device.

4. Configure the Ethernet settings in the device.

5. To check whether the network is connected or not, following steps shown in Figure 2.18 should be done.

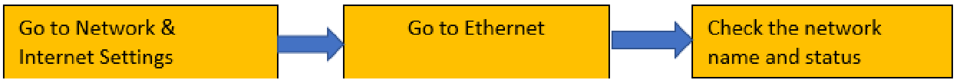

Go to Network & Internet Settings
Go to Ethernet
Check the network name and status

Fig.2.18: Connecting Devices Using Wired Ethernet

2.5.3 Connecting Devices Using Wi-Fi

The gateway may have an integrated Wi-Fi access point to which wireless devices can be connected. To connect a Wi-Fi device, following steps should be performed shown in Figure 2.12.

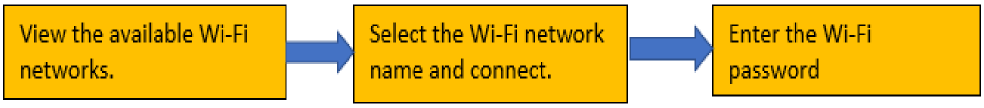

View the available Wi-Fi networks.
Select the Wi-Fi network name and connect.
Enter the Wi-Fi password

Fig. 2.19: Connecting Devices Using Wi-Fi

2.6 Types of Cables and Connectors

There are various types of connectors used for connecting communication cables as shown in the Figure 2.20.

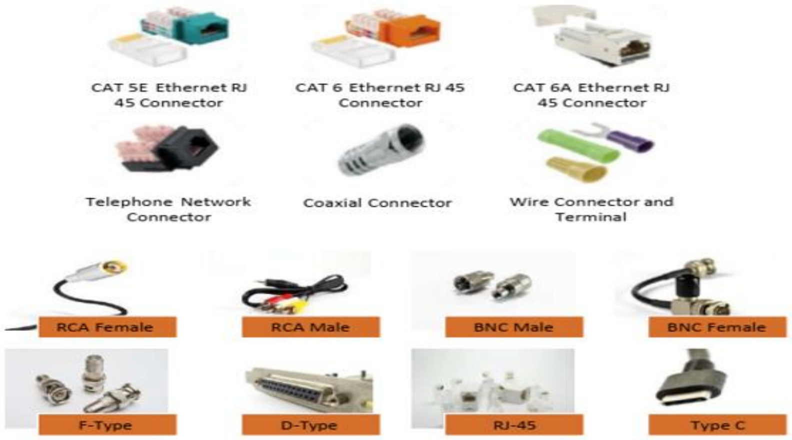

CAT 5E Ethernet RJ 45 Connector
CAT 6 Ethernet RJ 45 Connector
CAT 6A Ethernet RJ 45 Connector
Telephone Network Connector
Coaxial Connector
Wire Connector and Terminal
RCA Female
RCA Male
BNC Male
BNC Female
F-Type
D-Type
RJ-45
Type C

Fig. 2.20: Different types of connectors

The cables used in connecting the microcontrollers are network cables as shown in the table 2.3.

Table 2.3 types of cables

SN	Types of cable	Image	Applications
1.	Portable cord		These cords are used to supply power to the PCBs with microcontroller boards. These are basically 9V DC power adaptors and can be used to power sensor, actuators and the microcontroller boards.
1.	Audio-Video (AV)		These cables are used for audio and video signal transmission. These cables are used in Raspberry Pi boards.

3.	Video graphics array (VGA)		These are used to transfer picture signals from the microcontroller boards to the output devices such as screen and monitor. These can be used in Raspberry Pi.
4.	USB Cable		These cables are used for low voltage DC power supply and connecting peripherals like microcontroller boards and sensors. These can be used in both Raspberry Pi and Arduino boards.
5.	HDMI Cable		These cables are used to connect any audio/video source, such as a set-top box, DVD player or A/V receiver to an audio and/or video monitor, like digital television (DVD), with a single cable. HDMI has support for standard, enhanced or high definition video. Multi-channel digital audio support is also there. These are used for Raspberry Pi boards only.

Practical Activity 2.1: Crimping RJ45 Cable

Material Required: RJ45 cables, Crimping tool, Utility knife

Step 1. Safety Note- Ensure that you handle the utility knife with care to avoid accidents.

Step 1. Stripping the Cable-Use a utility knife to carefully strip approximately 2 inches of the outer cover from one end of the RJ45 cable. Be cautious not to cut the internal wires.It is shown in Figure 2.20.

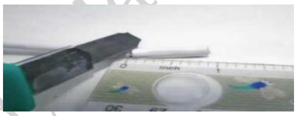
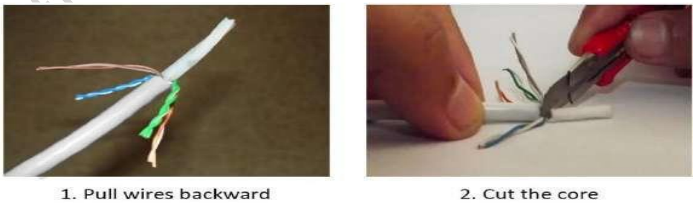


Fig. 2.20: Stripping the Cable

Step 3. Cutting the Core-Pull the twisted pairs of wires backward and use the utility knife to cut the core. Make sure not to cut the wires too short.It is depicted in Figure 2.21.

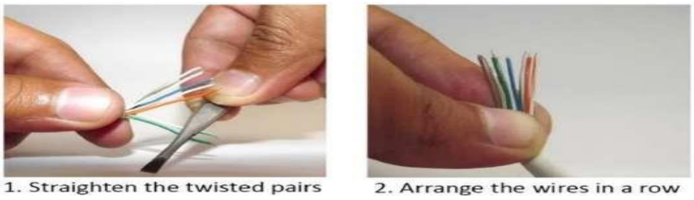


1. Pull wires backward

2. Cut the core

Fig. 2.21: Cutting the Core

Step 4. Straightening and Arranging the Wires-Use tweezers to straighten and arrange the wires in a row according to the color code as shown in Figure 2.21.



1. Straighten the twisted pairs

2. Arrange the wires in a row

Fig. 2.22: Straightening and Arranging the Wires

Step 5. Trimming the Wires-Trim the wires up to a suitable length to ensure they fit into the RJ-45 connector as shown in Figure 2.23.

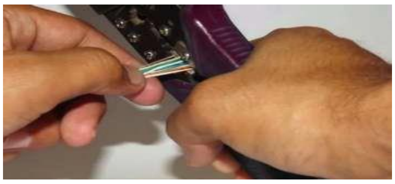
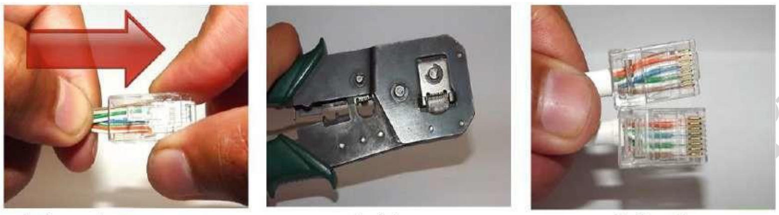


Fig. 2.23: Trimming the Wires

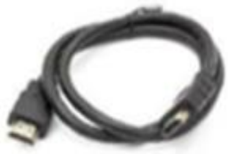
Step 6. Crimping the connector- Insert the wires into the RJ-45 connector following the color code. Use the crimping tool to compress the jacket and cable into the connector. Ensure the connector's wedge is securely pushed into the jacket as shown in Figure 2.24.



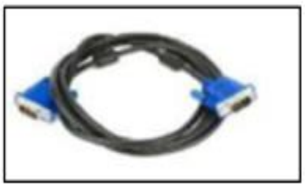
1. Insert into connector
2. Crimp
3. Result

Fig. 2.24: Crimping the connector

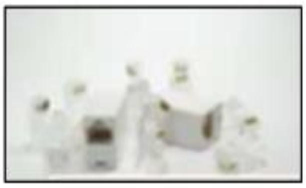
Practical Activity 2.2: Identify the cables and connector given below in the image.



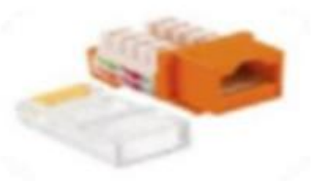
(a)



(b)



(c)



(d)

Summary

- This chapter focuses on establishing communication in IoT.
- It introduces communication types like Point-to-Point and Multipoint. Transmission media, physical and wireless, are discussed.
- Ethernet's characteristics and types are outlined in the chapter.
- Practical skills like crimping cables and configuring networks are also covered here.
- This chapter equips students with essential IoT communication knowledge.

CHECK YOUR PROGRESS

A. Multiple Choice questions

1. What type of communication involves a single sender transmitting data to a single receiver? (a) Point-to-Point (b) Point-to-Multipoint (c) Broadcast (d) Multicast
2. Which transmission media consists of wires and cables? (a) Wireless Media (b) Physical Media (c) Data Media (d) Signal Media

3. Which of the following is an example of Unicast communication? (a) Sending an email to a specific recipient (b) Broadcasting a message to all users in a network (c) Sending a group message to subscribed users (d) Transmitting data to multiple nodes
4. What is the main purpose of a relay node in communication? (a) To connect multiple devices to a single node (b) To amplify the signal strength (c) To cooperate with the sender in transmitting a signal to the receiver (d) To establish a direct link between sender and receiver
5. Which wireless standard is denominated by the number 801.11 and is commonly known as Wi-Fi? (a) Bluetooth (b) Zigbee (c) Cellular Network (d) WLAN
6. What is the maximum data transmission speed of Ethernet? (a) 1 megabit per second (b) 10 megabits per second (c) 100 megabits per second (d) 1000 megabits per second
7. Which type of cable is commonly used for Ethernet ports and requires crimping for connection? (a) Twisted-pair cable (b) Coaxial cable (c) Optical fibre cable (d) RJ-45 cable
8. What does DHCP stand for in network configuration? (a) Dynamic Host Configuration Protocol (b) Digital Hardware Communication Protocol (c) Data Handling and Configuration Protocol (d) Direct Host Connection Protocol
9. Which type of communication sends data addressed to a specific group of subscribing users? (a) Point-to-Point (b) Broadcast (c) Multicast (d) Relay
10. Which type of connector is commonly used for connecting communication cables? (a) RJ-45 connector (b) USB connector (c) HDMI connector (d) VGA connector

B. Fill in the blanks

1. Transmission media is a communication channel that carries information from the ________ to the __________.
2. Physical Media consists of __________ and __________.
3. IEEE standards for WLAN are known by the number __________.
4. ______is the process of joining two metal objects by deforming one of them so that it can hold the other.
5. Multiple Access Techniques allow __________ senders to transmit signals to __________ nodes over a shared medium.
6. Ethernet transmits data at up to __________ megabits per second (Mbps).
7. Ethernet is a network protocol that establishes a common method for wired (LAN) connections between computers on a network.
8. The cables used in connecting the microcontrollers are __________ cables.
9. The gateway has _______ that are used to connect wired devices.
10. Ethernet is generally resistant to __________.

C. State true or False for the following

1. Twisted-pair cable is an example of physical media used in networking.
2. Ethernet provides data security through encryption.
3. Ethernet is widely accepted in the computer marketplace due to its backward compatibility with older technologies.
4. Ethernet ports are used to connect wired devices in a network.
5. Coaxial cables are often used for high-frequency applications.

6. RJ-45 cables are typically needed for Ethernet ports.
7. Wireless Media consists of air and wireless technologies like wireless LAN (WLAN), Bluetooth, and Zigbee.
8. Wireless networking avoid the costly process of setting up cable connections in a building.
9. Ethernet provides data security.
10. HDMA cables are used in raspberry pi boards.

D. Short Answer Type Questions

1. Define Point-to-Multipoint communication.
2. What are Multiple Access Techniques in communication?
3. Explain Relay communication and what are the intermediate nodes called?
4. Give an example of a technology that uses Broadcast communication.
5. What is the purpose of Multicast communication?
6. What is the role of transmission media in communication?
7. Give examples of physical media.
8. Mention some wireless technologies included in wireless media.
9. Briefly explain the process of crimping.
10. Name some of the different types of connectors used for connecting communication cables.

Session 3. Pre-installation preparation of IoT devices

Before installing an IoT device that contains a sensor, gateway, and nodes on site, the technician must complete some pre-installation steps, such as site analysis and evaluation of required tools and equipment. It is required for the installation of the IoT framework on the site. This helps to ensure that installation is done effectively.

3.1 Pre-installation Preparation

The Figure 3.1 shows the pre-installation steps for installation of IoT devices.

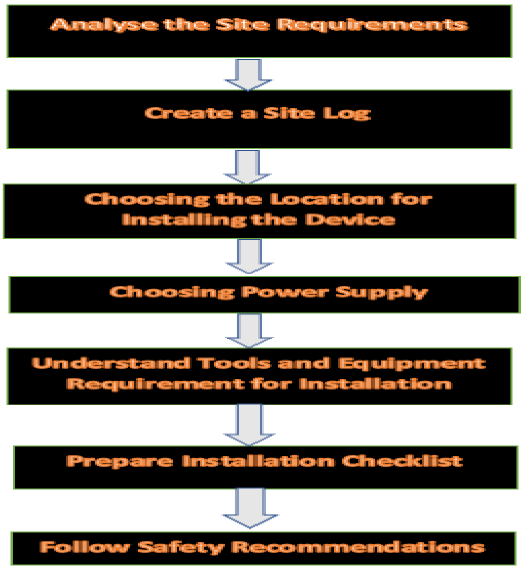

Analyse the Site Requirements
Create a Site Log
Choosing the Location for Installing the Device
Choosing Power Supply
Understand Tools and Equipment Requirement for Installation
Prepare Installation Checklist
Follow Safety Recommendations

Fig. 3.1: Pre-installation steps

3.1.1 Analysis of site requirements of IoT devices

The technician must understand the requirements of the site where the IoT setup needs to be installed. During an on-site analysis, the technician should know some details e.g. a suitable place to mount the sensors, the location of the power supply, and other factors affecting the IoT framework. It would also be helpful for the technician to understand the tools and equipment needed for installation. After analysing all important factors about the site, the technician can effectively perform the installation of the IoT setup.

The following points are important to be analysed by the technician before starting the installation:

- Suitable mounting locations for device or sensor
- Power source for the device or sensor
- A suitable method of communication between the sensor, node, and gateway

3.1.2 Create Site log

In site log creation, the technician notes down all the details of the site and the requirements at the time of installation. Information such as the mounting location for the device, wiring diagram, power source, and suitable communication network is noted down. Special requirements such as the tools and equipment which are required at the time of installation are also recorded. The Figure 3.2 shows a sample site log to be prepared after the site analysis:

Company Name Address	
Client Details Name of client: Address: Product Detail: Installation Date:	
Site Details Area: Location for Mounting Device: Special Site Requirement: Building Material Type: Power Source:	
Tools and Equipment needed Tools Required: Equipment Required: Special Requirements:	
Technician Signature	Authorising Person's Signature

Fig. 3.2: Site log

3.1.3 Choosing the Location for Installing the Device

For installing an IoT device such as a sensor or camera, the technician must select a location that does not affect the operation of the IoT device. There are few of them the common criteria are:

Keep out of the direct sunlight – The technician must install the IoT device in such a way that it functions safely in all weather conditions. Like any IoT device, such as a sensor or camera, it is designed to operate in temperature range. In order to avoid direct sunlight, the IoT camera in the Figure 3.3 is mounted in the shade.

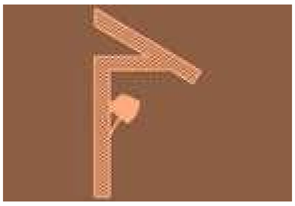


Fig.3.3: IoT camera installed in the shade to avoid direct sunlight

Keep the Device Within Network Range – Since an IoT setup relies on the Internet, any mode of communication, wired or wireless can be used to connect the devices. In order to prevent signal loss in the setup, the technician should install the IoT device close to a network setup, such as a router. A Wi-Fi router can be seen in direct line of sight from an Internet of Things camera in the illustration given below in Figure 3.4.

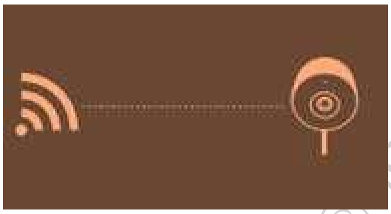


Fig.3.4: IoT camera considering a Wi-Fi router

Consider the Environment – The technician should be considered the surrounding area when installing the IoT device because there shouldn't be any obstructions like plants, walls, or other objects in the operating area or the area covered by the sensor or camera. In the Figure 3.5, a plant can be seen in an IoT camera's field of view.

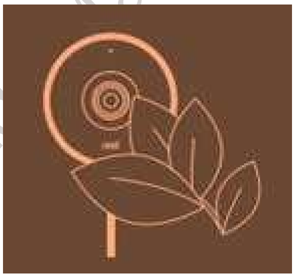


Fig.3.5: Installation under the field of view of the IoT camera

Place the device on height- A sensor installed as part of the Internet of Things should be placed at the ideal height for clear operation. For instance, a camera needs to be placed at a specific height in order for it to be able to recognize faces. The ideal height for mounting an IoT camera is shown in the Figure 3.6.

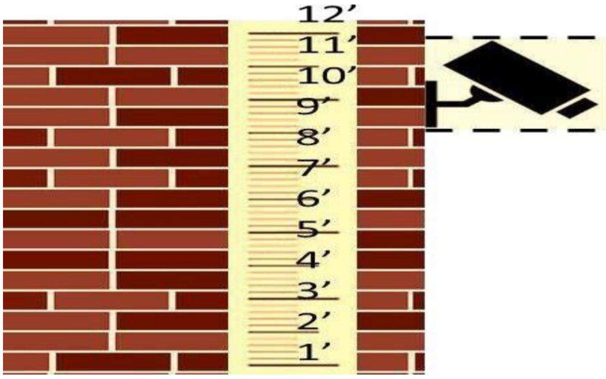


Fig.3.6: Camera installed at an optimum height

3.1.4 Choosing Power Supply

The technician should choose the power supply for the IoT device after deciding a suitable location for installation. The following factors should be taken into account by a technician when choosing the power supply:

- The IoT device and the power outlet should be as close as possible.
- The power source should be close to a well-ventilated, dry area. Avoid places like the kitchen, bathroom, or laundry.
- The power supply should be placed in a less busy area to prevent damage from people movement.
- The power source must be situated so that all of the indicators' lights are clearly visible from a distance.
- The main electric distribution box should be installed in the same building as the power supply, not in a separate garage or storehouse.
- Additionally, when connecting the power supply cord to the power supply and the device, the wiring must be done properly. The Figure 3.8 shows safe and unsafe power cable arrangement.

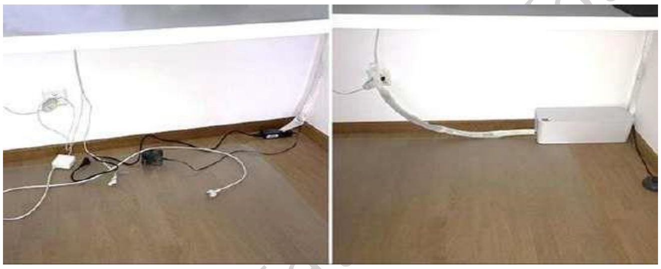


Fig.3.7: Safe and unsafe power cable arrangement

3.1.5 Understand Tools and Equipment Requirements for Installation

The technician uses a variety of tools to install devices and sensors, like drill, screwdriver, hammer, as well as different equipment, like a signal tester, multimeter. To complete the installation process, the technician must be familiar with the use and correct handling of these tools and equipment.

For example, to measure the electrical parameters like voltage, current and so on, a multimeter can be used. There are various settings available in a multimeter, such as the following:

- for AC and DC current in micro/milli-amps as well as amps.
- for AC and DC voltage in millivolts as well as hundreds of volts.
- for resistance in ohms as well as Megaohms.

There may be some additional settings for measuring frequency, capacitance, decibels, inductance and temperature. To test a speed sensor using a multimeter, the steps are as follows:

Step 1. Attach the red lead to the signal output and the black lead to the ground on the speed sensor as shown in the Figure 3.8.

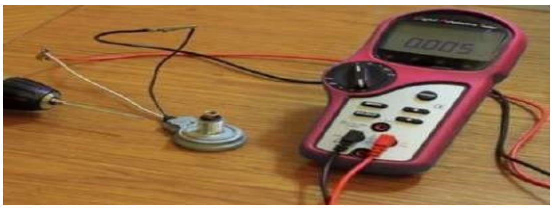


Fig.3.8: Attaching the sensor leads to the multimeter

Step 1. Take a moving device to generate the signal. For example, a drill is used here. Attach the drill to the sensor and power on the drilling machine. The Figure 3.9 shows increase in the voltage output of the sensor with increased rotation per minute (RPM) of the dril.

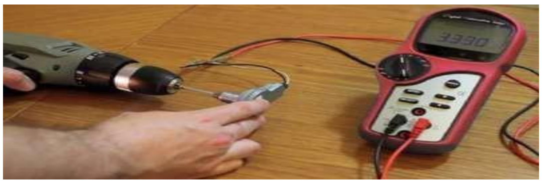


Fig. 3.9: Increased voltage output of the sensor with increased RPM of the drill

Step 3. Power off the drill and check the reading as shown in the Figure 3.3.

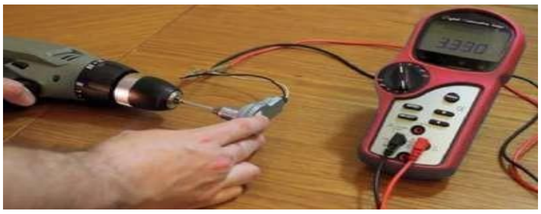
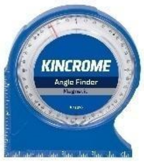


Fig. 3.10: Reading after powering off the drill

Device and Tools Used

The various tools and equipment required for the installation of IoT devices are mentioned in table 3.1.

Table 3.1: Tools required in installing IoT device

SN	Tool and Equipment	Use	Image
1.	Angle Finder	Used to find degree of bend and precision angle Used in proper positioning of the nodes and sensors according to the requirement	
1.	Spirit level	Used to measure vertical, horizontal and diagonal planes Used for mounting the nodes and edge devices at accurate level	
3.	Tape	Used for routing wiring through the walls and electrical conduits	
4.	Cordless drill	Used to drive screw into various substrates without damaging them Used to drill on the mounting surface	
5.	Drill bits	Used to remove material for creating different kinds of holes in different materials Are attached to a drill to cut through the work object by rotating it Available in various sizes and shapes	

6.	Torque wrench	Used to apply a specific torque to a nut or bolt at the time of assembling and installing the devices	
8.	Wire strippers	Used to strip the insulation part from electric wires	
8.	Crimpers	Used to crimp which is binding two pieces of metal by metal by deforming one or both of them such that they hold each other Used to crimp Ethernet cables while making network connection between nodes and gateways	
9.	Needle-nose pliers	Used to bend, re-position and snip wire Helps in reaching areas where fingers or any other tools/instrument cannot reach easily, such as microcontrollers within a device	
3.	Wire cutter	Used for cutting wires as small and large wire are needed for IoT device installation	
11.	Multimeter	Used to measure resistance, current and voltage of nodes and power supplies	
11.	Tape measure	Is a ruler made up of ribbon or cloth, fiberglass, plastic or metal strip Consists of linear-measurement markings Used for measuring distance of the node and gateway locations from the ground, ceiling and neighbouring surfaces	
13.	Heavy duty extension cords	Is flexible electrical power cable also know as flex, attached to a plug on one end and one/multiple sockets on the other end Used in case of high voltage power supply for heavy work operations such as power supply of large drilling machines on construction sites	
14.	Fuse pullers	Used to insert and remove electrical fuses from housing	

15.	Magnetic wristband	Is a band worn on the wrist that has magnetic mechanism to hold tools such as nails, fasteners and drill bits while working. Used for installing nodes and devices at a height	

3.1.6 Prepare Installation Checklist

The technician must prepare the site for installation after analysing the site and determining the equipment and tool requirements. Clearing the workspace, designating the location for mounting the devices, and choosing an appropriate power source are all steps in this process. To successfully complete the installation, each step should be listed in the checklist in the correct order.

3.1.7 General safety instructions for installation of IoT devices

The following details are included in general safety instructions:

Keep the cable connectors and delicate circuit ports free of dust both during and after installation. In order to shield ports and connectors from dirt, debris, and water, covers and caps can be used. Protect the tools and equipment during transportation from any damage.

When performing the installation, avoid wearing loose clothing. While performing the installation, wear safety gear. The following items are included in safety equipment:

- Helmet for head protection
- Goggles for eye protection
- Gloves for hand protection
- Shoes for foot protection
- Jackets for body protection
- Ear muffs for ear protection
- First-aid supplies

Safety with Electricity

The following points need to be kept in mind while working with electricity:

- Before making the electrical connections, find the electrical wiring setup and turn off the power. Prevent any potentially dangerous working environments, such as moisture, underground cables, or damage to the power chords.
- Take the appropriate precautions to avoid Electrostatic Discharge (ESD), such as:
- Grab the edges of the printed circuit board (PCB).
- Never put electrical components on a surface made of metal.
- When not in use, keep the components in ESD-safe packaging.
- When handling components, put on the safety equipment depicted in the Figure 9.11 that are susceptible to ESD.

Fig. 3.11: Safety gears for protection

Practical Activity 3.1. To familiarize with the basic functionalities of a multimeter and how it can be used to measure electrical parameters.

Materials Required:

Multimeter, Power source (e.g., battery), Wires with alligator clips, Resistor

Practical Activity 3.1. To familiarize with the basic functionalities of a multimeter and how it can be used to measure electrical parameters.

Materials Required:

Multimeter, Power source (e.g., battery), Wires with alligator clips, Resistor

Procedure

Step 1. Begin by introducing the multimeter and explaining its purpose-to measure various electrical parameters like voltage, current, and resistance.

Show the different parts of the multimeter (display, dial, probes, etc.) and explain their functions.

Step 1. Explain the various settings available on the multimeter dial (e.g., voltage, current, resistance, etc.). Demonstrate how to select the appropriate setting for different measurements.

Step 3. Connect the multimeter to a power source (e.g., battery) and set it to the voltage measurement setting. Show how to properly use the probes to measure the voltage across the battery terminals. Discuss the unit of measurement (volts) and the reading on the multimeter display. It is shown in Figure 3.11.

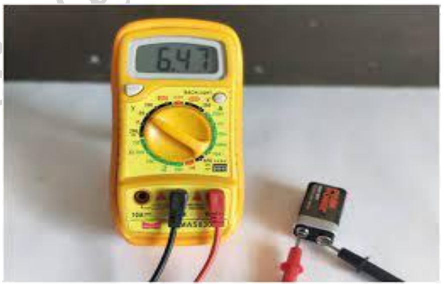


Fig. 3.12: Voltage measurement using multimeter

Step 4. Introduce a resistor into the circuit and set the multimeter to measure current. Explain how to properly connect the multimeter in series with the resistor to measure current flow. Discuss the unit of measurement (amperes) and the reading on the multimeter display. This arrangement is shown in Figure 3.13.

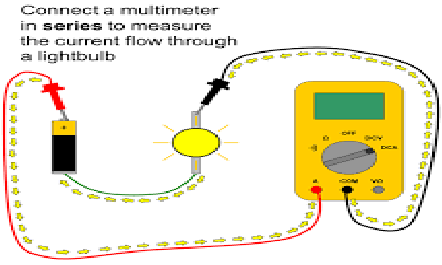

Connect a multimeter in series to measure the current flow through a lightbulb
OFF
DCV
DCA
A
COM
VΩ

Fig. 3.13: Current measurement using multi meter

Step 5. Disconnect the power source and set the multi meter to measure resistance. Connect the probes to both ends of the resistor to measure its resistance. Discuss the unit of measurement (ohms) and the reading on the multi meter display. It is shown in Figure 3.14.

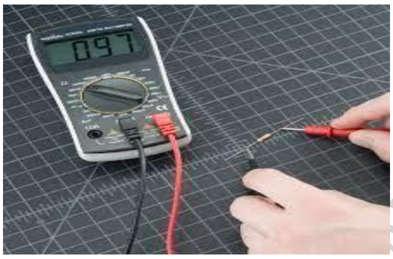


Fig. 3.14: Resistance measurement using multimeter

Step 6. Briefly explain other settings on the multimeter, such as continuity and diode testing, and when they might be used.

Demonstrate how to use these settings with simple examples (e.g., testing a diode).

Step 7. Discuss important safety precautions, such as not touching live wires, avoiding short circuits, and handling the multimeter carefully.

Assignment 3.1: Make a list of various devices and tools required for installation.

Summary

- This chapter introduces the critical pre-installation steps for effective IoT device setup.
- It covers site analysis, understanding site requirements, choosing installation locations, power supply considerations, required tools, checklist preparation, and safety instructions.
- The chapter gives emphasize on careful planning and execution to ensure successful IoT integration.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What are the key pre-installation steps for IoT device installation? (a) Site analysis and evaluation of required tools and equipment (b) Connecting sensors, gateways, and nodes (c) Installing software updates (d) None of the above
2. During on-site analysis, what are the important factors a technician should consider? (a) Suitable mounting locations, power source, and communication method (b) Weather forecast for the installation day (c) Names of neighbouring technicians (d) None of the above

3. What is the purpose of creating a site log after site analysis? (a) To record details of the site and installation requirements (b) To create a log of all technicians working on the site (c) To note down personal thoughts and observations (d) None of the above
4. When choosing the location for installing an IoT device, what should a technician consider regarding sunlight exposure? (a) Install the device in direct sunlight for better performance (b) Keep the device out of direct sunlight to ensure safe operation (c) It doesn't matter if the device is exposed to sunlight (d) None of the above
5. Why is it important to keep the IoT device within network range during installation? (a) To prevent interference from other devices (b) To ensure optimal communication and signal strength (c) It is not necessary to be within network range (d) None of the above
6. What should a technician consider regarding the environment when installing an IoT device? (a) Ensure there are no obstructions in the operating area or field of view (b) Install the device near plants for better aesthetics (c) Obstructions don't affect IoT device operation (d) None of the above
7. For clear operation, what is important when placing a sensor as part of the Internet of Things? (a) It should be installed at the lowest possible height (b) It should be placed at an optimum height for its intended purpose (c) Height doesn't affect sensor operation (d) None of the above
8. What factors should a technician consider when choosing the power supply for an IoT device? (a) Proximity to the IoT device and proper wiring (b) Choose any power source, as long as it is within the building (c) Install the power supply in a busy area for easy access (d) None of the above
9. What equipment can a technician use to measure electrical parameters like voltage and current? (a) Multimeter (b) Oscilloscope (c) Power drill (d) None of the above
10. Why is it important to follow general safety instructions during IoT device installation? (a) To ensure the devices function properly (b) To protect the technician from accidents or damage (c) Safety instructions are optional and not necessary (d) None of the above

B. Fill in the blanks

1. Technicians use various tools like ____________for IoT device installation.
2. Multimeters have settings for measuring __________ with additional options for _________and more.
3. When choosing a power supply, prioritize proximity to the IoT device and ensure _____________are visible from a distance.
4. The technician should wear _____________to ensure protection while working.
5. When handling components susceptible to Electrostatic Discharge (ESD), avoid putting them on a surface made of __________.
6. Site analysis involves _______________and communication methods for IoT components.
7. Ensure no obstructions __________ obstruct the field of view of IoT cameras or sensors.
8. When performing the installation, avoid wearing ______.
9. Magnetic wrist band is used for_______.
10. Angle finder is used to find__________.

C. State true or False for the following

1. It is important to install an IoT device in direct sunlight to ensure optimal performance.
2. The power source for an IoT device should be located in a well-ventilated, dry area.
3. The main electric distribution box can be installed in a separate garage or storehouse for convenience.

4. It is important to choose a location for installing an IoT device that does not interfere with its operation.
5. An IoT device should be kept within network range to ensure stable communication.
6. Obstructions like plants, walls, or other objects are negligible when installing an IoT device.
7. Site log creation involves recording details of the site and installation requirements.
8. When using a multimeter, there are settings available for measuring the distance.
9. IoT devices must be placed at a height that is not reachable to anyone.
10. The location for installing an IoT device should not interfere with its operation.

D. Short Answer Type Questions

1. What are the pre-installation steps required before installing an IoT device?
2. What details should a technician consider during on-site analysis?
3. Why is it important to choose a suitable location for installing an IoT device?
4. What are the common criteria for choosing a location to install an IoT device?
5. What factors should a technician consider when choosing a power supply for an IoT device?
6. Name some tools and equipment used for installing IoT devices.
7. What are the settings available in a multimeter for measuring electrical parameters?
8. What steps should be followed to test a speed sensor using a multimeter?
9. Why is it important to wear safety gear during installation?
10. What precautions should be taken while working with electricity?

Session 4. Mounting Devices at Desired Locations

At the time of installation of Internet of Things (IoT) devices, the place of installation is a matter of great concern. It affects how well the whole system works. Whether it is sensors collecting data or other IoT parts, where they are placed makes a big difference. It affects how accurate the data is, how well things communicate, and how the whole system performs. Hence there is a need to think about things like saving energy by putting devices in the right places, keeping them safe from unauthorized access, and making sure they work well together. So, deciding where to put IoT devices is crucial for making sure everything runs smoothly and stays reliable in different situations.

4.1 Surface Preparation

The first step in installing any IoT device is to prepare the surface on which the device has to be mounted. For example, installing the sensor on a wall or any surface, the surface must be prepared so that the device can be installed easily.

For the installation of an IoT device such as a wall-mounted camera, the technician needs to choose a suitable location and after that, steps shown in table 4.1 are performed for preparation of the mounting surface.

Table 4.1: Surface Preparation Steps

SN	Steps	Image

1.	Check the levelling of the surface using a spirit level.	
1.	Mark the area for creating holes to mount the frame on which the camera is to be installed.	
3.	Perform drilling to make holes for the screws which are to be mounted in the frame to hold the camera in place.	
4.	After creating a hole, clean the hole and then put wall anchors if needed.	

4.2 Mounting of Device

After preparing the surface and installing the frame, the next step is to mount the device. For different types of devices such as gateways or cameras, different types of mounting setups are present depending on the model and the making. Sensors are usually installed within a switch, light, or other device. Therefore, they do not require mounting.

For example, if a motion detector device needs to be installed, the steps are as follows:

Step 1. Choose a place to mount the sensor.

Step 1. Remove the tape from the back of the sensor and press the sensor firmly against the wall. The sensor should be placed in such a way that the LED light is at the top and the glass eye is at the bottom, as shown in the Figure 10.1.

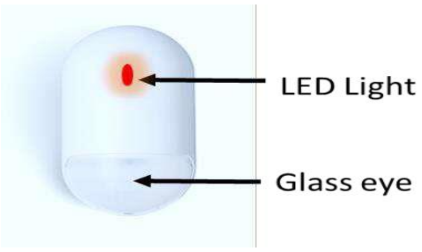
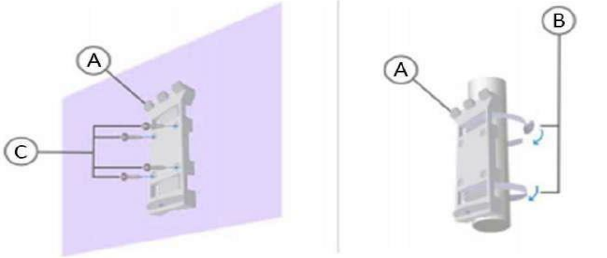


Fig. 4.1: Placing of motion detector sensor

To mount the camera, first install the camera bracket that holds the camera at its place on the wall. The steps to install an IoT camera are covered as follows:

1. Put the camera holding bracket on the wall and secure it with screws. If the mounting is on a pole, then use plastic ties to secure the camera bracket at its place. The Figure 4.2 shows the mounting of a camera bracket:



A: Mounting bracket, B: Straps, C: Mounting screws

Fig. 4.2: Mounting camera bracket on a wall

1. After placing the screws, tighten them using a screwdriver and check whether the bracket is installed tightly and is secured at its position or not. The Figure 4.3 shows a tightening of screws to mount the camera bracket:

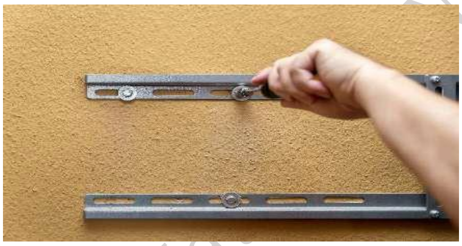


Fig. 4.3: Mounting camera bracket on wall

4.3 Factors for consideration in mounting

Choosing Distance between Network Devices-For proper communication and signal transmission between IoT network devices, a few factors should be considered. The factors that affect the signal between network devices are as follows:

Physical Obstructions – In wireless signal set up, physical objects such as walls, buildings and other objects create hindrance in the wireless network. So, the wireless device should be kept at a spot where the wireless signals cannot be obstructed. The Figure 4.4 depicts the line-of-sight communication inside a room between an edge device such as a camera and a gateway/router.

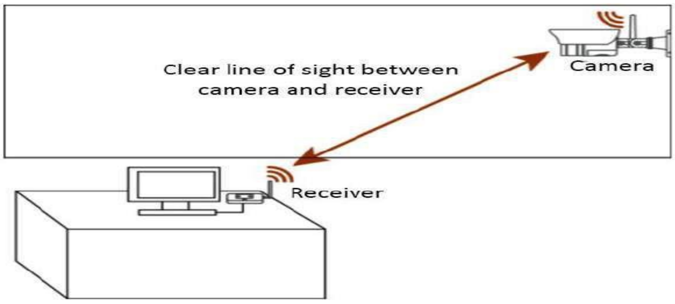


Fig. 4.4: Line of sight communication between camera and receiver inside a room

If heavy building materials cannot be avoided, the wired connection should be used. The example is shown in the Figure 4.5.

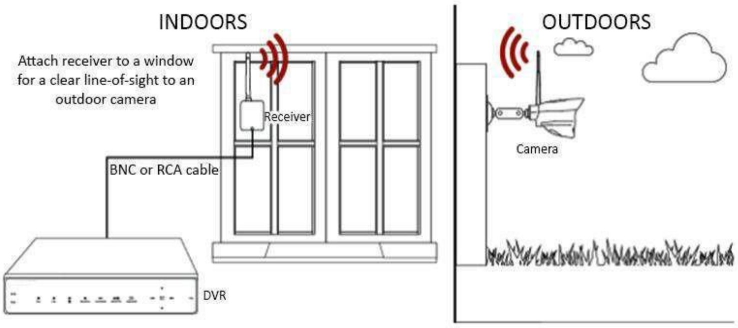

INDOORS
OUTDOORS
Attach receiver to a window for a clear line-of-sight to an outdoor camera
Receiver
BNC or RCA cable
Camera
DVR

Fig. 4.5: Line of sight between camera and receiver in outdoor and indoor areas

Network Range and Distance between Devices-Net strength between the distance between network devices is reduced by the inverse cube. So, at a distance of 2 meters, the signal strength decreases about 8 times compared to the signal strength device at a distance of 1 meter. The Figure 4.6 shows the weakening of the signal strength.

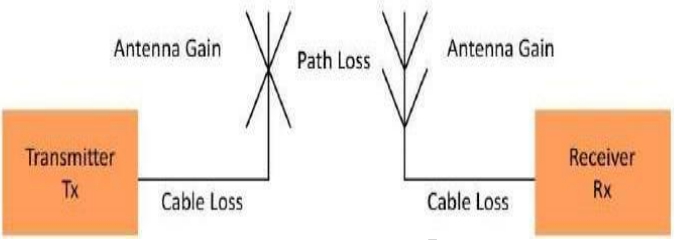


Fig. 4.6: Drop in signal strength

4.4 Selection of switch and router

When installing the IoT framework at a location, the technician must plan and design the local network agreement. This helps ensure compliance with all requirements, associated costs, and regulations based on the technical project and plan. When selecting devices for the IoT LAN network framework should consider the following factors:

Factors to be Considered while Selecting a Switch

Cost – The cost of the switch is based on its capacity and features as per its use. The capacity of the switch is based on the number of ports and the switching speed. The Figure 4.7 shows two networks set up with switches.

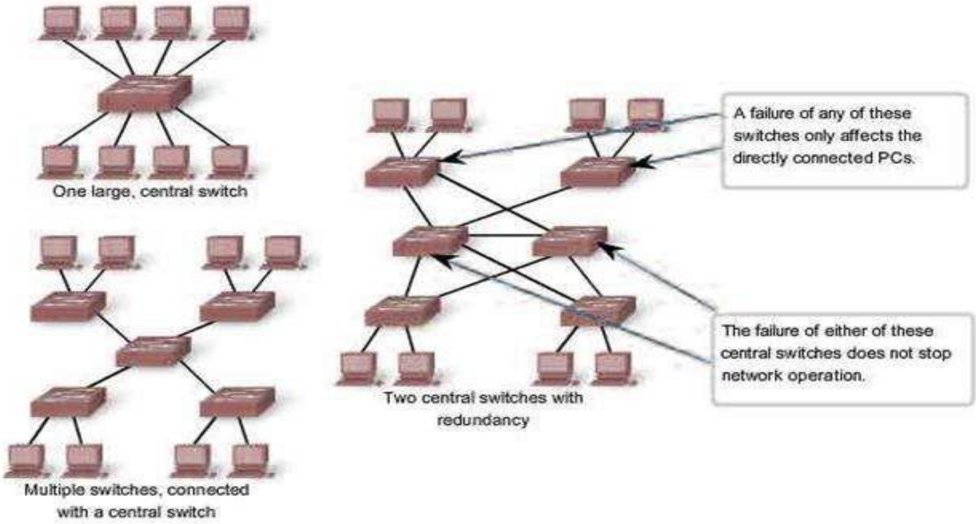

One large, central switch
Multiple switches, connected with a central switch
Two central switches with redundancy
A failure of any of these switches only affects the directly connected PCs.
The failure of either of these central switches does not stop network operation.

Fig. 4.7: Switch selection for a LAN network

Speed and Types of Ports – As per the usage of IoT network framework the switch is selected as different ports may provide different speeds. So, while choosing the best switch, network requirements should be checked. The Figure 4.8 shows different types of switches based on the speed.

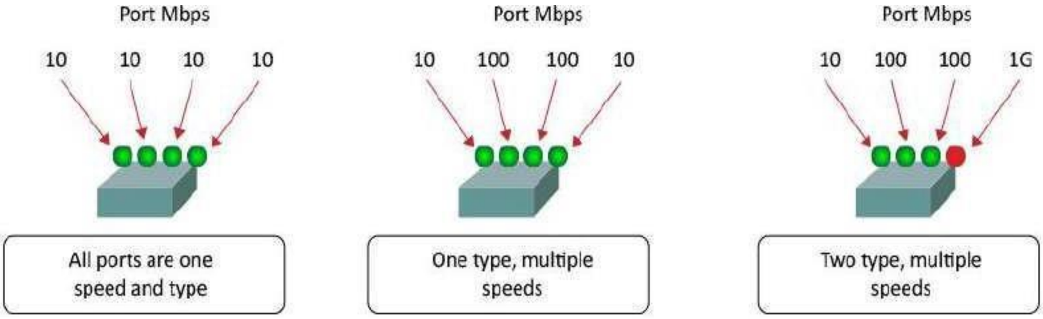

Port Mbps
10 10 10 10
All ports are one speed and type
Port Mbps
10 100 100 10
One type, multiple speeds
Port Mbps
10 100 100 1G
Two type, multiple speeds

Fig. 4.8: Speed factor for selecting switch for LAN network

Factors to be Considered while Selecting a Router

Expandability – While selecting a router, the number of devices to be connected in the entire network with the router should be checked. This will help in selecting the optimum router.

Operating System Features – Based on the type of security level, quality of service and the routing layer protocol, the router is chosen as per the best suitable version of router configuration for the network.

4.5 Signal and Power Loss during the Inter-device Communication

A signal that travels through network cables or signals that travel through a wireless channel gets low. This happens due to the loss of strength and power over a long- distance because of impairment or physical obstruction. A technician should check for signal loss over the network and select the correct cable to transmit signals on a fixed network. In a wireless network, the technician must select the router and wireless network settings to minimize signal loss. The Figure4.9 illustrates wireless and wired signal loss.

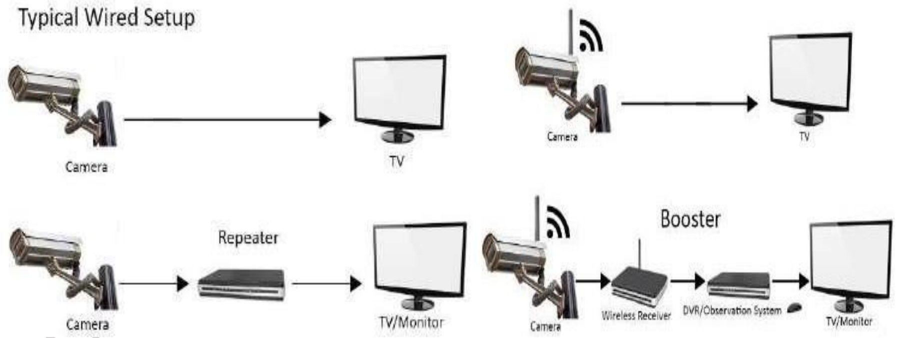


Fig. 4.9: Wireless and wired signal loss

4.6 Cabling

Total Cable Length – The maximum length for any kind of LAN cabling is 100 meters per channel. The patch cable length should be 5 meters in accordance with the standard. Signal loss is significantly influenced by cabling distance. Therefore, various types of cables are offered in accordance with the ideal cable distance to prevent signal loss.

For instance, Ethernet cables should not exceed a length of 90 meters. Fibre optic cable can be used to connect two points up to a few kilometres away. A LAN network's cabling setup is shown Figure 4.10.

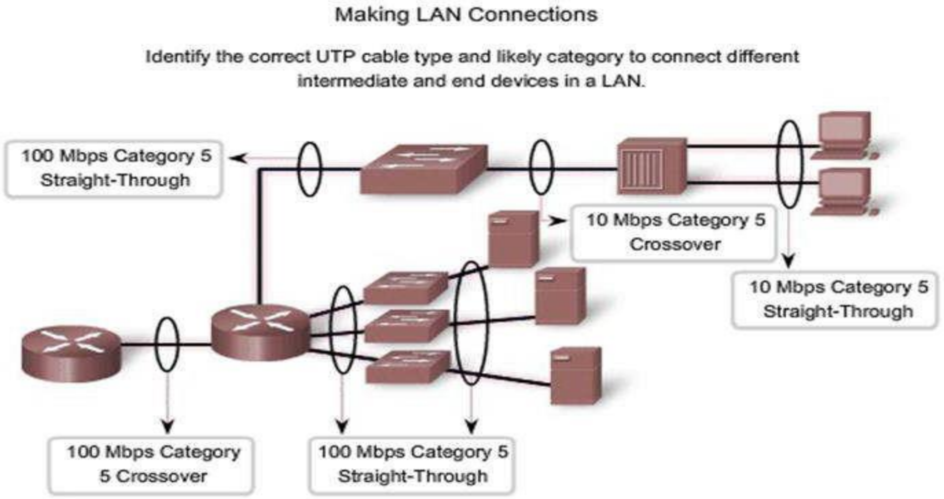

Making LAN Connections
Identify the correct UTP cable type and likely category to connect different intermediate and end devices in a LAN.
100 Mbps Category 5 Straight-Through
10 Mbps Category 5 Crossover
10 Mbps Category 5 Straight-Through
100 Mbps Category 5 Crossover
100 Mbps Category 5 Straight-Through

Fig. 4.10: Cabling set up for a LAN network

The technician must know the cable types used in the installation of the IoT framework for making the necessary cable connection. The following steps must be followed when connecting cables in an IoT framework.

1. Use more cable and leave some slack.

1. Test each network device installed.

3. Keep the cable structure away from sources of electrical inference.

4. Pull the cable through the wall and secure it with wire clips.

5. Mark and label the ends of each cable.

6. Be sure to use cable ties to keep cables together and organized.

Practical Activity 4.1: To mount a Camera device at specific locations

Step 1. Introduce a sample IoT camera and its mounting bracket.

Step 1. Install the camera bracket that holds the camera at its place on the wall.

Step 3. After placing the screws, tighten them using a screwdriver and check whether the bracket is installed tightly and is secured at its position or not as shown in Figure 4.4.

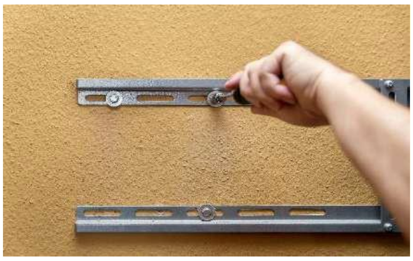


Fig. 4.11: Cabling set up for a LAN network

Step 4: mount the camera on this bracket.

Summary

- This chapter covers surface preparation, emphasizing tasks like level checking, marking mounting points, and using wall anchors.
- The chapter guides technicians through mounting processes for sensors, cameras, and gateways, providing clear instructions.
- It emphasizes strategic placement considering factors like signal obstruction and range.

- Selection tips for switches and routers, highlighting cost, port types, and expandability are discussed here.
- Managing signal and power loss due to distance or obstruction is addressed in the chapter.
- Proper cabling techniques are emphasized here including testing, interference prevention, and secure labeling.
- Overall, this chapter equips technicians with essential skills for IoT device installation.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the first step in installing any IoT device? (a) Mounting the frame (b) Surface preparation (c) Drilling holes (d) Choosing a location
2. What tool is used to check the leveling of the surface during surface preparation? (a) Screwdriver (b) Spirit level (c) Drill machine (d) Hammer
3. What is the purpose of marking the surface during surface preparation? (a) To create holes for screws (b) To check the levelling (c) To guide the installation process (d) To clean the surface
4. What is used to hold the camera in place on the wall during mounting? (a) Wall anchors (b) Mounting bracket (c) Plastic ties (d) Spirit level
5. Which device is usually installed within a switch, light, or other device and does not require mounting? (a) Gateway (b) Sensor (c) Camera (d) Router
6. What should be considered for proper communication between IoT network devices? (a) Physical obstructions (b) Network range (c) Switch configuration (d) Router selection
7. How does signal strength between network devices change with distance? (a) Decreases linearly (b) Decreases quadratically (c) Decreases cubically (d) Increases linearly
8. What factor should be considered when selecting a switch for an IoT network? (a) Cost and capacity (b) Operating system features (c) Expandability (d) Cable length
9. What is the maximum length for any kind of LAN cabling per channel? (a) 50 meters (b) 85 meters (c) 100 meters (d) 150 meters
10. What is a crucial step when connecting cables in an IoT framework? (a) Leaving no slack in the cable (b) Testing each network device installed (c) Keeping cable structure close to electrical sources (d) Avoiding the use of cable ties

B. Fill in the blanks

1. Check the levelling of the surface using a _______ level.
2. Put the camera holding bracket on the wall and secure it with _______.
3. A signal that travels through network cables or signals that travel through a wireless channel gets _______.
4. If heavy building materials cannot be avoided, the _______ connection should be used.
5. To mount the camera, first install the camera bracket that holds the camera at its place on the _______.
6. A technician should check for _________and select the correct cable to transmit signals on a fixed network.
7. The cost of the _______ is based on its capacity and features as per its use.

8. Keep the cable structure away from sources of _________.
9. Signal loss is significantly influenced by __________.
10. In a wireless network, the technician must ________ settings to minimize signal loss.

C. State true or False for the following

1. The signal strength between network devices increases proportionally with the distance between them.
2. A signal that travels through network cables or wireless channels experiences signal loss due to factors like physical obstruction.
3. The maximum length for any kind of LAN cabling is 200 meters per channel.
4. Sensors are usually installed within a switch, light, or other device, so they do not require mounting.
5. The selection of a switch for the IoT LAN network depends on factors such as cost, speed, and types of ports.
6. The router is chosen based on its capacity and features, considering factors like cost, speed, and types of ports.
7. In wireless signal setup, physical objects like walls and buildings do not affect the wireless network.
8. The first step in installing any IoT device is to choose a location.
9. When connecting cables in an IoT framework, it is important to test each network device installed.
10. Wall anchors are used to secure screws in the holes created for mounting IoT devices.

D. Short Answer Type Questions

1. What are the steps in installing any IoT device?
2. Sensors are usually installed in which situation?
3. What is the correct positioning for placing a motion detector sensor on the wall?
4. Why is it important to consider physical obstructions when choosing a location for network devices?
5. How does signal strength decrease with distance between network devices?
6. What factors should be considered when selecting a switch for the IoT LAN network?
7. What is the significance of expandability when selecting a router?
8. What can cause signal loss in a network?
9. What is the maximum length for LAN cabling per channel?
10. What steps should be followed when connecting cables in an IoT framework?

Session 5. Perform checks and connections of devices

Ensuring the smooth functioning of IoT devices relies on rigorous checks and robust hardware connections. Thoroughly examining physical links, verifying configurations, and employing tools ensure secure and consistent connections. Protocol-specific assessments and network diagnostics further optimize communication reliability. Regular firmware updates enhance device performance. This systematic approach establishes a resilient and efficient IoT ecosystem.

5.1 Connectivity check of devices

It is a mandatory procedure for a technician to check the connections of the devices after connecting the devices through the cable and connecting the power supply. The following steps shown in Figure 5.1 may be followed to check the connections of Modem.

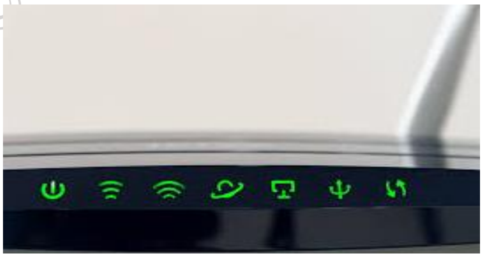
Steps	***Image***
Step 1. Turn on the power supply of the device	
Step 1. Check the power supply indicator light on the device	
Step 3. Check the indicator for network signals	
Step 4. Test the connection with testing tools and equipment if there is a problem in connection	

Fig 5.1 Connectivity check of devices

5.2 Checking Power Supply and Grounding

Power Supply – The power source should be selected to ensure that the device receives an uninterrupted power supply and can function without experiencing any electrical problems. The following factors should be considered when choosing the power supply for the IoT device:

1. The power source needs to be in a dry, comfortable area with the right temperature.
2. The power source should be properly grounded and in good condition.
3. The current and power rating of the device should match the power socket.
4. The connections should be tight and the wires should be protected.

Grounding the Connection – Connecting an electrical system to the ground through its non-current-carrying conductor component is known as "grounding" or "earthing." A system's grounding is crucial to the system's stability and safety. Electrical systems are vulnerable to harm or accidents with poor earthing. Every component of a system must be grounded in some way. The function of earthing is listed below:

- Fix the potential of active conductors with respect to the earth
- Limit the voltage in the electrical system between the non-current carrying parts and the earth
- Remove the risk of electric shocks by implementing protection devices
- Limit the rise in potential because of medium voltage faults in networks with low voltage Most of the IoT devices are wireless and run on battery. The Figure 5.5 shows plug points whose third pin is configured for grounding.

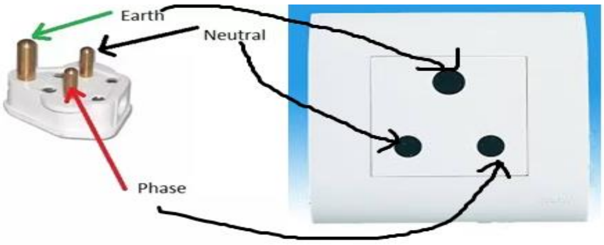


Fig. 5.2: Plug point with grounding pin

To safeguard against any unexpected voltage changes, the equipment and device are grounded. It aids in preventing equipment damage and safeguards users from electric shocks. The following are the steps for grounding an electrical connection:

1. Begin with the grounding wire, which is typically coded in black or green.

1. Using a utility knife, remove the wire's outer coating.

3. Connect the wire to the grounding point at the wall lining or in the socket as shown in Figure 5.6.

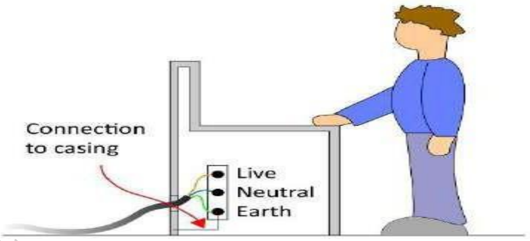


Fig. 5.3: Grounding of an electrical connection

5.3 Post-Commissioning Tests

The technician must take some actions to enable data transmission between IoT devices. The process for connecting IoT devices to enable data transmission is shown in the Figure 5.47.

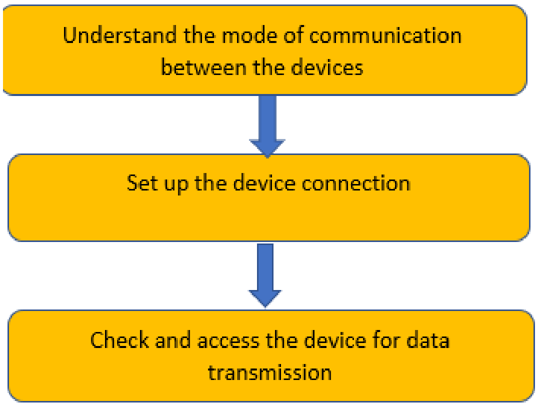

Understand the mode of communication between the devices
Set up the device connection
Check and access the device for data transmission

Fig. 5.4: Steps in IoT data transmission setup

Here, the technician must determine whether the IoT setup's devices are connected via cable or via a wireless network. Devices connected to an Ethernet cable-based wired network will immediately begin transmitting data after being plugged in. The following actions must be taken by the technician in order to configure devices over a wireless network:

1. Discover the information for the static IP, gateway, and netmask
2. Access the admin device and retrieve the username and password.
3. Set a permanent IP address.
4. Inspect the LAN for network connections.
5. Permit the device to be accessed by the network and test data transmission.

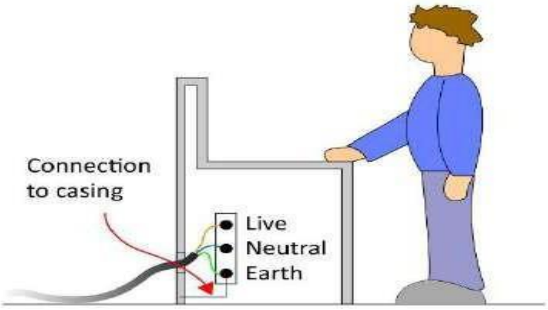
Several different types of tests are run on various components of the framework to examine the operation of the entire IoT setup. The tests conducted to examine an IoT setup include the ones listed below:

- Functional Testing: Based on the inputs provided, this test determines whether the device is operating in accordance with the customer's requirements.
- Compatibility testing: This ensures that the devices are compatible with each other's versions and operating systems. The device's hardware and software versions, as well as its protocols, are examined during this test.
- Usability testing: This is carried out to determine whether the user can operate the IoT devices and use the controls for their own purposes, one must be aware of them. This includes text, utility, and controls.
- Network Testing: This test is necessary to ensure that the entire network connections of the devices are functional as needed. There should not be a log and systems should work in accordance with each other.
- Security testing: This test examines the network's setup and data for security. encryption. This authenticates and verifies the data and performs data verification. the same to adhere to security procedures.
- Performance Testing: The technician must run a performance test on the setup after finishing all the tests. The operation and efficiency of the entire setup are examined. It is needed to make sure that the IoT setup is operating in accordance with the intended result and adhering to all the protocols.

Practical Activity 5.1. To check the connectivity and grounding

Materials Required: Sample IoT devices (sensors, cameras, etc.), Cables, power supply units, and necessary tools, Multi meter for checking power supply, Safety equipment (gloves, safety goggles, etc.)

Perform connectivity checks using a multi meter or other testing equipment.



Follow safety guidelines throughout the practical activity, especially when working with electrical components and tools.

Summary

- The chapter emphasizes the importance of ensuring proper connections and power supply in IoT installations.
- It covers steps for connectivity checks, power supply selection, and grounding procedures.
- The chapter also guides through post-commissioning tests including functional, compatibility, usability, network, security, and performance testing.
- These tests are crucial for ensuring the system operates according to specifications and adheres to security protocols.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the purpose of checking the connections between devices after installation? (a) To verify the color of the cables (b) To ensure the connections are correct and secure (c) To measure the temperature of the devices (d) To adjust the power supply
2. Which of the following factors should be considered when choosing a power supply for an IoT device? (a) The color of the power cord (b) The ambient temperature of the area (c) The type of device manual (d) The number of connected devices
3. What is the function of grounding or earthing in an electrical system? (a) To limit the voltage between non-current carrying parts and the earth (b) To increase the risk of electric shocks (c) To remove the need for protection devices (d) To disconnect all electrical components
4. How is the grounding wire typically coded? (a) Black or green (b) Red or blue (c) Yellow or white (d) Orange or pink
5. What actions must a technician take to configure devices over a wireless network for data transmission? (a) Retrieve the username and password (b) Connect an Ethernet cable (c) Access the admin device and retrieve the IP address (d) Plug in the devices and they will start transmitting data automatically
6. What type of testing determines whether the device is operating in accordance with the customer's requirements? (a) Functional Testing (b) Compatibility Testing (c) Usability Testing (d) Network Testing
7. Which test examines the network's setup and data for security? (a) Security Testing (b) Performance Testing (c) Compatibility Testing (d) Usability Testing
8. What is the purpose of performance testing in an IoT setup? (a) To verify the color of the cables (b) To examine the operation and efficiency of the entire setup (c) To check the power supply (d) To measure the temperature of the devices
9. Which step is performed first in preparing the surface for mounting an IoT device? (a) Marking the area for holes (b) Checking the surface level (c) Performing drilling (d) Placing wall anchors
10. What type of testing ensures that the devices are compatible with each other's versions and operating systems? (a) Compatibility Testing (b) Functional Testing (c) Usability Testing (d) Security Testing

B. Fill in the blanks

1. The power source needs to be in a dry, comfortable area with the right ____.
2. The power source should be properly grounded and in ______ condition.

3. Fixing the potential of active conductors with respect to ______ is one function of earthing.
4. Most of the IoT devices are wireless and run on ______.
5. To safeguard against any unexpected voltage changes, the equipment and device are ______.
6. Begin with the grounding wire, which is typically coded in black or ______.
7. The technician must take some actions to enable ______ between IoT devices.
8. Several different types of tests are run on various components of the framework to examine the ______ of the entire IoT setup.
9. Functional Testing determines whether the device is operating in accordance with the ______ requirements.
10. Network Testing is necessary to ensure that the entire network connections of the devices are functional as ______.

C. State true or False for the following

1. Functional testing determines whether the device is operating in accordance with the customer's requirements.
2. The current and power rating of the device should match the power socket.
3. Performance testing is necessary to ensure that the IoT setup is operating in accordance with the intended result and adhering to all the protocols.
4. Grounding limits the rise in potential because of medium voltage faults in networks with low voltage.
5. Network testing is necessary to ensure that the entire network connections of the devices are functional as needed.
6. Connecting an electrical system to the ground through its non-current-carrying conductor component is known as "grounding" or "earthing."
7. Devices connected to an Ethernet cable-based wired network will immediately begin transmitting data after being plugged in.
8. Security testing examines the network's setup and data for security and encryption.
9. Accessing the admin device and retrieving the username and password is a step in configuring devices over a wireless network.
10. The technician must discover the information for the static IP, gateway, and netmask when configuring devices over a wireless network.

D. Short Answer Type Questions

1. Why is it important to select the right power supply for an IoT device?
2. What factors should be considered when choosing the power supply for an IoT device?
3. What is the purpose of grounding or earthing in electrical systems?
4. How is the grounding wire connected to the wall lining or socket?
5. What steps must be taken to configure devices over a wireless network?
6. What are the different types of tests conducted to examine an IoT setup?
7. What is the purpose of functional testing in the context of IoT devices?
8. Why is compatibility testing important for IoT devices?
9. What is the role of usability testing in evaluating IoT devices?
10. Why is network testing necessary for ensuring the functionality of IoT devices?

Module 4 Occupational Health & Safety Standards

Module Overview

In today's dynamic work environment, prioritizing the well-being of employees and safeguarding the environment is of utmost importance. The Module "Organisation Work and Resources as per Health and Safety Standards" encompasses a comprehensive approach to workplace safety and environmental sustainability. It covers a range of critical topics, from precautionary measures and first aid techniques to fire safety, evacuation procedures, and safe working practices. This knowledge equips individuals with the skills needed to identify and address potential hazards, respond effectively to emergencies, and establish a secure work environment.

Furthermore, the Module delves into the organization's commitment to eco-friendly practices. It addresses waste management, including handling E-Waste and proper segregation of recyclable and non-recyclable materials. Understanding waste disposal methods and the sources of pollution is crucial for maintaining a clean and sustainable work environment. Additionally, the module emphasizes the integration of green practices into various job roles, contributing to a more environmentally conscious workplace. By adopting these principles, organizations can foster a culture of safety, health, and environmental responsibility, creating a better working environment for all stakeholders.

Learning Outcomes

After completing this module, you will be able to:

- Identify and follow essential workplace health and safety practices effectively.
- Understand and implement the organisation's green practices to support sustainability.

Module Structure

Session 1. Workplace Health and Safety Practices

Session 2. Organisation's Green Practices

Session 1. Workplace Health and Safety Practices

Employees have a right to a secure workplace. Because of this, the businesses set and follow the law and ensure a safe working environment. The highest requirements for worker safety and conditions are outlined in a workplace health and safety policy. Ensuring that the workplace complies with the highest safety regulations is the obligation of all organizations. When beginning a business, some things to consider are:

- Use furniture and equipment with ergonomic designs to avoid bending and twisting.
- Provide mechanical support to avoid having to lift or move heavy objects.
- Stock up on safety equipment for risky jobs.
- Make sure the emergency exits are present and in a handy location.
- Create health codes and ensure adherence to them.
- Adhere to the regular safety protocol.

1.1 Precautions to be taken while at work

Every employee has a responsibility to adhere to the organization's safety procedures. Every employee needs to develop the following habits:

1. Notify the supervisor of any unsafe conditions right away.
2. Identify and report any safety risks that could cause trips, falls, or slips.
3. Notify the supervisor of any accidents or injuries.
4. Put on the appropriate safety gear when necessary.
5. Acquire the knowledge necessary to operate the safety-related equipment properly.
6. Recognize and refrain from doing anything that can put other people in danger.
7. Constantly be aware
8. Inform the staff of the location of the fire extinguishers and the first/emergency exits on the floor.

1.2 First Aid Techniques

Injuries, Pain, illness, are all a part of life. This may occur in any case. Every person is vulnerable to disease and accidents at any time and in any location. In the event that any of these occur, prompt medical attention or treatment is required to lessen pain, discomfort, and condition progression. "First Aid" refers to the initial medical care provided before seeking professional medical assistance. First aid is the temporary care provided to an accident or sudden illness victim in the interim until "Medical Aid" arrives. First aid refers to giving victims of accidents or illnesses the necessary medical attention and life support in the beginning. First Aid, however, has its limitations and is not a substitute for professional medical treatment. A patient's life can be saved when a first aider provides appropriate, prompt assistance. Accidents and illnesses can occur anywhere: at home, at work, or in public. Regardless of the safety precautions we take, illness is a possibility for everyone occasionally. Some common injuries and their rescue techniques are described in the next section.

- Direct pressure must be applied to the cut or wound with a clean cloth, tissue, or piece of gauze, until bleeding stops.
- If blood soaks through the material, it is highly recommended not to remove it.
- More cloth or gauze must be put on top of it, and pressure must be continued.
- If the wound is on the arm or leg, the limb must be raised above the heart to help slow the bleeding.
- Hands must be washed again after giving first aid and before cleaning and dressing the wound.
- A tourniquet must not be applied unless the bleeding is severe and not stopped with direct pressure.

1.1.1 Clean cut or wound

1. The wound must be cleaned with soap and lukewarm water.
2. To prevent irritation and burning sensation, the soap solution must be rinsed out of the wound.
3. Hydrogen peroxide or iodine must not be used to clean or treat the wound since they are corrosive and can damage live tissues. It is shown in Figure 1.1(a).

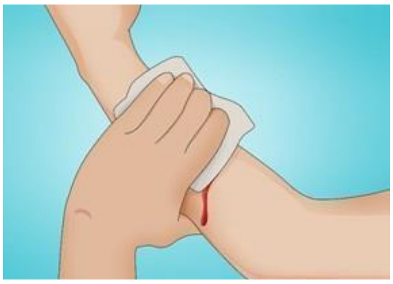


Fig. 1.1(a): Clean cut or wound

1.1.2 Protect the wound

4. Antiseptic cream or solution must be applied to the wound to reduce the risk of infection.
5. Then the wound must be gently covered with a sterile bandage.
6. Till the wound heals, the bandage must be changed (dressed) daily to keep the wound clean and dry. It is depicted in Figure 1.1(b) and 1.1(c).

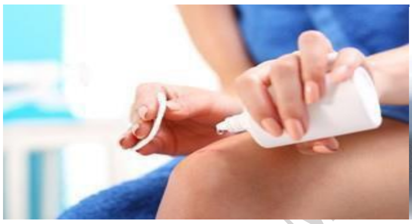


Fig. 1.1(b): apply antiseptic

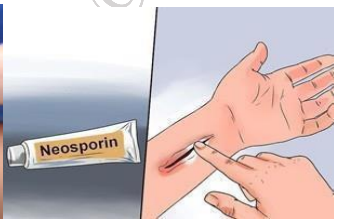


Fig.1.1(c): Protect the wound

Call the Emergency Helpline if:

7. The bleeding is severe and deep
8. You suspect Internal Bleeding
9. Abdominal or Chest wound exists
10. Bleeding continues even after 10 minutes of firm and steady pressure

1.1.3 For Burns:

11. Immediately put the burnt area under cold water for a minimum of 10 minutes as shown in Figure 1.1(d).

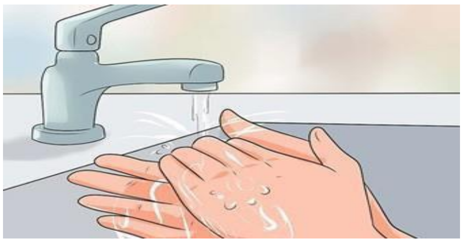


Fig. 1.1(d): Put Burnt Area under Water

12. If the burned area is covered, take clean scissors, cut, and remove the fabric covering the area
13. In case clothing is stuck to the burned area, leave it as it is Before sterile dressing application, remove jewellery (if any).

14. It is better to leave the burned area open. Do not apply any medication or ointment. Breaking a blister – it is an absolute no-no!

1.1.4 For Broken Bones and Fractures

1. Protruding bone must be left alone

a. If a bone has broken through the skin, it must not be pushed back into place.

b. The area must be covered with a clean bandage and immediate medical attention must be sought.

1. Bleeding must be stopped

a. Steady and direct pressure must be applied with a clean piece of cloth for 15 minutes and the wound must be elevated.

b. If a blood soaks through, one must apply another cloth over the first and seek immediate medical attention.

3. Swelling must be controlled

a. The RICE (Rest, Ice, Compression and Elevation) therapy must be applied to control and reduce swelling.

b. Rest the injured part by having the person stay off of it.

c. Ice must be applied on the area with the help of an ice pack or by wrapping the ice in a clean cloth. Ice must not be directly placed against the skin.

1.1.5 For Heart Attack/Stroke

a. Think FAST. Face: is there weakness on one side of the face?

b. Arms: can they raise both arms?

c. Speech: is their speech easily understood?

d. Time: to call Emergency helpline

e. Immediately call the medical/ambulance helpline or get someone else to do it. It is shown in Figure 1.1 (e).

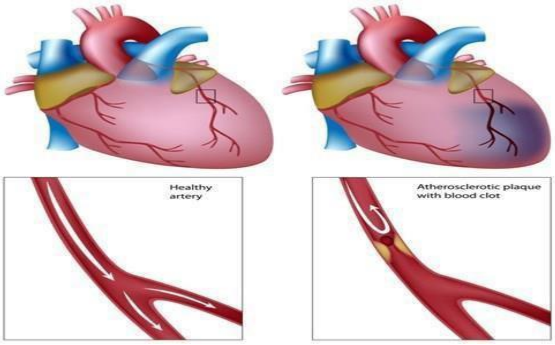


Fig 1.1(e): Anatomy of Heart Attack

1.1.6 For Head Injury

a. Ask the victim to rest and apply a cold compress to the injury (e.g. ice bag)

b. If the victim becomes drowsy or vomits, call the Medical helpline or get someone else to do it.

1.1.7 Chemical hazards

Caused by toxic materials, which are poisonous. And being poisonous in nature, they can either be fatal or cause serious damages in case the preventive actions are not taken on time. Now, the exposure to chemicals can be in 3 forms.

They can be:

- Inhaled (entering the body through nose)
- Directly in contact with skin

- Ingested (consumed)

The symptoms, in this case, will be:

- Seizures
- Partial or complete loss of responsiveness
- Burning sensation
- Stomach Cramping with bouts of excruciating pain
- Nausea
- Vomiting (and in times with blood-stains). It is shown in Figure 1.1 (f).

Fig 1.1 (f:) chemical hazards

Now, where there is a problem, their solutions come side by side. In such situations, the person giving first aid requires to be calm and take certain preventative actions.

Some of the essential actions are:

- Using insulated equipment
- Wearing protective clothing, goggles, masks, shoes and gloves
- Ensuring the place has enough ample ventilation

Remedial action

- The foremost thing that one should do is to provide immediate first aid.

However, it is to be remembered that the victim should not be given any kind of fluid (water, milk) until doctors from the Poison control unit give a green signal.

- Aside from this, there are a few things a person can perform to the victim of toxic material exposure.
- Remove the victim from the toxic zone or vicinity
- Call for an ambulance
- Remove contaminated clothing
- Splash water in the eyes
- If ingested, do not try to make the victim puke (vomit)
- Wash their mouth with water
- In case the victim's breathing has stopped, give CPR (Cardiopulmonary resuscitation) as shown in Figure 1.1(g).

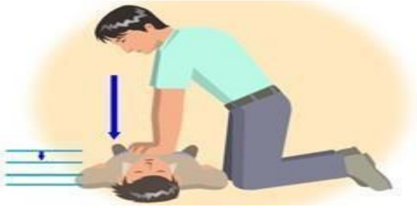


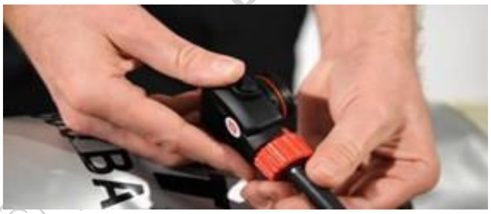
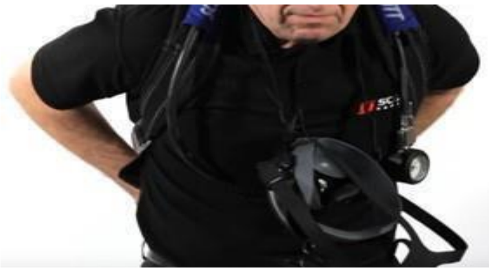
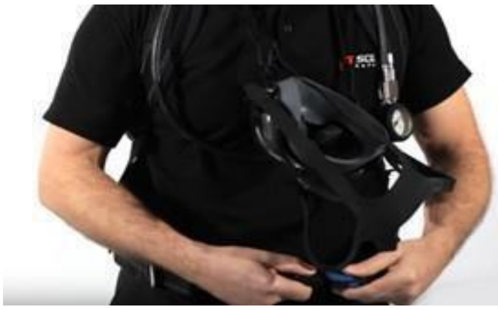
Fig 1.1(g): CPR

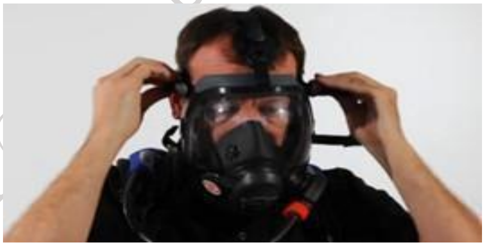
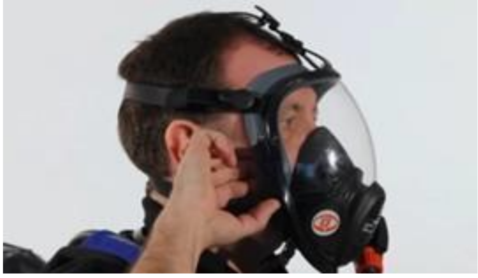
- In case of burning due to toxic material, apply burn gel or water gel on that area.
- Avoid any cream based or oil-based lotion or ointment

Even though giving first aid is the right thing to do in the first place, it is also important to report the incident to their supervisor.

1.1.8 Steps of using breathing apparatus

Table 1.1: Steps of using breathing apparatus

SN	Procedure	Image
1.	Check the parts of the breathing apparatus thoroughly	
1.	Check the bypass knob (red). Close it if you see it open. After this, press the reset button (area above bypass nob – black)	
3.	Inspect the facemask to see that it is undamaged	
4.	Lift the cylinder ensuring that on the top the cylinder valve should be present. The back plate of the cylinder should face the wearer. Wear the breathing apparatus on the shoulder like a bag pack and by the neck strap, hang the facemask.	
5.	After wearing the breathing apparatus tighten shoulder straps and fasten the waist belt.	

6.	The cylinder valve should be opened slowly to inspect the pressure gauge.	
7.	Make sure that 80% of the cylinder is full.	
8.	Wear the mask slowly by resting your chin in the resting cusp and pull the head strap slowly over your head. Pull the head straps for a snug but comfortable fit.	
9.	Breath in and normally to see if you can breathe normally or not.	
10.	Now insert a finger sidewise of the facemask for easy outward airflow.	
11.	Slowly close the cylinder valve without leaving the knob. Be steady for 10 minutes and hold your breath or extremely slow to listen to any wheezing sound. Also, check the pressure gauge for any dip in the pressure.	

11.	Normally Breathe to vent system. Listen for a whistle alarm while observing the pressure gauge at 55 bar (+/- 5 bar)	

1.1.9 Briefing and Guidance for Fire Fighters

There are basically three methods with the help of which people can be rescued from a building engulfed in a blazing fire. To ensure on-site reception, here are two of the important steps that we will discuss now. These come under the best safe lifting and carrying practices.

Conventional Technique – This is a good method if there is an open area close by. The first rescuers will make the victim sit reach under their armpits and finally, grab their wrist. The other rescuer will cross the ankle (victim), pull up that person's legs on his shoulder. Finally, on the count of 3, both will lift the person up and move out as shown in Figure 1.1(h).

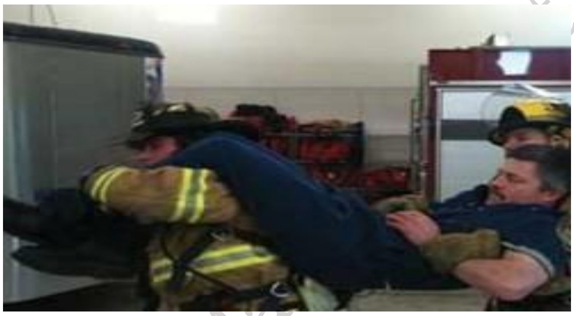


Fig. 1.1 (h): Fast Strap

Fast Strap – In case the victim is completely incapable of moving out of the fire zone. The rescuers should follow this method. One of the rescuers will place their knee between victim's shoulder and head. Pin the loop of webbing to the ground with the help of the knee. This acts as an anchor. With the non- dominant hand hold the other end of the webbing and make a loop. With steady hands, pull the victim's hand in from the loop, tie it securely and finally clip the webbing loops as shown in Figure 1.1(i).

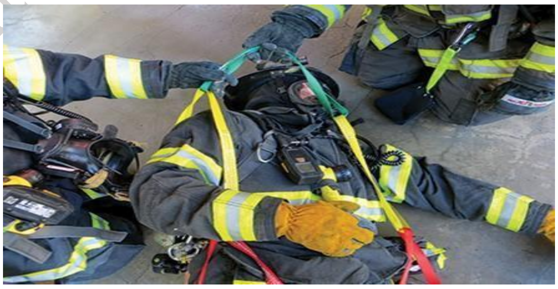


Fig. 1.1(i): Fast Strap

Essentials for Smooth Evacuation – The following are essential to have a smooth evacuation during an outbreak:

1. Clear passageways to all escape routes
2. Signage indicating escape routes should be clearly marked
3. Enough exits and routes should be present to allow a large number of people to be evacuated quickly
4. Emergency doors that open easily
5. Emergency lighting where needed

6. Training for all employees to know and use the escape routes
7. A safe meeting point or assembly area for staff
8. Instructions on not using the Elevator during a fire

Special Evacuation Requirements for Especially Abled Persons

The Visually Impaired

1. Announce the type of emergency
2. Offer your arm for help

With Impaired Hearing

3. Turn lights on/off to gain the person's attention, or indicate directions with gestures, or write a note with evacuation directions

People with Prosthetic Limbs, Crutches, Canes, Walkers

4. Evacuate these individuals as injured persons.
5. Assist and accompany the evacuation site if possible.
6. Use a sturdy chair, or a wheeled one, to move the person to an enclosed stairwell Notify emergency crew of their location

1.3 Importance of Fire Safety Drills

Any public or commercial building should have fire drills to practice what to do in the event of a fire. In addition, all employees of a company are required to work as per the Fire Safety Order of 2005, which is a legal requirement. Here's how to maximize your fire training experience. Fire drills are essential for a number of reasons. Firstly, they provide an opportunity to rehearse evacuation procedures to ensure that all personnel are familiar with them. Because everyone will know what to do in a real-life emergency, there won't be as much panic because the staff will leave the building swiftly. Fire drills are also useful for evaluating the effectiveness of escape routes.

It is also possible to verify that emergency exits are operational and alarm systems are functioning correctly during fire drills. In general, fire drills improve safety by preparing you for the best possible outcome in the event of a real fire. Two fire drills should ideally occur each year, though this can vary depending on the workplace and after reviewing the risk assessment of the company. If any employees work shifts, appropriate arrangements should be made to guarantee that every employee participates in a fire drill annually and receives training on how to handle emergency situations.

There are justifications for and against informing the public in advance of fire drills. Some claim that keeping employees in the dark adds a sense of surprise and makes them approach drills with greater sincerity. In a real fire, on the other hand, this could also have the opposite effect, as people might assume it's merely a drill after hearing the alarm. The advantage of informing all employees ahead of time about fire drills is that, at first, they won't become alarmed, preventing any injuries that might result from a hasty departure from the building. In addition, in the event that the alarm goes off without any prior notice, everyone will know it's a drill and react appropriately. In public places such as shopping centres, it is prudent to make members of the public alert when a drill is about to happen. The symbol for this alert is shown in Figure 1.1.

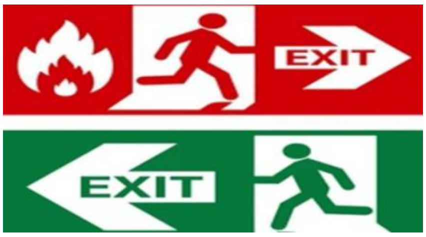


Fig. 1.2: Drill alert

1.4 Importance of safe working practices

There are millions of bacteria and viruses in the environment in which we live. Additionally, these microorganisms may use our bodies as a breeding ground. They proliferate, spread, and give rise to numerous illnesses that can occasionally be lethal to people. Each year, these microorganisms that cause disease claim the lives of over 17 million people. We can all experience amazing changes with a few easy tricks and small adjustments to our basic personal hygiene routines. If we practice good hygiene every day, we can avoid getting these diseases.

1.5 Importance of Social Distancing

Preventing communicable diseases

All these above practices will help us to prevent communicable diseases. These diseases are highly infectious and contagious and spread through air, urine, faeces, saliva, skin (through touch) and using the same towels and utensils.

Social Distancing and isolation, Self-Quarantine

Ever since the spread of the pandemic covid-19, several health organisations have been insisting on following social distancing and isolation. Communicable diseases mainly spread through coming close to the infected individual and through physical touch. If a person is infected with diseases like normal flu or cold and spreads it to others, the symptoms may remain with the infected person for a day or two. The virus may be destroyed by taking an antibiotic. But in severe cases like corona virus the infection is severe and can prove fatal to the affected people. To prevent the spread of the virus, the entire world adopted lockdown, ***social distancing*** and compulsory face mask. And the infected person has to be in ***self-isolation*** and ***quarantine*** till the time the symptoms are over. This was an advisory from the World Health Organisation, and the entire world followed it to prevent the rapid spread of the virus. The same can be applicable to all types of communicable diseases that are spread mainly through air and touch.

Anybody who is infected with a contagious disease needs to practice isolation in order to prevent the spread of the germs to their near and dear ones. This became very popular and was strictly adhered to during the covid-19 pandemic. People who were confirmed to have COVID-19, **isolation** was mandatory. Isolation is a health care term that means keeping people who are infected with a contagious illness away from those who are not infected. Isolation can take place at home or at a hospital or care facility. Special personal protective equipment will be used to care for these patients in health care settings. They are attended by well trained nurses and specialised doctors. And these people have to be in the PPE kits all through their presence in the hospital. It is shown in Figure 1.3.

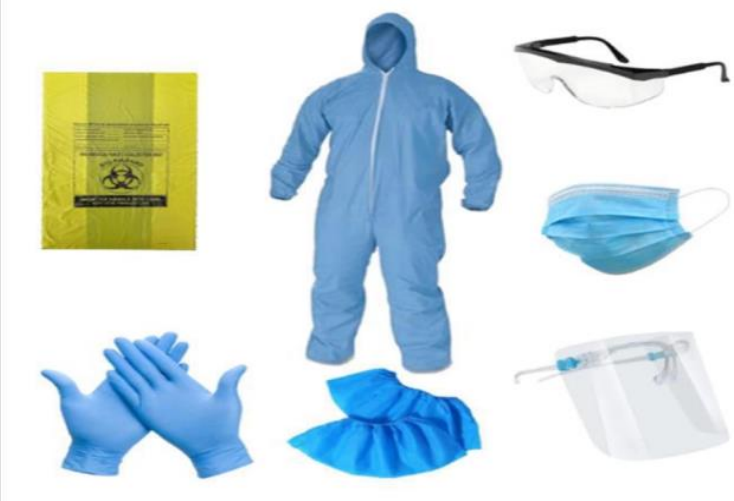


Fig. 1.3: Complete PPE Kit

Health professionals and physicians who treat patients with highly contagious diseases and who are segregated to stop the spread wear the personal protective equipment (PPE) kits. When their shift is over, they have to take it off. They have to wear it whenever they come in contact with the patient. The face mask and goggles can be reused as long as they are properly sanitized, but the majority of PPE components are meant to be used only once. PPE kits must be disposed of carefully because they may contain contaminants that are stuck to them and, if improperly disposed of, could infect a healthy person. The risk of contracting the illness may be higher for healthcare professionals.

1.6 Safe Workplace Practices

Every company has the provision of a first aid box. As you have already read about the types of injuries that technicians can receive in their field of work, it is imperative for the companies to have appropriate first aid accessories. The basic first aid supplies and accessories that a first aid box should have the components shown in Figure 1.4.

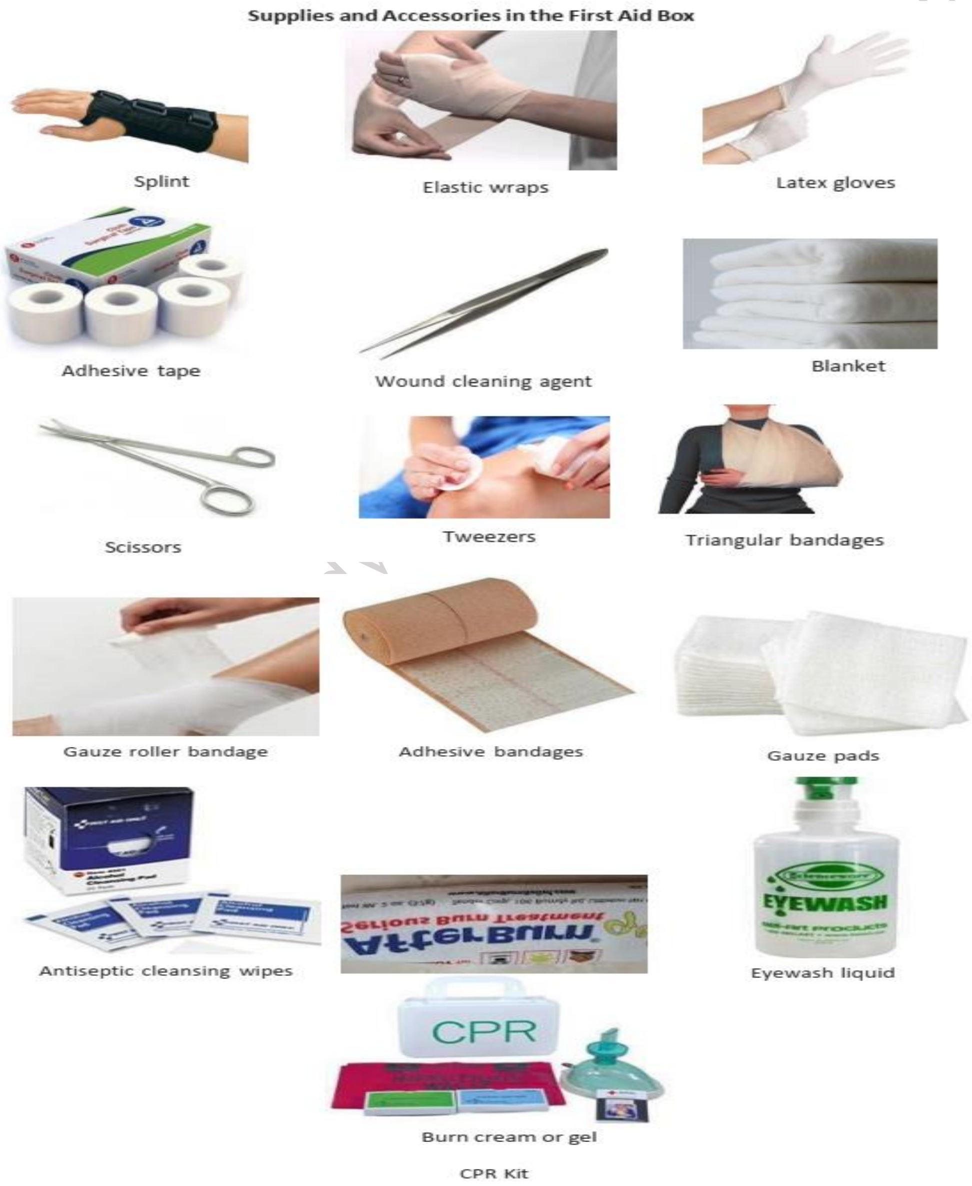


Fig. 1.4: first aid box contents

1.7 Methods of Reporting Safety Hazards

Every organization, from every industry, has a standard reporting protocol, comprising the details of people in the reporting hierarchy as well as the guidelines to be followed to report emergencies. However, the structure of this reporting hierarchy varies between organizations, but the basic purpose behind the reporting procedure remains the same.

The general highlights of the Organizational Reporting Protocol, commonly known as the 6Cs, are:

Communicate First

- The first source of information during an emergency is the preferred source.
- Crises situations are time-bound and hence it is important to communicate promptly.

Communicate Rightly

- Distortion of information due to panic must be avoided.
- Proper, accurate information must be provided to concerned authorities and this can save lives.

Communicate Credibly

- Integrity and truthfulness must never be forgotten during emergencies.

Communicate empathetically

- One must wear the shoes of the victims while communicating emergencies.

Communicate to instigate appropriate action

- Communicating to the right authorities help in taking the necessary action.

Communicate to promote respect

- Communicating with the victims with respect help in earning their trust and thus eases the disaster management process.

Hazards and potential risks / threats can be identified and then reported to supervisors or other authorized persons in the following ways:

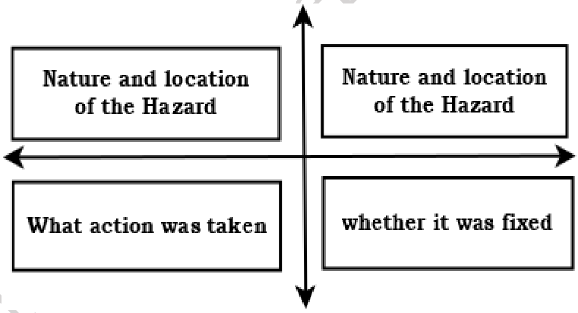

Nature and location of the Hazard
Nature and location of the Hazard
What action was taken
whether it was fixed

Fig. 1.5: Describing hazard matrix

Part A: To be completed by the Worker Details Required:

1. Name of Worker
2. Designation
3. Date of filling up the form
4. Time of incident / accident
5. Supervisor / Manager Name
6. Work Location / Address
7. Description of the hazard/what happened (Includes area, task, equipment, tools and people involved)
8. Possible solutions to prevent recurrence (Suggestions)

Part B: To be completed by the Supervisor / Manager Details Required:

9. Results of Investigation (Comment on if the hazard is severe enough to cause an injury and mention the causes of the incident / accident)

Part C: To be completed by the Supervisor / Manager Details Required:

10. Actions taken / Measures adopted (Identify and devise actions to prevent further injury, illness and casualty).

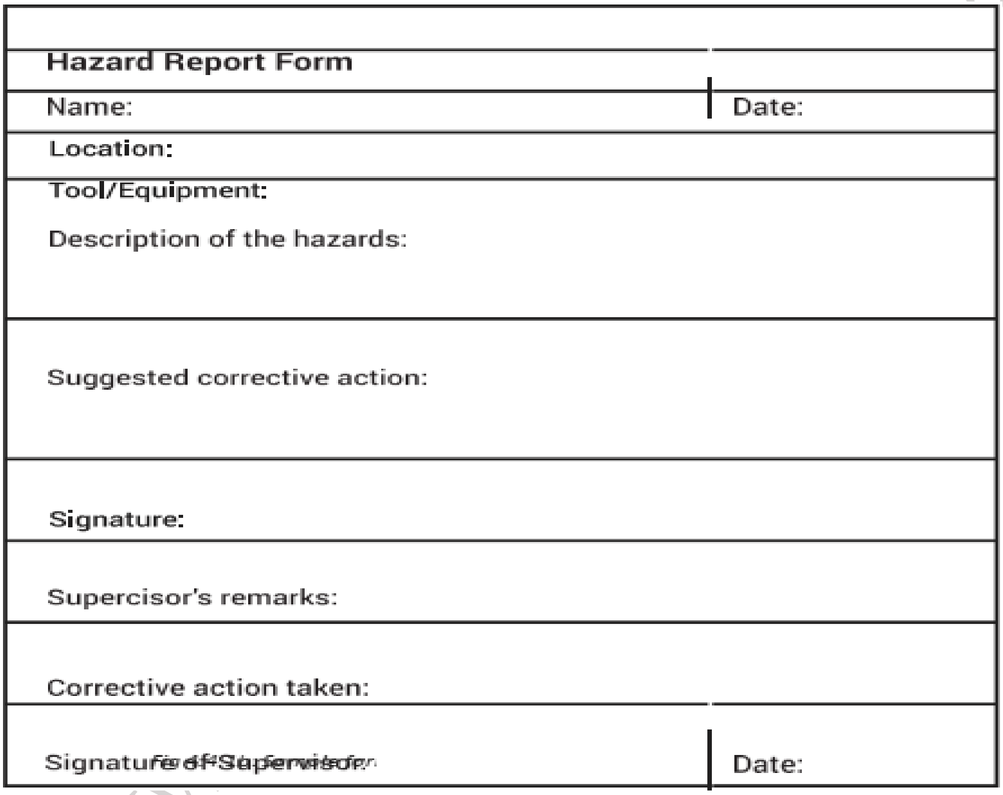
The reporting format is shown in following table 1.1.

Table 1.2: List of actions taken

Action	***Responsibility***	***Comletion Date***

Any job role and any occupation in this world have some hazards, in varying severity, associated with it. These are called Occupational Hazards. Occupational Hazard can be defined as “a risk accepted as a consequence of a particular occupation”. According to the Collins English Dictionary, it is defined as “something unpleasant that one may suffer or experience as a result of doing his or her job”. Occupational Hazards report form is shown in the following table 1.3.

Table 1.3: Hazards Report Form



Hazard Report Form

Name: Date:

Location:

Tool/Equipment:

Description of the hazards:

Suggested corrective action:

Signature:

Supercisor's remarks:

Corrective action taken:

Signature of Supervisor: Date:

Practical Activity 1.1. Workplace Safety Inspection to familiarize with potential hazards and safety measures in a workplace.

Step 1. Choose a workplace setting (e.g., office, workshop, construction site).

Step 1. Walk through the chosen setting and identify potential hazards (e.g., tripping hazards, unsafe equipment).

Step 3. Document the identified hazards along with suggested preventive measures.

Step 4. Discuss findings with colleagues or supervisors.

Practical Activity 1.1. Practice first aid techniques for common injuries.

Step 1. Select a specific injury scenario (e.g., cut, burn, broken bone).

Step 1. Simulate the scenario using props or role-play with a partner.

Step 3. Apply appropriate first aid techniques based on the provided guidelines.

Step 4. Evaluate the effectiveness of the applied first aid.

Practical Activity 1.3. Practice reporting safety hazards using a standardized reporting form.

Step 1. Review the provided Hazard Report Form given in the chapter.

Step 1. Choose a hypothetical workplace scenario with a safety hazard.

Step 3. Complete the Hazard Report Form (Parts A, B, and C) based on the chosen scenario.

Step 4. Discuss the identified hazard and proposed preventive measures with a peer or supervisor.

Practical Activity 1.4. Analyse different types of hazards and assess their associated risks.

Step 1. Review the list of hazards given in the chapter.

Step 1. Select a specific hazard (e.g., chemical exposure, ergonomic strain).

Step 3. Conduct a risk assessment for the chosen hazard, considering severity and likelihood.

Step 4. Propose appropriate preventive measures for the identified hazard.

Summary

- This chapter emphasizes the critical importance of workplace safety and compliance with legal regulations.
- It covers key elements of a comprehensive health and safety policy, including practical measures like ergonomic equipment and emergency preparedness.
- The chapter also provides guidance on employee precautions and first aid techniques for various situations.
- Additionally, it highlights the significance of fire drills and personal hygiene practices in preventing the spread of communicable diseases.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is the primary emphasis of the chapter on "Workplace Health and Safety Practices"? (a) Employee benefits (b) Legal obligations and safety compliance (c) Business profitability (d) Workplace aesthetics
2. Which of the following is NOT mentioned as a practical consideration for businesses in ensuring workplace safety? (a) Use of ergonomic furniture and equipment (b) Providing mechanical support for heavy objects (c) Stocking up on safety equipment for risky jobs (d) Maximizing office aesthetics
3. According to the chapter, what should employees do in case of unsafe conditions at the workplace? (a) Ignore them and continue working (b) Notify the supervisor right away (c) Wait until the end of the day to report them (d) Document them for personal reference
4. What is the purpose of a workplace health and safety policy? (a) To set the highest standards for worker safety and conditions (b) To maximize business profits (c) To control employee behaviour (d) To ensure compliance with taxation regulations

5. What is the significance of fire drills, according to the chapter? (a) To evaluate the effectiveness of escape routes (b) To test the fire alarm system (c) To improve workplace aesthetics (d) To assess employee performance
6. In the context of preventing the spread of communicable diseases, what is the role of personal hygiene practices, as mentioned in the chapter? (a) They have no impact on disease prevention (b) They play a crucial role in preventing diseases (c) They are only relevant during flu seasons (d) They are primarily for cosmetic purposes
7. According to the chapter, what is the primary purpose of reporting safety hazards? (a) To assign blame for incidents (b) To document incidents for legal purposes (c) To prevent future occurrences and ensure safety (d) To increase insurance premiums
8. What is the primary purpose of providing mechanical support to employees for lifting heavy objects? (a) To encourage regular exercise (b) To minimize the risk of injuries from lifting (c) To improve workplace aesthetics (d) To reduce the need for physical exertion
9. What is the recommended action if blood soaks through the material used to apply direct pressure on a wound? (a) Remove the material immediately (b) Add more material and continue applying pressure (c) Leave the material in place and add more on top (d) Wash the wound with soap and water
10. What does the RICE therapy stand for in the context of injuries? (a) Rest, Ice, Compression, Elevation (b) Run, Inhale, Cover, Exhale (c) Roll, Inflate, Check, elevate (d) Reduce, Instruct, Cover, Evaluate

B. Fill in the blanks

1. Use furniture and equipment with ergonomic designs to avoid __________ and twisting.
2. Make sure the __________ exits are present and in a handy location.
3. In case of a clean cut or wound, direct pressure must be applied until __________ stops.
4. Antiseptic cream or solution must be applied to the wound to reduce the risk of __________.
5. In case the victim's breathing has stopped, give __________
6. Clear passageways to all escape routes, signage indicating escape routes, and enough exits are essential for a smooth __________.
7. According to the chapter, personal hygiene practices play a crucial role in preventing __________ diseases.
8. The purpose of a hazard report form is to identify and report safety hazards for __________ action.
9. Using __________ equipment is recommended to prevent accidents and injuries at work.
10. The acronym FAST stands for Face, Arms, Speech, __________ in the context of stroke assessment.

C. State true or False for the following

1. Hydrogen peroxide or iodine should be used to clean and treat wounds, as they help in preventing infection.
2. In case of a broken bone protruding through the skin, it is recommended to push the bone back into place.
3. Using insulated equipment, wearing protective clothing, and ensuring ample ventilation are important preventive actions for chemical hazards.
4. Personal protective equipment (PPE) kits should be disposed of carefully to prevent potential contamination.
5. Social distancing and isolation are important practices for preventing the spread of communicable diseases, especially during a pandemic.

6. Reporting safety hazards is essential for preventing future incidents and ensuring workplace safety.
7. Occupational hazards refer to risks accepted as a consequence of a particular occupation.
8. Providing clear passageways, signage, and sufficient exits are not essential for a smooth evacuation during an emergency.
9. The purpose of a hazard report form is to assign blame for incidents and accidents in the workplace.
10. In the context of first aid, a tourniquet should be applied immediately to stop any bleeding, regardless of its severity.

D. Short Answer Type Questions

1. What are some of the considerations mentioned for businesses when it comes to ensuring workplace safety?
2. What is the recommended action for a clean cut or wound, and how should it be protected?
3. In case of chemical hazards, what are the three forms of exposure mentioned in the chapter?
4. What are some essential actions mentioned for providing first aid in case of exposure to toxic materials?
5. Why are fire drills considered important in a workplace or public setting?
6. What are the benefits of informing employees in advance about fire drills, according to the chapter?
7. Why is it important to practice social distancing and isolation during a pandemic or outbreak of a contagious disease?
8. What is the purpose of a hazard report form, and how does it contribute to workplace safety?
9. What are occupational hazards, and why is it important for individuals to be aware of them?
10. Why is it essential to have clear passageways, signage, and sufficient exits for a smooth evacuation during an emergency?

Session 2. Green Practices in Organisation

2.1 Waste Management

2.1.1 E-Waste

Electrical and electronic products are all around us. We can't imagine a world without these gadgets. Our life is indispensable without electricity and electronic devices. Growth in the IT and communication sectors has increased the usage of electronic equipment immensely. Frequent change in the technological features of electronic products is forcing consumers to discard their old electronic products very quickly, which, in turn, adds e-waste to the solid waste pool. What this translates to is mountainous masses of electrical and electronic waste which has a high potential to pollute the environment. This growing menace of e-waste calls for a greater focus on recycling e-waste and better e-waste management.

E-waste means electrical and electronic equipment, whole or in part discarded as waste by the consumer or bulk consumer as well as rejects from manufacturing, refurbishment, and repair processes. E-waste usually is made up of usable and non-usable material. Some of the waste if left unattended will be destructive to the environment. E-waste is made up of hazardous substances like lead, mercury, toxic material, and gases.

There are many companies these days who are engaged in the collection, handling, and disposal of this e-waste in a safer and more secure place to protect the environment**.**

The amount of e-wastes comprising computers and computer parts, electronic devices, mobile phones, entertainment electronics, refrigerators, microwaves, TV, fridges, and industrial electronics that are obsolete or that have become unserviceable is growing. All these electronic devices contain plastics, ceramics, glass, and metals such as copper, lead, beryllium, cadmium, and mercury and all these metals are harmful to humans, animals, and the earth. Improper disposal only leads to poisoning the Earth and water and therefore all life forms. Our effort is meant to preserve the environment and prevent pollution by proper handling of e-waste. While it will take a lot of effort to educate people to dispose of such wastes in the right way, we are doing our part by providing a channel to collect e-wastes and dispose of them in a sustainably safe manner. We convert waste to usable resources. The electronic industry is not only the world's largest industry but also a fast-growing manufacturing industry. It has been instrumental in the socio-economic and technological growth of the developing society of India.

At the same time, it poses a major threat in the form of e-waste or electronics waste which is causing harmful effects on the whole nation. E-waste is creating a new challenge to the already suffering Solid waste management, which is already a critical task in India.

Electronic goods/gadgets are classified under three major heads:

- White goods: Household appliances,
- Brown goods: TVs, camcorders, cameras etc.,
- Grey goods: Computers, printers, fax machines, scanners etc. The complete process is carried out as per the government guidelines.

2.1.2 E-waste Management Process

- Collection of e-waste from all the electronic stores, manufacturing companies, etc.
- Transport of e-waste to the disposal units
- Segregation of e-waste at the disposal unit
- Manual dismantling of e-waste to segregate components into various types such as metal, plastics and ceramics
- Convert into raw material (recycle and reuse)
- Supply recovered raw material to processors and electrical/electronic industries
- Dispatch hazardous e-waste for safe disposal
- Waste management is carried out to ensure that all types of waste and garbage are collected, transported, and disposed of properly. It also includes recycling waste so that it can be used again.
- The basic waste management hierarchy is shown in Figure 2.1.

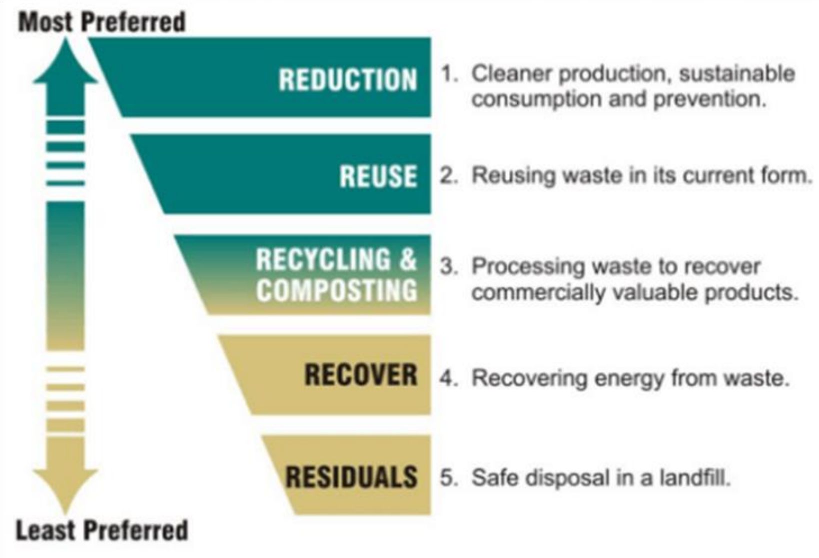

Most Preferred
REDUCTION
1. Cleaner production, sustainable consumption and prevention.
REUSE
2. Reusing waste in its current form.
RECYCLING & COMPOSTING
3. Processing waste to recover commercially valuable products.
RECOVER
4. Recovering energy from waste.
RESIDUALS
5. Safe disposal in a landfill.
Least Preferred

Fig. 2.1: E-waste Management Process

2.2 Recyclable and Non-Recyclable waste

Recyclable waste is renewable or can be reused. This means that the waste product is converted into new products or raw materials, like paper, corrugated cardboard (OCC), glass, plastic containers and bags, hard plastic, metal, wood products, e-waste, textile, etc. Recycling not only conserves important areas in our landfills but also assists decrease greenhouse gas emissions. Contrary to this,

Non-recyclable waste cannot be recycled and cause a major threat to the environment. The following items cannot be recycled: Shredded paper, aerosol cans, paper coffee cups, milk and juice cans, used baby diapers, and bottle caps.

Recycling is one of the best ways to have a favourable influence on the world where we live. Recycling will greatly help us to save both the environment and humans from pollution. If we take immediate action, we can control this, as the quantity of waste we are accumulating is increasing all the time.

2.3 Colour codes of waste collecting bins

India's urban population of 429 million citizens produce a whopping 62 million tonnes of garbage every year. Out of this, 5.6 million tonnes are plastic waste, 0.17 million tonnes are biomedical waste, 7.90 million tonnes are hazardous waste and 15 lakh tonnes is e-waste.

According to an estimate, 40% of municipal waste in the city is 'wet' waste, which can easily be composted and used as manure. Nearly 30% of the municipal waste comprises plastic and metal, which can be sent to an authorized dealer for recycling, and about 20% of it is e-waste, from which precious metals can be taken apart and recycled. However, out of the total municipal waste collected, 94% is dumped on land and only 5% is composted. To gather the garbage two colour bin systems were suggested. Green bin for wet waste and blue for dry waste. However, there is a drawback in that system. People go through the sanitary napkins and children's diapers along with wet waste causing the contamination of things. Hence the government has come up with three colored garbage collection bins.

1. Green Bin – The green coloured bin is used to dump biodegradable waste. This bin could be used to dispose of wet/organic material including cooked food/leftover food, vegetable/fruit peels, egg shell, rotten eggs, chicken/fish bones, tea bags/coffee grinds, coconut shells and garden waste including fallen leaves/twigs or the puja flowers/garlands will all go into the green bin.

1. Blue bin – The blue coloured bin is used for segregating dry or recyclable left over. This category includes waste like plastic covers, bottles, boxes, cups, toffee wrappers, soap or chocolate wrapper and paper waste including magazines, newspapers, tetra packs, cardboard cartons, pizza boxes or paper cups/plates will have to be thrown into the white bin. Metallic items like tins/cans foil paper and containers and even the dry waste including cosmetics, hair, rubber/thermo col (polystyrene), old mops/dusters/sponges.

3.Black bin – Black bin, make up for the third category, which is used for domestic hazardous waste like sanitary napkins, diapers, blades, bandages, CFL, tube light, printer cartridges, broken thermometer, batteries, button cells, expired medicine etc. These three coloured bins are shown in Figure 2.1.

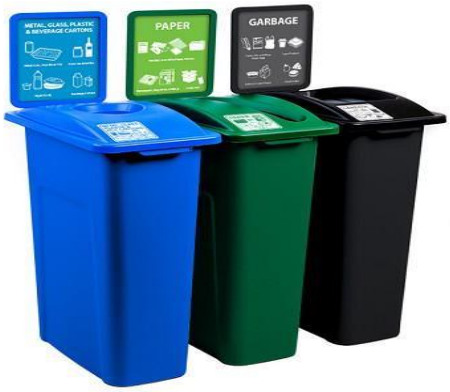


Fig.2.2: Tri colored Bins

2.4 Waste disposal methods

- ***Incineration*** – Combusting waste in a controlled manner to minimize incombustible matter like waste gas and ash.
- ***Waste Compaction*** – Waste materials are compacted in blocks and are further sent away for recycling.
- ***Landfill*** **–** Waste that can't be recycled or reused can be thinly spread out in the low-lying areas of the city.
- ***Composting*** **–** Decay of organic material over time by microorganisms.
- ***Biogas Generation*** **–** With the help of fungi, bacteria, and microbes, biodegradable waste is converted to biogas in bio-degradation plants.
- ***Vermicomposting*** – Transforming the organic waste into nutrient-rich manure by degradation through worms.

2.5 Sources of Waste

- ***Construction waste*** **–** waste coming from construction or demolition of buildings.
- ***Commercial waste*** **–** waste from commercial enterprises.
- ***Household waste*** **–** garbage from households is either organic or inorganic.
- ***Medical or clinical waste*** **–** wastes from the medical facilities- like used needles and syringes, surgical wastes, blood, wound dressing.
- ***Agricultural waste*** – Waste generated by agricultural activities that include empty pesticide containers, old silage packages, obsolete medicines, used tires, extra milk, cocoa pods, wheat husks, chemical fertilizers, etc.
- ***Industrial waste*** – The waste from manufacturing and processing industries like cement plants, chemical plants, textile, and power plants
- ***Electronic waste*** – The defective, non-working electronic appliances are referred to as electronic waste. These are also called e-waste. Some e-waste (such as televisions) contains lead, mercury, and cadmium, which are harmful to humans and the environment.
- ***Mining waste*** **–** chemical gases emitted in mine blasting pollutes the environment. And the mining activity greatly alters the environment and nature.
- ***Chemical waste*** **–** waste from the chemical substance is called chemical waste.
- ***Radioactive waste*** – radioactive waste includes nuclear reactors, extraction of radioactive materials, and atomic explosions.

2.6 Sources of Pollution

All the waste above mentioned also adds to environmental pollution. The contaminants that cause detrimental change to the environment are called pollution. It is one of the most serious problems faced by humanity and other life forms on our planet. The earth's physical and biological components have been affected to such an extent that normal environmental processes could not be carried out properly.

2.7 Types of Pollution

Types of Pollution	**Detail/Pollutants involved**
Air pollution	• Solid particles and gases mixed in the air cause air pollution. • Pollutants: emissions from the car, factories emitting chemical, dust, and pollen.

Water pollution	• Water gets polluted when toxic substances enter water bodies such as lakes, rivers, oceans, and so on. They get dissolved in it and cause it to be unfit for consumption. • Pollutants that contaminate the water are discharges of untreated sewage, and chemical contaminants, release of waste and contaminants into the surface.
Soil pollution	• It is the presence of toxic chemicals (pollutants or contaminants) in soil, in high enough concentrations to pose a risk to human health and/or the ecosystem • Sources of soil pollution include metals, inorganic ions, and salts (e.g. phosphates, carbonates, sulfates, nitrates)
Noise pollution	• Noise pollution happens when the sound coming from planes, industry or other sources reaches harmful levels • Underwater noise pollution coming from ships has been shown to upset whales' navigation systems and kill other species that depend on the natural underwater world
Light pollution	• Light pollution is the excess amount of light in the night sky. Light pollution, also called photo pollution, is almost always found in urban areas. • Light pollution can disrupt ecosystems by confusing the distinction between night and day.

2.8 Organization's focus on the Greening of Jobs

2.8.1 ESG

- The ESG is the short form of environmental, social, and governance. ESG guidelines are used to evaluate businesses on how well they control emissions, governance, human rights, and other factors of their business.

- Several companies audit these companies for ESG compliance. They will let the companies know how well the ESG policies are implemented in their company and let companies know how well their ESG policy is working.

- Every business enterprise is deeply intertwined with Environmental, Social, and Governance (ESG) issues. ESG has been looked at seriously by the corporate, government establishments and stakeholders.

- ESG is important as it creates high value, drives long-term returns, and global stakeholders are paying attention to the topic.

- ESG is said to have created high value, and focuses on long-term returns, and stakeholders are focusing more on this concept.

2.8.2 Factors of ESG

Several factors are used to determine how well a business is doing in maintaining its ESG policies. For creating the ESG Policy, thorough knowledge of these factors is critical.

The factors are divided into three categories; environmental, social, and governance. Knowing about these factors comes a long way in designing the effective ESG policy.

Environmental

Environmental factors relate to a business's impact on the environment. Examples include:

- Usage of renewable energy

- Effective waste management
- Policies for protecting and preserving the environment

Social

Social factors relate to the people of the organization. How they are treated in the organization is what it focuses on. The major entities are the stakeholders, employees, and customers. Examples include:

- diversity and inclusion
- proper work conditions and labour standards
- relationships with the community

Governance

Governance factors relate to the company policies for effectively running it. They include:

- tax strategies
- structure of the company
- relationship with stakeholders
- payments to the employees and CEO

Every factor is important and matters a lot to the overall rating of the company in ESG compliance. Ignoring one aspect in favour of another can affect the rating and in turn the reputation of the company.

The companies make a clear communication about these policies to all the employees, and to the public, they should mention what their various activities are that will protect the environment, people, and the governing factors.

Practical Activity 2.1. Raise awareness about proper e-waste disposal.

Step 1. Workshops: Educate employees on e-waste dangers and recycling benefits.

Step 1. Posters: Display informative posters on e-waste in the workplace.

Step 3. Collection Drive: Set up collection points for old electronic devices.

Step 4. Partner with Recyclers: Collaborate with certified e-waste recycling companies.

Step 5. Progress Tracking: Keep records and share e-waste collection progress.

Practical Activity 2.1. Educate employees on waste segregation.

Step 1. Educational Materials: Provide pamphlets on recyclable waste.

Step 1. Game: Have employees categorize waste into recyclable and non-recyclable.

Step 3. Discussion: Discuss the importance of waste segregation.

Step 4. Proper Bins: Label bins for recyclable and non-recyclable waste.

Practical Activity 2.3. Familiarize employees with tricolored bin system.

Step 1. Information Session: Explain green, blue, and black bins.

Step 1. Interactive Quiz: Test knowledge of bin usage.

Step 3. Bin Labeling: Ensure bins are labeled correctly.

Step 4. Role Play: Demonstrate proper waste disposal.

Summary

- The chapter focuses on green practices in organizations.
- It highlights e-waste management, introduces a tricolored bin system for waste collection, and explains various disposal methods.
- It identifies sources of waste and discusses types of pollution.
- The chapter emphasizes the adoption of ESG guidelines for environmental, social, and governance considerations.
- Overall, it underscores the importance of sustainable practices for both organizations and the environment.

CHECK YOUR PROGRESS

A. Multiple Choice Questions

1. What is e-waste? (a) Waste from construction activities (b) Electrical and electronic equipment discarded as waste (c) Biodegradable waste (d) Hazardous waste from medical facilities
2. What are the three major categories of electronic goods? (a) Red goods, blue goods, green goods (b) White goods, brown goods, grey goods (c) Recyclable goods, non-recyclable goods, hazardous goods (d) Electronic, electrical, and industrial goods
3. What is the purpose of the tricolored bin system in waste collection? (a) To create a visual appeal for waste bins (b) To confuse people about waste segregation (c) To improve the segregation of different types of waste (d) To reduce the number of waste bins needed
4. What is one of the methods mentioned for waste disposal? (a) Exporting waste to other countries (b) Throwing waste in rivers and lakes (c) Incineration to minimize waste gas and ash (d) Leaving waste in open areas for natural decomposition
5. What does ESG stand for in the context of organizations? (a) Environmental, Social, and Governance (b) Energy, Sustainability, and Growth (c) Efficiency, Safety, and Governance (d) Ecology, Standards, and Growth
6. Which factor is NOT part of the ESG framework for evaluating businesses? (a) Environmental (b) Social (c) Governmental (d) Governance
7. What is the significance of ESG compliance for businesses? (a) It has no impact on the business's reputation (b) It creates high value and drives long-term returns (c) It only matters to government agencies (d) It is only relevant for large corporations
8. What are some examples of environmental factors in ESG evaluation? (a) Diversity and inclusion (b) Effective waste management (c) Proper work conditions (d) Relationships with the community
9. Why is proper waste management important for the environment? (a) It creates more job opportunities (b) It conserves important areas in landfills and reduces greenhouse gas emissions (c) It increases pollution levels (d) It has no significant impact on the environment
10. What percentage of municipal waste in India is categorized as 'wet' waste? (a) 40% (b) 30% (c) 20% (d) 10%

B. Fill in the blanks

1. The tricolored bin system in waste collection includes green bin for biodegradable waste, blue bin for dry or recyclable waste, and black bin for domestic __________ waste.

2. Ignoring one aspect of ESG compliance in favour of another can affect the company's __________ and reputation.
3. Effective waste management is an example of an __________ factor in ESG evaluation.
4. Recyclable waste can be converted into new products or raw material, while non-recyclable waste cannot be __________.
5. India's urban population of 429 million citizens produces a _________of garbage every year.
6. E-waste contains hazardous substances like lead, mercury, and __________.
7. Light pollution is the ________ in the night sky.
8. The blue coloured bin is used for ___________.
9. Waste management is carried out to ensure that all types of waste and garbage are collected, transported, and ________.
10. The contaminants that cause detrimental change to the environment are called ___.

C. State true or False for the following

1. Recycling helps conserve space in landfills and reduces greenhouse gas emissions.
2. The black bin is used for disposing of biodegradable waste.
3. Composting is a method of waste disposal that involves the decay of organic material over time by microorganisms.
4. ESG factors include environmental, social, and geological considerations.
5. ESG compliance is important for creating high value and driving long-term returns.
6. Social factors in ESG focus on how people within the organization are treated.
7. Governance factors in ESG pertain to how a company is effectively run, including tax strategies and stakeholder relationships.
8. Soil pollution is caused by the presence of toxic chemicals in soil at low concentrations.
9. Non-recyclable waste can be converted into new products or raw materials.
10. Landfills are used for waste that cannot be recycled or reused.

D. Short Answer Type Questions

1. What is e-waste, and why is it a growing concern for the environment?
2. Explain the process of e-waste management.
3. What is the purpose of using tri coloured bins for waste collection?
4. Name three types of recyclable waste and explain why recycling is important.
5. Describe the factors used to evaluate a business's ESG compliance.
6. What is the impact of soil pollution on human health and ecosystems?
7. How does composting contribute to waste management?
8. What are the sources of electronic waste mentioned in the chapter?
9. What are the different methods of waste disposal mentioned in the chapter?
10. Why is it important to properly segregate waste into recyclable and non-recyclable categories?

Glossary

Internet of Things (IoT): A network of physical objects embedded with sensors, software, and other technologies to exchange data over the internet.

Connectivity: The ability of devices to communicate and share data through the internet or other network systems.

Smart Devices: Devices that can connect to the internet and operate autonomously or be controlled remotely.

Automation: The use of technology to perform tasks without human intervention.

Real-Time Data: Data that is delivered immediately after collection, allowing instant decision-making and actions.

Embedded Systems: Specialized computing systems that are designed to perform dedicated tasks within larger systems, like IoT devices.

Microcontroller: A small computer on a single integrated circuit, containing a processor, memory, and programmable input/output peripherals.

Microprocessor: A central processing unit (CPU) on a single chip, responsible for executing instructions in computing devices.

Arduino: An open-source electronics platform based on simple software and hardware that is commonly used for building IoT projects.

Raspberry Pi: A small, affordable single-board computer used for various applications, including IoT and automation.

GPIO (General Purpose Input Output): Pins on a microcontroller or board like Raspberry Pi used for reading or sending signals from/to external devices.

Firmware: Software that is permanently programmed into the controller board to manage hardware functions.

Sensor: A device that detects physical parameters (temperature, humidity, motion) and converts them into data that can be processed.

Actuator: A device that performs an action in response to a signal, such as moving a motor or opening a valve.

Analog Signal: A continuous signal that represents physical measurements like temperature or light intensity.

Digital Signal: A discrete signal that represents data in binary form (0s and 1s).

Input Device: A hardware component that sends data to a system for processing, such as a sensor.

Output Device: A hardware component that receives data from a system to perform a task, such as an actuator.

Node: A point in a network where data is generated or received, often representing an IoT device like a sensor.

Gateway: A device that connects two networks, typically between IoT devices and the internet, enabling communication between different networks.

Edge Device: A device located at the edge of the network that processes data locally, reducing the need to send data to a central server.

Configuration: The process of setting up a device or system to operate as intended, such as setting up communication protocols and security settings.

Network Topology: The arrangement of various elements (links, nodes, etc.) in a computer network, which defines how data flows between devices.

Firmware Setup: The process of installing and configuring the low-level software that controls hardware operations on devices.

Communication Protocol: A set of rules that define how data is transmitted and received in a network (e.g., MQTT, HTTP).

Wireless Network: A network that uses radio waves to connect devices, such as Wi-Fi, Zigbee, or Bluetooth.

Bluetooth: A short-range wireless technology used for connecting devices over distances typically less than 100 meters.

Wi-Fi: A wireless technology that allows devices to connect to the internet or local area networks using radio waves.

Pairing: The process of establishing a trusted relationship between two devices for secure communication.

Connectivity: The ability of devices to connect to each other or a network to share data and interact.

Authentication: The process of verifying the identity of a user or device before granting access to a network or system.

Authorization: The process of granting or denying access to specific resources based on the authenticated identity.

User Credential: Information (like username and password) used to verify the identity of a user or device.

Access Control: A security technique used to regulate who or what can view or use resources in a system.

Encryption: The process of converting data into a code to prevent unauthorized access.

Security Token: A piece of data used in the authentication process to verify a user's identity or session.

MQTT (Message Queuing Telemetry Transport): A lightweight messaging protocol used for transmitting data between devices, typically in IoT applications.

CoAP (Constrained Application Protocol): A protocol designed for simple devices to communicate in IoT, optimized for low-power devices and low-bandwidth environments.

HTTP (Hypertext Transfer Protocol): The foundation of data communication on the web, commonly used in IoT for transferring data between clients and servers.

LoRaWAN (Long Range Wide Area Network): A low-power wide-area network protocol designed for long-range IoT communication.

Zigbee: A wireless communication standard for low-power, short-range IoT devices, typically used in home automation.

Protocol Stack: A set of protocols that work together to manage data communication within a network, from physical transmission to application-level communication.

Cloud Storage: A service that allows data to be stored and accessed over the internet rather than on a local device.

Data Synchronization: The process of ensuring that data on different devices or servers is consistent and up-to-date.

Cloud Server: A virtual server hosted on the internet that stores and manages data for IoT devices.

IoT Platform: A cloud-based platform that connects, manages, and processes data from IoT devices.

Remote Access: The ability to access and control devices or data from a remote location over the internet.

Virtualization: The creation of virtual (rather than actual) versions of resources such as servers, storage devices, or networks, to optimize cloud services.

IoT Architecture: The design of the various components and their relationships in an IoT system, including sensors, actuators, and cloud platforms.

Device Layer: The layer in an IoT system that includes physical devices like sensors and actuators that collect or act on data.

Network Layer: The layer responsible for transmitting data between devices, usually through networks like Wi-Fi, Bluetooth, or cellular networks.

Application Layer: The layer that processes the data and provides the interface for end-users to interact with the IoT system.

Interoperability: The ability of different IoT devices and systems to work together and exchange data seamlessly.

Integration: The process of connecting various IoT components, systems, or devices to ensure they work as a cohesive unit.

Server: A computer or system that provides services and resources to other devices on a network, often central in IoT communications.

Data Transmission: The process of sending data from one device to another, typically over a network.

IP Address: A unique address assigned to each device on a network to identify and locate it.

Data Flow: The movement of data between devices or systems within a network, influenced by protocols and hardware capabilities.

Site Survey: The process of assessing the physical environment where IoT devices will be installed, considering factors like coverage and accessibility.

Power Supply: The system or device that provides electrical power to IoT devices to enable operation.

Network Availability: Ensuring that there is a reliable network connection (Wi-Fi, Ethernet, etc.) for IoT devices to communicate.

Device Compatibility: The ability of devices to work together without issues, such as using the same communication protocols or power requirements.

Pre-checklist: A list of tasks and requirements to be completed before the installation of devices to ensure readiness.

Installation Tools: Tools required for physically installing devices, such as screws, brackets, and cable connectors.

Mounting: The process of physically installing devices onto surfaces or supports in their operational locations.

Enclosure: A protective casing or housing that keeps IoT devices safe from environmental damage or tampering.

Orientation: The proper alignment of devices to ensure optimal performance, such as pointing antennas in the right direction.

Brackets: Supporting structures used to mount devices securely.

Wall Mount: The process of affixing a device to a wall or another vertical surface.

Cable Management: Organizing and securing cables to prevent damage, tangling, or interference with device operation.

Continuity Test: A test that ensures electrical circuits or connections are complete and operational.

Connector: A device used to join two or more electrical circuits together, allowing for data or power transfer.

Cable Routing: The process of guiding and securing cables along a specified path, ensuring they don't interfere with device functions.

Power on Self-Test (POST): A diagnostic process where a device checks its own hardware components to ensure proper operation before starting.

Functional Testing: The process of verifying that a device or system performs as expected.

Diagnostics: Tools and processes used to identify and troubleshoot issues within IoT systems.

Personal Protective Equipment (PPE): Gear worn to protect workers from hazards like chemicals, physical injuries, or electrical shocks.

Hazard: A potential source of harm or danger in the workplace.

Safety Protocols: Established procedures and rules designed to ensure the safety and well-being of workers.

Risk Assessment: The process of identifying hazards, assessing risks, and implementing safety measures.

Emergency Exit: A designated route for escaping from a building during an emergency, ensuring safe evacuation.

First Aid: Basic medical care provided to an injured person until professional help arrives.

Sustainability: The practice of using resources in a way that meets current needs without compromising the ability of future generations to meet their needs.

E-Waste: Discarded electronic devices and components that must be recycled or disposed of properly.

Energy Efficiency: Using less energy to perform the same tasks, reducing environmental impact.

Recycling: The process of converting waste materials into reusable material, especially in relation to electronic products.

Eco-Friendly: Products or practices that do not harm the environment and promote sustainability.

Environmental Impact: The effect that an activity, product, or service has on the environment, including resource consumption, pollution, and waste.

Answer Key

Module 1. IoT Devices and Systems

Session. 1. Basic Concept of IoT

A. Multiple Choice Questions

1. (c) 2. (a) 3. (a) 4. (b) 5. (d) 6. (a) 7. (a) 8. (a) 9. (b) 10. (d)

B. Fill in the blanks

1. Digital and physical worlds 2. Network layer 3. Cloud computing 4. Sensing layer 5. IP address 6. Smart homes, smart cities, healthcare, agriculture, etc. 7. To control appliances remotely using a smartphone 8. Application layer 9. Parts 10. Gateway

C. State true or False

1. (F) 2. (T) 3. (T) 4. (T) 5. (T) 6. (F) 7. (F) 8. (F) 9. (T) 10. (T)

Session 2. Controller Boards

A. Multiple Choice Questions

1. (c) 2. (a) 3. (b) 4. (b) 5. (a) 6. (a) 7. (c) 8. (d) 14 9. (b) 10. (a)

B. Fill in the Blanks

1. Linux-based 2. The brain 3. 4 4. Single-board computer 5. Two 6. Arduino 7. C/C++ 8. Pins 9. Raspbian 10. Voltage regulator

C. State true or False

1. (T) 2. (F) 3. (T) 4. (T) 5. (F) 6. (F) 7. (T) 8. (F) 9. (T) 10. (T)

Session 3. Functions of Sensors and Actuators in IoT

A. Multiple Choice Questions

1. (d) 2. (d) 3. (c) 4. (d) 5. (b) 6. (d) 7. (a) 8. (d) 9. (c) 10. (d)

B. Fill in the Blanks

1. Real-time 2. Transmitter and receiver 3. Linear and rotary 4. Thermistor 5. Calibration 6. Object 7. Electrical energy into mechanical motion 8. Touch or contact 9. Temperature, pressure, light, humidity, etc. 10. Application and environment

C. State true or False

1. (T) 2. (T) 3. (F) 4. (T) 5. (T) 6. (F) 7. (T) 8. (T) 9. (T) 10. (F)

Module 2. Networking of IoT Devices

Session 1. Initialize and Configure Nodes, Gateways, and Control Edge Appliances

A. Multiple Choice Questions

1. (b) 2. (c) . 3. (c) 4. (c) 5. (b) 6. (b) 7. (c) 8. (a) 9. (a) 10. (c)

B. Fill in the Blanks

1. Body 2. Wi-Fi 3. EnViewer 4. IP 5. Installed 6. Communication 7. Software 8. Ethernet cable 9. Module 10. Router

C. State true or False

1. (F) 2. (T) 3. (T) 4. (T) 5. (T) 6. (T) 7. (F) 8. (T) 9. (T) 10. (T)

Session 2. Establish Communication and Connectivity between devices

A. Multiple Choice Questions

1. (d) 2. (b) 3. (b) 4. (b) 5. (d) 6. (c) 7. (d) 8. (a) 9. (b) 10. (d)

B. Fill in the Blanks

1. Data transfer 2. Bulk transfer 3. USB addresses 4. Send 5. One 6. Simultaneously 7. Type and quality 8. Gateway/router 9. Wi-Fi, Bluetooth, or ZigBee 10. Content of the data

C. State true or False

1. (F) 2. (T) 3. (T) 4. (F) 5. (F) 6. (T) 7. (F) 8. (T) 9. (T) 10. (T)

Session 3. Authentication and Authorization Mechanism in IoT

A. Multiple Choice Questions

1. (b) 2. (c) 3. (b) 4. (c) 5. (b) 6. (a) 7. (c) 8. (b) 9. (a) 10. (c)

B. Fill in the Blanks

1. Identity 2. User 3. Groups 4. IP address 5. Slowdown 6. Verification 7. IoT devices 8. Biometric 9. 80 10. Authorized

C. State true or False

1. (T) 2. (F) 3. (T) 4. (F) 5. (T) 6. (T) 7. (T) 8. (T) 9. (F) 10. (F)

Session 4. Communication Technologies and Protocols for IoT

A. Multiple Choice Questions

1. (a) 2. (c) 3. (b) 4. (c) 5. (c) 6. (a) 7. (a) 8. (d) 9. (a) 10. (a)

B. Fill in the Blanks

1. Retransmission 2. Multipoint topology 3. Low-power 4. Radio signals 5. Power, short-range 6. Central hub 7. Low-power wide-area (LPWA) 8. Commonly 9. 4 cm 10. IEEE 802.15.4

C. State true or False

1. (F) 2. (T) 3. (T) 4. (T) 5. (F) 6. (T) 7. (T) 8. (T) 9. (T) 10. (T)

Session 5. Cloud Computing

A. Multiple Choice Questions

1. (b) 2. (c) 3. (b) 4. (a) 5. (b) 6. (d) 7. (c) 8. (b) 9. (d) 10. (c)

B. Fill in the Blanks

1. Multi-tenant 2. Demand increases or decreases 3. Third-party service 4. Diverse or fluctuating 5. Applications 6. Web-based 7. Security patches 8. Data 9. Intelligent IoT-enabled 10. Real-time

C. State true or False

1. (T) 2. (F) 3. (F) 4. (T) 5. (F) 6. (F) 7. (F) 8. (F) 9. (F) 10. (F)

Module 3. Installation of IoT Devices

Session 1. Establish Communication between Nodes, Gateway and Servers

A. Multiple Choice Questions

1. (d) 2. (b) 3. (c) 4. (c) 5. (a) 6. (b) 7. (d) 8. (b) 9. (b) 10. (b)

B. Fill in the blanks

1. Device 2. Data 3. Actuator 4. Power supply 5. Measures 6. Hub 7. Certain height 8. Cloud 9. Collecting data 10. Number

C. State true or False

1. (T) 2. (T) 3. (T) 4. (T) 5. (T) 6. (T) 7. (T) 8. (T) 9. (F) 10. (F)

Session 2. Establish Communication between Nodes, Gateway and Servers

A. Multiple Choice Questions

1. (a) 2. (b) 3. (a) 4. (c) 5. (d) 6. (d) 7. (a) 8. (a) 9. (c) 10. (a)

B. Fill in the blanks

1. Sender, receiver 2. Wires, Cables 3. 802.11 4. Crimping 5. Multiple, Multiple 6. 1000 7. True 8. Jumper 9. Ethernet portsb 10. Electromagnetic interference

C. State true or False

1. (T) 2. (F) 3. (T) 4. (T) 5. (T) 6. (T) 7. (T) 8. (T) 9. (F) 10. (F)

Session 3. Pre-installation preparation of IoT devices

A. Multiple Choice Questions

1. (a) 2. (a) 3. (a) 4. (b) 5. (b) 6. (a) 7. (b) 8. (a) 9. (a) 10. (b)

B. Fill in the blanks

1. Screwdrivers, pliers 2. Voltage, Current 3. Proper wirings 4. Safety gears 5. Styrofoam 6. Power sources 7. Should not 8. Loose clothes and jewellery 9. Holding small metallic components 10. The angle of inclination

C. State true or False

1. (F) 2. (T) 3. (T) 4. (T) 5. (T) 6. (F) 7. (T) 8. (F) 9. (F) 10. (T)

Session 4. Mounting Devices at Desired Locations

A. Multiple Choice Questions

1. (d) 2. (b) 3. (c) 4. (b) 5. (b) 6. (b) 7. (b) 8. (a) 9. (c) 10. (b)

B. Fill in the blanks

1. Spirit 2. Screws 3. Attenuated 4. Wired 5. Wall 6. Cable type 7. Switch 8. Electromagnetic Interference 9. Distance 10. Optimize

C. State true or False

1. (F) 2. (T) 3. (F) 4. (T) 5. (T) 6. (T) 7. (F) 8. (T) 9. (T) 10. (T)

Session 5. Perform checks and connections of devices

A. Multiple Choice Questions

1. (b) 2. (b) 3. (a) 4. (a) 5. (c) 6. (a) 7. (a) 8. (b) 9. (b) 10. (a)

B. Fill in the blanks

1. Ventilation 2. Good 3. Earth 4. Batteries 5. Grounded 6. Green 7. Data transmission 8. Performance 9. Customer's 10. Needed

C. State true or False

1. (T) 2. (T) 3. (T) 4. (T) 5. (T) 6. (T) 7. (F) 8. (T) 9. (T) 10. (T)

Module 4. Occupational Health and Safety Standards

Session 1. Workplace Health and Safety Practices

A. Multiple Choice Questions

1. (b) 2. (d) 3. (b) 4. (a) 5. (a) 6. (b) 7. (c) 8. (b) 9. (c) 10. (a)

B. Fill in the Blanks

1. Bending 2. Emergency 3. Bleeding 4. Infection 5. Rescue breaths (or CPR) 6. Evacuation 7. Communicable 8. Preventive 9. Insulated/protective 10. Time

C. State true or False

1. (T) 2. (F) 3. (T) 4. (T) 5. (T) 6. (T) 7. (T) 8. (F) 9. (F) 10. (F)

Session 2. Green Practices in Organisation

A. Multiple Choice Questions

1. (b) 2. (b) 3. (c) 4. (c) 5. (a) 6. (c) 7. (b) 8. (b) 9. (b) 10. (a)

B. Fill in the Blanks

1. Hazardous 2. Growth 3. Environmental 4. Recycled 5. Mountain 6. Cadmium 7. Excess light 8. Dry/recyclable waste 9. Disposed 10. Pollutants

C. State true or False

1. (T) 2. (F) 3. (T) 4. (F) 5. (T) 6. (T) 7. (T) 8. (F) 9. (F) 10. (T)