Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

Telecom
Sector
Skill
Council

Participant Handbook

Sector
Telecom

Sub-Sector
Network Managed Services

Occupation
Network Operation and Maintenance

Reference ID: **TEL/Q6210, Version 2.0**
NSQF Level 4

Telecom Technician - IoT Devices / Systems

Click/Scan this QR Code to access e-Book

This book is sponsored by

Telecom Sector Skill Council of India Estel House,

3rd Floor, Plot No:- 126, Sector 44 Gurugram,

Haryana 122003 Phone: 0124-2222222

Email: tssc@tsscindia.com

Web: www.tsscindia.com

All Rights Reserved © 2022

First Edition, July 2022

Printed in India

Copyright © 2022

Under Creative Commons License: CC-BY -SA

Attribution-ShareAlike: CC BY-SA

Disclaimer

The information contained herein has been obtained from sources reliable to Telecom Sector Skill Council of India. Telecom Sector Skill Council of India disclaims all warranties to the accuracy, completeness or adequacy of such information. Telecom Sector Skill Council of India shall have no liability for errors, omissions, or inadequacies, in the information contained herein, or for interpretations thereof. Every effort has been made to trace the owners of the copyright material included in the book. The publishers would be grateful for any omissions brought to their notice for acknowledgements in future editions of the book. No entity in Telecom Sector Skill Council of India shall be responsible for any loss whatsoever, sustained by any person who relies on this material.

Skilling is building a better India. If we have to move India towards development then Skill Development should be our mission.

Shri Narendra Modi
Prime Minister of India

Certificate

COMPLIANCE TO

QUALIFICATION PACK – NATIONAL OCCUPATIONAL STANDARDS

is hereby issued by the

TELECOM SECTOR SKILLS COUNCIL

for

SKILLING CONTENT: PARTICIPANT HANDBOOK

Complying to National Occupational Standards of
Job Role/ Qualification Pack: 'Telecom Technician - IoT Devices/Systems'
QP No:'TEL/6210, NSQF Level 4'

Date of Issuance: **Jan 27th, 2022**

Valid up to*: **Jan 27th, 2026**

**Valid up to the next review date of the Qualification Pack or the 'Valid up to' date mentioned above (whichever is earlier)*

Authorised Signatory
(Telecom Skill Development Council)

Acknowledgement

Telecom Sector Skill Council would like to express its gratitude to all the individuals and institutions who contributed in different ways towards the preparation of this “Participant Handbook”. Without their contribution it could not have been completed. Special thanks are extended to those who collaborated in the preparation of its different modules. Sincere appreciation is also extended to all who provided peer review for these modules.

The preparation of this Handbook would not have been possible without the Telecom Industry's support. Industry feedback as been extremely encouraging from inception to conclusion and it is with their input that we have tried to bridge the skill gaps existing today in the Industry.

This participant handbook is dedicated to the aspiring youth who desire to achieve special skills which will be a lifelong asset for their future endeavours.

About this Book

India is currently the world's second-largest telecommunications market with a subscriber base of 1.20 billion and has registered strong growth in the last decade and a half. The Industry has grown over twenty times in just ten years. Telecommunication has supported the socioeconomic development of India and has played a significant role in narrowing down the rural-urban digital divide to some extent. The exponential growth witnessed by the telecom sector in the past decade has led to the development of telecom equipment manufacturing and other supporting industries.

Over the years, the telecom industry has created millions of jobs in India. The sector contributes around 6.5% to the country's GDP and has given employment to more than four million jobs, of which approximately 2.2 million direct and 1.8 million are indirect employees. The overall employment opportunities in the telecom sector are expected to grow by 20% in the country, implying additional jobs in the upcoming years.

This Participant Handbook is designed to impart theoretical and practical skill training to students for becoming a Telecom Technician – IoT Devices/Systems. Telecom Technician – IoT Devices/Systems in the Telecom industry is also known as IoT installation and service technician.

IoT installation and service technician is responsible for on-site installation and configuration of IoT devices (nodes), set up of communication links between nodes and controller (gateway) and further to central servers or devices through external communication links on Wi -Fi, 3G/4G networks on GSM/CDMA. The technician also undertakes first level of troubleshooting.

This Participant Handbook is based on Telecom Technician – IoT Devices/Systems Qualification Pack (TEL/Q6210) & includes the following National Occupational Standards (NOSs)

1. Install and configure IoT devices at customer premises (TEL/N6234)
2. Perform Level 1 Troubleshooting of IoT devices (TEL/N6236)
3. Organize work and resources as per Health and Safety Standards (TEL/N9101)
4. Interact effectively with Team members and Customers (TEL/9102)

The Key Learning Outcomes and the skills gained by the participant are defined in their respective units.

Post this training, the participant will be able to keep sites live 24x7 through site maintenance.

We hope that this Participant Handbook will provide a sound learning support to our young friends to build an attractive career in the telecom industry.

Symbols Used

Key Learning Outcomes

Steps

Tips

Practical

Notes

Unit Objectives

Exercise

Table of Contents

S. No	Modules and Units	Page No.
1.	**Roles and Responsibilities of Telecom Technician-IOT Devices/System (TEL/N6234)**	1
	Unit 1.1 – Basics of Micro-processor Boards and Microcontroller Units	3
	Unit 1.2 – Functioning of Sensors and Actuators	15
	Unit 1.3 – Application of Communication Protocol in Internet of Things	25
	Unit 1.4 – Micro-controller Boards, PIN Configurations and Their Interconnectivity	34
	Unit 1.5 – Understanding Edge Devices	42
	Unit 1.6 – Nodes and Gateways	47
	Unit 1.7 – Cloud Computing	51
2.	**Install and Configure IOT devices (TEL/N6234)**	57
	Unit 2.1 – Establishing Framework for Internet of Things	59
	Unit 2.2 – Installing Gateway as per the Power Supply Requirements	67
	Unit 2.3 – Establishing Communication between Nodes, Gateway and Servers and Ethernet Connectivity and Establishing Ethernet Connectivity	78
	Unit 2.4 – Authentication and Access Control Mechanism	87
	Unit 2.5 – Preparing for Installation of IoT Edge Devices	121
	Unit 2.6 – Mounting the Devices at Desired Locations	135
	Unit 2.7 – Performing Checks and Connections	144
	Unit 2.8 – Connecting Microcontroller Boards for Data Transfer and Connecting the Boards	153
	Unit 2.9 – Installing Suitable Framework	166
	Unit 2.10 – Transferring Software Code to On-board Microprocessor and Compiling Code to On-board Microprocessor	174
	Unit 2.11 – Understanding Error Codes and Debug Software	184
	Unit 2.12 – Functioning of Micro-controller and Attached Devices	193
	Unit 2.13 – Initializing Nodes and Gateways	209
	Unit 2.14 – Launching the Software on Nodes and Gateways	232
	Unit 2.15 – Confirming Communication and Establishing Connectivity	234
	Unit 2.16 – Controlling Edge Appliances and Hubs and Checking for Data Transfer and Confirming from the Server End	247

S. No	Modules and Units	Page No.
		257
3.	Level 1 Troubleshooting of IOT (TEL/N6236)	259
	Unit 3.1 – Testing Connectivity between Devices	265
	Unit 3.2 – Checking Connectivity between Devices	270
	Unit 3.3 – Checking On-board Memory Storage Card	272
	Unit 3.4 – Testing Working of Connectivity Modules	276
	Unit 3.5 – Checking the On-board Power Supply	279
	Unit 3.6 – Checking Communication Link Performance Matrix	283
	Unit 3.7 – Checking Data Transfer from Gateway to Server	285
	Unit 3.8 – Checking Communication between Devices	287
	Unit 3.9 – Setting Connectivity Credentials	293
	Unit 3.10 –Project on Humidity and Temperature Sensing Device	294
	Unit 3.11 – Project on Air Pollution Sensing Device	297
	Unit 3.12 – Organizational Processes and Standards	307
	Unit 3.13 –Project Handling Concepts and Applications	311
	Unit 3.14 – Record Maintenance	313
	Unit 3.15 –Record Performance/Test Results	316
	Unit 3.16 – Maintain Records and Process Documents	318
4.	Organise work and resources as per health and safety standards (TEL/9101)	3212
		324
	Unit 4.1 – Workplace health and Safety	327
	Unit 4.2 – Different types of health hazards	331
	Unit 4.3 – Importance of Safe working practices	333
	Unit 4.4 – Reporting safety hazards	339
	Unit 4.5 - Waste Management	342
	Unit 4.6 - Organizations' Focus on Greening of Jobs	345
5.	Communication and Interpersonal Skills (TEL/N9102)	350
		355
	Unit 5.1- Interaction with supervisor, peers, customers and differently abled persons	358
	Unit 5.2: Explain the importance of developing sensitivity towards disabled persons	372

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

1. Roles and Responsibilities of Telecom Technician-IOT Devices/System

Telecom Sector Skill Council

Unit 1.1 - Basics of Micro-processor Boards and Microcontroller Units

Unit 1.2 - Functioning of Sensors and Actuators

Unit 1.3 - Application of Communication Protocols in Internet of Things

Unit 1.4 - Micro-controller Boards, PIN Configurations and Their Interconnectivity

Unit 1.5 - Understanding Edge Devices

Unit 1.6 - Nodes and Gateways

Unit 1.7 - Cloud Computing

Key Learning Outcomes

At the end of this module, you will be able to:

1. Explain the basics of IoT
2. Identify the applications of IoT in current world
3. Explain the basics of microprocessors and microcontrollers
4. Describe different processor boards and their applications
5. Explain how IoT works for roadside assistance and smart cities
6. List various types of sensors
7. Identify the importance of actuators
8. Explain the basic programming of a microcontroller board
9. List various short-range wireless communications systems
10. Identify the protocols used for communication in IoT
11. Compare different communication technologies
12. Identify the components of a microcontroller board
13. Describe the layout of various development boards
14. Explain the functions of edge devices
15. Identify the different types of edge devices
16. Explain nodes
17. Describe gateway architecture
18. List the steps in setting up an IoT framework
19. Explain the concept of cloud computing
20. List the characteristics of cloud computing
21. Explain how cloud computing is related to business analytics
22. Explain the advantages of cloud utilization

UNIT 1.1: Basics of Micro-Processor Boards and Microcontroller Units

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the basics of IoT
2. Identify the applications of IoT in current world
3. Explain the basics of microprocessors and microcontrollers
4. Describe different processor boards and their applications
5. Explain how IoT works for roadside assistance and smart cities
6. Explain the essentials of networking like TCP/IP,UDP,SSL protocols

1.1.1 Introduction to Internet of Things

Digital India program is an endeavour to make technology a great leveller for the citizens of India. The thorough research of digitization and its coherent approach to enhance the digital literacy in India could be a real game changer. The Telecom Sector Skill Council (TSSC) is playing a major role in training and creating digital platforms for the development of digital India programmes.

IoT is a connected ecosystem of mobile devices, appliances and other electronic devices that has been formed to establish communication among them. IoT connected devices can be controlled remotely and can be setup for certain actions, at specific times. The telecommunication lines are used to transfer data to get Internet connectivity for transferring, processing, and analysing data. This results in efficiency, accuracy, and ease in life without much human intervention. Combined with smart sensors and actuators, IoT gives the freedom to inter operate devices in a manner which is semi-automated or completely automated.

Devices which fall in the IoT ecosystem can include anything from heart monitoring implants or DNA analysis devices to automobiles with built-in sensors or home monitoring gadgets. The following image shows devices such as mobile phones, surveillance cameras, home security systems, PC, tablets and so on interconnected wirelessly, leading to an IoT system:

Click/Scan this QR code to view the video in IoT concepts

Fig. 1.1.1: Wireless interconnection of devices via Internet

1.1.2 Applications of Internet of Things

IoT spans its influence across a large number of sectors and also in daily life. The most famous applications of IoT include smart home devices, wearable technology, connected cars, telecom sector integration, healthcare, media, infrastructure management, agriculture, environmental monitoring, enterprises, and smart cities where everything is connected and assisted with artificial intelligence. Depending on the end-user experience, the IoT applications can be classified in the ways as follows:

1. **Smart Home**

   Modern homes are laden with technology, giving the homeowners utmost comfort and functionality, which enhances the overall lifestyle. All the devices in a smart home can interact with each other. This environment enhances the security or optimum energy management. Already leading names in the industry have numerous products based on IoT, providing cross-platform integration for smart homes. Smart home technologies are common use case areas for IoT application. They allow the home appliances and switches to be controlled by a mobile app. The various applications, such as thermostat control, TV remote control, air temperature control, light control and so on can be controlled by a software interface installed on the smartphone. The following image shows some smart home technologies at a finger-tip:

Fig. 1.1.2: Smart home technologies at a finger-tip

   Examples can be turning the lights ON or OFF at a particular time of the day using a smart phone or providing a friend a temporary access to the home via a smart door lock is an example of a smart home IoT application. Another example can be monitoring the home remotely when the owners are on vacation.

   Thermostats, home assistants, smart lighting and remotely controlled home security systems are some of the many products available in the market.

2. **Media**

   Media houses that use IoT are essentially concerned about analysing the market and the consumers' behaviour. The behavioural focus of these devices is on gathering significant data of millions of individuals. This data is used by the media houses to run better advertising campaigns, aligned with the consumers' known habits and locations.

   For example, a smart watch may have applications to track health status, listen to music and other media services, access mails and so on.

The following image shows a smart watch with various applications:

Click/Scan this QR code to view the applications of IoT

Fig. 1.1.3: Smart watch

3. Infrastructure Management

IoT plays a vital role in the infrastructure management. The checking and controlling of urban and rural roads, rail networks, bridges, off-shore and wind-farms are some of the key uses of IoT. The framework assists in monitoring changes in any structural conditions which otherwise can compromise the safety of people. The use of IoT devices effectively reduces the cost of operations in the large infrastructures which benefits from automation and advancement developed by IoT.

For example, in case of road and transportation, the traffic signals are Wi-Fi connected and the traffic is under video surveillance. It makes the management of traffic faster and easier and monitoring of vehicles effective. The following figure shows wireless connectivity at the traffic signal points:

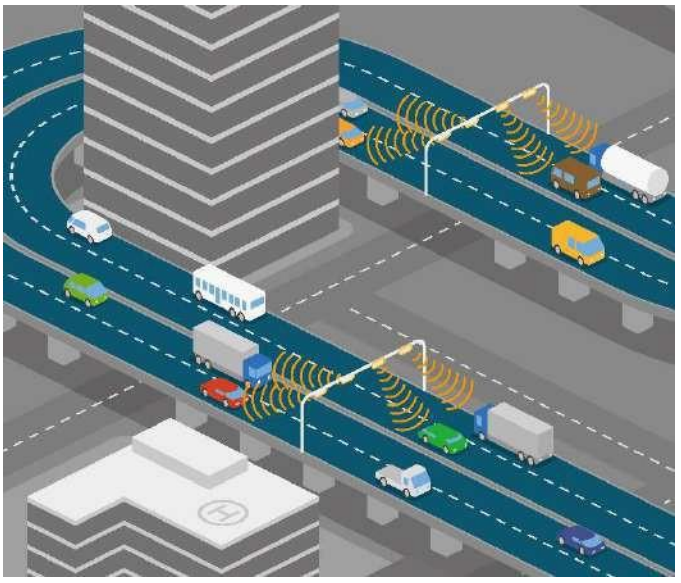


Fig. 1.1.4: Wireless connectivity for managing and controlling traffic

Click/Scan this QR code to view the video on smart parking using IoT

4. Agriculture

Challenges like weather conditions and population growth have made agriculturists think and move beyond traditional methods to more advanced technologies like IoT. The integration of wireless sensors with an agriculturist's mobile appand cloud platforms helps in gathering essential data related to the ecological conditions such as soil, seeds and much more. For example, the agricultural application interface can provide information about the weather and crop condition, climate change, rainfall, pest infestation, costs/availability of fossil fuels, limited arable land, crop yields and soil nutrition. It helps the farmers to improve production and protect crops. The following image shows a mobile interface giving information about the weather and crop condition:

Fig. 1.1.5: A mobile interface showing weather and crop condition

5. Environmental Monitoring

The sensors in IoT devices help by observing environmental conditions such as quality of air, water and atmospheric or soil conditions. Improvement in the resource-constrained devices, when connected well with the Internet, allows the use of applications such as earthquake or tsunami warning systems. These can be utilized by the emergency services for effective aid.

The following image shows a Tsunami alert system placed in the middle of the sea, which senses the changes in the sea and gives an alert if the changes are beyond the standard limits and condition:

Fig. 1.1.6: Tsunami alert system

6. Enterprise

"Enterprise IoT" or EIoT refers to the gadgets and devices used in the corporate settings and businesses. EIoT sector is likely to increase by estimated 40 percent or 9.1 billion devices by 2019 as per an article given by BI intelligence.

For example, retailers incorporate Radio Frequency Identification (RFID) tags to manage inventory and maintain the storage costs. In case of mining, driverless trucks or autonomous haul trucks are used to work round the clock. It leads to increased output, lower cost and reduced maintenance. In smart robotic assembly line, the automation of the devices helps in making the production cycle faster and of better quality.

The following figure shows an employee controlling the machines of a robotic assembly line by using a tablet interface:

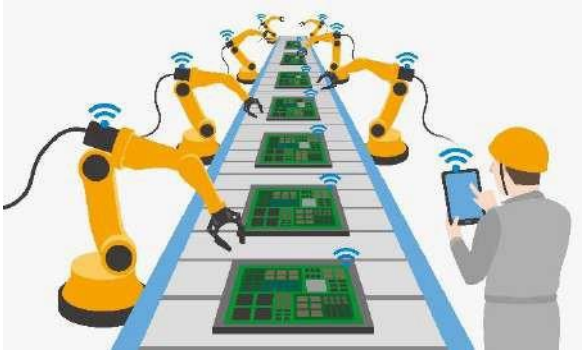


Fig. 1.1.7: Smart robotics assembly line

7. Wearable Technology

This is one of the latest applications of IoT which revolves around health, fitness and entertainment. For wearable technology, IoT is possible in small devices that have tiny sensors which consume less power, thus making them highly efficient. Smartwatches, sleep analysers, interactive fitness trackers and health trackers are some of the most popular wearables in the market. This proves IoT is going to gain more popularity in near future.

These wearables are loaded with sensors and paired with software applications to collect data. They enable tracking body statistics, resulting in better health. For instance, Fitbit is an IoT wearable that monitors every move (tracks steps, distance covered, calories burnt and stairs climbed). It automatically syncs to the computer or selected smartphones and tablets to have a better control over the data collected by the fitness device. The following image shows a fitness tracking band to track a person's daily activities:

Fig. 1.1.8: Fitness tracking band

8. Healthcare Industry

Healthcare is one sector which is highly influenced by IoT. Vital data collected by sensors helps in determining underlying illnesses or ailments that might affect the patient in future. Data collected with health monitors over a period of time can be used to determine methods to improve health or cure any current ailments.

IoT in healthcare is vital due to the use of connected healthcare equipment and devices which help medical practitioners in providing quality healthcare. Practical example of IoT in healthcare is the use of smart pills (or ingestible sensors). Once the pill is consumed, the sensor is activated by electrolytes in the body and a signal is conveyed to the small, battery-powered patch worn on the torso. The data then gets transferred via Bluetooth to the family member's smartphone. Other examples of IoT in healthcare include insulin delivery devices, connected inhalers, smart beds, robotic surgeons and biosensors.

The following image shows the sensor of a glucose monitoring system placed on an arm and a medical device displaying the glucose level after scanning the sensor:

Fig. 1.1.9: Glucose monitoring system

9. Telecom Industry

IoT facilitates data management in telecom sector to create a global network which enhances interaction between tangible and non-tangible objects. The data collected enriches the user's experience which helps in devising product development strategies and planning maintenance tasks.

In the telecom sector, IoT is playing an important role in development of the entire telecom network by providing useful data whenever required. Also, IoT is used in the telecom tower fuel monitoring systems integrated telecom site monitoring.

The following image shows that the security system, the big data analytics and so on are connected to the communication devices such as a mobile or a laptop via a telecom network:

Fig. 1.1.10: Various systems connected through telecom network

A good example of IoT implementation in telecom sector is product monitoring by providing easy and timely tracking of products and services given to the customers. Also, IoT is being used for customer monitoring. This helps companies to monitor customers through the digital devices, such as smart phones and smart watches, which they carry with them always.

This adds value to the ecosystem as IoT-based systems work in tandem for seamless security, connectivity and technological advantage.

1.1.3 Introduction to Microprocessor and Microcontroller

Microprocessor

First introduced in the 1970s, a microprocessor is a standalone chip which acts as the controlling brain of computer. A microprocessor is a computer processor which has all the functions of a central processing unit incorporated on a single integrated circuit (IC). Intel created the first ever microprocessor, 4004, for personal computers which was a low-cost solution for the masses.

Microprocessors these days are categorised into general purpose and high-end ones. The microprocessors used in computers and mobile devices are general purpose microprocessors, also known as digital signal processor (DSP).

Whereas, those used for graphical processing like real time rendering of 3D images are specialized microprocessors called as graphics processing unit (GPU). The following image shows a microprocessor placed on a printed circuit board (PCB):

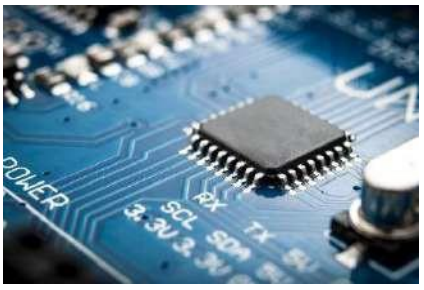


Fig. 1.1.11: Microprocessor

Microcontroller

A microcontroller (or VLSI microcomputer) is a computing unit integrated on a single chip, and it has a processor CPU, RAM, ROM and other required peripherals. In a way it is a mini computer on a circuit, which enables IoT-based hardware to communicate efficiently with other devices. All microcontrollers are designed to perform certain specific tasks. Microcontrollers can be of 4-bits, 8-bits, 64-bits or 128-bits configuration, depending on the functionality of the embedded system.

The following image shows a microcontroller:

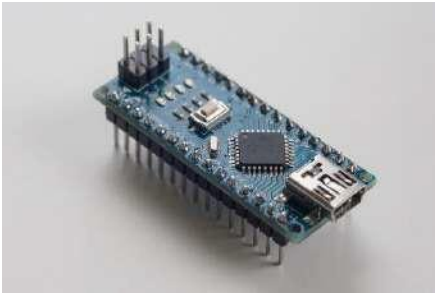


Fig. 1.1.12: Microcontroller

Applications of microcontrollers:

The various applications of a microcontroller are as follows:

- Temperature sensing system
- Light sensing system
- Fire detection system
- Process control devices
- Handheld metering systems

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

Microprocessor	Microcontroller
External peripheral in microprocessor has external circuits.	External peripheral in microcontroller has RAM, EEPROM.
Processing speed of microprocessors is above 1 GHz.	Processing speed of microcontrollers is from 8 MHz to 50 MHz.
No power saving system with external components, so power consumption is high.	Power saving system, such as idle mode or power saving mode, for low consumption of power.
Bulky and preferred for larger applications.	Compact, favourable and efficient system for small products and applications.
Task performed are software development.	Tasks performed are limited and generally less complex.
Based on von Neumann model where program and data are stored in same memory module.	Based on Harvard architecture where program memory and data memory are separate.

Table 1.1.1 Difference between microprocessor and microcontroller

1.1.4 Getting Acquainted with Various Boards

Processor Boards

These are PCBs which have a microprocessor and support logic to assist an engineer in programming. Processor boards have the needed circuit for controlling tasks such as I/O control, clock, RAM and so on. The following image shows a PCB:

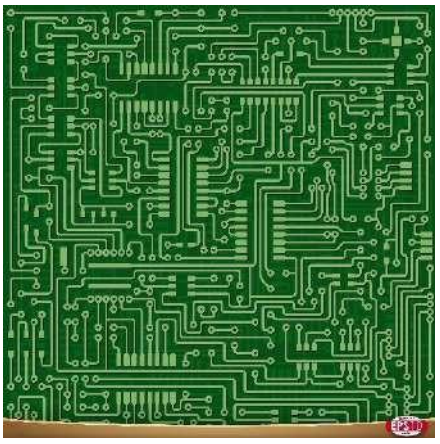


Fig. 1.1.13: PCB

The microprocessor boards can be classified as follows:

- **Arduino**

  It is an open source single-board microcontroller used for creating digital devices and interactive objects for controlling any device or functionality. Arduino processor boards are readily available as do it yourself (DIY) kits which add unique functionality to daily objects. They are loaded with digital and analog input/output (I/O) pins which interact with other boards or circuits. The processor board is coded in C and C++ programming language for pre-programmed functions. The following image shows an Arduino board:

Fig. 1.1.14: Arduino

- **Raspberry Pi**

  It is a small, single-board computer developed by Raspberry Pi Foundation to promote basic computer learning in developing countries. More than 15 million Raspberry Pi units have been sold so far since its introduction in February 2015. This microprocessor board has a Broadcom system on a chip (SoC) having an Advanced RISC Machine (ARM) compatible CPU and an on-board Graphics Processing Unit (GPU). Depending on the Raspberry Pi model, it can have single USB or four USB ports.

Raspberry Pi runs best on a Debian-based Linux operating system called Raspbian, but it can also run on Ubuntu MATE, Snappy Ubuntu Core and Windows 10 IoT Core. Other than this, the processor board can run third party application software such as AstroPrint, C/C++, Minecraft, RealVNC and Wolfram Language. The following image shows a Raspberry Pi:

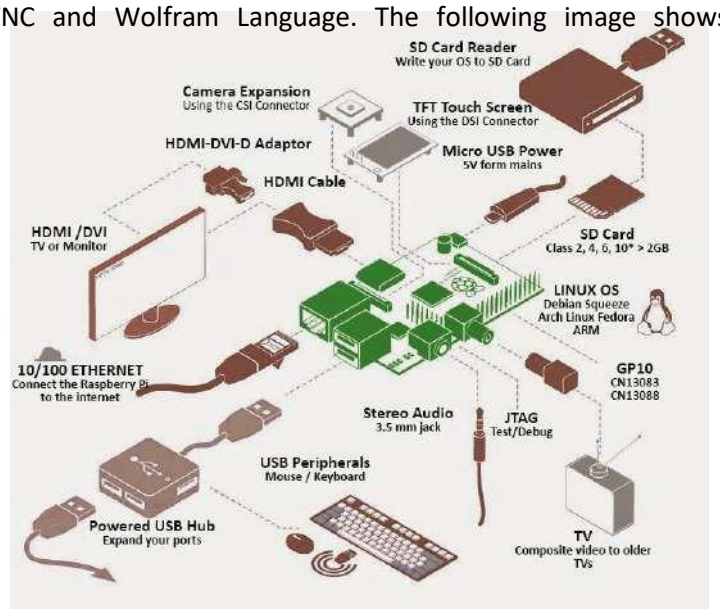


Fig. 1.1.15: Raspberry Pi

- **Customized Single Board Platform**

  A single board computer (SBC) comes handy for aready-to-use embedded platform, which reduces the time and the cost. Moreover, SBCs can be customized according to the need. The off-shelf solution has a Computer on Module (CoM) and carrier board. A user can scale the platform to accommodate hardware modules like processor, memory, RAM and so on. The following image shows a single board computer that includes memory, power requirements and real world multimedia and connectivity interfaces:

Fig. 1.1.16: Single board computer module

1.1.5 Framework for Internet of Things for Roadside Assistance Services

IoT has expanded its applicability in consumer market with avenues like Intelligent Transportation System (ITS) and Smart Cities. It is an integral part of connected road infrastructure and roadside assistance services. This comprises of technologically advanced features like lane detection, safety and emergency alerts for roads, assisting drivers and passengers in locating nearby fuel stations and emergency alert systems, courtesy the V2X communication and On-Board Unit (OBU). This will be the step forward for high-end roadside assistance services aided by Intelligent Transportation System and Internet of Things for building smart cities. The system can have an open interface and APIs so that third party developers can create their own custom roadside assistance applications.

The following image shows a traffic assistance system that senses if there is any blockage on the road and tells the car to move to another direction in such a case:

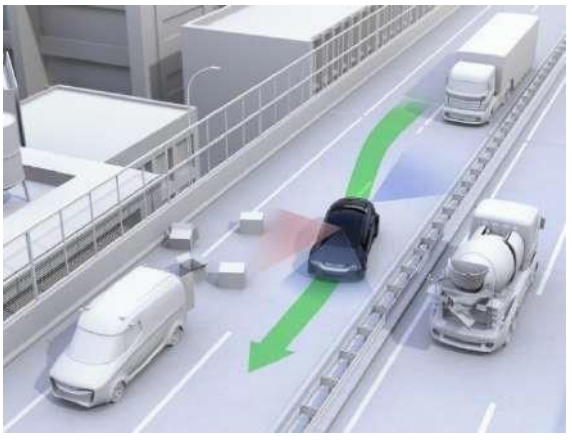


Fig. 1.1.17: Traffic assistance system

Advantages of IoT for roadside assistance are as follows:

- Improved safety for vehicles and drivers with remotely controlled vehicle diagnostics to prevent road mishaps occurring due to driver fatigue, driving error or natural disasters
- Easy access for towing, repair or gasoline supply
- Increased reliability aided by performance tracking system which notifies maintenance issues
- Relevant information pertaining to weather, gasoline stations, rest stops, hotels and restaurants

Exercise

1. List any two applications of IoT used by people in their daily lives.

2. List two differences between a microprocessor and a microcontroller.

Microprocessor	Microcontroller

3. Describe one example each of use of IoT in healthcare industry and in enterprise.

Healthcare Industry:

Enterprise:

UNIT 1.2: Functioning of Sensors and Actuators

Unit Objectives

At the end of this unit, you will be able to:

1. List various types of sensors
2. Identify the importance of actuators
3. Explain the basic programming of a microcontroller board

1.2.1 Sensors and their Usage

With the advent of IoT, the importance of sensor-based devices and their usage has increased by three folds. Sensors are small devices which detect electrical or optical input, and then convert it into a physical value; for example, temperature, humidity and altitude. A sensor can be classified based on accuracy, environmental condition, measurement range, calibration and cost.

By combining the data collected through various sensors and their usage, smart autonomous or semi-autonomous functionalityis made possible. Sensorscan also be combined and synced with each other to provide unique functionality, which was earlier not possible. For IoT applications, sensors have a wide range of usage right from the agricultural sector to the healthcare industry.

Different Types of Sensors

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

- **Temperature Sensors:** Earlier temperature sensors were only used for sensing current temperature in appliances. For example, they were used in air conditioners and refrigerators to detect accurate temperature. But with IoT coming to the fore, temperature sensors are now being used in virtually every industry and application. These sensors dynamically measure the slightest of changes in temperature for accurate measurement.

  Usage: 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 temperature in the houses.

  Connectivity Options: These sensors may have in build power supply through small cells or through a power source depending upon its type of build.

The following image shows repairing of the temperature sensor of a heating and cooling thermostat:

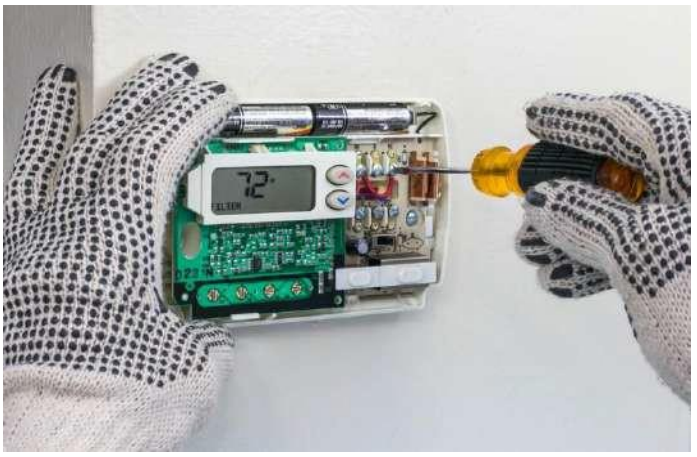


Fig. 1.2.1: Temperature sensor in a heating and cooling thermostat

- **Proximity Sensors:** This is a sensor which can detect an object within its range by the latter's movement. This is done by directing an electromagnetic field or electromagnetic radiation, and then reading the changes in the return signal. Due to the lack of any mechanical parts, proximity sensors have a longer life. Such sensors are used in mobile devices, autonomous vehicles or home monitoring gadgets to detect the presence of a targeted object.

  Usage: Proximity sensors are used in garage doors to open and close the door when a car is nearby. They are also used future cars which will be able to detect nearby cars in traffic.

  Connectivity Options: These sensors are basically very small in built. So, they usually require batteries for power supply. They can then be connected to devices to provide information about any movement or to motors and actuators to perform mechanical operation.

  For example, proximity sensors are used in mobile phones systems to detect the presence of a human ear. This helps in disabling the touch screen to avoid the unintentional touches by the cheek. These sensors are mounted on car bumpers to sense the distance of nearby cars while parking. The following figure shows the sensors in a car detecting a truck nearby:

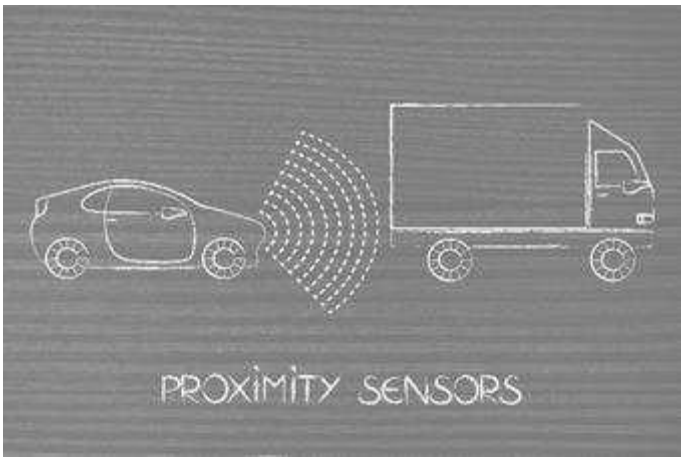


Fig. 1.2.2: Proximity sensor in a car

- **Pressure Sensors:** These are used to detect the pressure level of gases or liquids; pressure sensors make the measurement in force per unit area. Such sensors are used for monitoring applications, and they can also be used to measure material flow, speed and altitude. The detected pressure level is converted into analog electrical signal; therefore, pressure sensors are also known as pressure transducers.

  Such sensors are used in manufacturing, aviation, automotive and hydraulic measurement applications. A common example is the touchscreen of smartphone which has pressure sensors in the display that responds to the slightest of pressure with a finger or stylus. Another example is the pressure sensors used in car engine which regulates the amount of power needed, corresponding to the accelerator input.

  Usage: Pressure sensors are used in industries where pressure is involved in warning a system of non-suitable conditions.

  Connectivity Options: Pressure sensors are connected to the part where pressure needs to be checked. The power to these sensors is given either by small batteries or by electrical power sources depending upon the type of the sensor and its size.

  For example, the air pressure on the tyre of a car is measured with a pressure gauge that has a pressure sensor in it.

  The following image shows measuring the air pressure of a tyre using a sensor:

Fig. 1.2.3: Measuring the air pressure of tyre using pressure sensor

- **Accelerometer Sensors:** These are dynamic sensors which can measure the rate of change of velocity of an object using Micro-Electro-Mechanical Sensors (MEMS). Such sensors are used for measuring vibrations in machines or sensing the change of speed in moving objects. Accelerometer measures the change in velocity in one, two or three axes. The communication interface of accelerometer sensors can be in either analog, digital or pulse-width modulated.

  Usage: The accelerometer sensor is used in cars and machine parts to check acceleration and to warn in case of unsuitable acceleration conditions. The sensor can be installed in a system which detects velocity, vibration, position or the acceleration of gravity to determine the device's orientation.

  Connectivity Options: The accelerometers are connected to the moving parts and are powered either by small batteries or direct electric sources based on the type and the size of the sensor module.

  - **Analog Interface** – Measures acceleration by detecting varying voltage levels
  - **Digital Interface** – Communicates over SPI or I2C protocols and are less prone to noise
  - **Pulse Width Modulated**– The output data is over pulse-width modulation

For example, the sensors in the smartphones help to rotate their display depending on how the phone is tilted. The following image shows the changing of the display orientation of a smartphone:

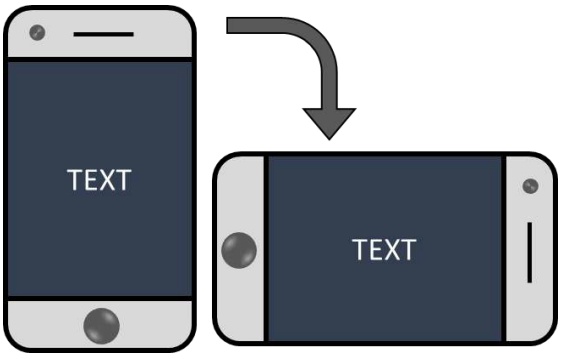


Fig. 1.2.4: Changing the display orientation of a smartphone

- **Gyroscope Sensors:** Working in combination with the accelerometer sensors, the gyroscope sensors additionally measure the angular rotation velocity or twisting motion along with the velocity change measured by accelerometer. The sensor is used in robotics or autonomous navigation systems to measure the deviation in balanced position movement to correct the movement. Gyro sensor can be either in digital or analog interface.

  Usage: The gyroscopic sensor is used in virtual reality glasses and modern self-balancing scooters or hover boards.

  Connectivity Options: These sensors are connected to the actuators and motors which work upon the signals given by these sensors. These sensors are powered either by small batteries or by an electric connection depending upon the size of the sensor module.

  For example, gyroscope sensors allow mobile applications to trigger an event based on a set of motions by the user such as shaking the phone to lock the screen, autorotation of the display and so on. The following image shows gyroscope sensor implemented in a self-balancing scooter:

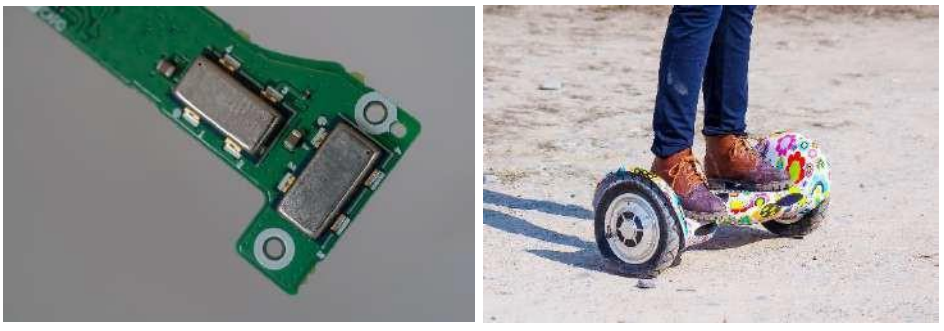


Fig. 1.2.5: Gyroscope sensor and a self-balancing scooter

- **Humidity Sensors:** A humidity sensor, also known as hygrometer, measures the moisture level in the environment. It measures relative humidity which is the ratio of water content in air to the maximum moisture content that can be sustained at a particular air temperature. This is done by measuring the changes in temperature or electrical current.

  Usage: These sensors are used in refrigerators and air conditioner units basically to maintain the humidity in the area.

Connectivity Options: These are connected to the thermostats to change the temperature based on the input obtained and to maintain the humidity content in the atmosphere. These are connected either by an electric power supply or with small batteries as per the size and design of sensor modules.

The following image shows a device with a humidity sensor installed in it, and the display of the device showing the temperature and the humidity level detected by the sensor:

Fig. 1.2.6: Humidity sensor device

- **Touch Sensors:** A touch sensor is a sensitive equipment that registers physical touch on a device to provide the relevant action. Such sensors are used in mobile devices, home appliances and other commercial equipment to initiate a particular action. A touch sensor works with a controller and software to provide the needed input/action.

  Usage: These sensors are nowadays used broadly in security systems and locks such as those used in office premises and mobile phones.

  Connectivity Options: The touch sensors are very low energy based modules. Thus, they can be powered by a small battery and a low direct current (DC) voltage supply.

  For example, the employees of a firm need to check in on the biometric device installed at the door to enter into the office. The touch sensor installed in the device senses any touch and generates a signal. The following figure shows working of a touch sensor:

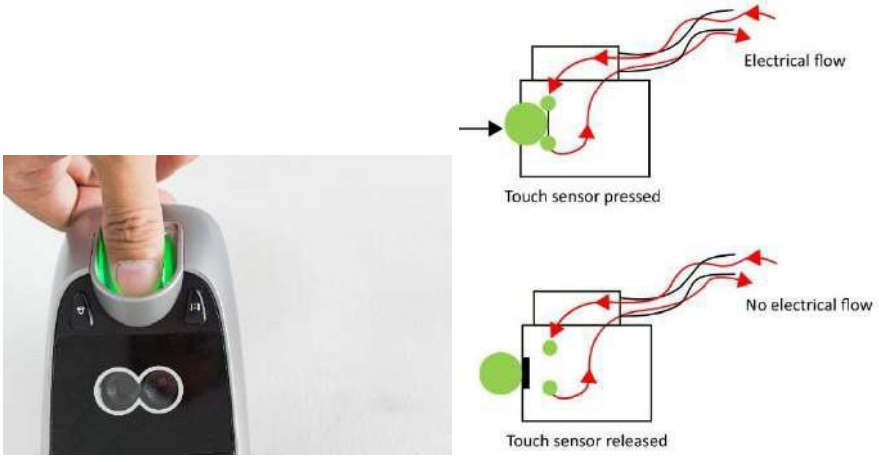


Fig. 1.2.7: Touch sensor in a door lock and its working

- **Reed Sensor:** This is an electromagnetic switch made from ferrous reeds which controls the electricity flow in a circuit. The reeds are placed in a small glass tube and are magnetized, which results in movement towards the switch. When these reeds are in contact, electricity flows in the circuit. There is no mechanical wear in such sensors as no physical pressure is applied.

  Usage: These sensors are used in smart voltage controlling stabilizers for controlling the voltage fluctuation in the power supply.

  Connectivity Options: These are connected to the actuators which changes the voltage fluctuation in the modules. They are directly connected to power sources so they just require low DC supply for operation.
- **Analog Sensors:** Sensors that produce continuous analog output signal are known as analog sensors. Signals produced by these sensors are measured proportionally. There are various types of analog sensors. Accelerometers, pressure sensors, light sensors, sound sensors and temperature sensors are some good examples.
- **Digital Sensors:** Sensors in which data conversion and transmission takes place digitally are called digital sensors. The digital sensor majorly comprises three components: senor, cable and transmitter. The signal measured is converted into digital signal output inside the digital sensor itself. The cable transmits this digital data digitally. There are different types of digital sensors. Digital accelerometer and digital temperature sensor are a few good examples.

1.2.2 Actuators

For IoT applications, accuracy of data is of utmost importance, and actuators with sensors make sure of that.

Actuator: As the name suggests, an actuator is a device which actuates the movement by converting energy into motion. Typically, a sensor provides the input for the actuator to perform the required movement. There is a coupling mechanism which is the interface between the actuator and the mechanical system that performs the movement. Actuators can be of four major types – hydraulic, pneumatic, electric and mechanical.

Example: Actuators are attached to sensors like in a door lock with a finger print scanner. As the scanner confirms the finger print, the actuator releases the magnetic force holding the door to allow the door to open. The following image shows PCB integrated sliding switch actuators that are installed in door lock systems; when the actuator gets a signal to open the door, its switch is slid and the door gets opened:

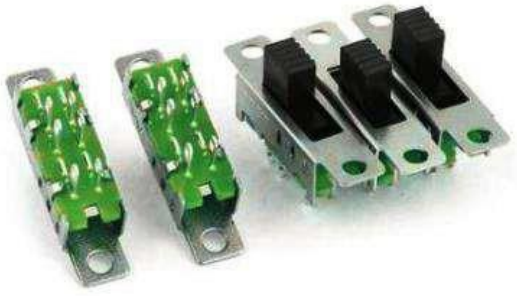


Fig. 1.2.8: PCB integrated sliding switch actuator

How Sensors Work with Actuators?

Sensors and actuators work in tandem to produce the intended output to solve a functionality.

For example, in an appliance such as a beer dispenser, the sensors detect the amount of beer flowing through the keg by detecting the electrical impulses from the hardware installed. The electrical signals are relayed to a computer which then translates those signals into an input for the actuators. Then, the actuator performs the necessary action, that is, to determine the amount of beer that should flow into the glass without any spillage.

Basically, sensors accumulate all the data with the help of the sensing hardware. Thereafter, it works as an input for the actuators to perform the mechanical action by moving or controlling the mechanism. A simple example is closing or opening of a valve by the actuator which regulates water flow/level in a dam model. The data provided by the sensors measures the level of water in the reservoir and the time interval when these valves need to be opened or closed. The following image shows a water flow system with a pressure sensor and an actuator installed in it:

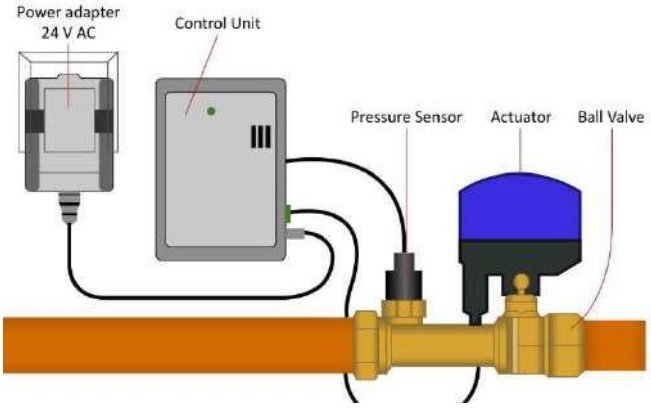


Fig. 1.2.9: A water flow system

1.2.3 Importance of Accurate Sensors

The accuracy of sensors is very important to get correct input for the actuators so that the intended function is performed precisely. The accuracy of any sensor is defined as the maximum deviation of the intended value (under certain set of conditions) at the output of the sensor. To be precise, it is the difference between the real-time value and the indicated value, taking into consideration all the errors that can occur in real -life situation. The representation of actuator's accuracy can be defined in either a percentage or a full-scale representation.

Sensor Calibration

The method by which sensor errors are eliminated by performing structural error removal (difference between expected and measured output) in the output is known as calibration. This improves the overall efficiency of the system as accuracy of the sensors is optimized to its maximum. No sensor can be 100% accurate, but eliminating all possible errors to the maximum yields good output.

Calibration process has a routine of placing Device under Test (DUT) in a configuration where inertial input stimulus of the sensor is known. This helps in understanding the actual error in measurement to perform the offset which will actuate the required output.

There are certain factors which can mar the accuracy of sensors, and for this reason calibration is very important. It minimizes errors and thereby ensures that the sensor produces the intended output.

Choosing the right sensors for a specified task is important as some of them come with auto calibration features for certain variables. For example, some sensors have temperature actuation capability.

Factors such as time and hardware degradation of the sensors also require calibration. This is a part of routine maintenance tasks which need to be performed accurately. Also, the installation phase of sensor is the most important. Improper installation can affect the sensor output, which in turn disturbs the whole system. For example, if pressure sensors are installed incorrectly, there can be a shift in the output calibration of the sensor.

1.2.4 Programming a Microcontroller Board

To make the PCB sensors work according to the desired function, they are programmed with various coding languages by the board developers. Different boards are supported and coded with different languages. The following table shows the difference in IoT development boards under various categories:

Board name	GPIO pins	Processor speed	Power supply	Programming	Connectivity
Arduino uno	6 analog, 14 digital	16 KHZ	9-12V DC, or 5V 500mA USB or 9 - 12 V on VIN pin	C language	By default none. Can be added with shields.
Raspberry Pi	40 I/O pins, including 29 digital	1.2 GHZ	5V 2.5A micro USB port	JAVA, Python	Wi-Fi, Ethernet, Bluetooth

Table 1.2.1 Difference in IoT development boards

Programming Basics

There are different languages in which the program can be written for the microcontroller boards. The language can be C, C++, Python and so on. The code is written on the related editor that comes with the board. For example, Arduino programming can be done on Arduino Sketch or Arduino IDE. 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 “Build Successful” 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.

For running a simple Python program, the following steps can be followed:

- Download and install Python IDE from the Python site and use it for compiling a code.
- Type 'python' in command prompt to call the interpreter as shown in the following image:

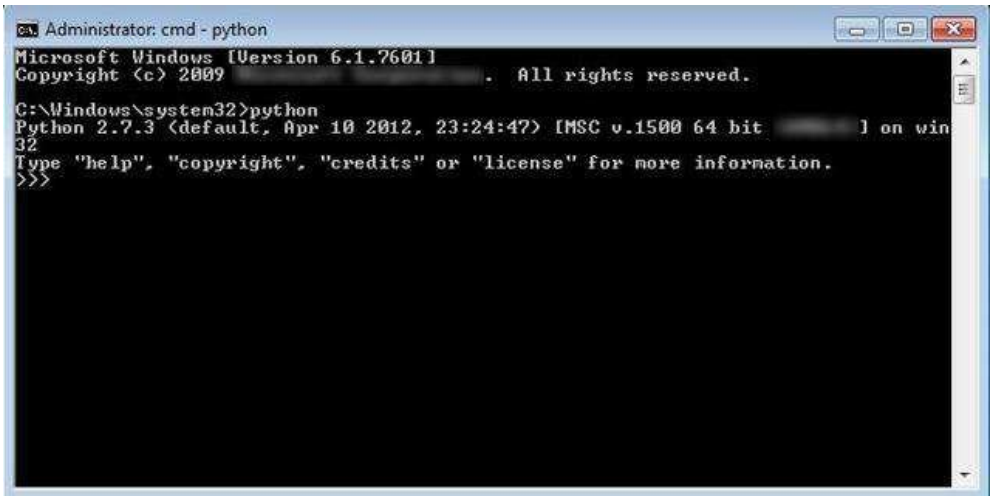


Fig. 1.2.10: Python interpreter

- To write a python script, 'gedit' command can be used.
- After writing the code, save it with the extension your_script_name.py
- To run this script, copy and paste the code in a file and save the file with the extension .py and the open command line in the directory of the script.
- Then, type:

  python your_script_name.py.

Exercise

1. Write the application/usage areas of the following sensors:

   a. Temperature Sensor _____

   _____

   b. Pressure Sensor _____

   _____

   c. Touch Sensor _____

   _____

   d. Accelerometer Sensor _____

   _____

   e. Proximity Sensor _____

   _____

2. Write the differences between accelerometer sensor, proximity sensor and gyroscope sensor.

Accelerometer Sensor	Proximity Sensor	Gyroscope Sensor

UNIT 1.3: Application of Communication Protocol in Internet of Things

Unit Objectives

At the end of this unit, you will be able to:

1. List various short-range wireless communications systems
2. Identify the protocols used for communication in IoT
3. Compare different communication technologies

1.3.1 Short-range Communications Systems and their Typical Operating Ranges

Short-range communication is a wireless communication system in which signals traverse from a short range of few millimetres to several meters. The term wireless is defined as the technology used in communication or transmission of information over a distance from one end to the other end between electronic devices without requiring wires, cables or any other electrical medium. Today, wireless communication is one of the most used, and hence is an important means of data/information transfer to other devices. The communication is established, and the information is sent through air, using electromagnetic waves; such as radio frequencies and infrared in a wireless communication network.

On the other hand, signals in long-range wireless communication travel from a few kilometres to several thousand kilometres. Some good examples of short-range wireless communications are Bluetooth, Infrared, Near Field Communication (NFC), ZigBee, Wi-Fi and so on.

The following figure shows various short-range communications technologies and their typical operating ranges:

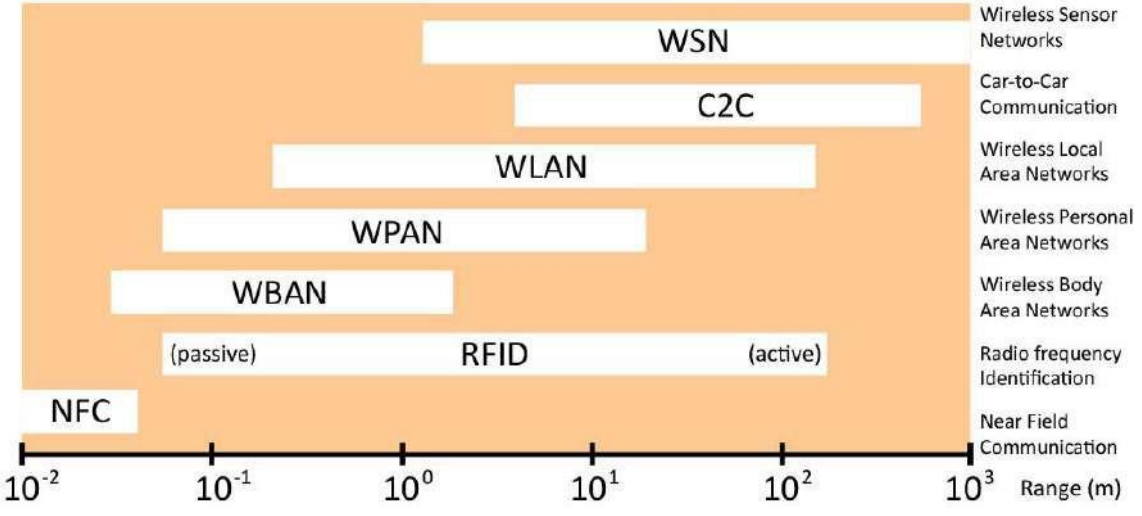


Fig. 1.3.1: Short-range communications technologies and their typical operating ranges

Various Types of Short- range Communications

As discussed before, short range communication refers to communication between two wireless channels/devices located at a distance. Short-range communications are developed with the advancement of technology to facilitate ease of use and safety. These advancements have opened new avenues for innovations in electronics industry, allowing various devices to connect and interact with each other without requiring any cables or wires for the purpose of easy accessibility, data transfer and much more. One of them is the IoT, which is defined as the concept of connecting devices to the Internet. Consumer electronic devices such as refrigerators and televisions are getting connected to the Internet. The mechanisms by virtue of which these devices can get a wireless connectivity to the internet are as follows:

1. **Direct:** with the help of built-in modem
2. **Indirect:** with built-in wireless module connected to an access point

Indirect mechanism has big relevance to IoT as this involves short-range wireless communications. The types of short range wireless technologies that are currently in use for connecting devices to the Internet are as follows:

- Wi-Fi
- Thread
- ZigBee
- Bluetooth
- RFID and NFC

For example, the NFC technology used in mobile communication allows a user to pay for goods by waving the mobile phone on the payment device instead of swiping a card. The following image shows using NFC technology for doing transaction between devices:

Fig. 1.3.2: NFC technology for transaction through a mobile phone

Short-range Communication Architecture

In the past five years, right from its infancy stage, IoT has rapidly emerged and developed as a web of Internet-connected devices to such an extent that many desperate measures have been taken to establish standards. Some of them are being governed by independent standard bodies while others are developed by a single company, and some are in wide use and accepted worldwide while others are in their early adoption stage.

The purpose behind their origin was to address specific requirements like wireless connectivity, range, power consumption, scalability and so on. These components constitute one part of IoT wireless communication network.

Firstly, it is important to understand the communication network architecture needed for the IoT application that further defines its compatibility with existing technology standards. The communication network architecture in IoT are basically of three types as follows:

1. Point-to-point
2. Star
3. Mesh

Point-to-Point

Point-to-point network in short range communication system is defined as a direct connection or communication between two network nodes or devices, that is, communication takes place only between two devices. A cell phone connected to an ear piece through a Bluetooth link is the best example of point-to-point network. This type of networking comes with its own highs and lows. For instance, ease of use and setup as well as low cost are the biggest advantages, while zero scope for scalability beyond two devices is the biggest disadvantage because the connection exists as one-to-one relationship between the two devices. One device acts as the master device while the other one acts as the slave.

Star Network

As the name suggests, this network architecture mainly consists of a central device called hub to which all other nodes or devices are linked, forming a star-like shape. The hub acts like a mother ship which is home to all other nodes/devices in the network. This way, communication happens between the hub and the nodes in the form of reception at the nodes' end and transmission from the central hub.

Mesh Network

This network comprises three types of nodes which are as follows:

- A hub for transmission
- Sensor nodes
- Sensor nodes with repeater/routing ability

Mesh network is quite similar to a combination of point-to-point and star networks where nodes are arranged in a way that every node is within transmission range of at least one other sensor/router node. Transmission happens through multiple sensor/routers nodes to reach the hub. This array is generally used for a long range and broad area coverage of applications such as home automation, energy management, industrial automation and so on.

The following figure shows the different types of short-range communication architecture:

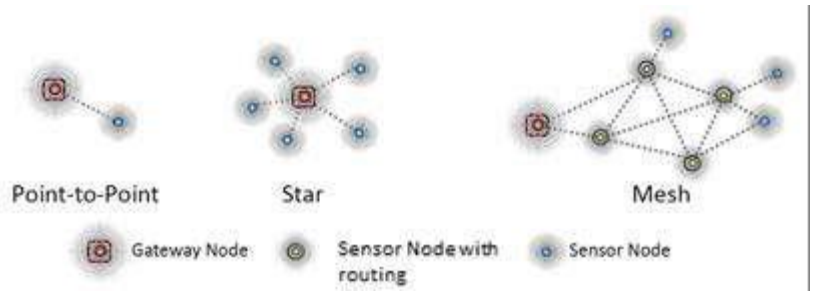


Fig. 1.3.3: Types of short-range communication architecture

1.3.2 Data Transfer Types and Protocols in Internet of Things

IoT is the new trend in home automation that enables the home appliance, be it a refrigerator, an oven or a dishwasher, to connect with the Internet. This new fad has given rise to a complex network of IoT devices where a huge amount of data is being churned out every second by multiple devices. This leads to challenges like monitoring data flow through the system, retrieving and capturing the data real time or in sets, and last but not least, analysing the collected data for future use. The data is created and collected in three steps. The first step involves creation of data on the device and transferal over the Internet. The second step involves collection and categorization of the data by the central system. The third step is about analysing the data for future use.

The information/data collected by each connected device and sensor is sent back to the central application over the network. For transferring this data back, the most common standard protocols are used.

Technicians have a range of connectivity technologies to choose from for (IoT) applications. The choice may vary according to preferences like range, speed, data requirements, security, battery life and so on. The choices need to be made well in advance so that the technologies and the tools used are right and most suited for the application. Some of the most popular in the bunch are as follows:

- **WI-FI:** WI-FI is a short-range communication system that uses radio waves to enable two devices to communicate and transfer data with each another. It is used to connect Internet routers to devices like computers, tablets and phones. Wi-Fi is often an obvious choice for technicians because of its widespread use and popularity within the home environment and as well as outdoors. It enables fast data transfer rate as well as the ability to handle high volumes.

Presently, the most common Wi-Fi standard used in homes and businesses is 802.11n that offers high throughput. It is appropriate for file transfers but high power-consuming for IoT applications. The following image shows full strength Wi-Fi in a mobile phone:

Fig. 1.3.4: A mobile phone connected to full strength Wi-Fi

- **Thread**: It is a new IP-based networking system developed for the purpose of home automation. It is based on various standards like IEEE802.15.4, IPv6 and 6LoWPAN, and is slightly different IoT applications protocol from Bluetooth. It is designed to complement Wi-Fi as it is less power consuming.
- **ZigBee:** ZigBee is the latest wireless technology in the Low-Power Wide-Area Network (LPWAN) segment that is specifically designed for mobile to mobile (M2M) networks. Low running cost and low power requirements are some of the biggest advantages that make it an ideal solution for IoT applications. The communication system has a low latency and low duty cycle, allowing maximum battery life in devices. It offers data exchanges at low data-rates within a range of 100m, making it ideal for home or building use.
- **Bluetooth:** Bluetooth is a short range wireless communication system which is used to transfer data at high speeds using radio waves. This communication system requires proximity of 10 meters or less between two devices to achieve a data transfer rate of about 2 Mbps. The frequency band in which Bluetooth signals operate is 2.45 GHz.

  The following image shows that a head phone is connected to the mobile phone via Bluetooth:

Fig. 1.3.5: Bluetooth headphone connected to mobile phone

- **RFID and NFC:** RFID refers to a communication technology in which digital data encoded in the RFID tag is identified by a device via radio waves. RFID bears similarity with barcoding in which data is collected through a device from a tag and stored in a database. However, there are some distinctions that differentiate RFID from barcode, like one can read RFID tag data outside the line-of-sight, which is not possible in case of barcode. For example, RFID technology is used in retail sector.

  The following image shows a device detecting the RFID tags after the button is clicked:

Fig. 1.3.6: RFID technology in retail sector

NFC, as the names implies, is a communication technology that enables two or more electronic devices, like smartphones, to interact with each other and perform simple, safe, contactless data transfers, transactions and data access. Performing at data range of 100-420kbps, the communication technology enables two or more devices to share information at a distance of 10 cm or less. The NFC technology has automated gate check-ins. For example, within an NFC-enabled departmental store, if the NFC mode in the mobile phone is on, it will offer the user the default card for payment option after verification. The users have to authenticate the purchase by means of a Touch ID or a passcode, for sending the payment information.

The following image shows an NFC field being detected by a mobile phone:

Fig. 1.3.7: NFC technology with automated gate check-ins

The following table lists the characteristics of different wireless technologies and their applications:

Technology	Band	Range (in m)	Standard	Power	Data Rate	IoT Applications
Wi-Fi	2.4 / 5 GHz	Medium 50	802.11b/ g/n/ac	High	High 500Mbps -1Gbps	• IP camera • devices
Bluetooth	2.4 GHz	Medium 50-150	Bluetooth 4.x specification	Medium/ Low	Medium 1Mbps	• Wearable devices • Sensors' nodes connection
Sub GHz	868 MHz / 915MHz	High	802.15.4 6LowPAN	Low	Low 500kbps	• Smart street light • Energy meters
NFC	13.56 MHz	Low 0.10	ISO/IEC 18000-3	Low	Low 100– 420kbps	• Access management • Payment
Zigbee	2.4GHz	10-100	802.15.4	Low	Low 250kbps	• Smart street light • Smart building

Table 1.3.1 Difference types of wireless technologies

1.3.3 Multiprotocol Readers and Sensors in Internet of Things

IoT, also known as "smart everything," is all about wireless communication and embedded sensors. The wireless protocols, the IoT follows have many common traits. Multiprotocol sensors that are used to connect the systems simplify the wireless designs. Simplification of the architecture or the circuit design is important because in the present era one will find multiple wireless devices in a single building, be it home, office, hotel or shopping mall. A decade ago, the scenario was very different; it was limited to a single protocol, like Wi-Fi.

The following figure shows a multiprotocol IoT environment:

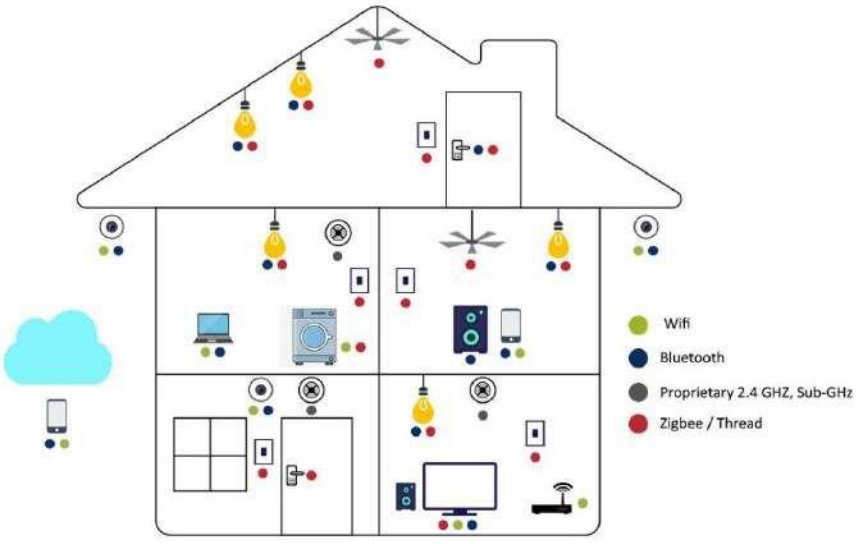
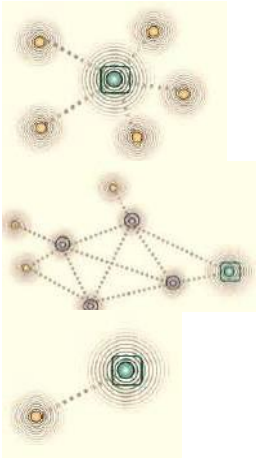


Fig. 1.3.8: Today's multiprotocol IoT environment

Today, things have changed, and they are further changing very fast. In today's world, it is hard to imagine a home without Wi-Fi and Bluetooth-enabled devices in a multiprotocol IoT environment. More the technical advancements, higher the expectations – this is where latest technological advancements have landed the humanity. A user wants to control the lighting and home appliances with a single button, which has given birth to smart hubs. The technology is desired to keep a tab on burglary, theft, smoke and fire when not at home. With the arrival of multiprotocol technology, deployment of new wireless sensors in IoT has made this possible. This is a combination of hardware and software to facilitate support for multiple wireless protocols (Bluetooth, ZigBee and so on) on a single device. IoT infrastructure is built on legacy systems; the devices are made in a way that adding 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.

Exercise

1. Match the following.



Point-to-Point

Star

Mesh

2. List some differences between RFID and NFC.

RFID	NFC

3. Write the data rates and bands available for the technologies given in the table.

	Band	Data Rate
Wi-Fi		
Bluetooth		
NFC		
ZigBee		

UNIT 1.4: Micro-controller Boards, PIN Configurations and Their Interconnectivity

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the components of a microcontroller board
2. Describe the layout of various development board

1.4.1 Microcontroller

Microcontrollers are the heart of any IoT device as they are small, require less power and perform the required function just like any other high-end microprocessor. In current times, the lines between a microcontroller and a microprocessor have become blurred as more processing power and the ability to integrate all the peripherals has given microcontrollers more power and versatility in their function. For IoT applications, a microcontroller is preferred because most of the on-board pins are programmable by the user and the components can be integrated on a single board, which reduces the size of whole computing unit. The following image shows a microcontroller:

Fig. 1.4.1: Microcontroller

1.4.2 Components of Microcontroller

The basic components of microcontroller can be classified as follows:

Power USB

It is also known as retail USB/USB Plus Power/ USB + Power. The power USB port is used for high power devices to derive power from the USB alone, eliminating the need for a separate power unit. The following image shows a power USB attached to a device:

Fig. 1.4.2: A power USB attached to a device

Voltage Regulator

To provide a stable AC or DC voltage to a microcontroller, a voltage regulator comes handy. Regardless of the input voltage, the voltage regulator provides a fixed output to prevent any short circuits. This electronic circuit uses electromechanical mechanism or electronic components to do this. Every voltage regulator has two types of goals, primary and secondary. The following image shows a voltage regulator:

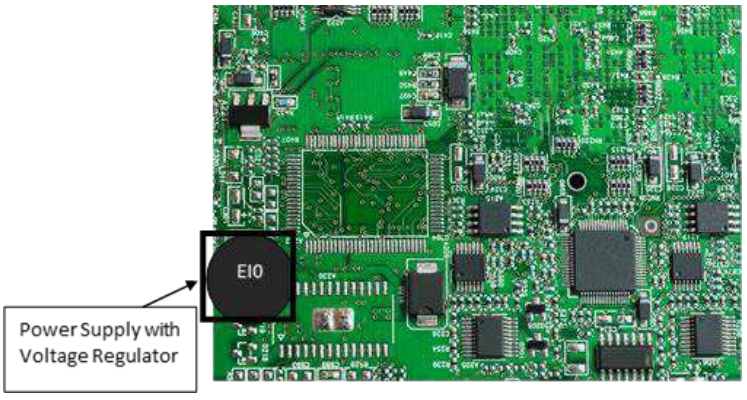
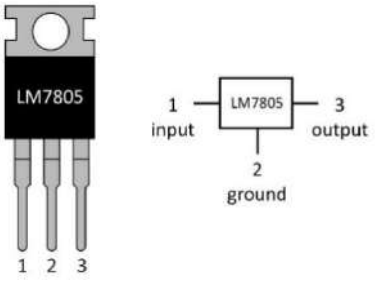


Fig. 1.4.3: Voltage regulator

Pin configuration for a 7805-voltage regulator IC are as shown in the following figure:



Pin No	Function	Name
1	Input voltage (5V-18V)	Input
2	Ground (0V)	Ground
3	Regulated output; 5V (4.8V-5.2V)	Output

Fig 1.4.4: 7805 *Voltage regulator IC pin configuration*

Linear Voltage Regulators

For designing low-cost and low-power applications, a linear voltage regulator is used to divide the voltage on the circuit by toggling the effective series resistance. Mostly 3-pin linear voltage regulators like LM7805 are used for this purpose as they provide 5 volt 1-amp output with a varying input of up to 36 volts.

The only disadvantage of linear voltage regulators is the considerable voltage drop of 2.0 volts. This makes the regulator dissipate a lot of energy which makes it less efficient. For example, if 10 volts input is regulated to 5 volts then 5 watts of energy is dissipated. In a way, it acts as a resistor for voltage stabilization, wasting a lot of energy. Therefore, it is not recommended for IoT devices that require low power consumption.

Switching Voltage Regulator

For high efficiency IoT devices that have a stark difference between the input and the output voltage, switching voltage regulators are preferred as they are highly efficient. In fact, they are almost 85% or more efficient than linear voltage regulators. Such voltage regulators use a controlled switch to toggle the output voltage by storing and then feeding it to the circuit depending on the input voltage. The charge levels of switching regulators are kept in check with the help of transistors which turn on when energy is required. Also, they don't require any heat sink to dissipate energy.

One disadvantage of switching voltage regulators is that they are noisy due to the constant switching, and this switching also makes them change from conductive to non-conductive stage, reducing the conversion efficiency. Also, they require more components on-board, thereby increasing the overall cost of the project.

Crystal Oscillator

This is an electronic oscillator which creates electric voltage signals by utilizing the mechanical resonance produced by the vibration of piezoelectric quartz crystals. For IoT devices using a microcontroller, the crystal oscillator creates an electrical signal at a frequency which helps in keeping track of time. This is vital for microcontroller functions that are triggered after a set interval of time. The following figure shows a crystal oscillator:

Fig. 1.4.5: Crystal oscillator

Arduino Reset

Arduino reset is required to reset the values of Arduino board to their inherent values. This is useful when coding a new program function. Although Arduino comes with its own reset button, but the user can also have an external Arduino reset button, so that it can be reset externally.

Arduino Pins GND, Vin

The Arduino microcontroller has several pins which are labelled and used for varied functions. These are as follows:

- GND Pin – This is the "Ground pin" which is used to ground the circuit
- 5V & 3.3V Pin – This indicates the 5 volt or 3.3 volt pin present on the Arduino board
- VIN Pin – Mostly a 9 volt pin, it acts as a conductor of input voltage directly via the power jack.

The following image shows Arduino pins:

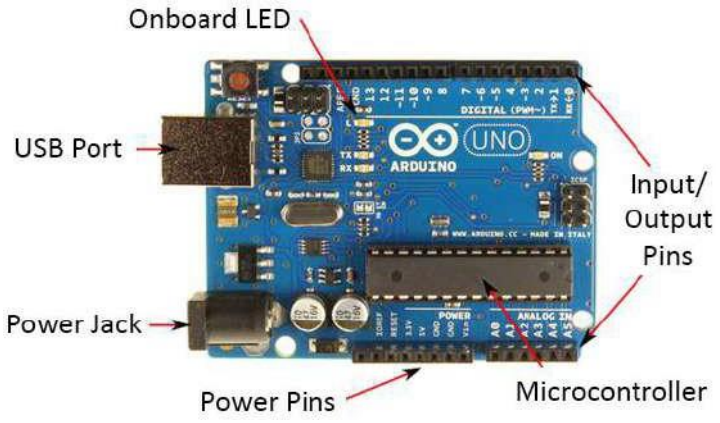


Fig. 1.4.6: Arduino pins

Analog Pins

Analog pins are used in a circuit to input the voltage which can range from 0V – 5V. The Analog pin on the Arduino can also be used as a digital output if needed.

Main Microcontroller

The main microcontroller on a microprocessor board is used to perform all the complex functions of an IoT device. Generally, it is embedded along with the microprocessor.

ICSP Pin

In Circuit Serial Programming (ICSP) pin also known as Serial Peripheral Interface (SPI) is an AVR tiny programming header used for Arduino. It is an expansion of output where output device is slated to the master of SPI bus.

Power LED Indicator

The power LED indicator denotes the power supply in the microcontroller device. Current generation 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 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

The orange/yellow coloured 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.

The following image shows an Arduino power LED indicator:

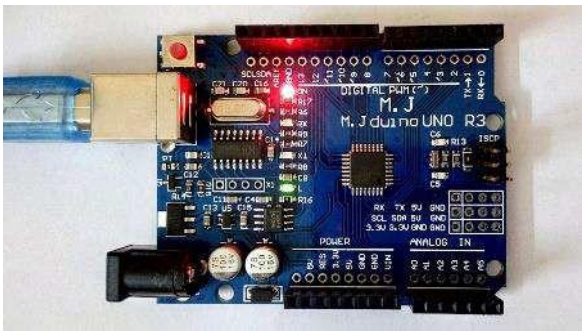


Fig. 1.4.7: Arduino power LED indicator

Digital I/O

Digital I/O interface board is used to input or output digital signals in an electronic circuit board. This enables the microcontroller to keep a tab on the current status of measuring devices and the relays or operation switches integrated on a control circuit.

Analogue 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 3.3V is directed to the AREF pin.

Raspberry Pi Development Board

It is a single board computer developed by Raspberry Pi foundation to promote basic computer learning in developing countries and for students in primary schools. A Raspberry Pi can have a speed in the range of 700 MHz – 1.2 GHz, RAM ranging from 256 MB – 1 GB and processor which has evolved from Broadcom BCM2835 SoC to the latest generation Broadcom BCM2837 SoC having 1.2 GHz 64-bit quad-core ARM Cortex-A53 processor. The single board computing unit can be easily operated with a USB keyboard and a mouse.

The following image shows a Raspberry Pi and Broadcom BCM2837 SoC:

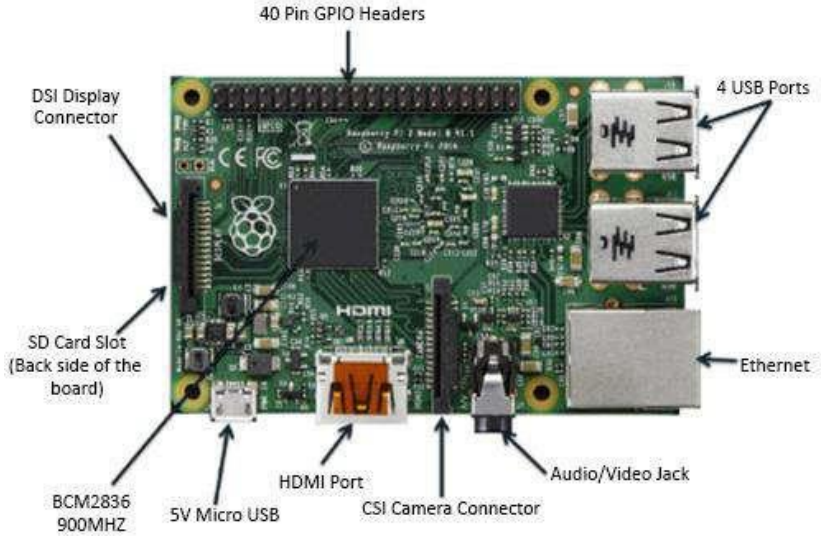


Fig. 1.4.8: Raspberry Pi

BeagleBone Black Development Board

Developed by Texas Instruments in collaboration with Digi-Key, this is an open source single-board computer which uses low-power. The main motive behind its development is to promote the learning of open source hardware and software in educational institutes. Beagle Board has dimensions 75x75 mm, making it a suitable tiny computer for various applications of IoT.

It runs on Linux OS (such as Debian, Gentoo, Fedora), Windows Embedded CE and Android too. The board runs on 1GHz Sitara AM3358BZCZ100 processor along with 512MB DDR3L RAM. It also behaves as a standalone PC, since it has its own USB connector, audio jacks, NAND flash memory and power supply. The following image shows a Beagle Bone Black development board:

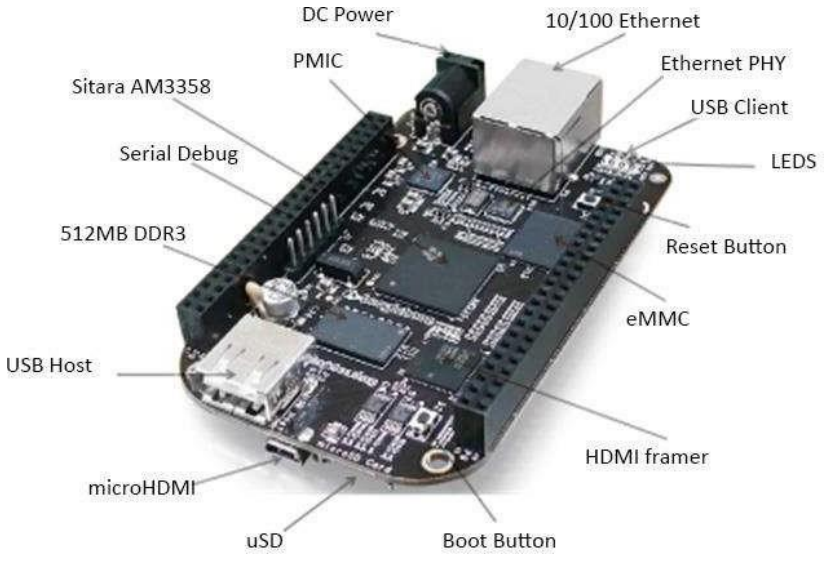


Fig. 1.4.9: BeagleBone Black development board

Adafruit FLORA Development Board

FLORA is a compact Arduino compatible microcontroller development board by Adafruit for wearables. It is designed to be sewed onto clothes and is circular in design, measuring 1.75" in diameter and weighing 4.4 grams. The board has built-in USB support which makes it easily programmable.

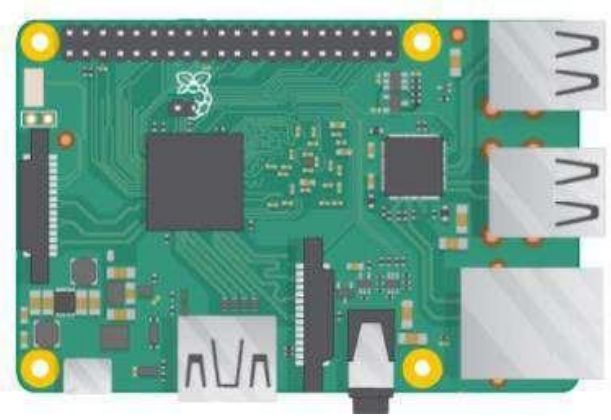
The following table shows a comparison between main types of microcontroller boards:

	Arduino Yun	**BeagleBone Black**	**Adafruit FLORA**	**Raspberry Pi**
CPU	MIPS32 24K and ATmega32U4	ARM Cortex-A8		ARM1176
Speed	400mhz (AR9331) and 16mhz (ATmega)	1ghz	8mhz	700mhz
Memory	64MB (AR9331) and 2.5KB (ATmega)	512MB	30 K	256MB (model A) or 512MB (model B)
GPU	None	PowerVR SGX530		Broadcom VideoCore IV
Internal Storage	16MB (AR9331) and 32KB (ATmega)	2GB (rev B) or 4GB (rev C)	5.25 bytes	None
External Storage	MicroSD (AR9331)	MicroSD	USB support	SD card
Networking	10/100Mbit Ethernet and 802.11b/g/n Wi-Fi	10/100Mbit Ethernet	USB	None (model A) or 10/100Mbit Ethernet (model B)
Power Source	5V from USB micro B connector, or header pin.	5V from USB mini B connector, 2.1mm jack, or header pin.	3.3V power regulator with 150mA output capability	5V from USB micro B connector, or header pin.
Dimensions	2.7in x 2.1in (68.6mm x 53.3mm)	3.4in x 2.1in (86.4mm x 53.3mm)	1.8 inch x 0.3 inch	3.4in x 2.2in (85.6mm x 56mm)

Table 1.4.1 Comparison between microcontroller boards

Exercise

1. Label all the parts of the Raspberry Pi board.



2. Label all the parts of the Arduino board.

3. State the use of a voltage regulator.

UNIT 1.5: Understanding Edge Devices

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the functions of edge devices
2. Identify the different types of edge devices

1.5.1 Introduction to Edge Devices

The edge device in a network is where the real action takes place. It mainly constitutes a wide range of sensors, actuators, and devices for automation in ways that ensure interoperability, extendibility, and scalability. In IoT network, controlling edge devices for creating a two-way tunnel for data sharing means the ability to configure and control any device from anywhere. The challenge is to simplify the complex system so that they behave as a single unit while interacting with each other and while communicating real-time data.

For example, different devices like smart pill boxes, heartbeat sensors, blood pressure sensors and weight scales are connected to a network via a router. The edge device acts as an entry or an exit point for the framework. The following figure shows the concept of an IoT edge device:

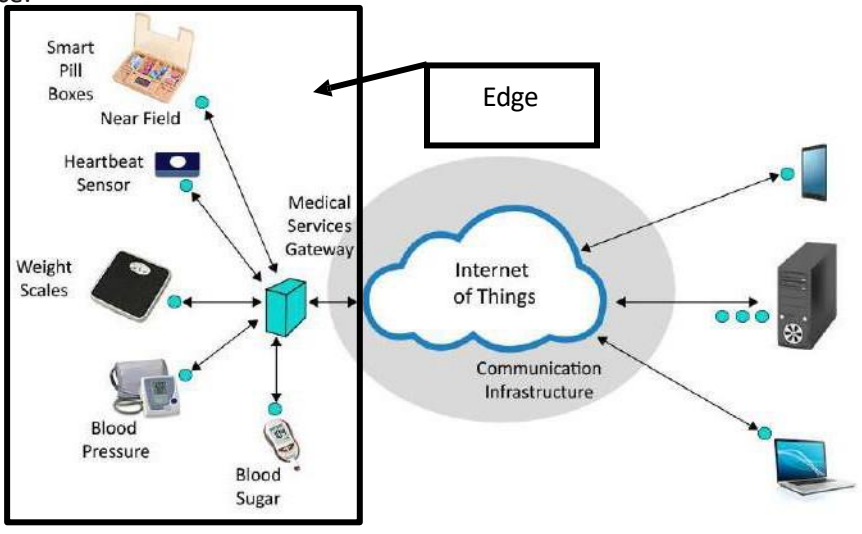


Fig. 1.5.1: IoT edge device

Before delving into the method of bypassing the hub, it is important to understand the definition and working of an edge device. These devices work on the edge (entry point or boundary) of a network to allow access into a network. Furthermore, an edge device is a device that provides an entry point into an enterprise's or a service provider's core networks. Routers, routing switches, multiplexers, metropolitan area network (MAN) and wide area network (WAN) are some good examples of edge devices that a communication technician can notice around him/her. Providing connections to the carrier's and the service provider's networks is another role of edge device.

Function of Edge Devices

Edge devices in most cases are routers for providing (authenticated) access to a core network. An edge router is a device located at the boundary of a network to enable an internal network to connect to external networks. They are mainly used at two points— the wide area network (WAN) and the Internet. They generally send or receive data directly to or from external networks, using static or dynamic routing capabilities by utilizing Ethernet over single or multimode fibre optics. In some cases, multiple isolated networks can be used with the help of edge routers to link them together rather than using a core router. Edge routers are hardware devices, but in some cases, their functions can be performed by a software.

The following figure shows the types of edge routers:

Subscriber edge router	• This type of router belongs to the enterprise network. It's configured to broadcast external Border Gateway Protocol (BGP) to the service provider's Autonomous Systems (AS).
Label edge router	• These routers assign labels to each packet of outgoing data or information based on what information the packet carries and sends them to the network. They are not internal routers that partition a given AS network into separate subnets.

Fig. 1.5.2: Types of edge routers

Multiplexer: Multiplexer, also known as MUX or MPX, is a device that has multiple inputs and a single line output by the application of a control signal. The select lines determine which input is connected to the output, and also to increase the amount of data that can be sent over a network within certain time. Multiplexers operate as a very fast acting multiple position rotary switches, which connecting or controlling multiple input lines called "channels", one at a time to the output. Edge devices act as an authentication link between devices and core networks.

The trend is to make them more and more intelligent, rendering core devices like modems and hubs fast. So edge routers often include Quality of Service (QoS) and multi-service functions to manage different types of traffic. They provide network translation between networks using different protocols. For example, an edge device will translate and transfer packets and cells in between an Ethernet and ATM network. The following image shows a multiplexer:

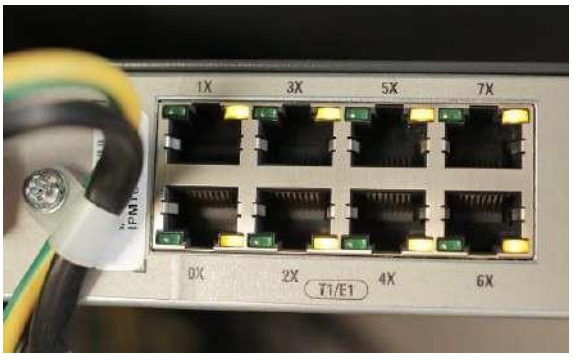


Fig. 1.5.3: Multiplexer

Click/Scan this QR code to view the video on edge devices

Routing Switch: In a network, a routing switch is a combination of a switch and a router. It is a device that combines the functions of a switch that forwards data by looking at a device address, and a router that forwards packets by locating the next hop address. The following image shows a network routing switch:

Fig. 1.5.4: Routing switch

Types of Edge Devices

In IoT, edge devices include a wide array of sensors, actuators and devices that interact with smart products and networks and communicate real-time data from one end to the other. The process of gathering data and communicating it in real time in a secure manner from one end to the other in the edge architecture involves key elements like sensors and actuators with 'read and write' capabilities. In most cases, these components are built into the smart product or environment. However, they can be added later as and when the need arises.

Sensors

As defined, the sensors are used to monitor any change in parameters to stimulate an action through the actuators.

Example: A water flow sensor is a good example of a sensor that measures liquid flow rate using a water rotor, whose speed changes depending on how fast the water is flowing. The signal output comes from a Hall Effect sensor, which pulses as the rotor turns.

Actuators

As already discussed, actuators are the ones which perform the action or any physical movement in response to the sensors' information. A valve that can be opened and closed or a light that can be turned on and off are some good examples of actuators. The followingimage shows an actuator motor:

Fig 1.5.5: An actuator motor

The following image shows some examples of an actuator:

Lights

Valves

Motors

Fig. 1.5.6: Examples of actuator

Example: 6000 series indexing valve from K-Rainis a distribution valve that is used in high-flow city water and wastewater applications. The valve can be coupled in an IoT network with an intelligent valve monitor to ensure even water distribution and to alert operators about potential errors. Also, in access-controlled security system, the doors automatically open as the actuators get information of authorised access through sensors. In a security surveillance system, the motors in the cameras keep rotating the camera around its axis to cover the entire area.

Local Area Network (LAN) Edge: In the LAN, the first-hop security is enabled on the access layer switches, known as the edge devices of the LAN. The QoS is also recommended as close as possible to the source. However, QoS might be implemented in different network segments for different reasons, but the place where a technician enables it remains unchanged. In the LAN, QoS might be implemented to protect voice traffic at the network edge.

Service Provider Edge: When it comes to service providers, such as those supplying virtual private network (VPN) services, the provider edge (PE) devices always offer more in the way of configuration, policy and control plane state. PE edge or network element plays a key role in Multiprotocol Label Switching (MPLS) infrastructure.

The PE router is an interface between the customer-end network and the MPLS core as well as the point where customer data is given an MPLS label. Data enters the MPLS network through the PE router, navigates the network and exits through another PE router.

Datacentre Edge: In the datacentre network, the edge may not be defined clearly, especially after virtualization. However, the edge can be thought of as the virtual access switch.

Consider the use case of an IoT-connected office building environment. There may be hundreds or thousands of sensors with dozens of different functions including measuring temperature, light, noise, movement, security and more. But IoT is not just about sensing; it is also about controlling systems. Turning the lights on and off, heating, ventilation, air conditioning (HVAC), establishing networks and more can be done through connected systems. In this connected environment, an IoT gateway performs several critical functions such as device connectivity, data filtering and processing, updating, and managing devices. Newer IoT gateways also operate as platforms for application code that processes data and becomes an intelligent part of a device-enabled system. The following image shows a house with smart appliances:

Fig. 1.5.7: A house with smart appliances

UNIT 1.6: Nodes and Gateways

Unit Objectives

At the end of this unit, you will be able to:

1. Explain nodes
2. Describe gateway architecture
3. List the steps in setting up an IoT framework

1.6.1 Nodes and Gateways in Internet of Things

Gateways

For IoT applications in telecommunication sector, a gateway is a stopper for data on the networks. It makes transmission of data possible back and forth. In a way, it is an access window which provides an added layer of security for data transfer in the network to prevent any hack attacks. For example, in home networks, the Internet service provider is the gateway to access the Internet.

IoT Gateway

An IoT gateway, also known as control tier, can be a hardware appliance or a coded application which acts as a bridge between the cloud, the sensors and the smart devices. It provides security to the data that is being transported on the network as it prevents leaks or phishing attacks with the help of tamper detection or encryption tools.

The following figure shows an IoT gateway architecture:

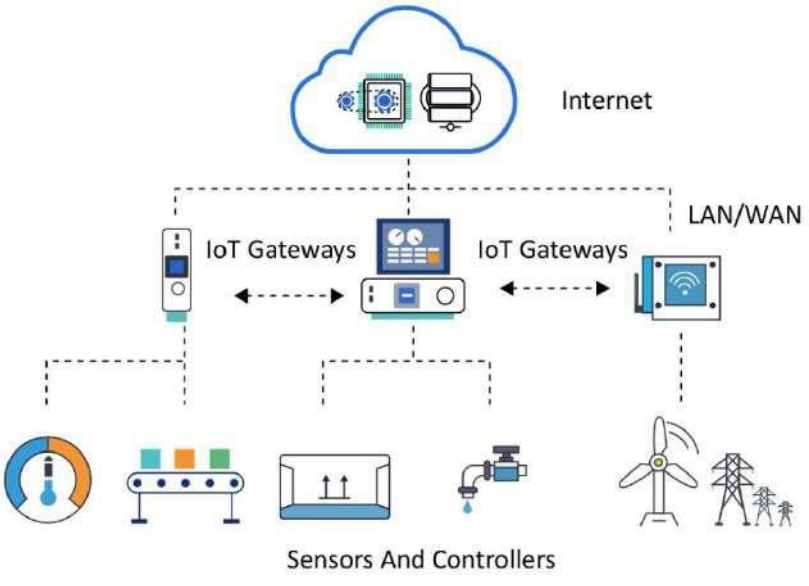


Fig. 1.6.1: IoT gateway architecture

In the current scenario, IoT gateways are very important as protocols, connectivity models and energy profiles. They play a vital role in controlling a complex networking environment.

They are also useful for device connectivity, protocol translation, data filtering and processing. For example, smart IoT gateways delivered by companies such as Dell and Wind River are developed for computing platforms that run up to date operating systems like Linux or Window.

Nodes

A node is a communication point (active electronic device) which can create, receive or transmit data in a communication channel for a telecommunication network.

For data communication networks, the hardware node can be a data communication equipment like a switch, a modem, a hub, a bridge or a data terminal equipment like a telephone handset. In case of fixed telephone networks, the node can be a telephone exchange or a host computer providing intelligent network service. In case of a cellular communication network, a node is a Gateway GPRS Support Node or Servicing GPRS Node (SGSN).

The following figure shows how an IoT gateway is connected to nodes:

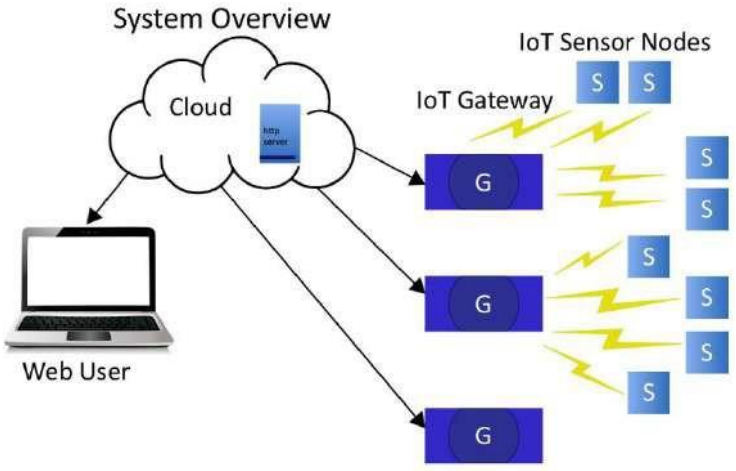


Fig. 1.6.2: IoT gateway and nodes

IoT Edge Device/Node

In an IoT application, an edge device is generally the networking device which connects LAN with the WAN (or Internet). Edge devices commonly used in telecommunication sector are edge switches, routers or multiplexers; for example, an IoT edge gateway on a Raspberry Pi 3 that runs Raspbian Linux. The gateway is constructed using IoT edge, and the sample uses a Sensor Tag Bluetooth Low Energy (BLE) device to gather temperature data.

A node provides connectivity and traffic translation between the boundaries of the varying networks using different networking protocols. A good example would be the transmission of packets between Ethernet and bank ATM network.

Basic Steps in Setting up an IoT Framework

The steps that are taken to set up an IoT framework are as follows:

- **IoT Device and Gateway Installation Point**

  The IoT devices and their respective gateway installation points need to be figured out based on the network they are going to be operated on. This ensures smooth flow of information and security on the local area network as well as the wide area network to which it is connected. Since gateways are vital for a successful IoT ecosystem, therefore installation points are important for the overall IoT architecture. The selection of the installation point and the installation process are important and are discussed later.

- **Configuring Installation Points**

  Properly configuring the installation points is the vital step in ensuring overall success of the IoT implementation in any kind of environment. Once the configuration is done, it becomes easy to manage the system, add modules or change the IoT device architecture in case the IoT ecosystem is big. The configuration of the installed IoT framework will be discussed later.

- **Positioning IoT Devices to Suitable Locations**

  A new dynamic category of positioning devices in an IoT ecosystem is the Location of Things. This is the correct positioning of IoT devices for optimized performance. With so much data being transferred on local as well as global networks, Location of Things plays a pivotal role in filtering the relevant information. Location based services such as Google Maps, Uber or Foursquare are good examples of this.

  Indoor positioning systems (IPS) come in handy for implementing IoT inside buildings or homes. The correct positioning of IoT devices is an important part of the positioning concept. With the help of IPS, the data gathered comes handy for tasks such as finding devices and equipment or navigating inside indoor spaces like in shopping malls or in geo-fencing sensitive data. The positioning of the IoT devices at a location will be discussed later.

- **Installation of Devices to the Appropriate Points/Locations**

  Installing the IoT devices at their optimum location is the very first step in having a smooth network. Each device should be installed to the location by carefully mapping the network details. For example, in case of Google Wi-Fi, the Wi-Fi units include a software called Network Assist that ensure a strong signal by constantly selecting the clearest wireless channel. When using multiple "points," Network Assist seamlessly transitions a coupled device to the closest Wi-Fi point to ensure the best connectivity. The complete process of installation of IoT devices will be discussed later.

- **Reinstallation of Devices**

  Reinstallation of IoT devices is required in case there is some hardware malfunction or a software glitch which is resulting in jamming of the network or causing encumbrance in one or more than one nodes in the network. Reinstallation may also be required in case there are unnecessary hang-ups in the data transfer equipment.

Exercise

1. Write the basic steps involved in setting up an IoT framework.

Exercise

1. List some of the components that can be included in IoT edge.

2. Mention the functions of edge devices.

UNIT 1.7: Cloud Computing

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the concept of cloud computing
2. List the characteristics of cloud computing
3. Explain how cloud computing is related to business analytics
4. Explain the advantages of cloud utilization

1.7.1 Introduction

IoT includes devices which are connected via the Internet to perform the services for which they are made. This involves storage and processing of data for which storage is required. The cloud storage helps in storing the data over the Internet. There are several advantages of providing the services to the user based entirely on the Internet.

For example, consider an employee who needs to submit a few reports to his/her manager but they are on different locations. The cloud computing can resolve this issue by using an app which is hosted on the Internet. The data on the app is managed remotely over the Internet. For temporary or permanent storage, a cloud platform can be used.

Concept of Cloud Computing

As in IoT a large amount of data is stored, processed and accessed, it requires cloud computing. This also helps in developing the IoT. The collaboration of IoT and cloud computing helps in developing the monitoring devices and processing the sensor data.

For example, data from the sensors can be uploaded and downloaded from the cloud storage platform. This data can be accessed for monitoring and actuating other smart things. The main motive is to get a more productive solution, which is cost effective also. A cloud platform also helps in analysing data, taking decisions and optimising interactions.

The integration of IoT and cloud involves various aspects such as QoS, quality of experience (QoE), security of data, privacy and reliability over the data. Cloud computing offers a model which is utility based and allows a business to access the data and information anytime from anywhere.

The following figure shows the concept of a cloud platform:

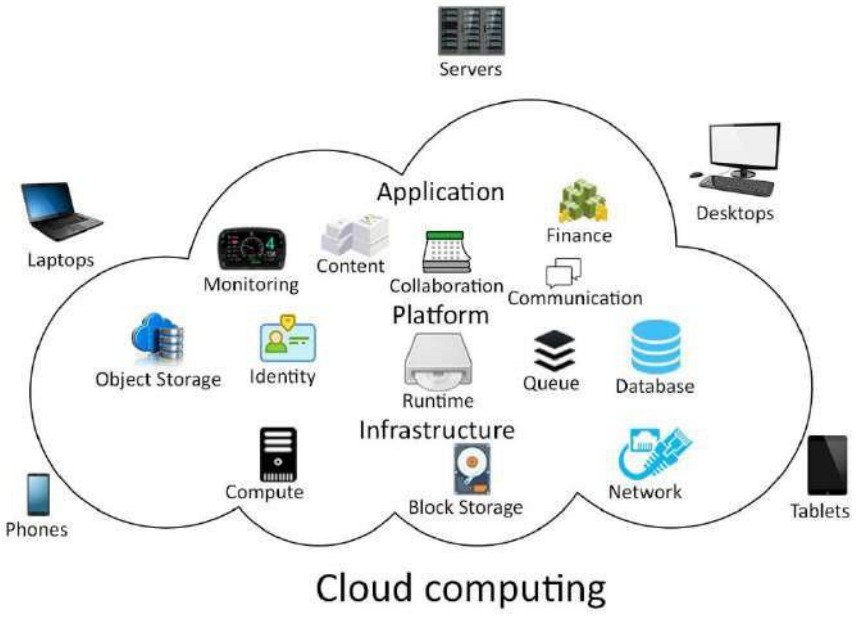


Fig. 1.7.1: Concept of cloud computing

Characteristics of Cloud Computing

There are a few characteristics of cloud computing which determine its working. The following figure shows these characteristics:

- Cloud computing can be accessed anytime from anywhere with Internet access
- It involves Internet access and thus data can be retrieved from any device which is Internet enabled
- It allows resource pooling, thus, anyone can access and use the data for collaborating the information
- It offers a wide range of services as per need such as adding and removing users and handling storage space
- It is measurable in respect of storage, processing and the number of users accessing the data

Fig. 1.7.2: Characteristics of cloud computing

Deployment Models

Deployment in cloud computing comprises four deployment models: private cloud, public cloud, community cloud and hybrid cloud.

A private cloud has an infrastructure that is provisioned for exclusive use by a single organisation comprising multiple consumers, such as business units. It may be owned, managed and operated by the organisation, a third party or some combination of them, and it may exist on or off premises.

A public cloud is created for open use by the general public. It sells services to anyone on the Internet. (Amazon Web Services is an example of a large public cloud provider.) This model is suitable for business requirements that require management of load spikes and of the applications used by the business; activities that would otherwise require greater investment in infrastructure for the business. As such, public cloud also helps to reduce capital expenditure and to bring down operational IT costs.

A community cloud is managed and used by a particular group or organisations that have shared interests, such as specific security requirements or a common mission.

Finally, a hybrid cloud combines two or more distinct private, community or public cloud infrastructures such that they remain unique entities but are bound together by standardized or proprietary technology that enables data and application portability. Normally, information that is not critical is outsourced to the public cloud, while business-critical services and data are kept within the control of the organisation.

1.7.2 Cloud Optimization and Business Analytics

It is mandatory for all organisations to keep track of their analytics. Every organisation has data which they should gather, analyse and interpret. But this is not an ordinary task. With the evolution of technology, the amount of data and sources of data are growing exponentially. Assessing new data sources and being able to distinguish valuable data from the sources is not possible without a means (a technology) that is flexible enough to grow with the business and the changing data.

Businesses have found refuge in cloud – the flexible technology capable of growing with the changing requirements of the former. Most businesses today have begun to re-evaluate their infrastructure to move faster and be flexible in understanding the data they produce. Businesses are moving to the cloud for analysing and interpreting their HR, sales, marketing and even financial data. So, there is a need to understand why cloud is the ideal choice for business analytics.

The following figure shows the characteristics that make cloud an ideal choice for business analytics:

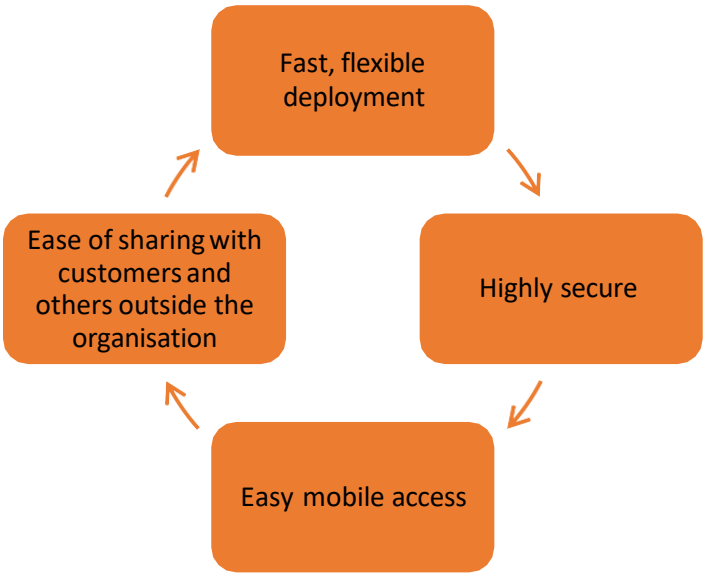


Fig. 1.7.3: Characteristics of cloud

- **Fast, Flexible Deployment**

  Ease of deploying is considered one of the primary reasons for the shift to cloud services; it is an even more convincing factor than cost. Cloud enables a quick start without the need for any additional hardware, configuration or installation. Simply host, then share the dashboard and one is good to go.

- **Highly Secure**

  Security is another important reason that people are shifting to cloud. This is primarily because cloud vendors keep round the clock vigil, perform regular checks and threat assessments, and have a team in place that can deploy a new patch as and when required. All these things would otherwise require additional cost in an office setup of the business.

- **Easy Mobile Access**

  Cloud solution can be accessed from anywhere without getting into the firewall; which means, business owners and their IT team can access and take advantage of secure system and authentication control on the go.

- **Ease of Sharing with Customers and Others Outside the Organisation**

  Since there is no real requirement to get into the firewall every time, a business can give access to their cloud system to the outsiders – including customers and have them access the dashboard easily.

  For example, marketing companies use analytics to analyse campaign results and Return on Investment. This data interpretation is then used to make right offers for customers and ensure the offers are delivered to customers at the right time. The data analytics also helps to predict what customers will respond to next, or in the near future.

Role of Cloud in IoT

IoT is used in everyday objects, such as consumer devices, vehicles, buildings and so on. It includes embedded software, sensors, electronics and network connectivity, allowing the objects to send, receive and collect data.

Given the utility, IoT is transforming the way the daily tasks are being completed today. But there is a catch; IoT generates a large amount of Big Data, which puts a lot of strain on the Internet infrastructure of an organisation. To meet the requirement of large amount of data analysis, organisations are using cloud computing, which provides scalability in deliverance of enterprise applications and Software as a Service (SaaS).

1.7.3 Advantages of Cloud in Internet of Things

Cloud computing is about accessing data and programs from a centralized computed resource as and when required. IoT or Internet of Things on the other hand is connection of devices (besides computers) through software, sensors and so on. IoT allows devices to be connected and automated in a cost effective and intelligent manner to ensure real-time monitoring and control. The following figure shows how cloud computing is integrated with the devices and allows the data to be managed with efficiency:

Fig. 1.7.4: Integration of cloud computing in IoT

The two may seem different but both IoT and cloud computing increase efficiency in everyday tasks. Both the concepts have a very complementary relationship – where IoT generates huge amount of Big Data, the cloud offers a pathway for that data to travel. It makes it easier for the developers to access the massive quantities of Big Data via the cloud.

Cloud computing service is generally chargeable at pay per use model. So, the business only pays for the resources that it uses and nothing more. This allows IoT companies to meet their economies of scale, as the overall infrastructural cost is minimized.

Cloud computing also benefits IoT with better collaboration of data, and ease of use. Cloud allows the developers in IoT to access and store data remotely, or on the move. This saves time and labour.

Exercise

1. List the characteristics of cloud computing.

2. List some advantages of cloud computing.

Practical

1. Perform the prototyping of Raspberry Pi kit.

Required Tools/Equipment:

- A Raspberry Pi 2 Model B
- Two 0.1" (2.54mm) female pin header strips
- A SYB-170 breadboard
- An open top Raspberry Pi Case
- A double-sided sticky pad
- A short length of wire
- A soldering iron
- Wire cutters/strippers
- A small lump of Blue-tack
- A needle file
- A sharp craft knife

1.7.4 Networking Essentials

The **Internet** (or **internet**) is the worldwide system of interconnected computer networks. It uses the Internet protocol suite (TCP/IP) to communicate between the connected devices in the networks.

It is a *network of networks* that consists of networks which may be a private or public domains academic or business domain, or government networks, linked by a wireless optical networking technology.

The Internet is central repository of information and services, hypertext documents that are linked and applications of the World Wide Web (WWW), electronic mail, internet telephony, and sharing of files.

The protocol plays a major role in encoding and decoding information that is transferred through the network. The most widely used protocol is TCP/IP. It's a collection of two protocol namely, Transmission Control Protocol and Internet Protocol. It is used to connect networked devices in the world wide web.

TCP/IP defines how the data is exchanged over the internet. It provides end to end communication, that identify how the data should be broken into packets, addressed, transmitted and routed. And at the destination it is received and unpacked. TCP/IP is a reliable protocol because it ensures data is recovered automatically from network failure or device failure.

The two protocols serve specific purposes. TCP defines the standard for applications as to how they have to create communication channel across the network. It also defines how a message in broken into different packets, defines the header and footer for the packets and the order in which it has to be transmitted. And at the destination it is received and reassembled as per the header and footer information

Internet Protocol is responsible for defining the address and route each packet and ensures it reaches the right destination. Each computer in the network checks this IP address to determine the address of the destination.

Subnet mask, helps in identifying the network address and the ID of the device in the network. Every IP address has two components the network ID and the host ID. The host ID and the network ID is determined by the network class.

TCP/IP first establishes a connection with the destination host before transmitting the packets. This is called handshake. Only after the connection is established it starts sending the data. this ensures that the data is not lost, and reaches the intended receiver.

TCP/IP protocol suite include the following:

- **Hypertext Transfer Protocol (HTTP)** handles the communication between a web server and a web browser.

- **HTTP Secure** handles secure communication between a web server and a web browser.

- **File Transfer Protocol** handles transmission of files between computers.

Why is TCP/IP important?

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.

User Datagram Protocol

User Datagram Protocol is one of the important protocols of the Internet protocol suite. with the help of UDP, applications can send messages, which are called as *datagrams*, to the destination hosts on an Internet Protocol (IP) network. Unlike the TCP/IP, UDP does not inform the destination host about the packets being sent. Due to this reason, it is called non reliable protocol. During the transmission if a datagram is lost, it does not resend the data. It is lost once for all. Because of this this protocol is not in use.

Prior communications are not required in order to set up communication channels or data paths.

UDP is a connectionless communication protocol. UDP provides checksums for data integrity, and port numbers for addressing different functions at the source and destination of the datagram. Connectionless also means that it does not handshake, and thus exposes the user's program to any unreliability of the underlying network; it does not guarantee deliver of the packets.

Secured Socket Layer

Secured Socket Layer protocol is developed by Netscape for transmitting data through encrypted link between a web server and web browser. It is an industry standard which ensures that private data is sent securely over the internet by encrypting it. Most of the websites use this to protect the online transactions of their customers.

The Secured socket layer existed from 1995 till 2011, when the SSL 2.0 got deprecated. It has been replaced by a much more complex protocol called Transport Layer Security protocol is being widely used for securing the private data.

Exercise

1. TCP/IP stands for _____
2. Secured socket layer is developed by _____
3. UDP is connection less because_____
4. _____ protocol is used to transfer files over the internet
5. HTTP handles communication between _____ and _____

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

2. Install and Configure IOT Device

Telecom Sector Skill Council

Unit 2.1 - Establishing Framework for Internet of Things
Unit 2.2 - Installing Gateway as per the Power Supply Requirements
Unit 2.3 - Establishing Communication between Nodes, Gateway and Servers
Unit 2.4 - Establishing Ethernet Connectivity
Unit 2.5 - Authentication and Access Control Mechanism
Unit 2.6 – Mounting the Devices at Desired Locations
Unit 2.7 – Performing Checks and Connections
Unit 2.8 – Connecting Microcontroller Boards for Data Transfer and Connecting the Boards
Unit 2.9 – Installing Suitable Framework
Unit 2.10 – Transferring Software Code to On-board Microprocessor and Compiling Code to On-board Microprocessor
Unit 2.11 – Understanding Error Codes and Debug Software
Unit 2.12 – Functioning of Micro-controller and Attached Devices
Unit 2.13 – Initializing Nodes and Gateways
Unit 2.14 – Launching the Software on Nodes and Gateways
Unit 2.15 – Confirming Communication and Establishing Connectivity
Unit 2.16 – Controlling Edge Appliances and Hubs and Checking for Data Transfer and Confirming from the Server End

Key Learning Outcomes

At the end of this module, you will be able to:

1. List the steps of installation of IoT framework
2. Explain how to collect data
3. List the input parameters for a sensor
4. List the characteristics of power sources available for the nodes and gateways
5. Identify the characteristics of battery used for IoT framework
6. Execute connection establishment between the nodes and gateways
7. Explain the communication channels
8. Describe wireless sensor network
9. Explain sensor connectivity
10. Identify the connectivity options
11. Describe how to configure network setting
12. List the steps of crimping
13. Execute the establishment of Ethernet connection
14. Identify the importance of authentication and authorization in IoT
15. Explain access control system
16. Identify the software interface characteristics.
17. List different software available for access control management
18. Describe how to secure wireless connection
19. Describe malware and DDoS attacks

UNIT 2.1: Establishing Framework for Internet of Things

Unit Objectives

At the end of this unit, you will be able to:

1. List the steps of installation of IoT framework
2. Explain how to collect data
3. List the input parameters for a sensor

2.1.1 Installing the IoT Framework

For establishing a functional IoT framework, the technician needs to understand the requirements of the site by analysing the framework. The IoT framework includes the type of IoT device, the type of connectivity between IoT devices, the communication channel and database management.

One of the most practical examples of IoT devices is the motion sensor used in an alarm system. The sensor works by getting activated when it senses an object or any person close to it. The following image shows a motion sensor:

Fig. 2.1.1: Motion sensor

The following figure lists the steps for installing a framework for a sensor:

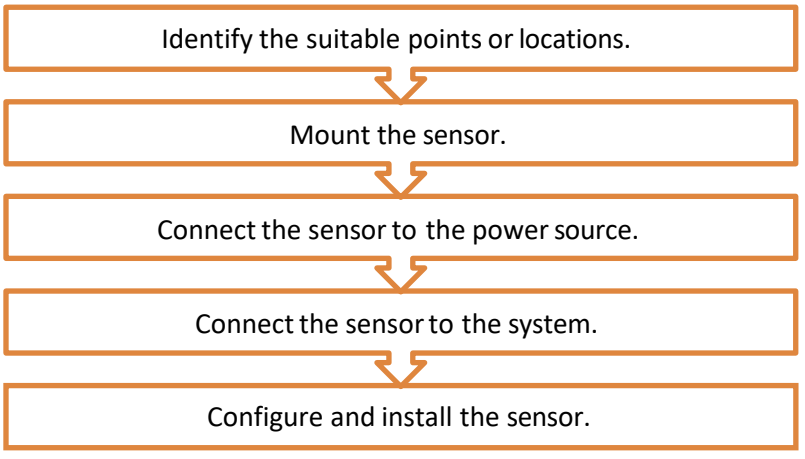


Fig. 2.1.2: Steps for installing a motion sensor

Identification of Suitable Points or Locations

It is very much important to find a suitable location for the access points of the sensors. The access points should be in such places where they cannot be reached easily, so that they are not easily tampered. In general, to keep an IoT system secure, the criteria to be taken into consideration are as shown in the following figure:

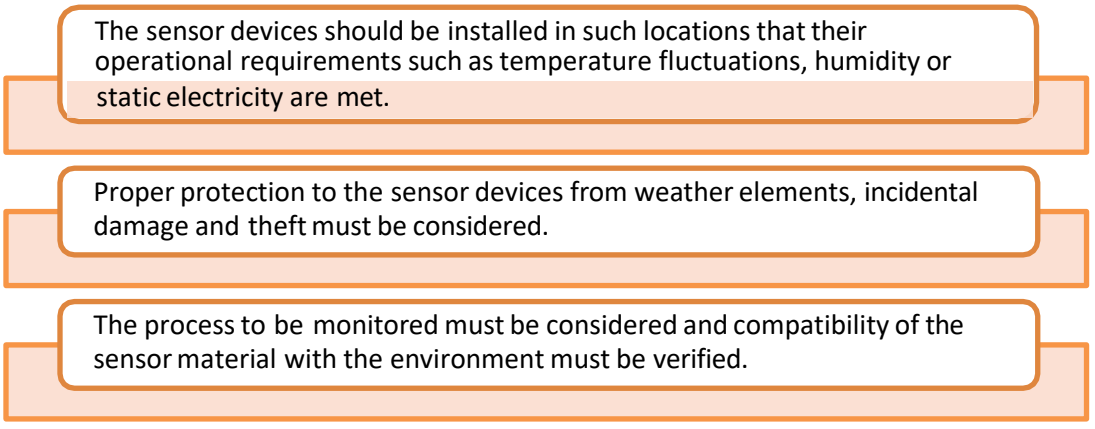


Fig. 2.1.3: Criteria for securing IoT devices

The following figure shows some suitable locations for outdoor sensors:

Fig. 2.1.4: Suitable location for outdoor sensors

A sensible area for the scope of the motion sensor must be considered for mounting a sensor on a wall and a ceiling. The following image shows the scope of a motion sensor:

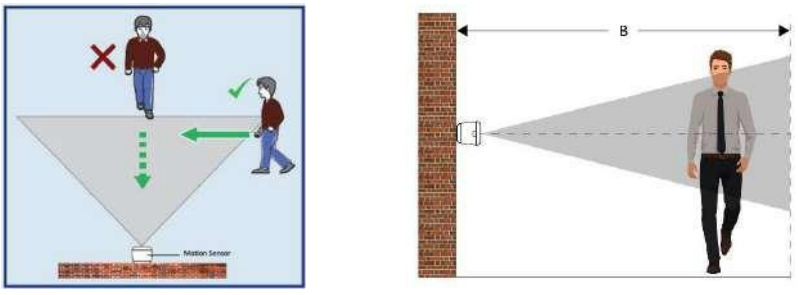


Fig. 2.1.5: Scope of a motion sensor

Mount the Sensor

A motion sensor can be mounted either on a wall or on a ceiling. The mounting can be done using an adhesive or using the knockout holes on the unit's base. The following figure shows the steps for mounting the sensor using knockout holes:

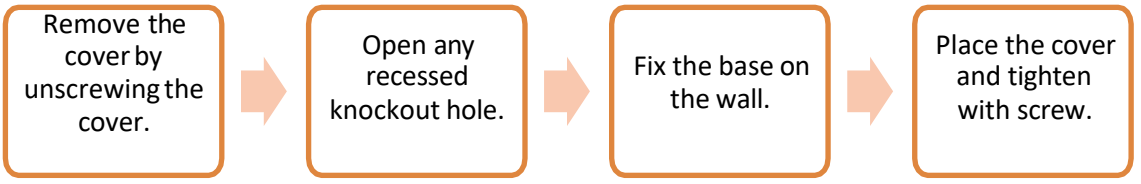


Fig. 2.1.6: Steps for mounting a sensor

There are some key points that should be kept in mind. These are as follows:

- The sensor must be attached to a stable surface which can support 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:

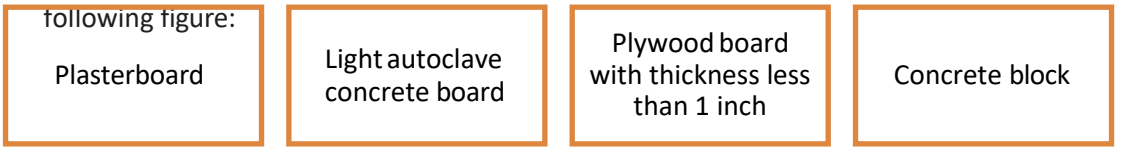


Fig. 2.1.7: Surfaces to be avoided for mounting

The following figure shows some examples of suitable and unsuitable surfaces for mounting:

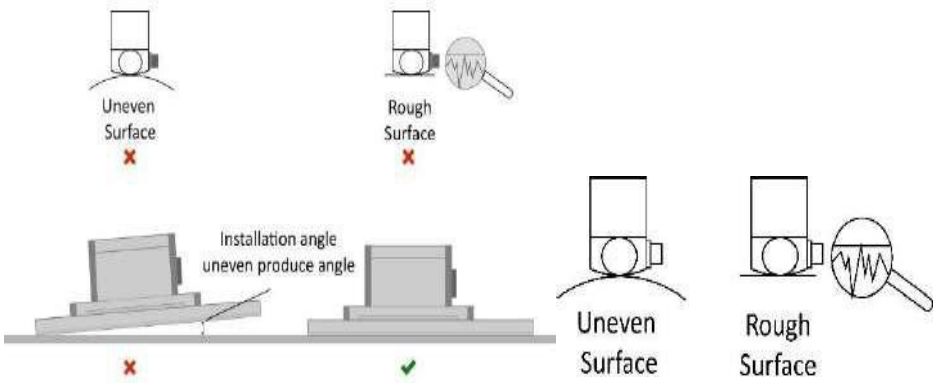


Fig. 2.1.8: Suitable and unsuitable surfaces for mounting

Connect 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 are as follows:

- Open the battery cover by using a flathead screwdriver as shown in the following figure:

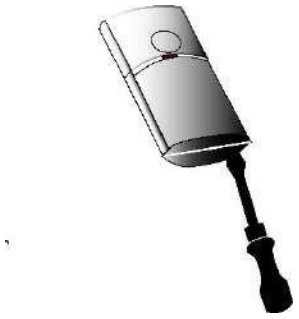


Fig. 2.1.9: Opening the battery cover

- Install the battery according to the indicated polarity as shown in the following figure:

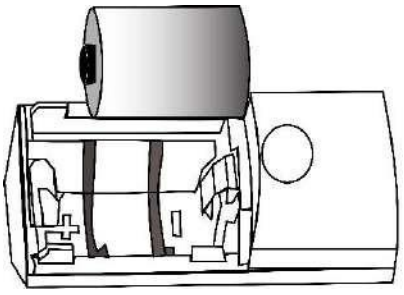


Fig. 2.1.10: Installing the battery

The sensors can be connected to the mains or to the utility using cables also. The following diagram shows connection of multiple sensors to the power supply:

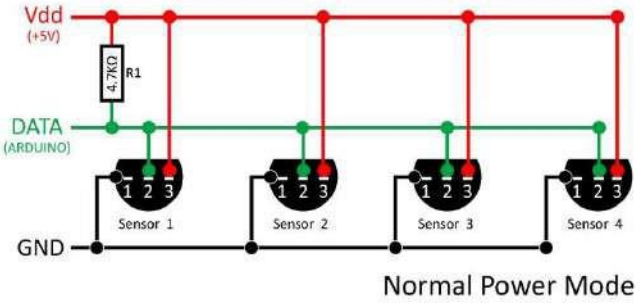


Fig. 2.1.11: Schematic diagram of sensor connectivity to the power supply

Connect the Sensor to the System

Motion sensors come with an attached speaker cable. The other end of the cable needs to be attached to a switch port on the alarm system. The sensors can be connected to the alarm system wirelessly via Wi-Fi or Bluetooth network. For example, the current transformer (CT) sensors are used to measure alternating current (AC). These are useful for measuring the electricity consumption of a building.

The following image shows a schematic diagram for connecting a CT sensor to a display monitor:

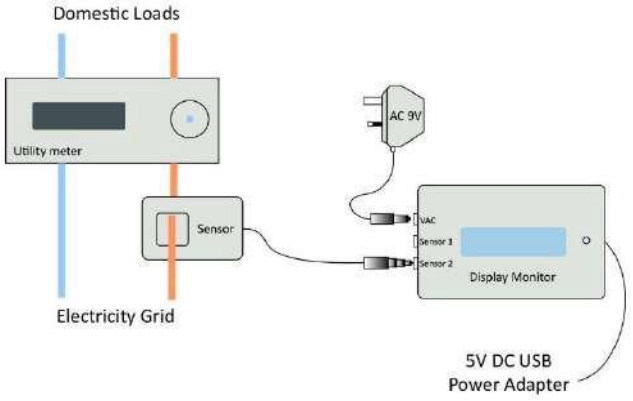


Fig. 2.1.12: Schematic diagram for connecting a sensor to a display monitor

The steps are as follows:

- Connect the jack from a CT sensor, into either sensor1 or sensor2 socket on the monitor system.
- Plug the AC 9V adapter from the VAC, into a power outlet.
- Plug the DC 5V adapter into another power outlet, for a backup power.
- Temperature sensors can be connected to the display via an RJ45 connector.

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 smart phone application. The following image shows configuring the sensor:

Type	Sensor Name	Signal	Battery	Data	Last Check In
	Button			Detected	7/2/2018 11:30 AM
	Temperature			75.9°F	7/2/2018 11:30 AM

Fig. 2.1.13: Configuring the sensor

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 as shown in the following image:

Fig. 2.1.14: Power detected by the sensor

- Check the network status shown on the display as shown in the following image:

Fig. 2.1.15: Network detected and displayed

2.1.2 Collating Installation Points and Collecting Data

An IoT system requires several devices installed at various places. These installation points must be collated to one point, so that the data they receive can be analysed. Hence, all the devices are connected to a master device, which is used as a central point as shown in the following figure:

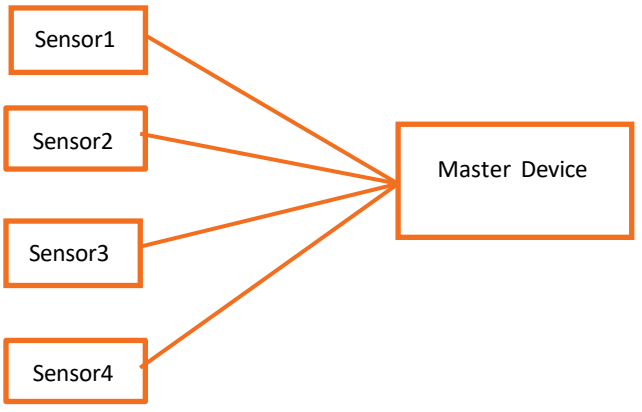


Fig. 2.1.16: Collating installation points

Data is created by a device in three stages as shown in the following figure:

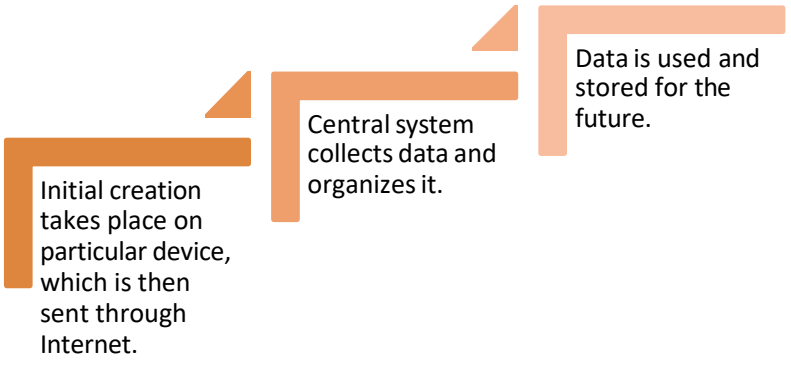


Fig. 2.1.17: Data creation stages

There are several ways in which data can be collected. Several systems that may be involved in the data collection scenario are as follows:

- **Smartphones:** Cloud or internal memory or memory cards
- **Wearables:** Cloud or internal memory or memory cards
- **Computers:** Cloud or hard disk or flash drives

2.1.3 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.

Parameter is a property of a sensor. Most of the sensors are based on a parameter that come in form of messages. Parameters can be of any names which are predefined in device configuration. Some of the examples are TEMP, param199 and param240. The device specification should be checked to know the available parameters and what they measure.

While editing a sensor configuration, the parameters from the last message appear in the dropdown list of available parameters. If there is any required parameter missing, it can be added manually. The same parameter may be used for any number of sensors.

To configure the sensor, combination of the fields as shown in the following table must be added:

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 ID of the worker to which the sensor is attached.

Table 2.1.1 Sensor configuration fields

Most of the sensors require some additional input. The parameters may have a key, value and description which needs to be added by accessing the sensor control panel or adding the information in the sensor through a computer. These descriptions are as shown in the following screenshot of a sensor control system figure:

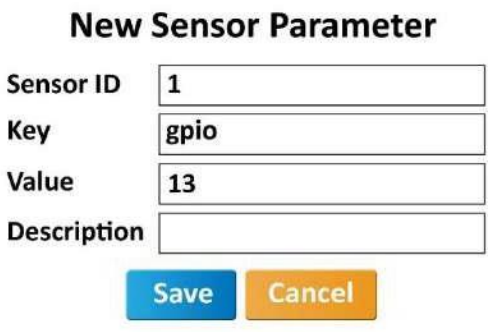


Fig. 2.1.18: Input parameters of sensors

2.1.4 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.

Exercise

1. Put a (✓) if the statement is true, otherwise put a (X).
   a. Sensors can be attached on soft surfaces. ( )
   b. Motion sensors should not be installed near an air discharge grill. ( )
   c. A sensor on a wall surface can sense elements within the range of an angle of 90 degrees. ( )

2. List the input parameters for a sensor device.

3. Mention the location constraints for mounting a sensor.

UNIT 2.2: Installing Gateway as per the Power Supply Requirements

Unit Objectives

At the end of this unit, you will be able to:

1. List the characteristics of power sources available for the nodes and gateways
2. Identify the characteristics of battery used for IoT framework
3. Execute connection establishment between the nodes and gateways

2.2.1 Power Supply of the Edge Nodes and Gateways

A large amount of data is generated per second by the sensors. The data is pre-processed locally at the edge, before being sent to the cloud. A gateway is the place where the local processing happens.

IoT is a proliferation of several interconnected sensors, actuators and processors. The brains of the embedded chips have reliable communications capabilities and are becoming cheaper and more sophisticated. The power is required to manage the gateway functionalities, including the embedded processing, multiple sensor interfaces and Internet connection. Hence, the devices require to be plugged into a mains power source or need to be recharged frequently.

The correct power supply should be selected on various aspects such as follows:

- Availability of power points at the site
- Type of sensor
- Number of sensors and other modules connected within the IoT framework
- Type of power, DC or AC, supported by the device
- Suitable power supply for the IoT framework set up
- Usage of sensor and other modules

After considering these factors, the technician should choose the power source/supply for the sensors and other modules. For reference, a technician can consider the installation documents to check the power source suitable for any module.

Most of the edge nodes require rechargeable batteries. Usually, a LiPo or a Li -Ion battery is used. Common IoT gateways are unlikely to require a multi-output adapter or a 250W adapter. But, it may be designed for use with a single-voltage AC/DC supply of above 6V or a sub-6V low-voltage supply in the under-1W or 1W-49W category.

The characteristics of a battery that must be considered while choosing the power supply are as shown in the following figure:

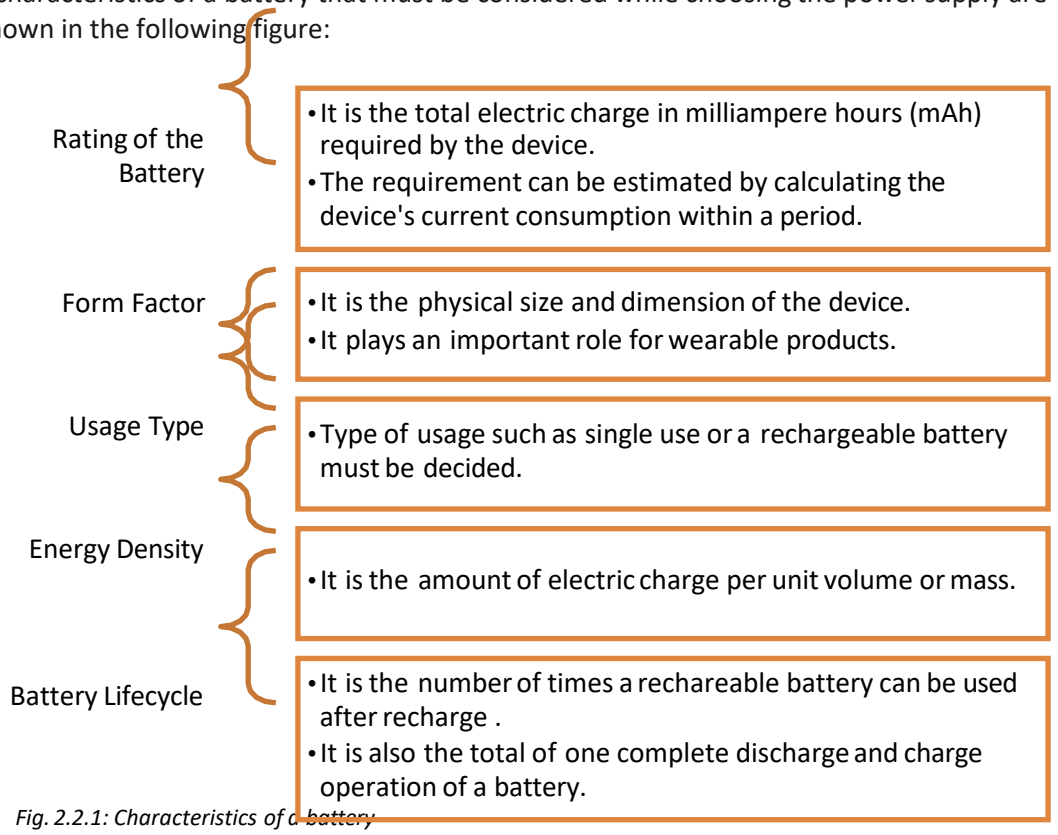


Fig. 2.2.1: Characteristics of a battery

2.2.2 Setting up the Installation Points

To set up an IoT framework, the installation points must be established first. Then, the installation points must be calibrated for the power supply requirement. The following figure shows the steps in connecting power supply with gateway and nodes setup:

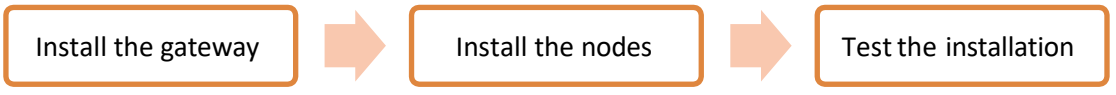


Fig. 2.2.2: Steps for connecting power supply with gateway and nodes setup

Install the Gateway

The first important task for installing the gateway is selecting a proper location for it.

The following figure shows the installation steps of a gateway:

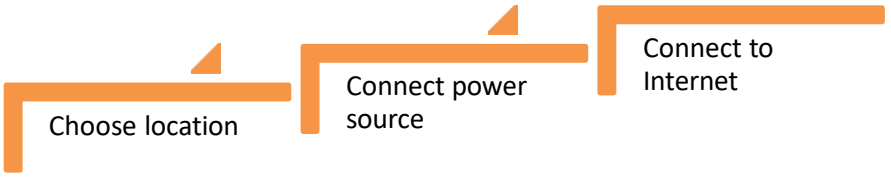


Fig. 2.2.3: Installation steps of IoT gateway

Choose Location

IoT gateways need to be placed at the intersection of the edge nodes, which are devices, controllers, sensors and the cloud. The gateway should be installed at a location elevated at certain height, which is not easily reachable, to make sure that the position is not disturbed. The gateway should be in clear line of sight of all the nodes. For example, a gateway installed for a Wi Fi network over a building or house should be installed approximately 6 feet above the maximum height of the surrounding buildings for clear line of sight.

The following figure shows the position of an IoT gateway as discussed in the example:

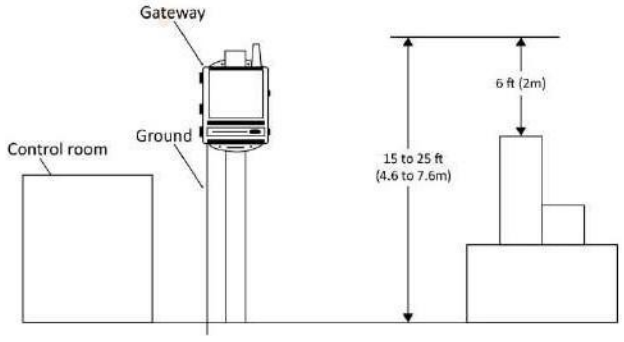


Fig. 2.2.4: Position of IoT gateway

When choosing the location of the gateway, the practices that should be kept in mind are as shown in the following figure:

- 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 the wireless devices such as cellular transmitters, Wifi 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.

Fig. 2.2.5: Best practices for the gateway location

The following image shows a metal enclosure for the gateway:

Fig. 2.2.6: A metal enclosure for the gateway

Connect Power Source

The power source has to be determined. A gateway can be powered by a 5 VDC wall adapter. It can also be connected via a wired connector. If the power supply is the mains, the gateway device must be installed near any plug point, so that minimum cable can be used.

Adoption of wireless charging requires compliance to standards across specific areas, such as frequency, induced current density, electric field and absorption rate.

Connecting the Power Adapter

To use the wall adapter, the adapter has to be plugged into the connector that is fixed on the back of the enclosure of the gateway. The technician should perform the following steps:

- Open the enclosure by removing the screws. The important task is to ensure that there is no static electric charge present in the internal electronics.
- Connect the right end of the power adapter cable to the gateway power port.
- Push the stripped wires into the appropriate connection terminals on the circuit board.
- Fit the enclosure around the circuit board and wire, then fasten the enclosure together using the screws.
- Connect the power plug to the power outlet.
- Check that the power light blinks green and then steadily remains green.

The following figure shows a gateway connected to a power outlet:

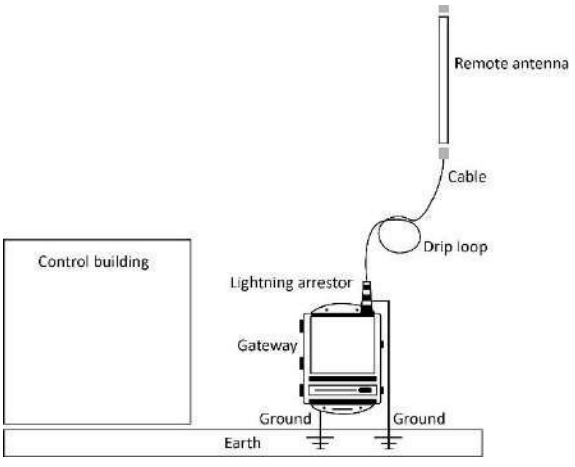


Fig. 2.2.7: A gateway connected to a power outlet

Connect to Internet

Typically, gateways are connected to Internet through Wi-Fi, Ethernet or GPS. Gateways, mounted in moving vehicles, can work in Wi-Fi and GPS modes. Some gateways are connected to the local networks (LAN). Business logic needs to be applied against the data collected by the gateway to understand which messages need to be sent over GPS networks and which can be stored on the device for offline processing. The gateway software is responsible for collecting messages from the sensors and storing them appropriately until they can be pre- processed and sent to the data centre.

Among the wireless technologies, such as Bluetooth, Wi-Fi, and ZigBee, ZigBee is the most preferred protocol in terms of cost and efficiency for the IoT devices. The technician should perform the following steps:

- Connect one end of the digital subscriber line (DSL) cable to the DSL port on the gateway.
- Connect the other end to the power outlet.

The connection can also be made through WAN Ethernet port by performing the following steps:

- Connect the Ethernet cable to the WAN Ethernet port on the gateway.
- Connect the other end to the WAN Ethernet jack.

The following figure shows the overview of cabling a gateway:

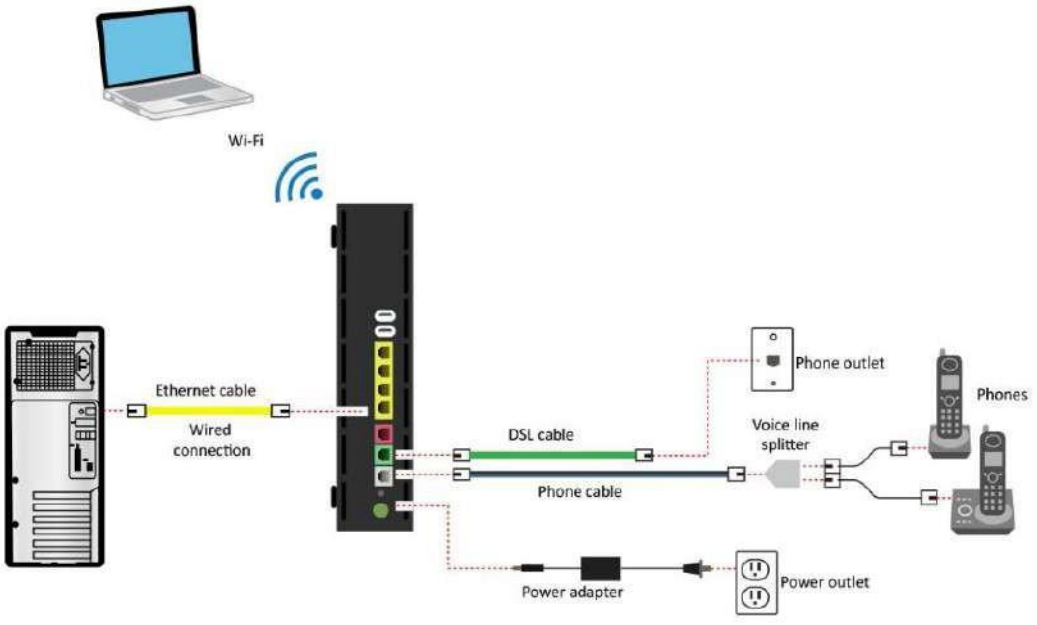


Fig. 2.2.8: Overview of cabling a gateway

Connecting the Gateway Relays

The gateway may contain normally closed relay contacts for connecting the system to automation panel inputs. The working of the relays can be configured using a software user interface. For example, a relay is opened when there is a motion detected and another relay is opened if there is a loss of node power.

The following image shows a relay module:

Fig. 2.2.9: A relay module to be connected to the gateway

Install the Nodes

The following figure shows the installation steps of a node:

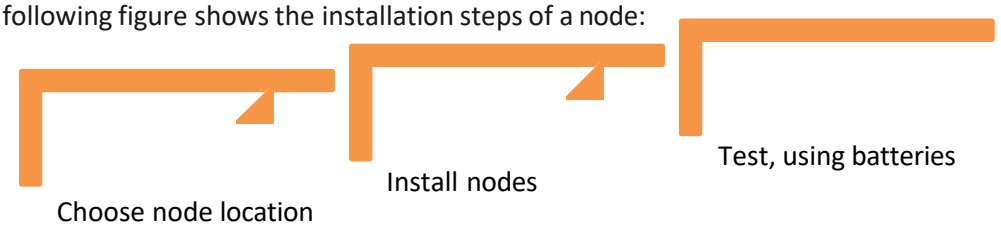


Fig. 2.2.10: Installation steps of IoT nodes

Choose Node Location

The nodes should be installed in the locations after considering all the aspects such as reachability, power requirements, Internet connectivity and so on. The best practices are:

- The nodes should be installed within the range of each other. The user interface settings must be checked to verify that all nodes are well connected.
- The nodes should be installed within the range of the gateway so that the gateway can communicate with all nodes.
- The nodes should be installed at 0.5-1.0 meters off the ground.
- When the area to be sensed is surrounded by walls, the nodes should be installed on the interior side of the walls.

  For example, to detect any movement in a room, the sensors should be installed at a place from where it can cover most of the area. The best place is to install it on a roof.

The following figure shows sensor locations in a room to detect movement in a surrounded area:

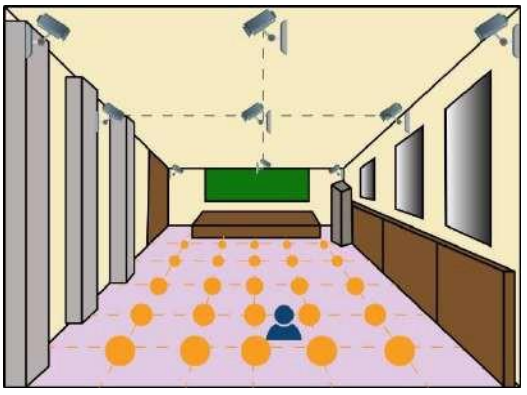


Fig. 2.2.11: Sensor locations in a surrounded area

- 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.

Connection of the Nodes

After completing the installation of IoT nodes and gateways, the IoT devices are connected to the power supply, as well as the gateway.

For example, for an IoT framework for motion detection with IR illuminated sensors, the nodes need to be connected with a power supply unit. The following figure shows a sample schematic diagram for the connection among the nodes for the same case:

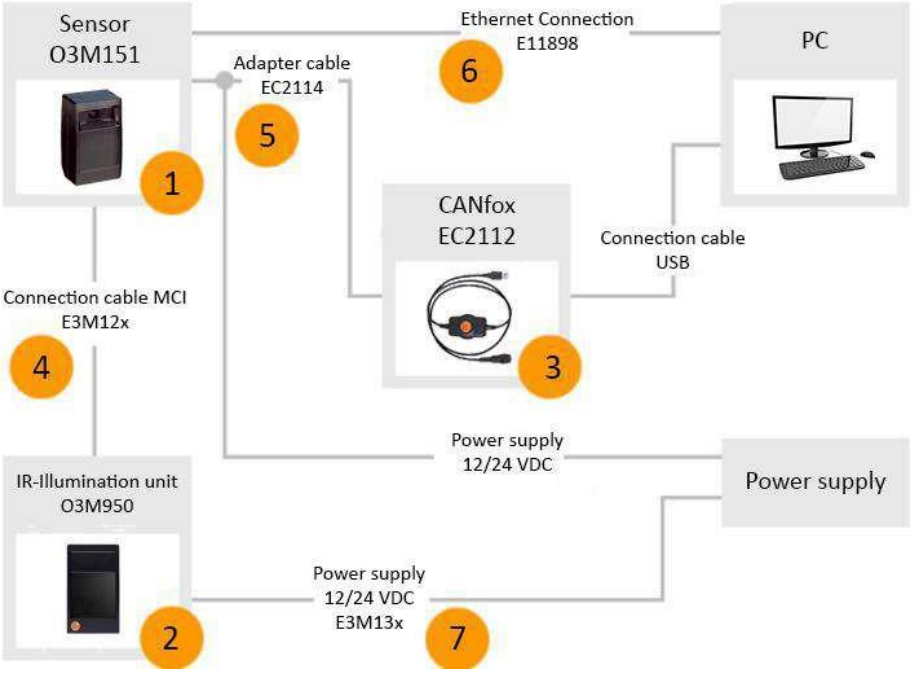


Fig. 2.2.12: Connection of IoT nodes

The power from the main power supply goes to the relay, then to the sensor, and then to the lamp. The technician should understand the schematic diagram and connect the wires accordingly.

Relay modules supports the microcontrollers such as Arduino and PIC which have digital outputs, control devices with large loads such as AC/DC motors, solenoids and bulbs.

Installing Plug-In Nodes

Plug in nodes are type of nodes which can be directly plugged in to a power supply and can be used. This node is configured by the plug in driver for the node from a computer system. It is useful as it reduces the effort in managing the wiring but there is signal loss in the node as it works without wires. Thus, it can be only used in a small area.

The following image shows a plug-in node on a wall:

Fig. 2.2.13: A plug-in node on a wall

Installing Wired (DC) Nodes

The following figure shows the connection of DC nodes:

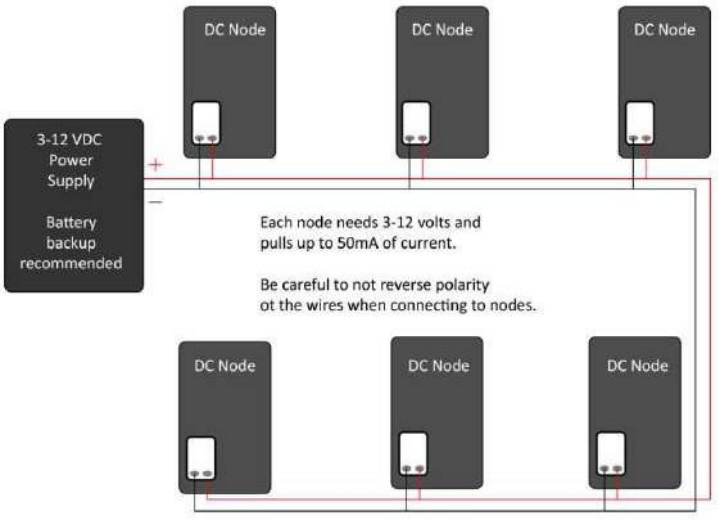


Fig. 2.2.14: Connection of DC nodes

The technician should perform the following steps:

- Remove the circuit board from the enclosure. The following image shows the parts of a node or a hub:

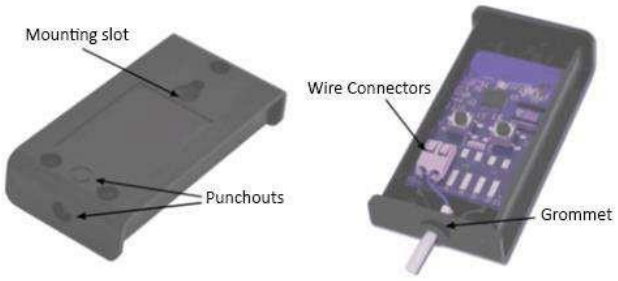


Fig. 2.2.15: Parts of a node or hub

- Choose a punch-out location to feed the wire. Install the rubber grommet and cable in the punch-out as shown in the following image:

Fig. 2.2.16: Inserting the grommet and cable of a node/hub

- Connect the cable to the wire terminals.
- Replace the enclosure and fix the screws.

The nodes have to be connected to the gateway also. The following figure shows the connection diagram of the gateway:

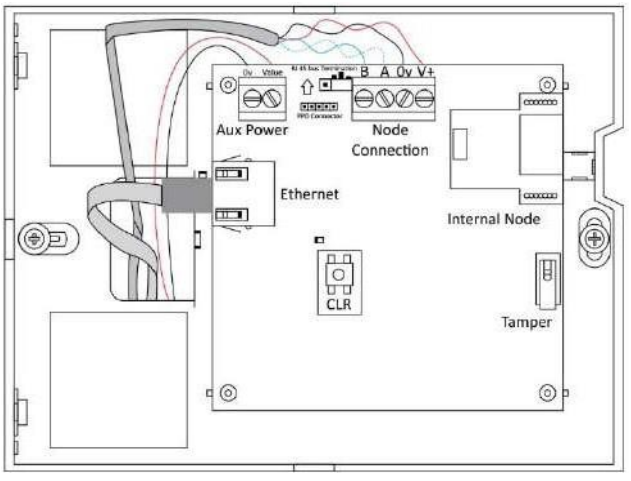


Fig. 2.2.17: Connection diagram of the gateway

Connecting Devices Using Wired Ethernet

The gateway has Ethernet ports that are used to connect wired devices. The technician should perform the following steps:

- Connect one end of the Ethernet cable to Ethernet port.
- Connect the other end to the port on the device.

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, the steps that should be performed are as shown in the following figure:

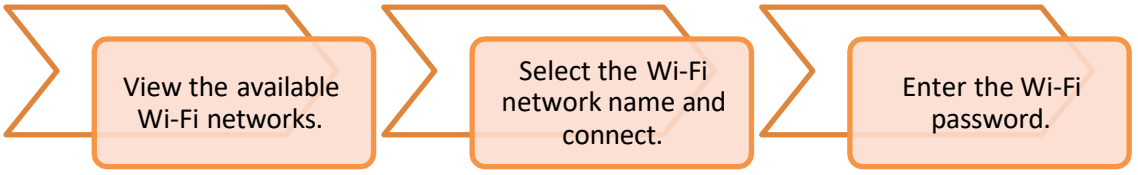


Fig. 2.2.18: Connecting a Wi-Fi device

Test the Installation

The nodes need to be tested by switching them on and off continuously to check whether they are working. The devices, for example a lamp, can be plugged in and the switch is connected to an electrical socket to check whether all the connections are made correctly. The technician should ensure the following points:

1. All wireless connectivity and power metrics are fully functional.
2. The nodes are correctly placed according to the plan.
3. Any outside motion will not cause a false trigger.

Exercise

1. List the features of a power supply source.

2. Mention the steps to connect a Wi-Fi device to the gateway.

3. Mention the locations where a gateway device can be installed.

UNIT 2.3: Establishing Communication between Nodes, Gateway and Servers and Ethernet Connectivity and Establishing Ethernet Connectivity

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the communication channels
2. Describe wireless sensor network
3. Explain sensor connectivity

2.3.1 Communication Channel at a Glance

Channels, also known as links, lines or path, are used to interconnect the nodes in a network. They may be comprised of one or more 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

Signals from one type of network may be routed to another network that has completely different characteristics. The quantityof data that can be passed through the channel at a time is known as channel capacity. It is also denoted by the channel bandwidth.

Physical Transmission Media

Cable form the physical transmission media for a network. 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 lists different types of cables used in networking:

Type of Cable	Image	Description
Twisted pair		These have two conductors 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.

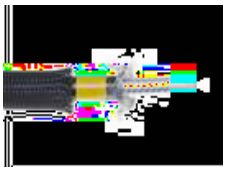
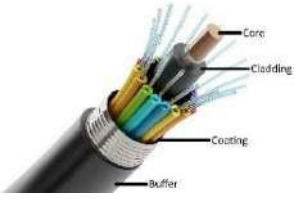
Coaxial/Helix cable		This has a thin conducting wire inside a tubular conducting shield, which is protected by a tubular insulating jacket. It is used to connect video equipment and carry television signals.
Optical fibre cable		This contains one or more optical fibres for carrying light. The optical 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 dimetral 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 (multi-mode)		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 decreases over long distances because of the increased dispersion and attenuation. This is used for backbone applications in buildings because of the reliability and high capacity.
Cross over cable		This connects computing devices, often of the same type such as two switches.

Table 2.3.1 Types of cables in networking

Wireless Transmission Media

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 network are WLAN, Bluetooth, cellular network and so on.

Types of Channels

In networks, the communication media is shared among the nodes. The following figure lists the different types of communication channels:

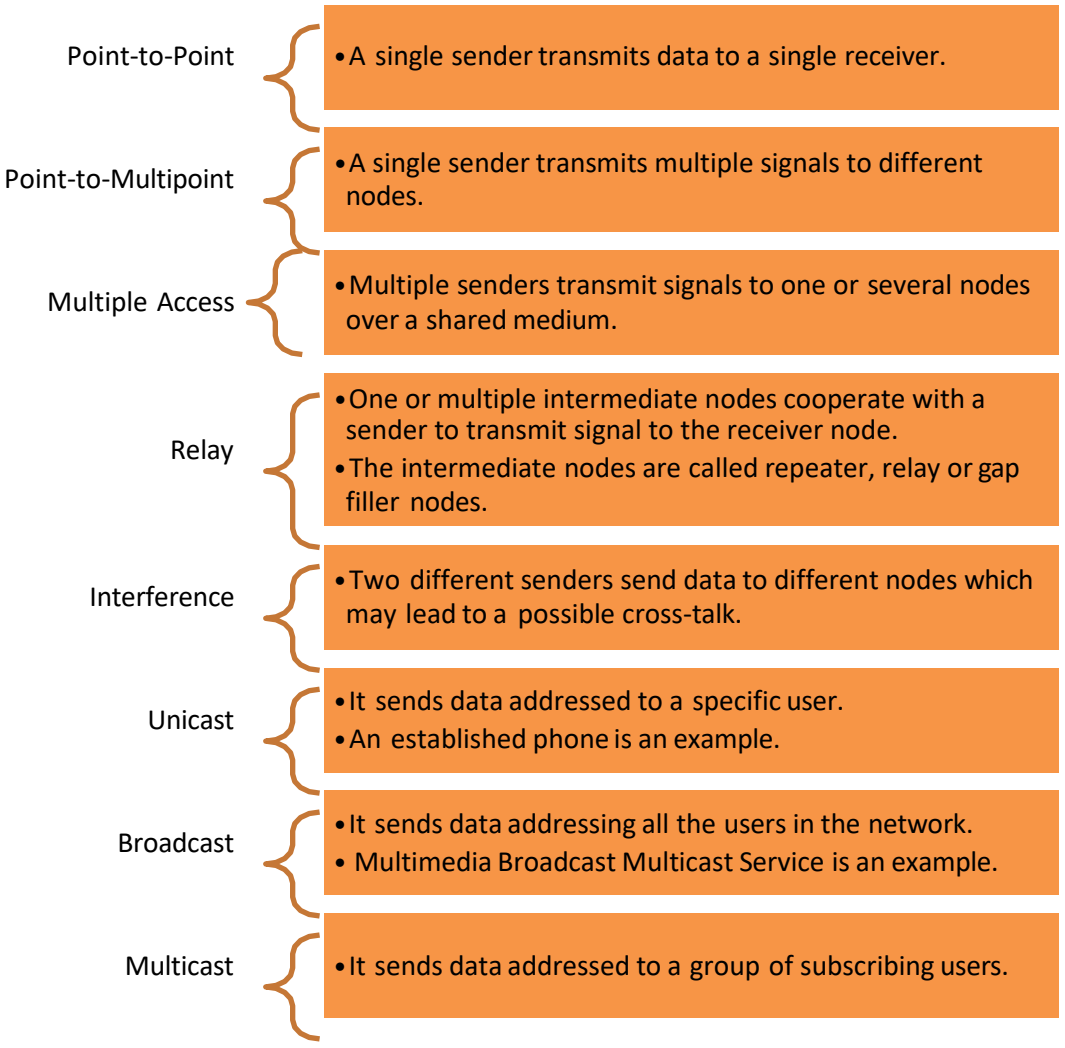


Fig. 2.3.1: Types of channels

2.3.2 IoT Cloud Framework

The deployment of the connected devices, applications, storage, power and intelligence is shifting from endpoints such as desktop computers and laptops to the cloud systems. The cloud-based services provide platforms to deploy and manage IoT applications and collect, store and analyse data from smart, connected product endpoints. These platforms provide scalability and easy access to third-party applications and services.

The IoT cloud is a platform that can run the applications and store data on the Internet. The technology used by it is also slightly different. For example, the cloud platform of Microsoft runs Windows Azure not the Windows Server.

The following figure shows the Azure framework:

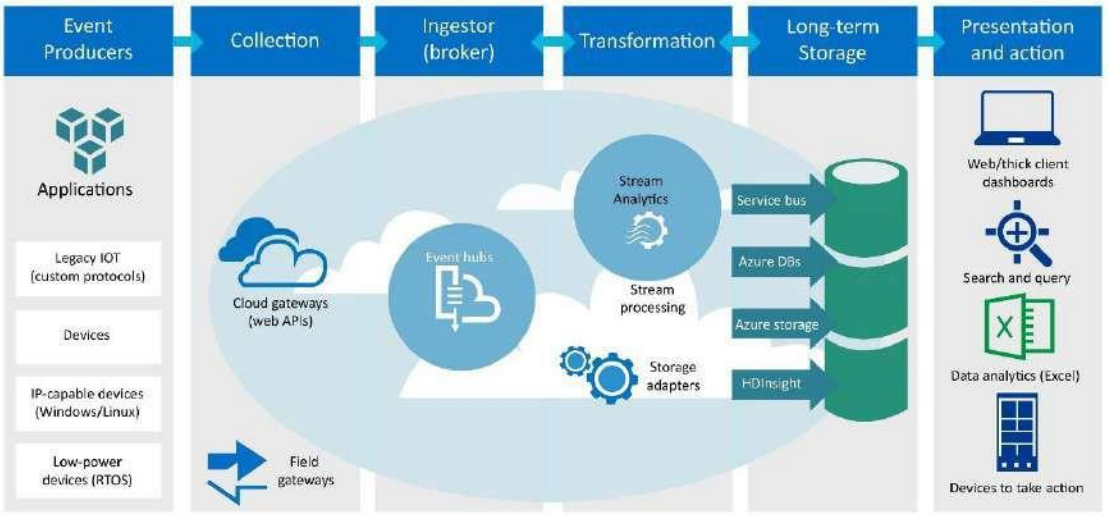


Fig. 2.3.2: Azure framework

Microsoft Azure Stream Analytics is a cloud service for real-time data processing. It helps to do real-time computations on data streaming from various devices, application and sensors. It supports high-level languages, such as sequential query language (SQL), which simplify the logic to act in real-time. It helps to monitor and achieve analytic insights from various devices that includes mobile phones as well as connected cars.

The following figure shows the stages of IoT data management in cloud platform:

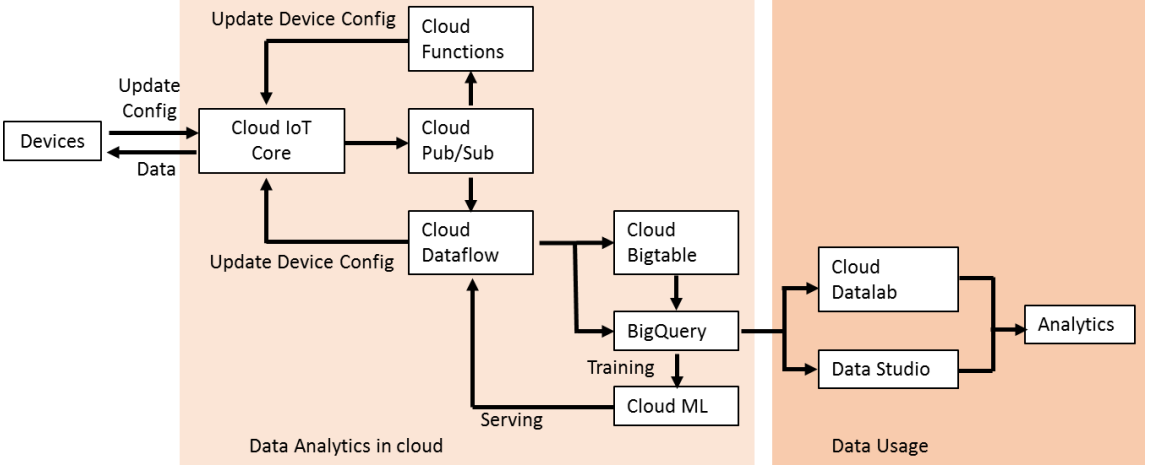


Fig. 2.3.3: IoT data management in cloud platform

Click/Scan this QR code to view the video on Data Management in IoT

2.3.3 Sensor Gateway and Channels

A sensor node is a node in the sensor 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 shows a WSN:

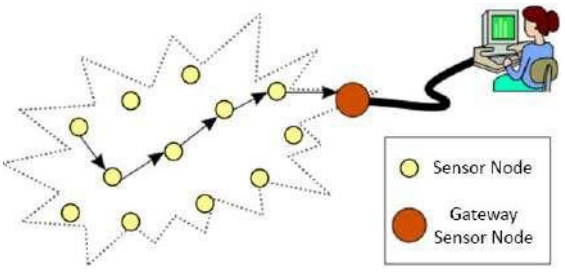


Fig. 2.3.4: WSN

The following figure shows the structure of a sensor node:

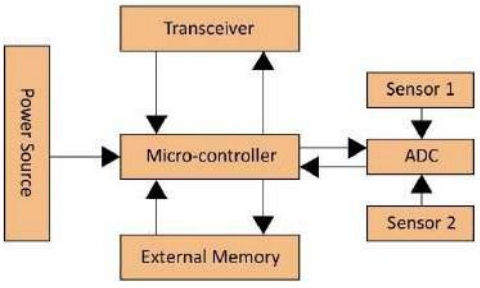


Fig. 2.3.5: Structure of a sensor node

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.

Sensors

Sensors are hardware devices which generate a measurable response as a result to any variation in physical conditions, such as temperature or pressure. The analog signal generated by the sensors is digitized by a converter and transmitted to the controllers for processing.

Gateway

The gateway is the bridge in between the sensor network and the Wi-Fi or other networks.

Channels

A sensor has multiple channels in which data is handled. In the channel settings, the type of display of data can be defined. Data may be displayed in graphs, gauges and tables. The following table lists some of the various sensor channel settings:

Name	A meaningful name should be entered to identify the channel. The name appears in graphs and tables.
Unit	It shows the units for the values of the sensor output.
Value Lookup	A file should be selected to be used with a specific channel.
ID	It displays the IDof the channel. It cannot be changed.
Graph Rendering	It defines if the channel will be viewed in graphs.
Table Rendering	It defines if the channel will be viewed in tables.
Line Colour	It defines the channel colour displayed in graphs.
Limits	It defines the thresholds for the channel. It has: • Upper Error Limit • Upper Warning Limit • Lower Error Limit • Lower Warning Limit
Error Limit Message	The message is shown whenever the error limits are crossed along with the error status.
Warning Limit Message	The message is shown whenever the warning limits are crossed along with the warning status.

Table 2.3.2 Sensor channel settings

2.3.4 Sensor Connectivity

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 following figure shows a sensor connectivity model:

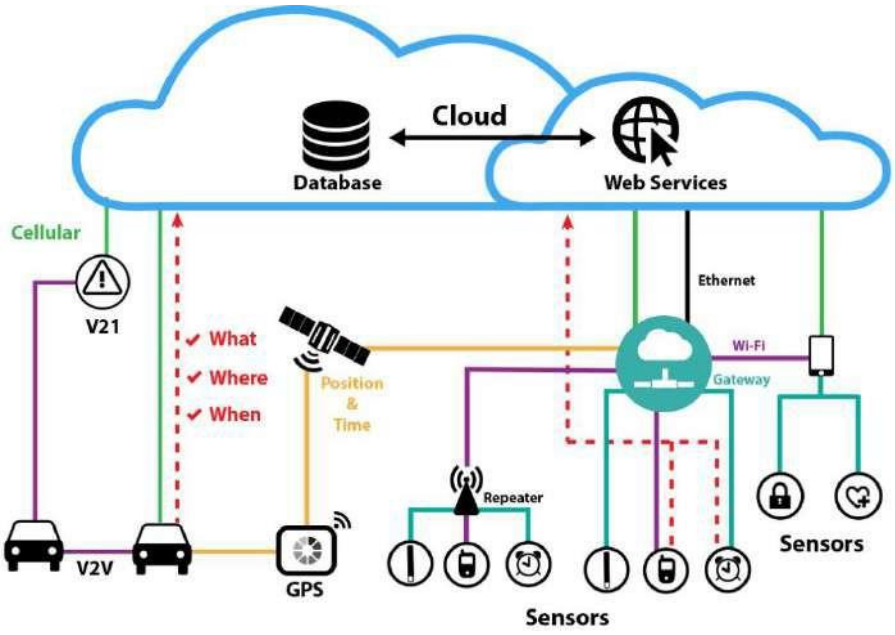


Fig. 2.3.6: Sensor connectivity model

The following figure shows the topology used in the communication technologies of IoT framework:

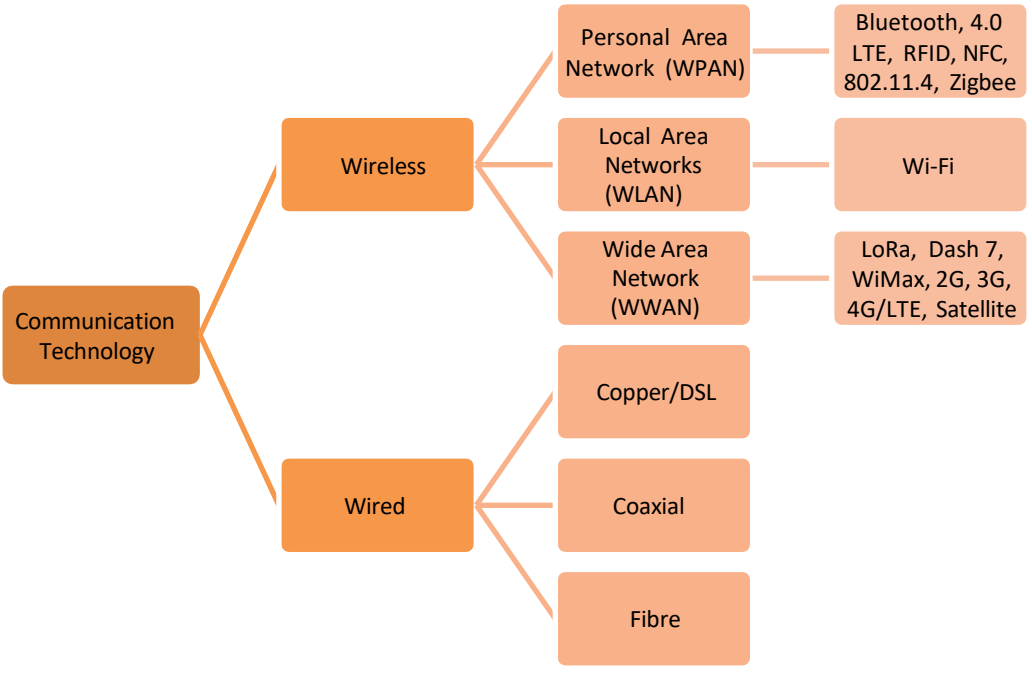


Fig. 2.3.7: Communication technologies

The following table differentiates the technologies according to their characteristics:

	Personal Area Network	Local Area Networks	Wide Area Network	Wired
Range	Short	Intermediate	Long	Long
Bandwidth	Narrow	Broad	Intermediate/Broad	Intermediate
Battery Life	Long	Short	Intermediate	Short

Table 2.3.3 Types of networks

The data created in the sensors and other devices are sent back to the central application over the network. The data creation standard and the communication medium must be determined. For delivering the data back, some protocols such as MQTT, HTTP and CoA P are used.

The following figure shows the protocols:

HTTP facilitates exchanging of data back and forth between central systems and the devices. In low bandwidth, HTTP is less suitable as it includes more data in the data headers of the messages.

MQTT was developed for the deployment of IoT and machine-to-machine. It is based on publish / subscribe model to pass the messages out from the device back to a central system, where they can be transferred back to all of the other devices that will consume them.

CoAP works well in less power, low-bandwidth environments. It is suitable for one-to-one connections.

Fig. 2.3.8: Protocols

Exercise

Answer the following.

1. List the different types of communication channels.

2. Briefly explain WSN along with its applications.

3. Fill in the comparison details for the networks.

	Range	Bandwidth	Battery Life
PAN			
LAN			
WAN			
Wired Network			

2.3.5 Ethernet Connectivity Options

For establishing a network connection in an IoT framework, a basically wired or wireless network connection is required. A wired connection requires Ethernet cable connectivity.

Ethernet is a network protocol which defines a standard way to connect computers on a network over a wired connection (LAN). The most common LAN technology used in present time is the Ethernet.

The following figure lists the characteristics of Ethernet:

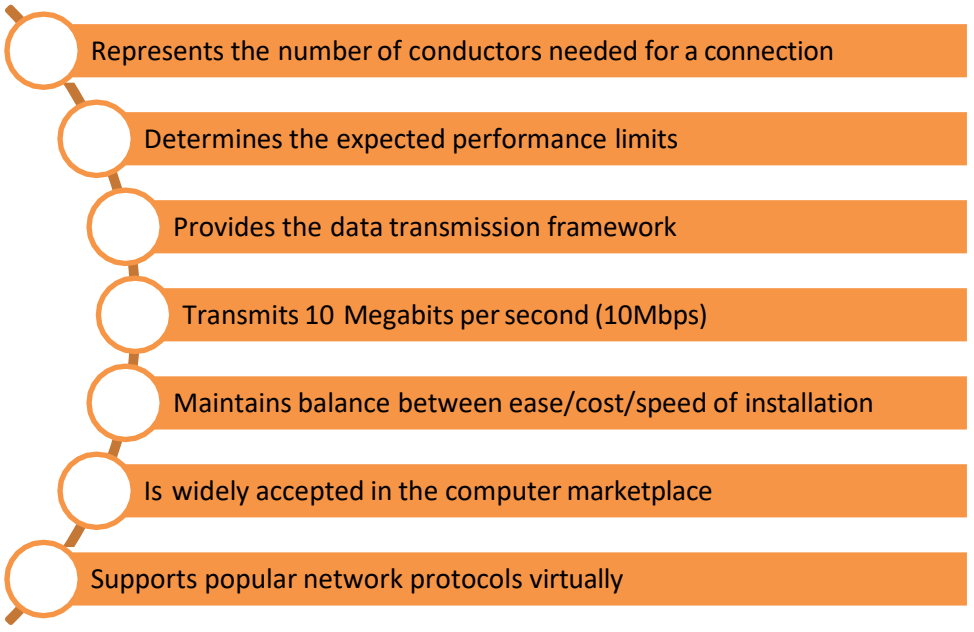


Fig. 2.3.9: Characteristics of Ethernet

The following figure lists the types of Ethernet:

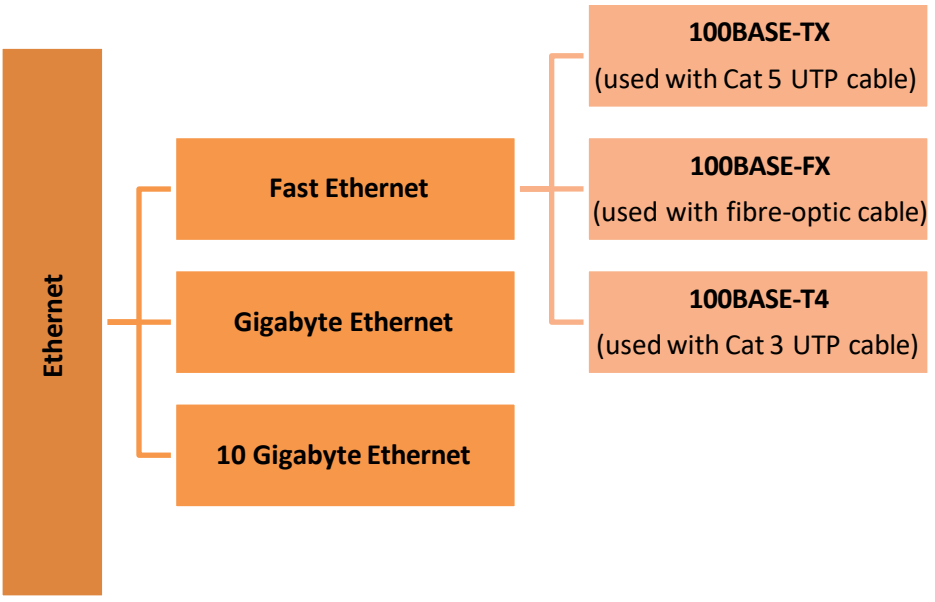


Fig. 2.3.10: Types of Ethernet

Each of these protocols support taking information or updates from an individual device and sending it over to a central location. However, where there is an opportunity, thedata is stored and used in the future. There are two main concerns here; how the data is acted upon as it comes into the application, and how it is stored for future use. The following table compares the different types of cables and Ethernet connections:

Type of Cable	Ethernet Connection	Transfer Rate
Twisted Pair	Ethernet	10 Mbps
	Fast Ethernet	100 Mbps
	Gigabit Ethernet	1000 Mbps
Coaxial Cable	Thin Wire Ethernet (10base2)	10 Mbps
	Thick Wire Ethernet(10base5)	10 Mbps
Fibre-optic Cable	10baseF	10 Mbps
	100baseFX	100 Mbps

Table 2.3.4 Types of Ethernet cable

WLAN Standards

Institute of Electrical and Electronics Engineers (IEEE) has created some standards for WLAN. Wi-Fi is known by the number 802.11. Different frequency and speed bands are denominated by the letters mentioned afterwards.

The following figure lists the standards:

802.11

- 1-2 Mbps speed with a band of 2.5 GHz
- Due to the standards being old, most products in the market are not supported by it
- The mentioned standards have a slow speed

802.11a

- An amendment to original rules, it came into the market at a second place
- has range of operation of 5-6 GHz, giving an advantage over lesser interference
- Uses Orthogonal Frequency Division Multiplexing(OFDM), giving greater resistance to interference with radio frequency; this helps in attaining a greater speed of 54 Mbps

802.11b

- First networking cards (wireless) in market
- Operates at a range of 2.4 GHz and at 11Mbps or some operate at 22 Mbps
- Mbps speed tends to diminish in case of signal quality issues
- Complementary Code Keying modulation used in this standard has lesser chances of interference in multi-path propagation and rates of data are higher or duplicate signals bounces off the walls

802.11g

- Considered better than the 802.11a and 802.11b
- Operates at a range of 2.4 GHz with high data rates of 54 mbps covering limited distance.
- Some forms go up to 100/125 Mbps

802.11n

- This promises to put out 100 Mbps, and is predicted to give a better operating distance than current networks

Fig. 2.3.11: WLAN standards

2.3.6 Connecting IoT Devices to the Network

To connect the devices to a wired network, cables must be prepared. Generally, RJ-45 cables are required for Ethernet ports. The cables and connectors must be crimped for this purpose.

Crimping

Crimping means joining of two pieces of metal, generally a wire and a connector, together by deforming one of them and enabling one to hold the other. The resultant deformity is known as a crimp.

The following image shows the various steps involved in crimping:

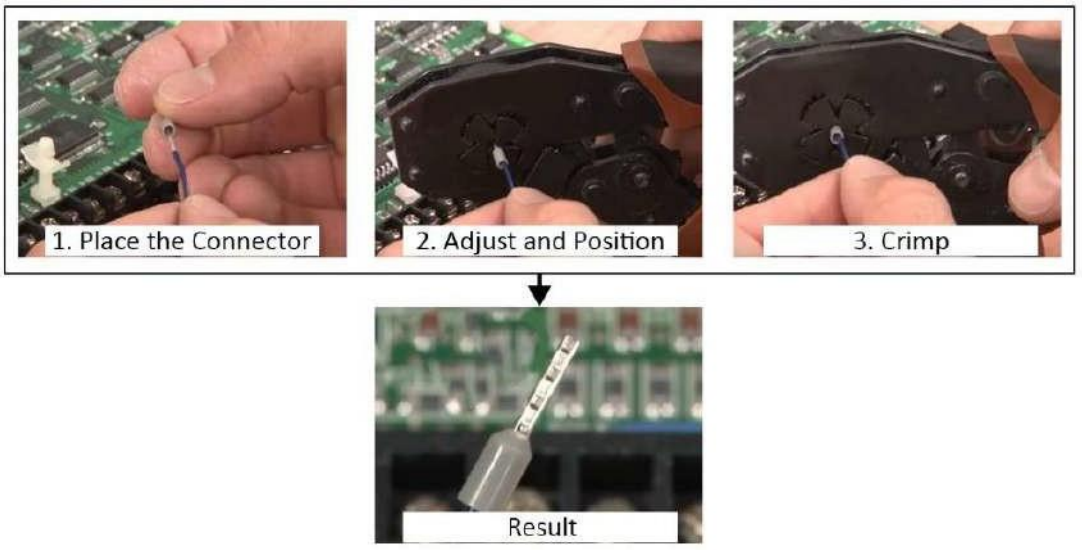


Fig. 2.3.12: Crimping

Tips

- In case of crimping, pliers should not be used as the deformity cannot be formed properly.
- If there is air in between the crimp and the connector, it collects moisture. This eventually causes corrosion in the wire and can lead to a connection failure.

Steps 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 following figure:

Fig. 2.3.13: Colour code for crimping RJ45 straight cable

- To make a crossover cable, the colour code is listed in the following figure:

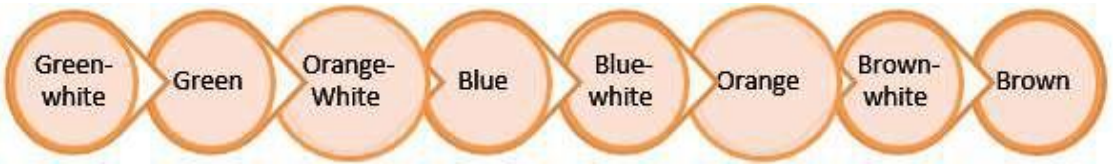


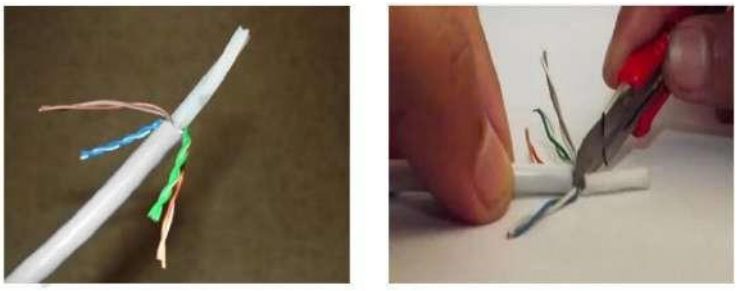
Fig. 2.3.5: Colour code for crimping RJ45 crossover cable

The steps for crimping an RJ45 cable are as follows:

- **STEP 1:** Strip 2 inches of the outer cover from the cable end with a utility knife as shown in the following image:

Fig. 2.3.14: Stripping the cable

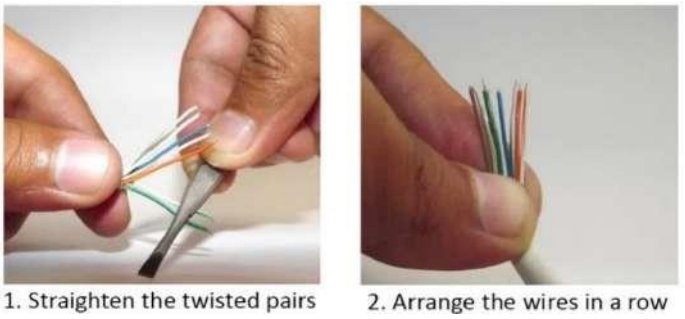
- **STEP 2:** Pull the twisted pairs of wires backward and cut the core as shown in the following image:



1. Pull wires backward 2. Cut the core

Fig. 2.3.15: Cutting the core

- **STEP 3:** Make the twisted wires straight using tweezers and keep them arranged in a row as shown in the following image:



1. Straighten the twisted pairs 2. Arrange the wires in a row

Fig. 2.3.16: Straightening and arranging the wires

- **STEP 4:** 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 shown in the following image:

Fig. 2.3.17: Trimming of wires

- **STEP 5:** The wires are to be inserted into an RJ-45 connector. 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 shown in the following image:

Fig. 2.3.18: Crimping the connector

Tips

- At the time of inserting the wires into the connector, it is to be made sure that the coloured wire goes into the channel appropriate for that.

Connecting Devices Using Wired Ethernet

The gateway has Ethernet ports that are used to connect wired devices. The technician should perform the following steps:

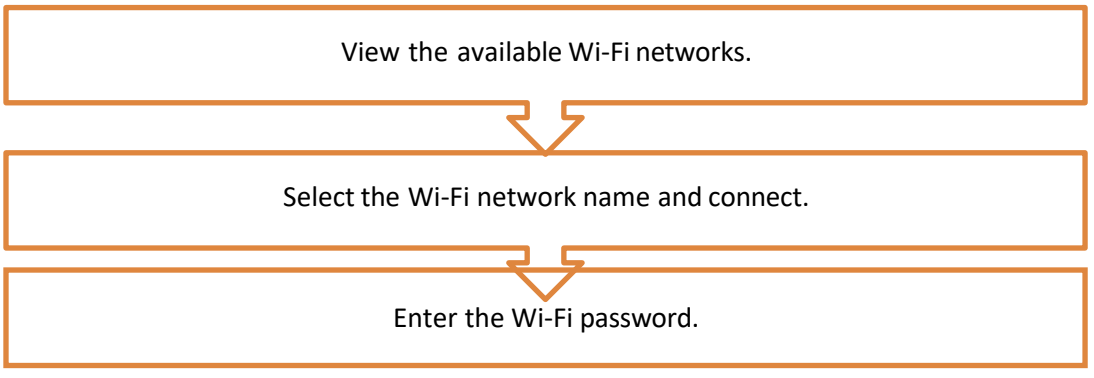
- Connect one end of the Ethernet cable to the Ethernet port as shown in the following image:

Fig. 2.3.19: Ethernet ports

- Connect to the WAN or Internet, if it is a modem. Otherwise, the LAN ports are connected for a router.
- Connect the other end to the port on the device.
- Configure the Ethernet settings in the device.

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, the steps that should be performed are shown in the following figure:



2.3.7 Configure Network Settings

The main aspect in the IoT system is Internet connectivity. The network settings in the devices must be configured so that the devices can connect to the network. In most of the devices, the network is configured automatically using a Dynamic Host Configuration Protocol (DHCP). But, if it is not done automatically, the settings need to be configured manually.

To check whether the network is connected or not, certain steps should be performed as shown in the following figure:

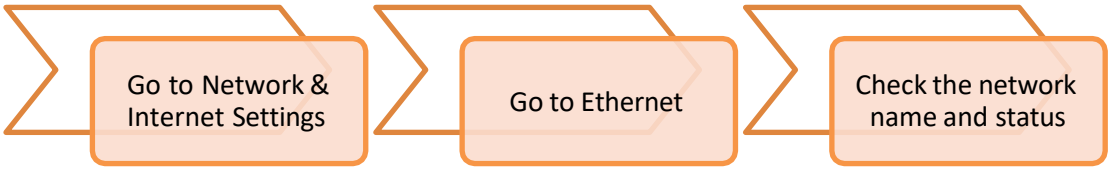


Fig. 2.3.21: Steps to check the network connectivity

The following image shows the network status in a Windows laptop:

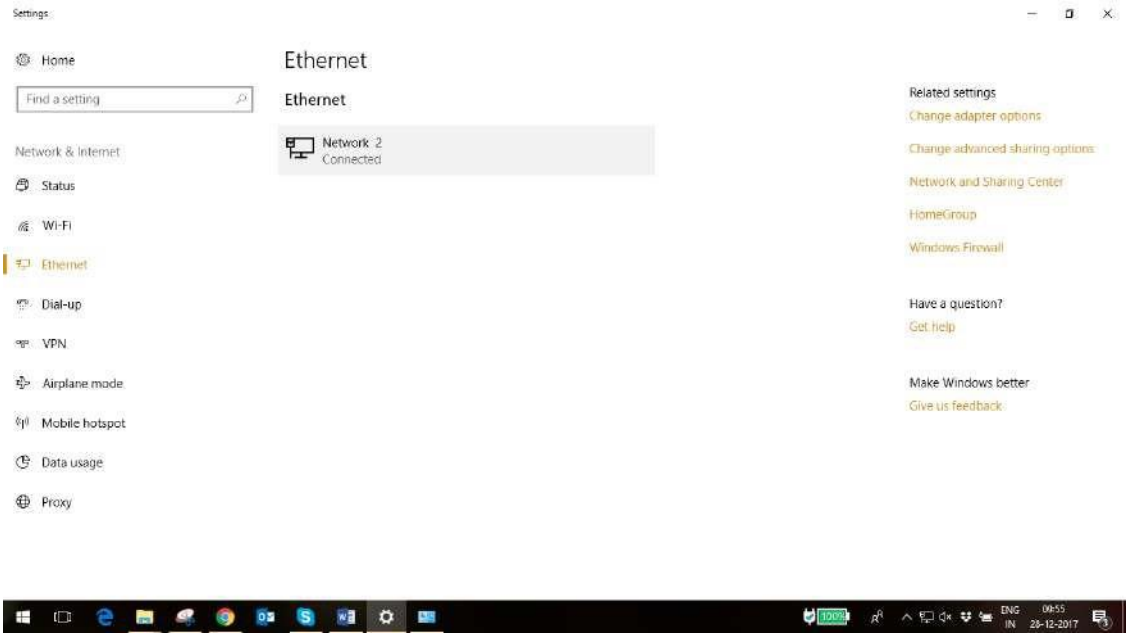


Fig. 2.3.22: Steps to check the network status in Windows

The steps for configuring the network are as follows:

- **STEP 1:** The Network & Internet window is to be opened. The following image shows the various options under the Network & Internet:

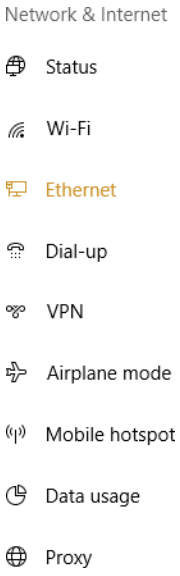


Fig. 2.3.23: Network & Internet window

- **STEP 2:** The interface that needs to be configured (Ethernet or Wi-Fi) should be clicked. In the above image Ethernet is selected.

  Then Network and Sharing Centre is to be opened as shown in the following screenshot:

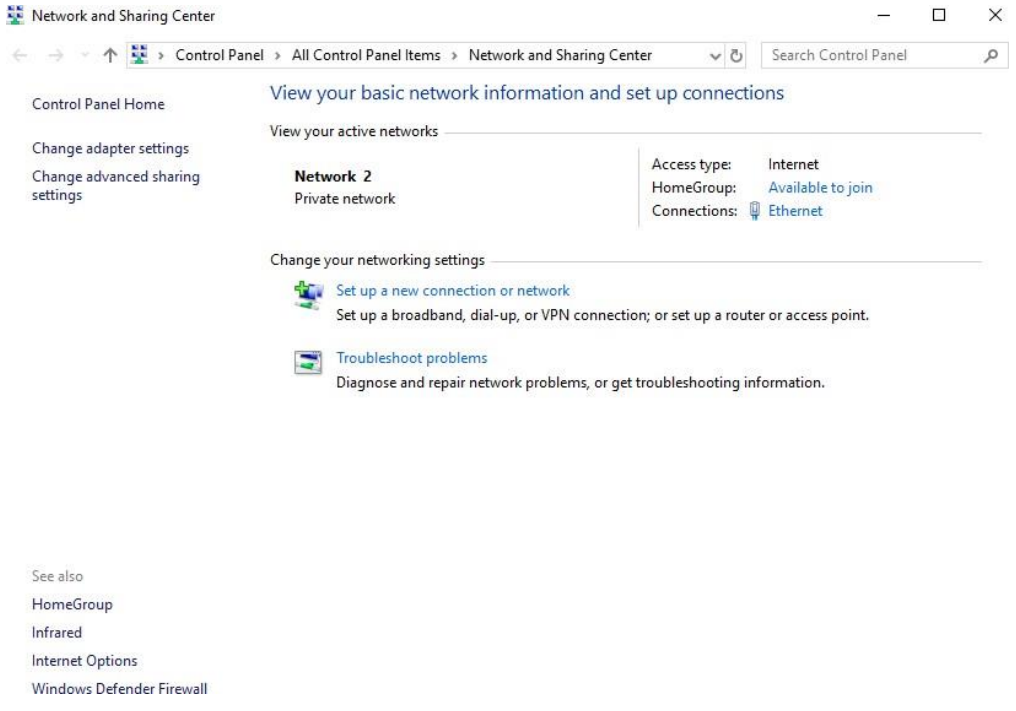


Fig. 2.3.24: Network and Sharing Centre window

- **STEP 3:** The window as shown in the following screenshot will appear after clicking "Set up a new connection":

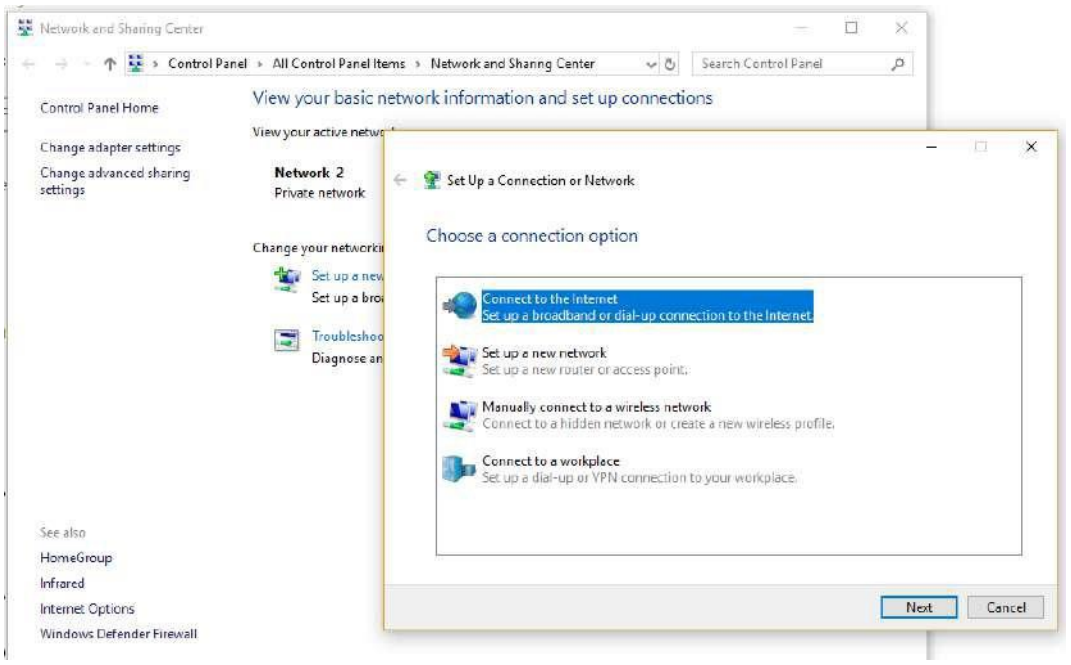


Fig. 2.3.25: Set up a connection window

- **STEP 4:** Various connection options appear as shown in the following screenshot. The desired option should be clicked:

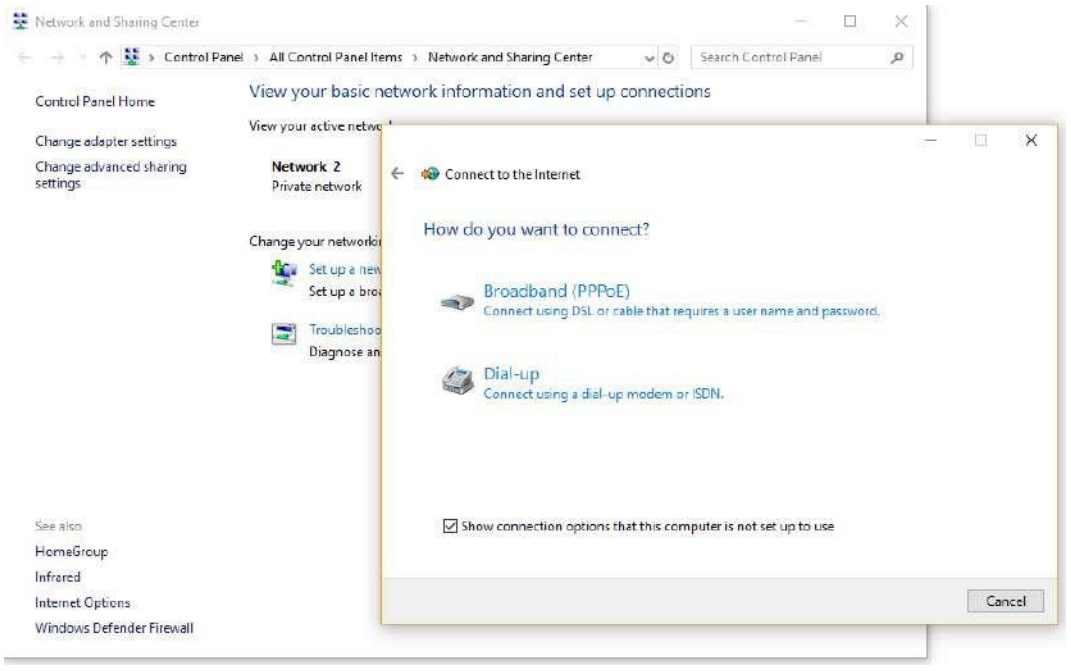


Fig. 2.3.26 Internet connection options

- **STEP 5:** The information as shown in the following screenshot must be entered to connect to the network:

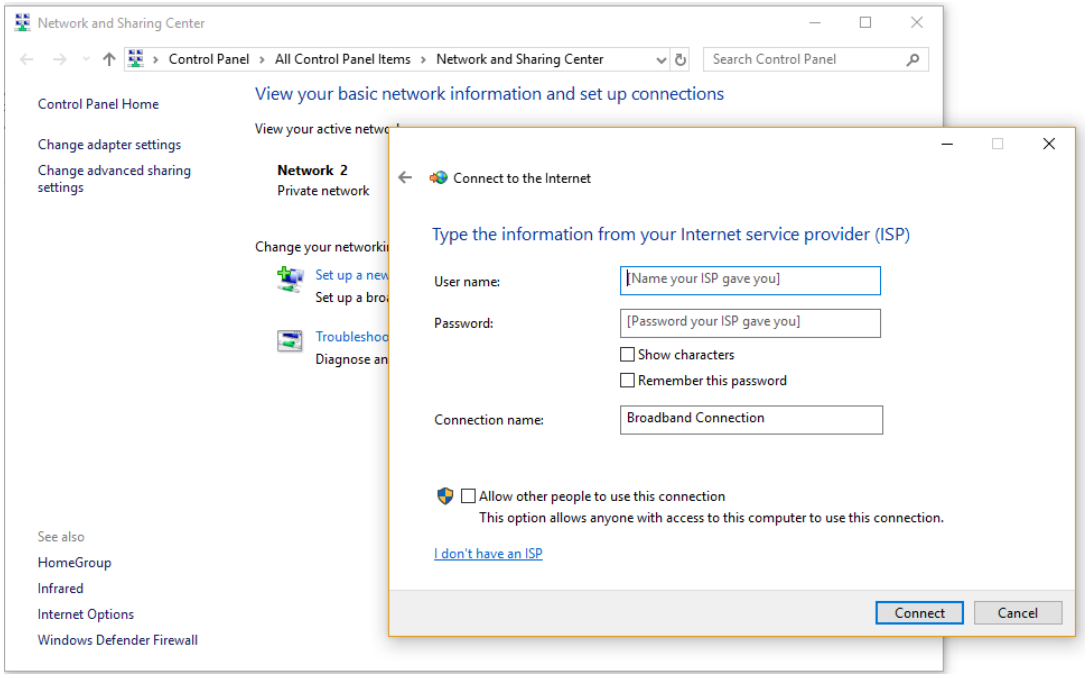


Fig. 2.3.27: Entering connection information

- **STEP 6:** The following screenshot shows the Ethernet Properties window in which the "Internet Protocol Version" must be double-clicked:

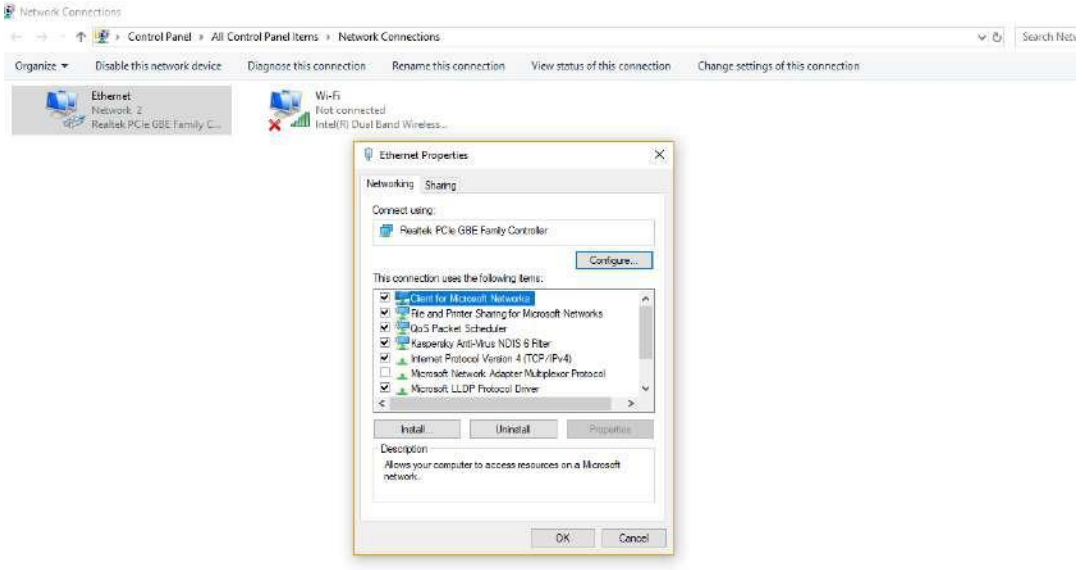


Fig. 2.3.28: Ethernet Properties window

- **STEP 7:** The information of the network must be entered to connect to the network. The following screenshot shows the Internet properties window:

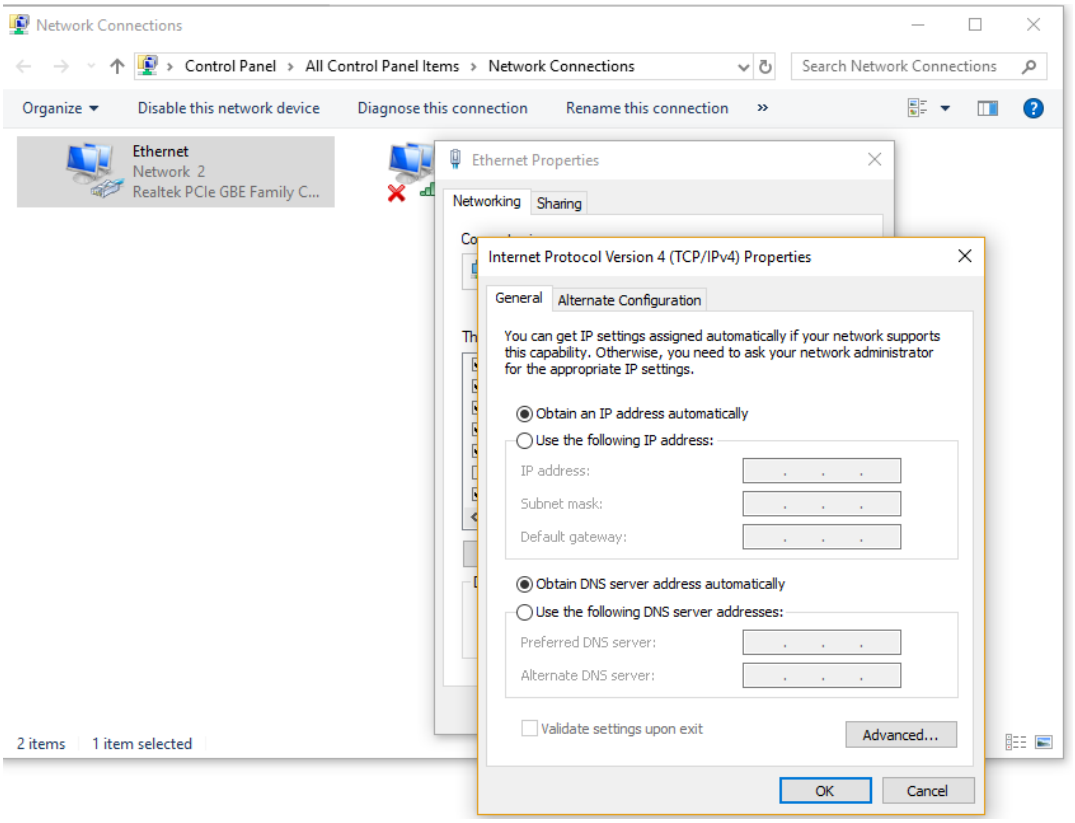


Fig. 2.3.29: Internet properties window

2.3.8 Overcoming Challenges of Ethernet Connectivity

There are some challenges that are to be faced with Ethernet connections. The wired connection needs lots of wires and infrastructure to be set up. In wireless connection too, a minimum set of wires and good infrastructure are required. The impediments in Ethernet connectivity and the ways to overcome them are as follows:

- **Managing Traffic in Ethernet Networks:** A broad range of traffic is handled by Ethernet network. Time-sensitive as well as cyclic data are passed between the devices. Ethernet wire also contains traffic from the sources such as network applications, protocols for network management and diagnostics and Ethernet data standards.

  Traditional techniques for traffic control are affected by the ongoing evolution of factory networks. For example, segmentation through properly configured and managed Ethernet switches is done. But, it is not possible to isolate all multicast and network management traffic from the devices.

  The issue can be handled by distinguishing the Ethernet traffic types using a purpose-built microprocessor and a proper mechanism. Time-sensitive data received from industrial Ethernet solutions are passed through the communications controller and then to a special channel, isolated from the regular traffic. It helps the data to reach the device application without any interruption.

- **Use of Router:** If the device is directly connected to the modem, it can face potential security risks. A router is used for that to protect the device from unauthorised access by discarding all data that were not requested. Internet Security program needs to be installed and it is to be made sure that the system firewall is enabled to minimize the security risks.
- **Network Failure:** Configuring the various components in a network may be complex, as there are many components interacting simultaneously. Some configuration may fail, and some may malfunction. The network adapters, drivers and the settings must be checked if there is a network failure.
- **Man-in-the-Middle Attacks:** IoT devices are vulnerable to Man-in-the-Middle attacks. It is not often feasible to utilize a specific software or configuration. Technologies such as Domain Name System Security Extensions (DNSSEC) may be useful in mitigating the risk. Applications that require high security utilizes a cellular communications channel, along with a private virtual private network (VPN) connection from the network providers to the IoT application. This allows greater control over the server.

Exercise

1. Fill in the blanks.
   - IP Address is _____.
   - Subnet Mask is _____.
   - Router is _____.
   - Proxy Settings is _____.

2. Write a short note on the advantages and the disadvantages of connecting the devices with wired Ethernet and with Wi-Fi.

_____

_____

_____

_____

_____

_____

UNIT 2.4: Authentication and Access Control Mechanism

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the importance of authentication and authorization in IoT
2. Explain access control system
3. Identify the software interface characteristics
4. List different software available for access control management
5. Describe how to secure wireless connection
6. Describe malware and distributed denial of service (DDoS) attacks

2.4.1 Importance of Authentication and Authorization in IoT

As Internet of Things (IoT) becomes an integral part of every enterprise, security becomes the major concern for all IoT systems. It is an unwarranted situation given the fact that more than half of all major business processes will have at least some element of IoT in them in future. This makes security of IoT systems a major concern, even if it means covering for only an inconsequential data.

What the edge device is in an IoT setup, depends on the use case. For example, in telecommunication industry, the edge would be a phone or a cell phone tower, whereas, in an automotive industry, an edge device would be an engine sensor or a car.

In the IoT use case, edge devices are designated to collect data – which can at times be massive – depending on the case, and send the collected data to the data centre or cloud, ideally for processing and analytics.

With edge computing, which is making IoT analytics even more real time, the data is processed locally, close to the edge device, so that the latency can be minimized. This results in transfer of data from the edge devices to the cloud or a remote data centre. With edge computing, data produced by the IoT devices and collected by the edge devices can be processed really close to where it is created, instead of being transferred over a long distance for processing.

It becomes important to secure and authenticate the network's edge, for this is where the enterprise's most sensitive information resides.

2.4.2 Authenticating the Edge Devices

Securing the edge device is necessary to confer confidence to the operation of an end to end IoT solution. For proper authentication, the edge should have a layer of identification security, over password or personal identification number (PIN).

The authentication can be based on biometrics or a combination of two or three security options. When identification and authentication credentials match, authentication is guaranteed. An IoT edge device security framework requires unique certificate identities for all devices interacting through a network connection.

It is a matter of utmost vigilance, hard work and planning to secure the edge devices against IoT security issues. Since the edge device is where the data converges and collects, it is the most high voltage point; so not everything here should be openly permissible. It i s important to control the convergence point with security policies and architectures. The following image shows authenticating edge devices in IoT:

Fig. 2.4.1: Authenticating edge devices in IoT

Begin with identification of devices to be secured and determination of what the devices are required to do within the cyberspace. Now, work closely with operational technology to secure the devices. Operational technology is in charge of control and automation technologies, but for beefing up security, both IT and OT must cooperate. Once in place, the two should be used to constantly monitor and check for possible security-related abnormalities, especially in the edge devices.

For example, if a security video camera shows HTTP requests being generated, the IT team should identify the route, go ahead, and block it if it is a threat.

Security Check List for Edge Devices in IoT

The following figure shows the security checklist for edge devices:

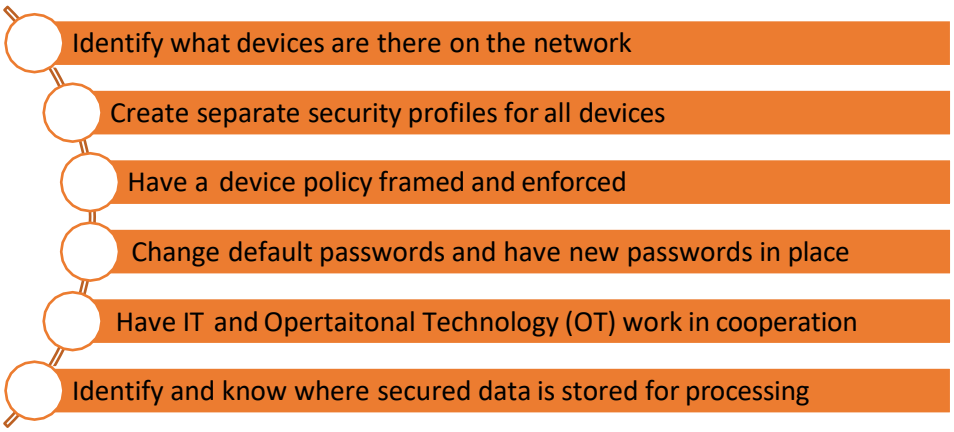


Fig. 2.4.2: Security check list for edge devices

It is recommended to identify the devices on a network and to perform continuous monitoring of the edge devices. The IT should know what edge devices are in the network, what information they are collecting and sharing and the potential risks that they are subject to in the environment, and then devise continuously working security solutions for the devices.

2.4.3 Security Challenges in Authentication

Most of the security risks in IoT are because of the nature of the edge devices, which, many believe, are designed to trust without verifying a connected source. It is thought, if all devices were to blindly trust each other to share data, then security is surely compromised.

In IoT, edge devices are small devices that are making more devices smart and connected. With connectivity, the risk of threats increases manifold. Today, the IoT security industryis in a nascent stage. It is at the same place where the PC era was when suddenly Internet connectivity gained momentum, and no one recognized at first the threats it posed, and the ways to secure them. Moreover, as of now, most IoT products lack security because the manufacturers are spending less time than required in making their products secure; the race is primarily to deliver the first product in the market. The following image shows security challenges in authentication:

Fig. 2.4.3: Security challenges in authentication

2.4.4 Authorization of the Edge Devices

It is crucial to delegate control and authority to arrive at a fundamental security principle. The edge devices might gain access to data and resources within their permissible scope or when it is architecturally possible. This means that the devices would have some permission by configuration and some enabled with architecture. Authorization here would mean providing role-based access control (RBAC) and certificate signing rights for better functioning of top security.

2.4.5 Access Control

Access control facilitates restricted access, achieved by certain groups, people or access levels. This assures the users easy and secure access to the facility. Intelligent locks, keypads, card readers and other related devices are generally used for access control.

Any malicious activity in the range of the access system triggers an alert and generates the detailed notification on the management software controller.

The devices are configured for different operating conditions, sensitivity, specifications and authority in control software. The control software is used as the controller for the entire framework. A duplicate control can be configured via a mobile app on mobile devices so that the notifications can be received in real time.

The following image shows a mobile app connected to a home alarm system:

Fig. 2.4.4: A mobile app connected to a home alarm system

Every authorised mobile device needs to use its unique Internet protocol (IP) address to get an access into the main controller for using the security system. The main server also possesses a unique IP address for establishing the communication among access control system components.

Access Control System Architecture

Access control for IoT can be implemented in two ways as shown in the following figure:

Fig. 2.4.5: Two ways of implementing access control

In a distributed architecture, the control server offers access tokens to the users, so that they can enjoy a direct access to the IoT devices.

The following figure shows the distributed architecture:

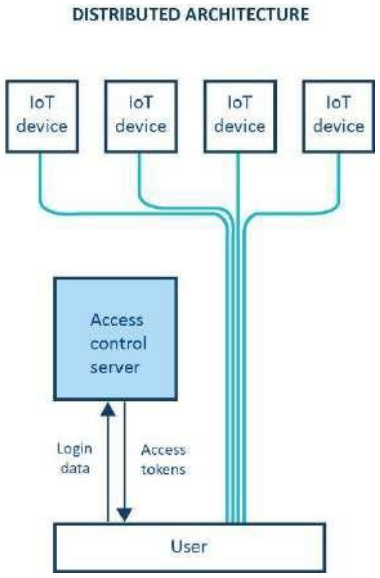


Fig. 2.4.6: Distributed architecture

In a centralized architecture, the users have the access to the cloud-based servers which then authorises the request of the users and relay data between the IoT devices and the user. The following figure shows the centralized architecture:

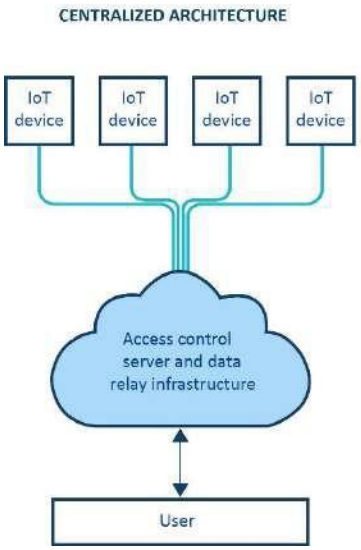


Fig. 2.4.7: Centralized architecture

It can be a challenging task to manage an access control system. To set up the system, a technician must have the knowledge of the following tasks:

- Adding a new access point to the control system
- Keeping the system secure
- Identifying the users and devices
- Troubleshooting the problems with the set up
- Ensuring that the servers are kept up to date
- Ensuring appropriate firewalls and the latest security patches are installed

2.4.6 Third Party Software for Access Control

The most important component of an access control system in case of IoT is the integration of physical and logical access, which means that the physical security system is linked with the logical assets.

There are various tools and software available in market for access control and security.

Courion Access Assurance Suite

It is comprised of several modules and every module performs a specific function. It has the following features:

- Enforces strong password policies
- Automates account creation, modification and disablement
- Remediates inappropriate and high-risk access

The following screenshot shows an access modification window:

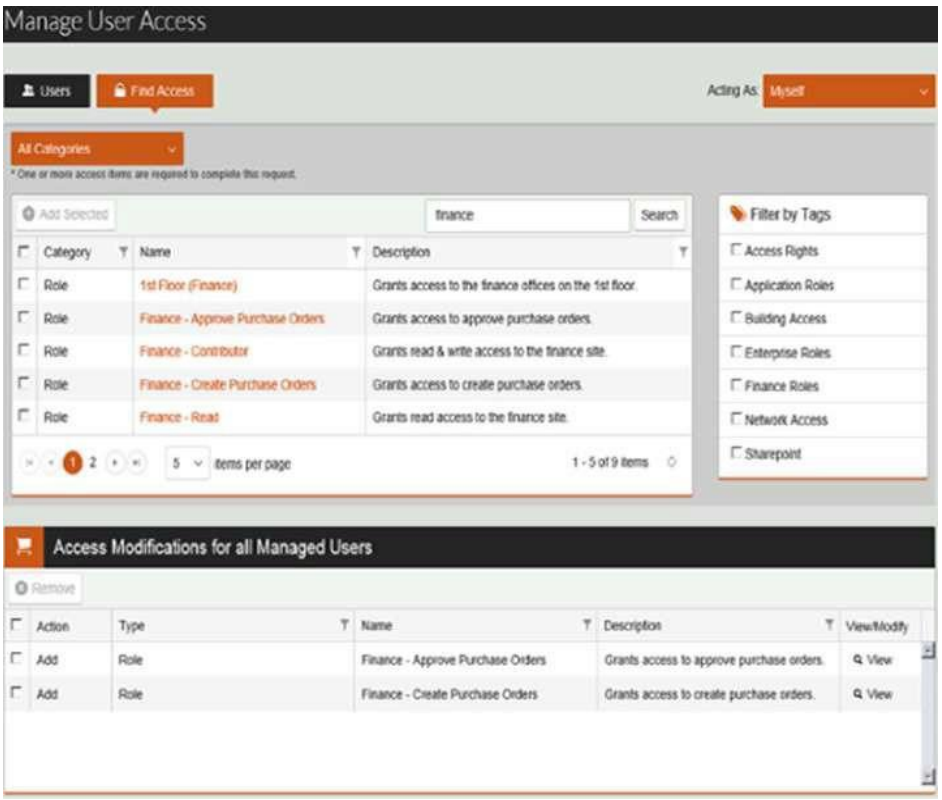


Fig. 2.4.8: Access modification window

Oracle Identity Governance Suite

This is suitable for large organisations. It utilizes analytics for managing the privileged account management, identity intelligence and user administration. It provides a simplified and customizable user interface that offers durability across patches and upgrades.

The following screenshot shows the Oracle Identity Self Service window:

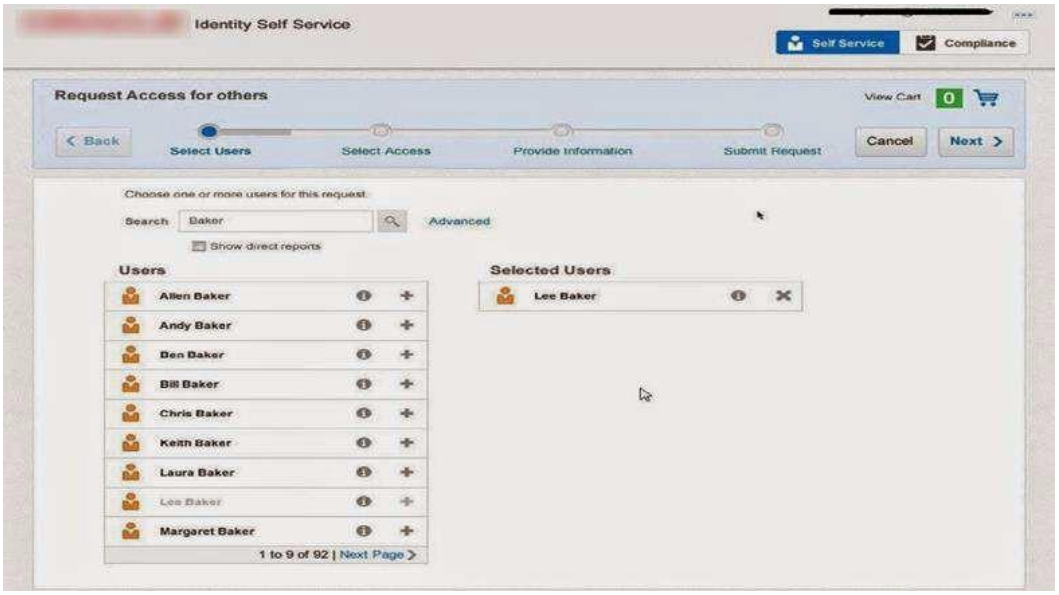


Fig. 2.4.9: Oracle Identity Self Service window

IBM Security Identity Governance and Administration

This suite integrates Security Identity Governance system and Security Identity Manager. It facilitates the following actions:

- User access management
- Identity management and governance

The following screenshot shows the login window of IBM Security Identity Governance:

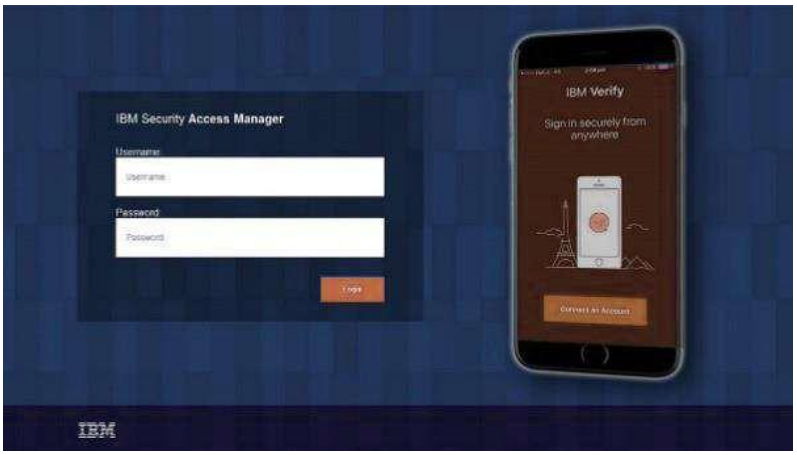


Fig. 2.4.10: Login window of IBM Security Identity Governance

Identity card Access Control

It provides customizable credentials and ID badges for authorised persons and thus enables access control.

The following screenshot shows an Identity card Access Control window:

Fig. 2.4.11: Identity card Access Control window

2.4.7 Control Access Using Security

The access control system provides security to the organisation by offering access only to the authorised people. The following image shows two examples of granting and denying access to a person:

Fig. 2.4.12(a): Access granted

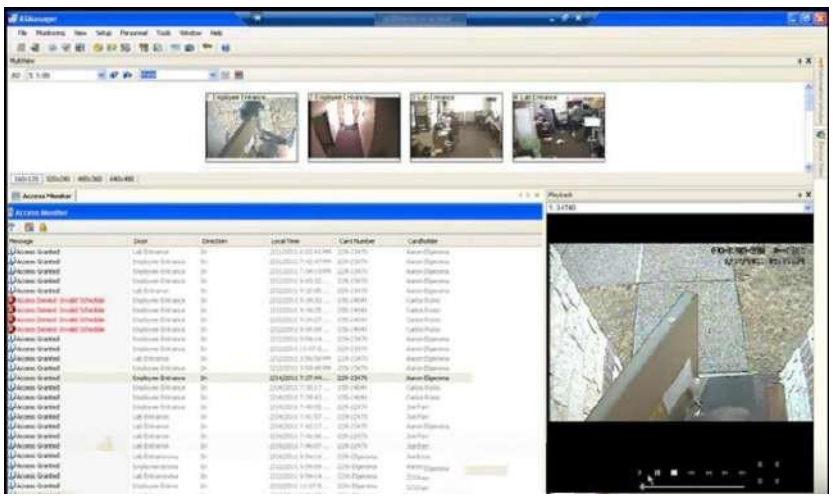


Fig. 2.4.12(b): Access denied

It is of high priority to ensure the following precautions:

- Eliminate risk with security tools
- Track everything with the software interface
- Set the remote access rules restriction options properly
- Use advanced authentication method for restricting the access to unauthorised users
- Set email connection notifications

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 the following screenshot:

Fig. 2.4.13: Software login window

- **Step 2:** Edit the controller settings by entering the network details and product details. The following screenshot shows the edit controller window:

Fig. 2.4.14: Edit controller window

- **Step 3:** Edit the device or machine settings. The following screenshot shows the device settings window:

Fig. 2.4.15: Device settings window

- **Step 4:** Create the time zone settings as per requirement. The following screenshot shows the time settings window:

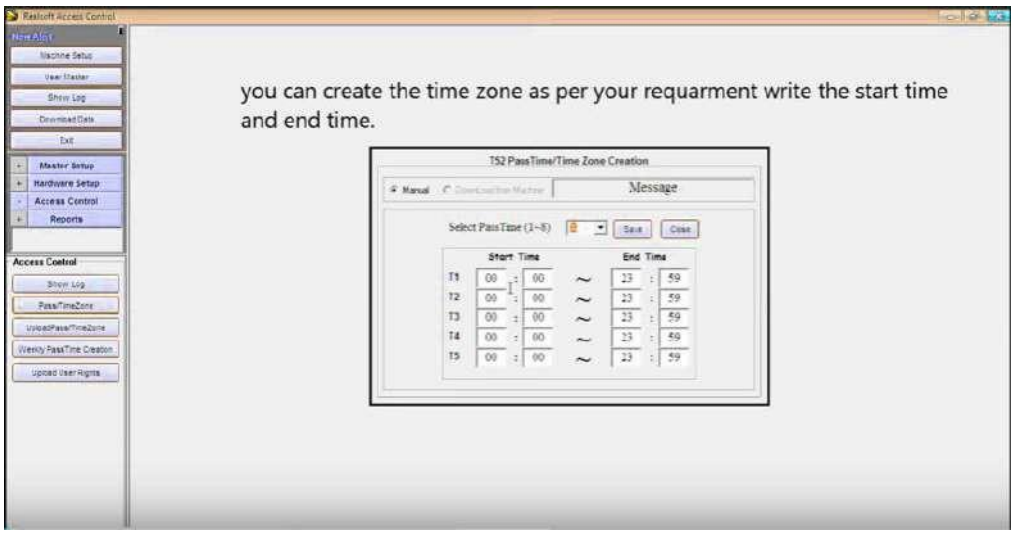


Fig. 2.4.16: Time settings window

- **Step 5:** Fill the employee records. The following screenshot shows the employee records window:

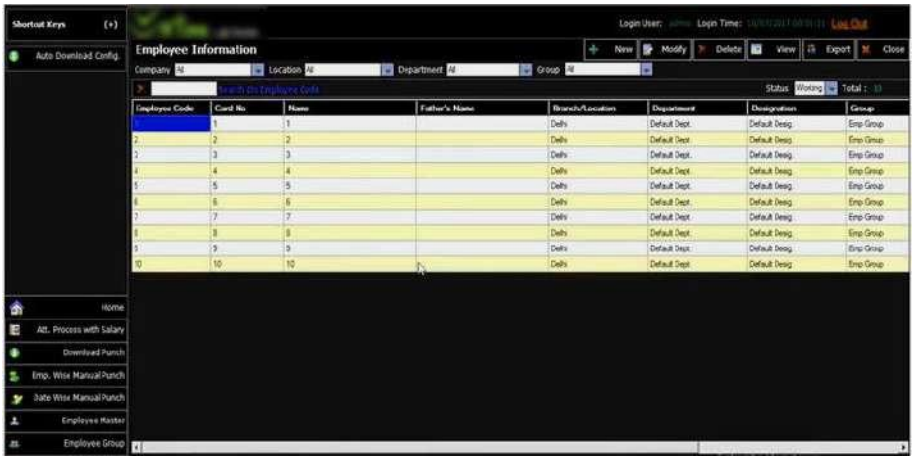


Fig. 2.4.17: Employee details window

- **Step 6:** Click on a row to create or update the employee details. The following screenshot shows editing the employee records window:

Fig. 2.4.18: Editing employee records window

- **Step 7:** Connect the device and select the time zone and upload it to the machine as shown in the following screenshot:

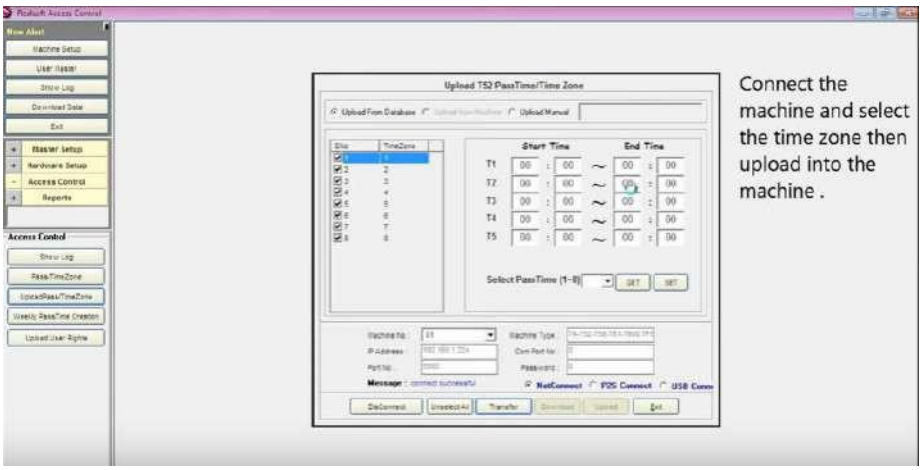


Fig. 2.4.19: Uploading time zone to the device

- **Step 8:** Upload the user rights to the device as shown in the following screenshot:

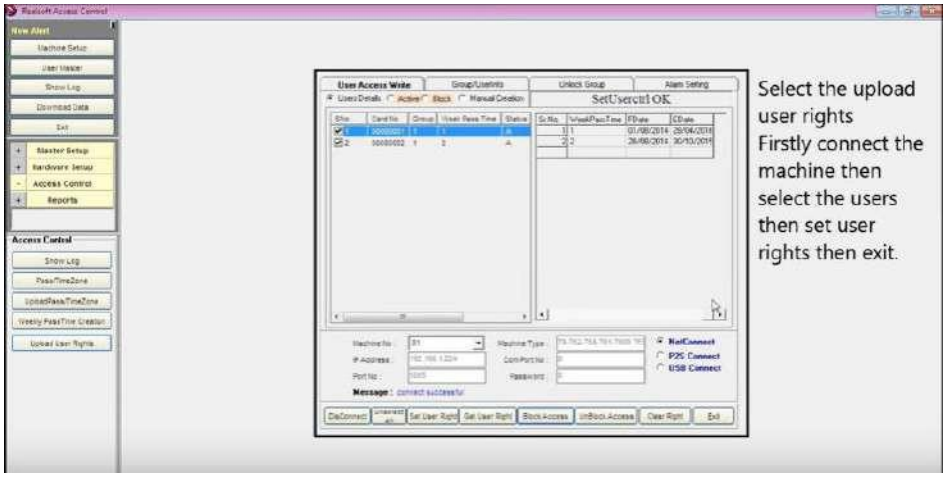


Fig. 2.4.20: Uploading user rights to the device

- **Step 9:** Generate report as shown in the following screenshot:

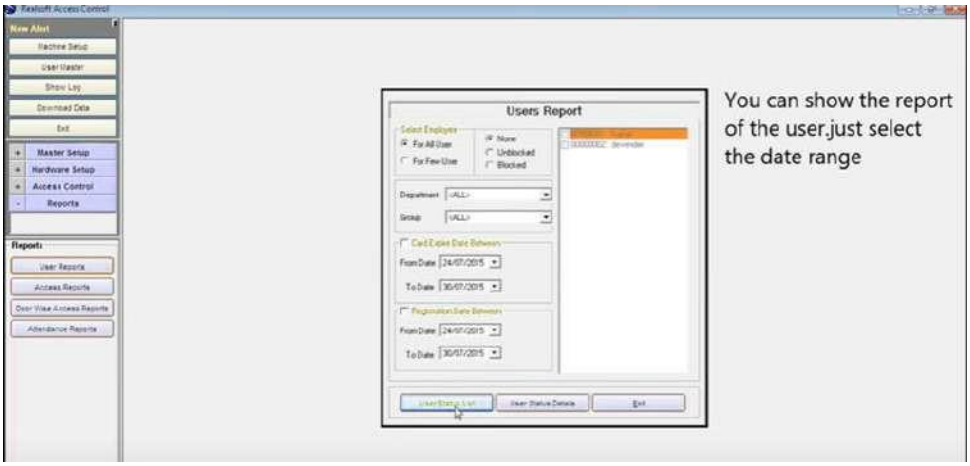


Fig. 2.4.21: Generating report

Securing Wireless Connection

Securing the network connection is very important. There are some ways to secure the wireless connection. They are as follows:

- The following default settings of the router must be changed:
  - Router password must be changed
  - IP address and the subnet mask should be updated
  - Remote management should be disabled

The following screenshot shows changing the default settings:

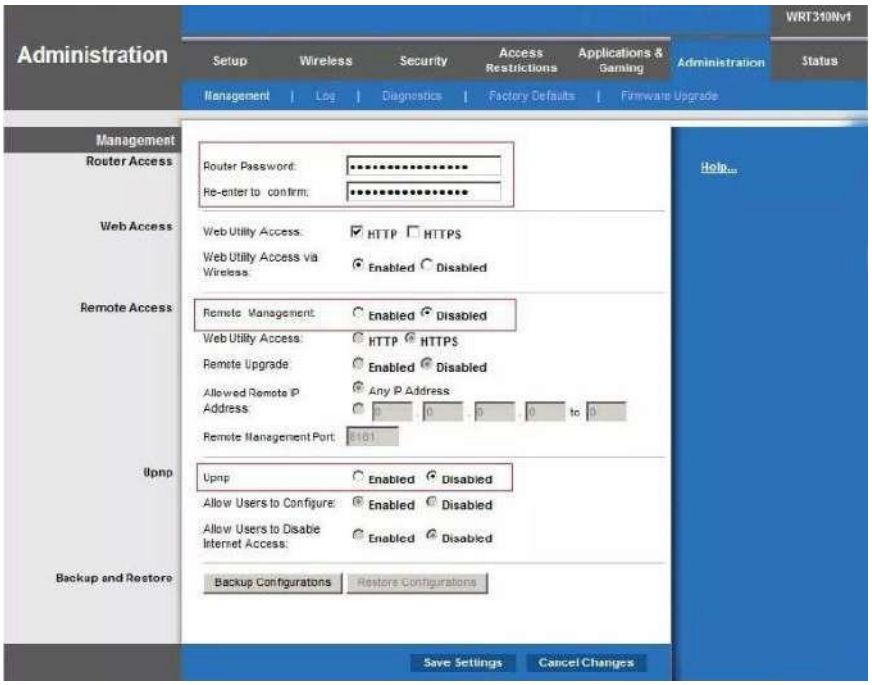


Fig. 2.4.22: Changing the router default settings

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

Fig. 2.4.23: Changing the wireless settings

- Reliable encryption standard must be selected. The following image shows the WAP2 selected as encryption method:

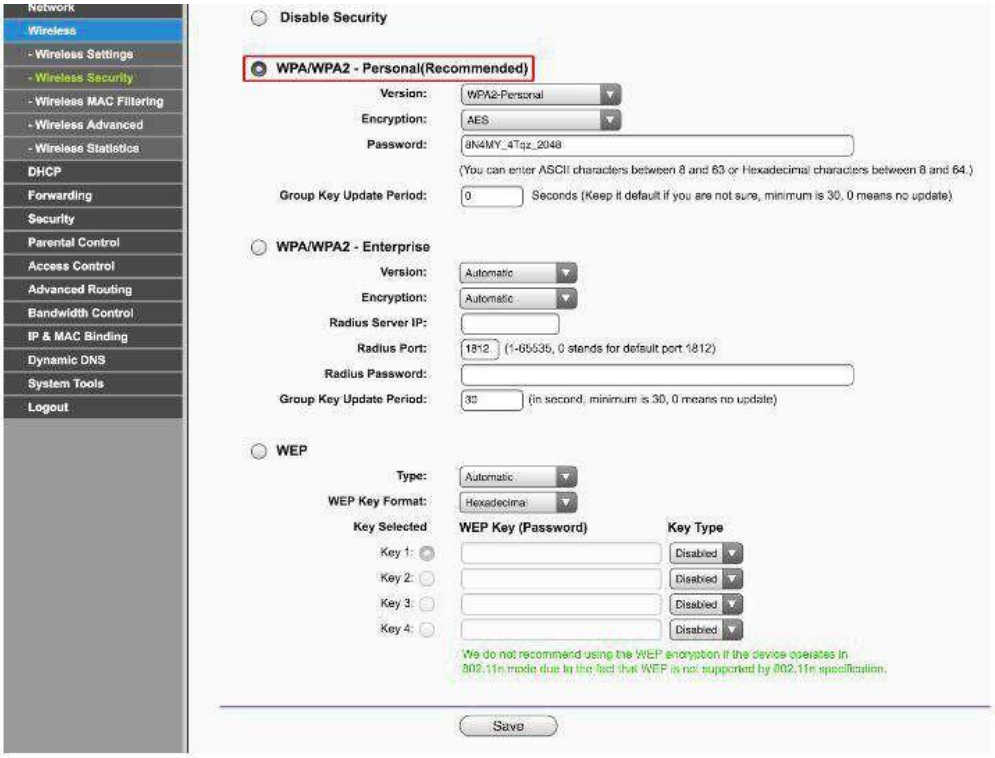


Fig. 2.4.24: WAP2 selected as encryption method

- Router firewall must be enabled and the firmware must be updated. The following screenshot shows the upgrading of firmware:

Fig. 2.4.25: Upgrading of firmware

2.4.8 Check for Malware and DDoS Attacks

Many IoT devices become soft targets and often victims of malware because of poor security. Most of the IoT malware targets the devices that are not PC embedded and does not have any advanced security features.

The following figure lists some symptoms that indicate that the device is malware affected:

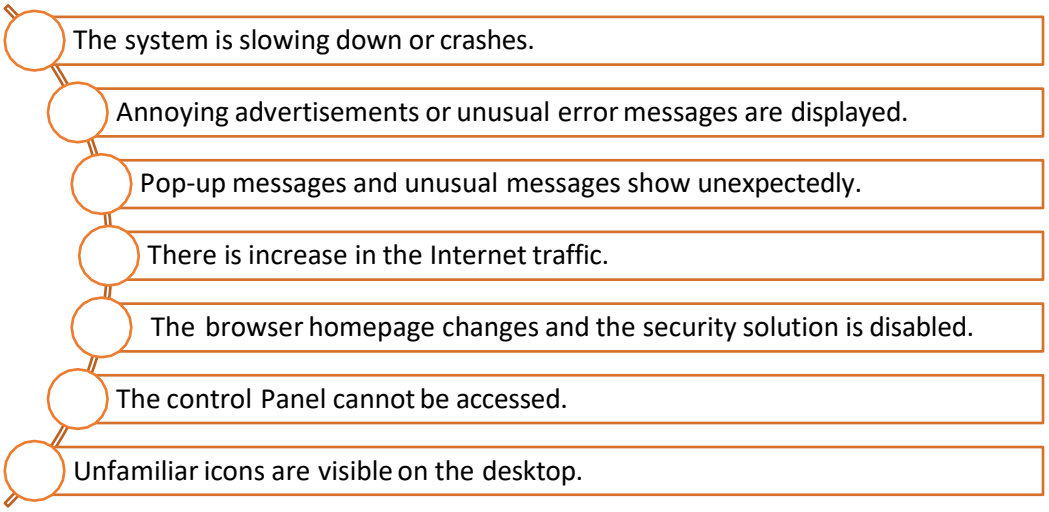


Fig. 2.4.26: Symptoms of malware affecting a device

The malware can be removed by performing the following actions:

- Deleting temporary files
- Running a malware scan
- Using a good antivirus software

DDoS is an attack in which a group of systems target a single target, causing denial of service for the users of the victim. The most common symptom in a DDoS attack is the flooding of the incoming packets to the victim. The steps for detecting DDoS in Windows are as follows:

- **Step 1:** Select start -> Select Run -> Type "cmd" -> Select OK.
- **Step 2:** In the command prompt type netstat – ano - netstat.txt and then press Enter key. The NETSTAT command displays the current TCP/IP network connections and protocol statistics in a system. The command is as follows:

  netstat -ano

  a – Shows the connections and listening ports.

  n – Shows addresses and port numbers.

  o – Shows the process ID related to each connection.
- **Step 3:** Check the total number of connection at port 80 using netstat -ano | find /i /c "80" command.
- **Step 4:** Check for the IP addresses with the maximum number of connections.
- **Step 5:** Block the access of such IP

Exercise

1. List some symptoms which indicate that the device is malware affected.
   1. _____
   2. _____
   3. _____
   4. _____
   5. _____
   6. _____

2. List the steps of installing an access control system.

_____

_____

_____

_____

_____

_____

Practical

Install a BMP280 temperature and pressure sensor on an Arduino.

Required Tools/Equipment:

- BMP280 temperature and pressure sensor
- Arduino board
- Connecting probes
- Bread board
- Plier
- Computer system

Practical

Check the power supply connectivity to an installed IoT camera.

Required Tools/Equipment:

- Power cables
- Installed IoT camera
- Power source
- Tool kit

Practical

Install a Viconics Wireless Gateway (VWG) and related wireless controllers, ensuring clear line of sight.

Required Tools/Equipment:

- An Ethernet adapter with TCP/IP support.
- Computer system with installed web browser
- Wireless TP link router and adapter

Practical

Connect Raspberry pi to another device through wired Ethernet.

Required Tools/Equipment:

- Router
- Ethernet cable
- Raspberry pi kit
- Connector
- Computer system

Practical

Identify suitable location perform installation of a motion sensor and CCTV camera at a site.

Required Tools/Equipment:

- Motion sensor device
- CCTV camera device
- Tool kit

Practical

Perform configuration of motion sensors with the network provided on the site.

Required Tools/Equipment:

- Installed motion sensors
- Installed internet network
- Router
- Computer system

Practical

Perform a power, Ethernet and other types of cable connections to a gateway on a site.

Required Tools/Equipment:

- Gateway with power cable
- Ethernet cable
- Tool kit

Practical

Perform connection of a sensor (nodes) and a router to through wired and unwired manner.

Required Tools/Equipment:

- An installed sensor
- A router with network connection
- Connecting cables
- Laptop

Practical

Perform preparation of an Ethernet cable and connector.

Required Tools/Equipment:

- Crimping tool, tweezer, cutting knife
- Network tester
- Ethernet cable
- Ethernet cable connector

Practical

Configure Ethernet connection on a Laptop/computer system.

Required Tools/Equipment:

- Ethernet wire
- Established network
- Laptop/Computer system with latest configuration

2.5 Pre-installation Preparation

Before performing the installation of the set up for an IoT device, which includes sensor gateway and nodes connection at the site, the technician needs to perform few pre-installation steps such as site analysis and assessment of the tools and equipment required for the installation of the IoT framework at the site. This helps to make sure that the installation is carried out effectively.

The following figure shows the pre-installation steps included in IoT device installation:

Fig. 2.5.1: Pre-installation steps

Analyse Site Requirements

First of all, the technician needs to understand the requirement of the site at which the IoT set up needs to be installed. By analysing the site, the technician would know the details such as suitable location for mounting the sensors, power source location and various other factors that contribute to the IoT framework. This would also help the technician to understand the tools and equipment required for the installation. After analysing the site, the technician can carry out the installation of the IoT set up at the site effectively.

The following image shows the points which are analysed by the technician before starting the installation:

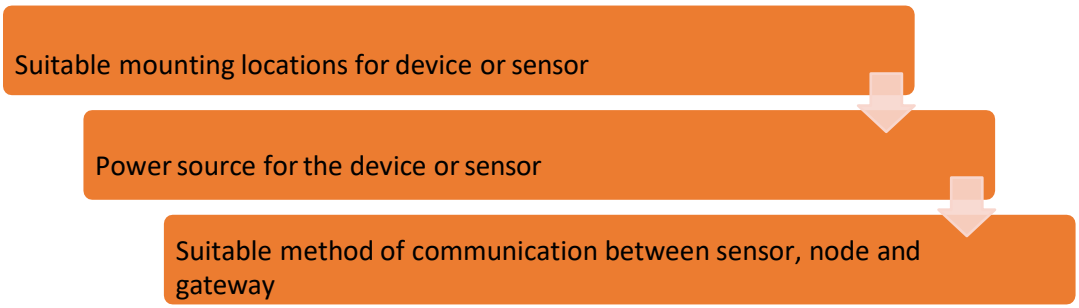


Fig.2.5.2: Site analysis

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 mounting location for 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 following figure shows a sample site log to be prepared after the site analysis:

Company Name

Address

Name of client:

Address:

Product detail:

Installation date:

Site details

Area: **Building material type:**

Location for mounting device: **Power source:**

Special site requirement:

Tools and equipment's needed

Tools required: **Equipment required:**

Special requirements:

Technician signature **Authorising person's signature**

Fig. 2.5.3: Site log

Understand Tools and Equipment Requirement for Installation

For installation of devices and sensors, the technician uses several tools such as a drill, a screw driver and a hammer as well as different equipment such as a signal tester and a multimixer. The technician should know the use and proper handling of these tools and equipment to perform the installation process.

To operate a drilling machine, the steps are as follows:

Step 1: Mark the point of drill on the wall. The following image shows the point to be marked:

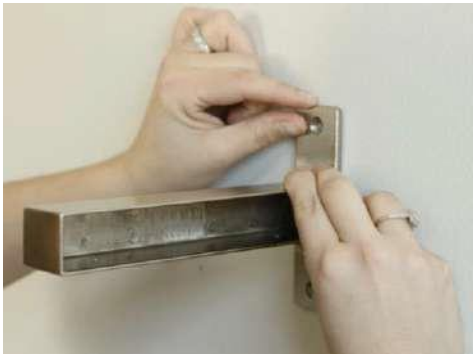


Fig. 2.5.4: Point to be marked for drilling

Step 2: Choose the drill bit and adjust the speed of the drill as shown in the following image:

Fig. 2.5.5: Adjust the speed of the drill

Step 3: Mark the required depth as shown in the following image:

Fig. 2.5.6: Mark the depth of the drill

Step 4: Place the drill on the mark on the wall and start the machine at a low speed as shown in the following image:

Fig. 2.5.7: Drilling on wall

Step 5: Make a shallow hole to make a base for the drill and then set high speed for the drill.

Step 6: Stop drilling after reaching the desired depth.

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 following image:

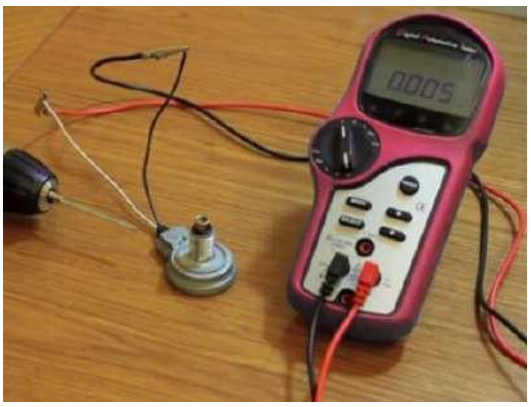


Fig. 2.5.8: Attaching the sensor leads to the multimeter

Step 2: 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 following image shows increase in the voltage output of the sensor with increased rotation per minute (RPM) of the drill:

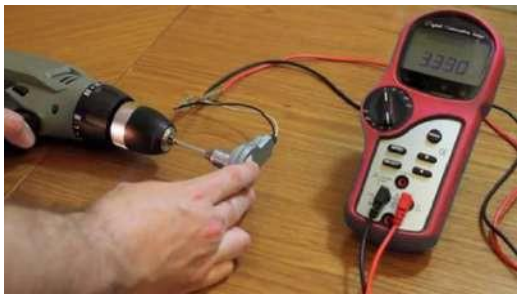


Fig. 2.5.9: Increased voltage output of the sensor with increased RPM of the drill

Step 3: Power off the drill and check the reading as shown in the following image:

Fig. 2.5.10: Reading after powering off the drill

This equipment basically help in installing the setup and testing it. Some of the tools and equipment are very costly and they need to be handled with care. They may require special skills to be used effectively.

Prepare Installation Checklist

After analysing the site and understanding the requirements of tools and equipment, the technician needs to prepare the site for installation. This step involves clearing the work area, marking the area for mounting the devices and selecting suitable power source. In the checklist all the steps are noted down in a sequential manner to complete the installation effectively.

Follow Safety Recommendations

General safety instructions include the following points:

- Keep the sensitive circuit ports and cable connectors dust-free during and after installation. For this, covers and caps can be used for ports and connectors to protect them from dust, debris and water.
- Keep the devices and equipment safe from any damage during transportation.
- Avoid wearing loose clothing while performing the installation.

- Wear safety equipment while performing the installation. Safety equipment includes the following items:
  - Head protection: helmet
  - Eye protection: goggles
  - Hand protection: gloves
  - Feet protection: shoes
  - Body protection: jackets
  - Ear protection: ear muffs
  - First aid kit

Safety with Electricity

The following points need to be kept in mind while working with electricity:

- Locate the electrical wiring set up and disconnect the power supply before performing the electrical connections.
- Avoid any hazardous working conditions such as moisture, ungrounded cables or damaged power chords.
- Take necessary measures to prevent any Electrostatic discharge (ESD) such as:
  - Hold the printed circuit board or PCB by its edges
  - Never place electrical components on a metal surface
  - Keep the components in ESD-safe packaging while not in use
  - Use the protective gears shown in the following image while handling components that are prone to ESD:

Fig. 2.5.11: Safety gears for protection from ESD

Safety Guidelines for Network Devices

The guidelines that need to be adhered to ensure the safety of network devices are as follows:

- Avoid touching or moving antennas of the router or gateways while the system is on, as it may hamper the equal radiation of signals in all directions.
- Avoid handling the antenna set up if there is lightning.

2.5.1 Device and Tools Used

The various tools required for installation of IoT devices are mentioned in the following table:

Tool and Equipment	Use	Image
Angle finder	Used to find degree of bend and precision angle Used in proper positioning of the nodes and sensors according to the requirement	
Spirit level	Used to measure vertical, horizontal and diagonal planes Used for mounting the nodes and edge devices at accurate level	
Tape	Used for routing wiring through the walls and electrical conduits	
Cordless drill	Used to drive screws into various substrates without damaging them Used to drill on the mounting surface	

Tool and Equipment	Use	Image
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	
Torque wrench	Used to apply a specific torqueto a nut or bolt at the time of assembling and installing the devices	
Wire strippers	Used to strip the insulation part from electric wires	
Crimpers	Used to crimp which is binding two pieces of 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	
Needle-nose pliers	Used to bend, re-position and snip wire Helps in reaching areas where fingers or any other tool/instrument cannot reach easily, such as microcontrollers within a device	

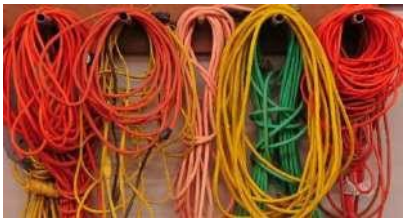
Tool and Equipment	Use	Image
Wire cutter	Used for cutting wires as small and large wire are needed for IoT device installation	
Multimeter	Used to measure resistance, current and voltage of nodes and power supplies	
Tape measure	Is a ruler made up of ribbon or cloth, fibre glass, plastic or metal strip Consists of linear-measurement markings Used for measuring distance of the node and gateway locations from the ground, ceiling and neighbouring surfaces	
Heavy duty extension cords	Is flexible electrical power cable also known 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	
Fuse Pullers	Used to insert and remove electrical fuses from housing	
Magnetic wristband	Is a band worn on the wrist that has magnetic mechanismto hold tools such as nails, fasteners and drill bits while working Used for installing nodes and devices at a height	

Table 2.5.12 Tools required in installing IoT devices

2.5.2 Choosing the Location for Installing the Device

For installing an IoT device such as a sensor or a camera, the technician needs to choose a location which does not affect the working and functioning of the IoT device. There are a few common criteria as follows:

1. Avoid Direct Sunlight

As any IoT device, such as a sensor or a camera is designed to operate within a temperature range, the technician should install the IoT device such that it can operate safely under all weather conditions. The following figure shows an IoT camera installed in shade to avoid direct sunlight:

Fig. 2.5.13: An IoT camera installed in shade to avoid direct sunlight

2. Keep the Device in Range of the Network

As an IoT set up works on Internet, the communication between the devices can be through any mode; wireless or wired. The technician should install the IoT device near a network set up such as a router so that there is no signal loss in the setup. The following figure shows an IoT camera placed in line of sight of a Wi Fi router:

Fig. 2.5.14: An IoT camera in line of sight of a Wi Fi router

3. Consider the Surrounding

While installing the IoT device, the technician should consider the surrounding of the installation location as there should be no hindrance in the operating area or the area covered by the sensor or the camera; such as a plant, a wall or any object. The following figure shows a plant under the field of vision of an IoT camera:

Fig. 2.5.15: A plant under the field of vision of an IoT camera

4. Place Device at a Height

While installing an IoT device such as a sensor, it should be installed at an optimum height which would help in operating it clearly. For example, a camera should be installed at a certain height so that it can detect the faces of people. The following figure shows the optimum height of installing an IoT camera:

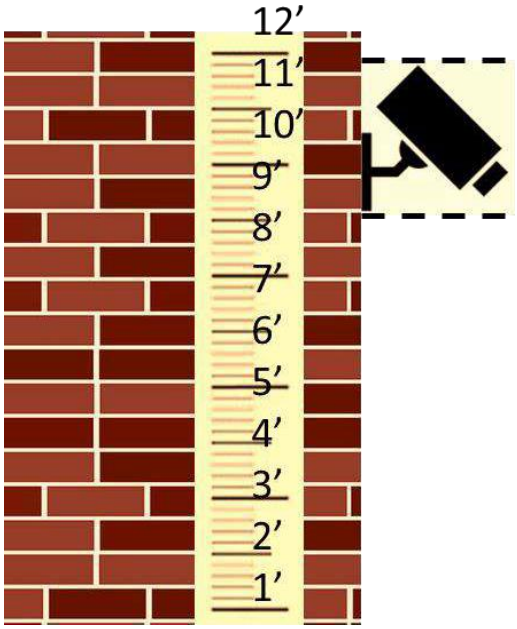


Fig. 2.5.16: Camera installed at an optimum height

2.5.3 Choosing Power Supply

After selecting a suitable location for installation of an IoT device, the technician should choose the power supply for the device. For selecting the power supply, a technician should consider a few points as follows:

- The power point should be as close as possible to the IoT device.
- The power supply should be near a dry ventilated area. Places such as kitchen, bathroom or laundry should be avoided.
- The power supply should be in a less active area to avoid any damage from any movement of people.
- The power supply should be at a place where all the indicators' light can be seen easily from a distance.
- The power supply should be in the same building where the main electric distribution box is installed; not in any separate garage or store house.

Also, the wiring should be done correctly while connecting the power supply chord to the power supply and the device.

The following image shows the correct and incorrect method of securing a power cable to a wall:

Fig. 2.5.17: Safe and unsafe power cable arrangement

Exercise

1. Write down the steps to use a power drill for making holes in a wall.

   a. _____

   b. _____

   c. _____

   d. _____

Exercise

1. Identify the tools and equipment in the table and write the name and use of the tool.

Tool and Equipment	Use	Image

Exercise

1. Write down the points to be considered while choosing the location for installing an IoT device.
   a. _____
   b. _____
   c. _____
   d. _____

Exercise

1. Write down the points which need to be considered while choosing the power supply for a network or an IoT device.

Exercise

1. List some uses of the following tools:
   a. Multimeter
   b. Magnetic wristband
   c. Wire cutter
   d. Crimpers
   e. Wrench
   f. Spirit level

2. List some points which needs to be considered by a technician while choosing a location for an IoT device which does not affect its working and functioning.

UNIT 2.6: Mounting Devices at Desired Locations

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the steps for surface preparation while mounting devices
2. Identify the correct distance between the devices
3. Describe signal and power loss during inter-device communication
4. Evaluate the resource consumption of the set-up
5. Identify the correct set of sources for power and other utilities

2.6.1 Surface Preparation

The first step in installation of any IoT device is to prepare the surface on which the device is to be mounted. For example, while mounting a sensor on a wall or any surface, the surface needs to 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 the following steps are performed for preparation of the mounting surface:

1. Check the levelling of the surface using spirit level. The following image shows testing of the surface level:

Fig. 2.6.1: Checking the surface level

2. Mark the area for creating holes to mount the frame on which the camera is to be installed. The following image shows marking a surface:

Fig. 2.6.2: Marking the surface

3. Perform drilling to make holes for the screws which are to be mounted in the frame to hold the camera in place. The following image shows a technician making a hole using a drill machine:

Fig. 2.6.3: Drilling

4. After creating a hole, clean the hole and then put wall anchors if needed. The following image shows placement of wall anchors inside the drilled holes:

Fig. 2.6.4: Wall anchors in drilled holes

2.6.2 Mounting of Device

After preparation of surface and mounting the frame, the next step is to mount the device. For different types of devices such as gateways or cameras, different types of mounting set ups are present which depends upon the model and the make. Sensors are usually installed within a switch or light or any other device. Hence, 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 2: 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 following image:

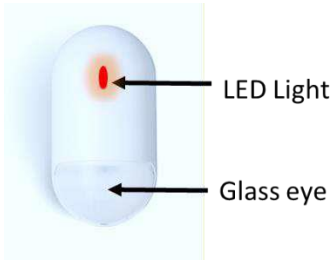
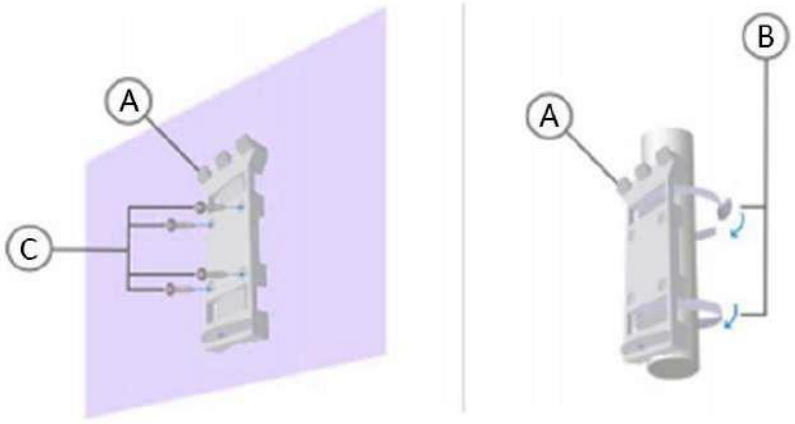


Fig. 2.6.5: Placing of motion detector sensor

For mounting a camera, the camera bracket is mounted first, which holds the camera at its place on the wall. The steps performed in mounting an IoT camera set up is discussed 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 following figure shows the mounting of a camera bracket:



A: Mounting bracket, B: Straps, C: Mounting screws

Fig. 2.6.6: Mounting camera bracket on a wall

2. After placing the screws, tighten them using a screw driver and check whether the bracket is installed tightly and is secured at its position or not. The following image shows tightening of screws to mount the camera bracket:

Fig. 2.6.7: Mounting camera bracket on wall

2.6.3 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 following figure shows the line-of-sight communication inside a room between an edge device such as a camera and a gateway/router:

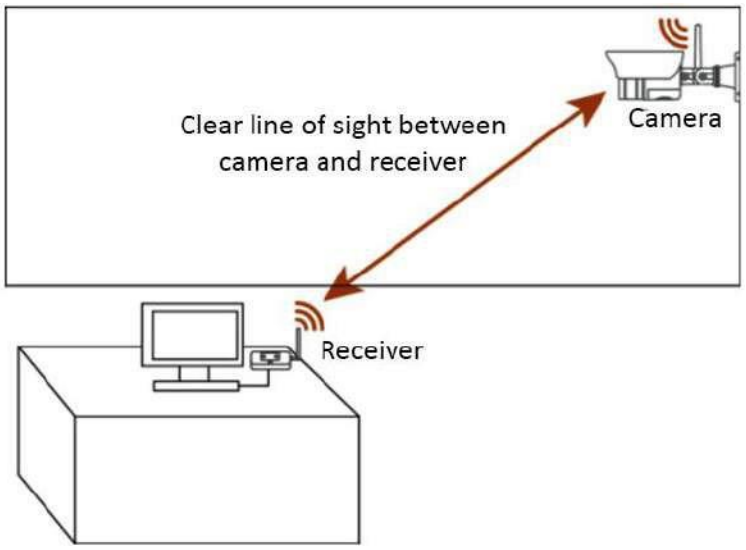


Fig. 2.6.8: Line of sight communication inside a room

If heavy building materials cannot be avoided, wired connection should be used. The example is shown in the following image:

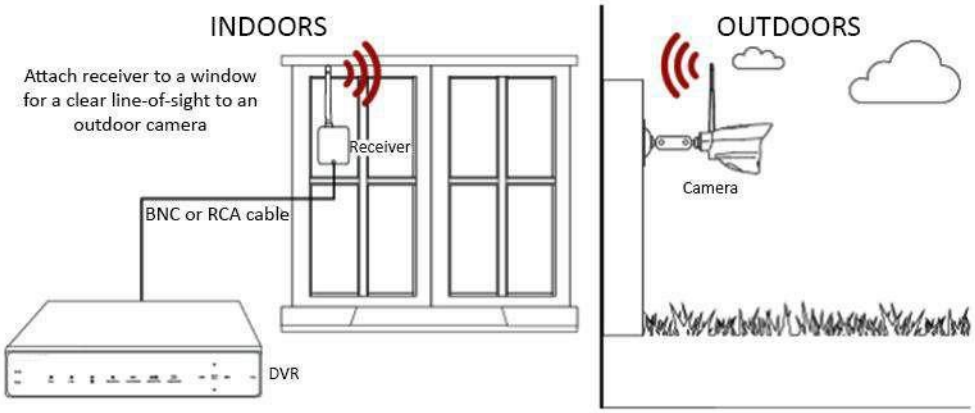


Fig. 2.6.9: Line of sight between outdoor and indoor areas

- **Network Range and Distance between Devices:** The network strength between the network devices drops by an inverse cube of the distance between the devices. So, for a distance of 2 m, the signal strength will drop to about 8 times of the signal strength for a device at a distance of 1 m. The following image shows drop in signal strength:

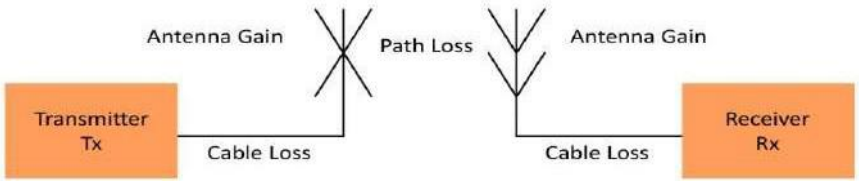


Fig. 2.6.10: Drop in signal strength

2.6.4 Evaluating the Resource Consumption of the Set-up

While setting up the IoT framework at a site, the technician needs to design and plan the LAN arrangement. It helps in ensuring that all the requirements, the cost involved, and the set-up is on the basis of a technical design and plan. While selecting devices for an IoT LAN network framework, the following factors should be considered:

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 following image shows two networks set up with switches:

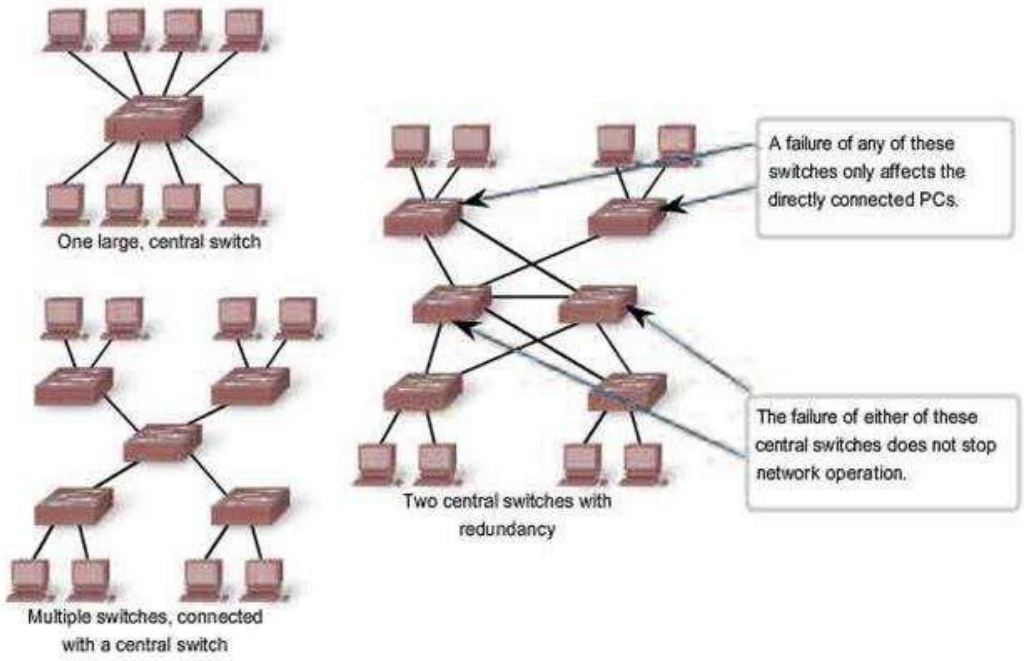


Fig. 2.6.11: Switch selection for a LAN network

- **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 following image shows different types of switches based on the speed:

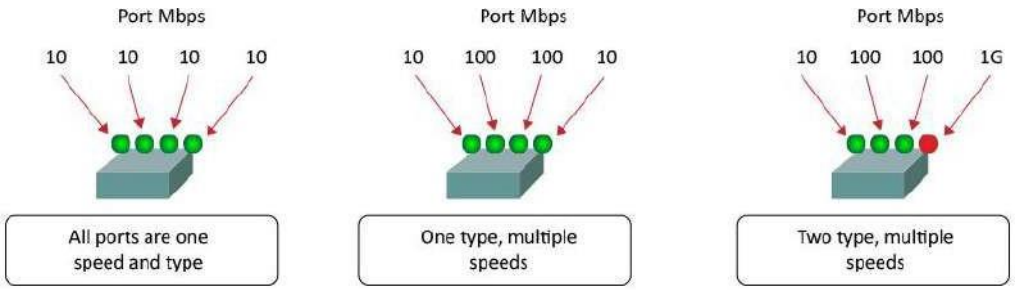


Fig. 2.6.12: Speed factor for selecting switch for LAN network

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.

Factors Affecting Cable Length

- **Total Cable Length:** All type of LAN cabling is restricted to around 100 meters per channel. As per the standard, the patch cable length should be 5 meters. Cabling distance is a significant factor for loss of signal. So as per the suitable cabling distance, different types of cables are provided to avoid signal loss. For example, Ethernet cable length should be up to maximum 90 meters. Fibre optic cable can be used for a distance up to 500 meters to some kilometres. The following image shows a cabling set up in a LAN network:

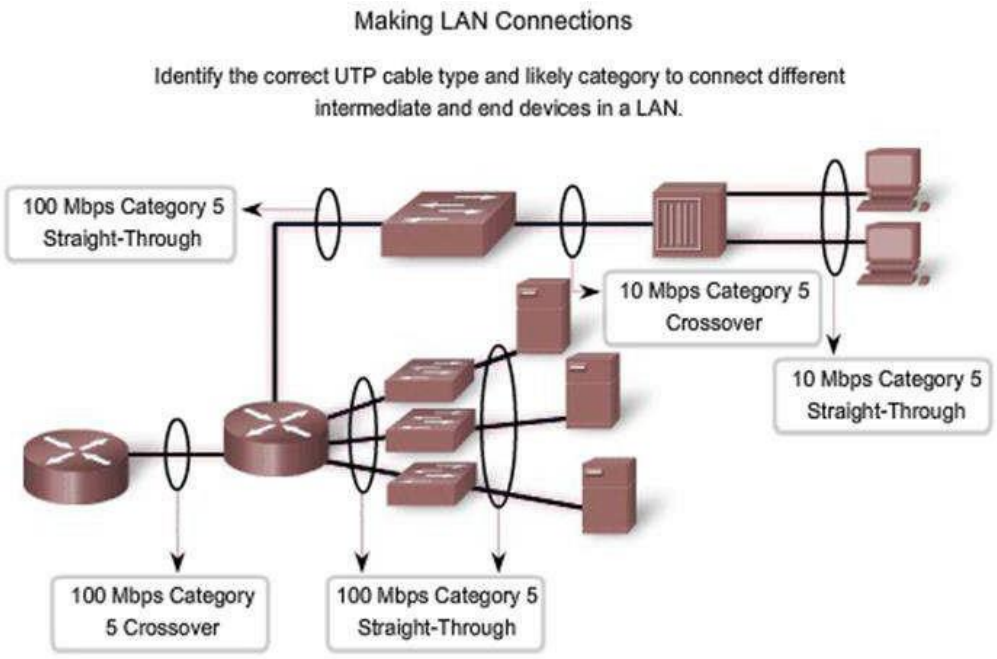


Fig. 2.6.13: Cabling set up for a LAN network

2.6.5 Cabling and Power Connections

After mounting the IoT device such as a camera, the connection between the camera's power supply and the input output from the camera for surveillance is done. For making the necessary cabling connection, the technician should know the types of cables used in setting up an IoT framework.

The following steps should be taken care of while connecting the cables in an IoT framework:

1. Use more cable and leave a little slack.
2. Test each part of the network set up installed.
3. Keep the cabling structure away from any sources of electrical inference.
4. Run the cable through wall and secure it with wire holding pins.
5. Mark and label the ends of every cable.
6. Make sure to use cable ties to keep the cables together and arranged.

The following image shows a basic wiring set up for a camera used for surveillance in IoT:

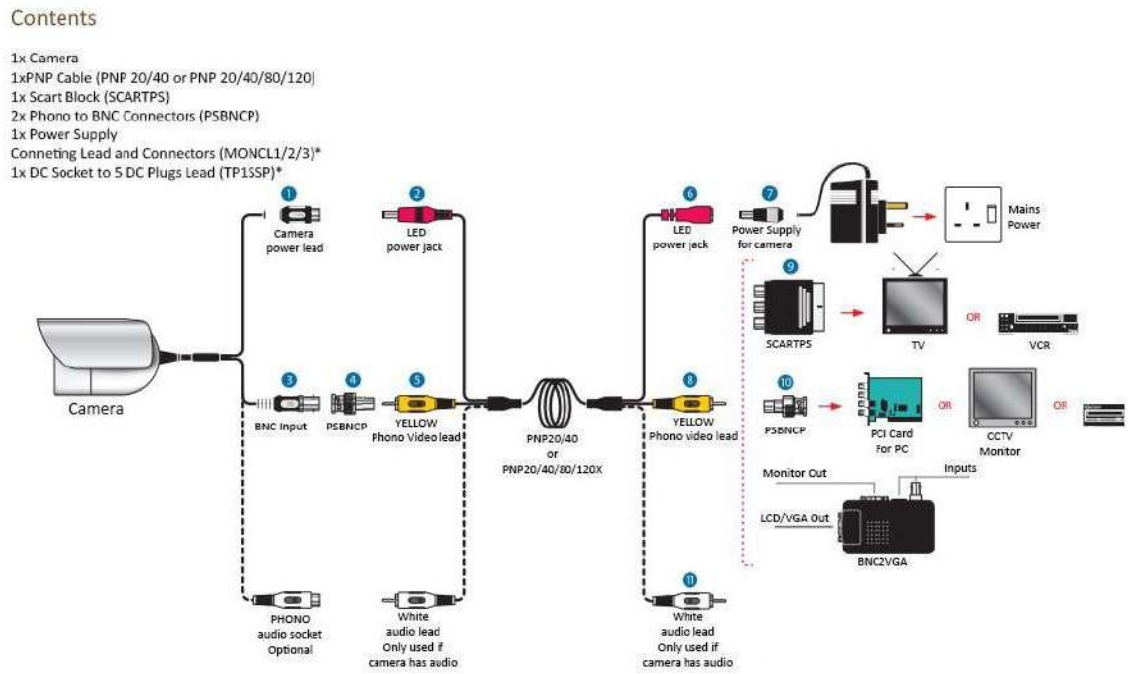


Fig. 2.6.14: Wiring set up for a camera in IoT

For wiring of an RGB cable, the following points should be considered:

1. Power off the device first.
2. Connect the red, yellow and white connector to the respective coloured slots on the device.
3. Connect red, yellow and white connector to the respective coloured slots on the other device for monitoring or recording.
4. Make sure that the connections are tight and fit.
5. Make sure that the slack wire is managed properly.
6. Turn on the device and check the audio and video streaming.

Signal and Power Loss during the Inter-device Communication

The signal travelling through a network's cables or through signals via a wireless channel gets low. This happens because of power and strength loss over the long distance due to attenuation or physical obstruction. The technician should check the loss of signal over the network and select the proper cable for transmission of signals over wired network. In wireless network, the technician should select the router and wireless configuration setting to minimise the signal loss.

The following image shows wireless and wired signal loss:

Fig. 2.6.15: Wireless and wired signal loss

Exercise

1. Write down the factors which need to be considered while:
   a. Selecting a switch: _____
   _____
   b. Selecting a router: _____
   _____
   c. Selecting cable length: _____

2. Write down the points that need to be considered while choosing the distance to be kept between network devices.
   a. _____
   b. _____
   c. _____
   d. _____

UNIT 2.7: Performing Checks and Connections

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the connectivity between the devices
2. Describe preparation of devices for transmission of data
3. Explain power supply selection and grounding
4. Identify post commissioning checks

2.7.1 Checking the Connectivity between Devices

After connecting the devices through cable and connecting the power supply, the technician need to check whether the connections are correct or not.

The following figure shows the steps to be taken to test the connections:

Turn on the power supply of the devices.

Check the power supply indicator light on the devices.

Check the indicator for network signals.

Test the connection with testing tools and equipment if there is problem in connection.

Fig. 2.7.1: Steps in checking the connections

Testing of the edge nodes will be done after they are installed and configured. The technician needs to power on the devices and check whether there is any problem in power connection and network strength. Network can be tested visibly by the indicators and signal tester. The power connection and the continuity of the circuit is checked using a multimeter.

2.7.2 Selecting Power Supply and Grounding

Grounding or earthing means connecting an electrical system to the ground through its non- current carrying conductor part. The grounding of a system plays a vital role for stability and safety of the system. With poor earthing, electrical systems are prone to damage or accidents. All the devices in a system need to be grounded in some way. The following figure lists the purpose of earthing:

Purpose of Earthing	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

Fig. 2.7.2: Purpose of earthing

Most of the IoT devices are wireless and run on battery. The following image shows plug points whose third pin is configured for grounding:

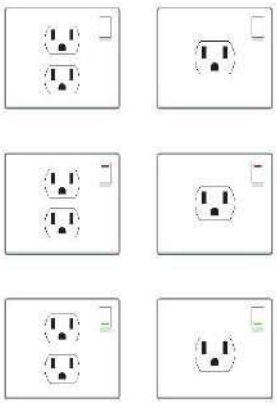


Fig. 2.7.3: Plug point with grounding pin

Selecting the Power Supply

The power supply should be chosen so that the device can get uninterrupted power supply and can operate without any electrical fault. While selecting the power supply for the IoT device, the following measures should be considered:

1. The power source should be at a place which is dry and at an optimum temperature.
2. The power source should not be damaged and it should be properly grounded.
3. The power socket should match the current and power rating of the device.
4. The wires should be secured and the connections should be tight.

Grounding the Connection

The grounding is done to protect the equipment and device from any sudden change in voltage. It helps to prevent any damage to the equipment and also protects the users from getting any shocks. The grounding steps for an electrical connection is as follows:

1. Take the grounding wire which is basically coded in green or black colour.
2. Take out the outer coating of the wire using a utility knife.
3. Attach the wire to the grounding point in the socket or at the wall lining.

The following image shows a basic grounding connection for a power supply connection:

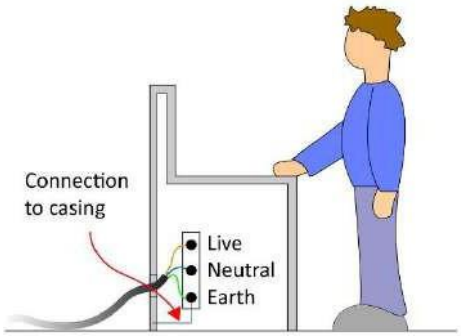


Fig. 2.7.4: Grounding of an electrical connection

2.7.3 Post Commissioning Tests

For enabling data transmission between IoT devices, the technician needs to perform some steps. The following figure shows the steps that are performed to connect IoT devices for enabling data transmission:

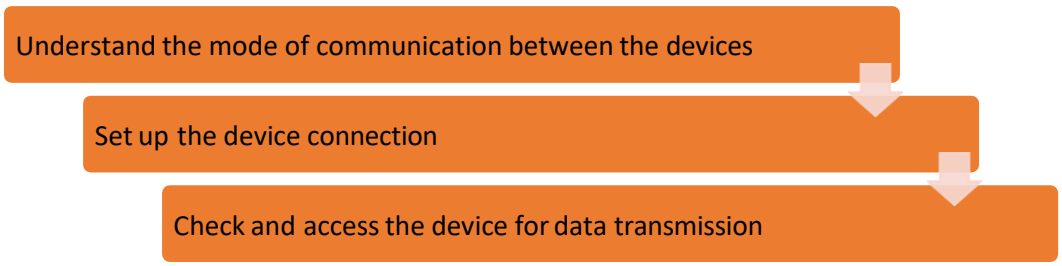


Fig. 2.7.5: Steps in IoT data transmission set up

Understand the Mode of Communication between the Devices

In this, the technician needs to check whether the devices in an IoT set up are connected with a cable or they are working on a wireless network. For a wired network, which is Ethernet cable, the devices will automatically plug and play and start transmitting the data. For configuring devices over a wireless network, the technician needs to perform the following steps:

1. Find the static IP, Gateway and Net Mask information
2. Get the username and password from the admin device
3. Set the static IP address
4. Check for network connections in LAN
5. Enable the network to access the device and test the data transmission

The following screenshot shows the settings to be configured in a PC:

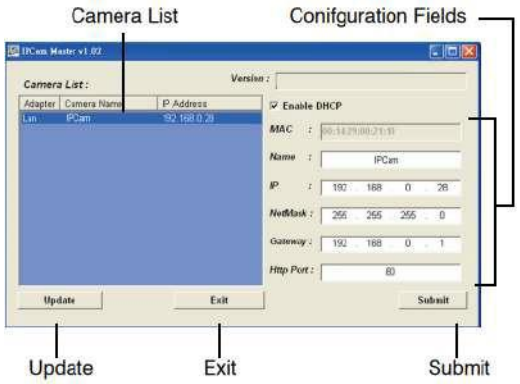


Fig. 2.7.6: Configuration of device through PC

2.7.4 Connectivity between Devices

After installing an IoT set up, the technician should perform a basic test for checking the connectivity between the devices. The testing of the set up covers various aspects in an IoT framework. The following figure shows the scope of IoT testing:

Components validation	• Device hardware • Embedded software • Network connectivity
Function validation	• Interaction between devices • Basic device testing
Performance validation	• Device performance • Data transmit frequency
Security and data validation	• Data packets validation • Data encryption/decryption

Fig. 2.7.7: IoT testing scope

To check the IoT set up, various types of tests are performed on different aspects of the framework to check the functioning of the entire framework. The following checks are the tests performed to examine an IoT set up:

- **Functional Testing:** This test is done to check whether the device is working as per the requirement of the customer, based on the inputs given.
- **Compatibility Testing:** In this, the version and compatibility between the devices are checked to make sure that they work well together. In this test, protocols and versions of hardware and software of the device are checked.
- **Usability Testing:** This is done to check whether the customer can use the IoT devices and understand the controls to use them as per its own use. This includes usefulness, text and appeal of the controls.
- **Network Testing:** This test needs to be done to check whether all the network connections between the devices are working as required. There should be no log and the devices should perform in sync.
- **Security Testing:** This test is done to check the security of the network set up and data encryption. This performs verification and authentication of the data and verifies the same to follow security protocols.
- **Performance Testing:** After completing all the tests, the technician needs to perform a performance test of the setup. The working and functioning of the entire set up is checked to ensure that it is working as per the desired outcome and following all the protocols.

Exercise

Write down the purpose and importance of earthing/grounding.

1. _____

_____

_____

2. _____

_____

_____

Exercise

Write down the scope of IoT testing for each type of validation given below.

Components validation	• _____
Function validation	• _____
Performance validation	• _____
Security and data validation	• _____

Exercise

Create a checklist for the tests performed in testing an IoT setup.

1. _____

2. _____

3. _____

4. _____

Practical

Test the speed of 3 Wire Speed Sensors using a multimeter.

Required Tools/Equipment:

- 3 Wire Speed Sensor
- Multimeter
- Drill machine
- Connecting probes

Practical

Mount a security camera system and connect it to the monitor and the DVR. Also, perform earthing connection of the same.

Required Tools/Equipment:

- Camera
- DVR
- Power cord
- Cables
- Monitor
- Drilling machine

Practical

Perform all the pre-installation steps required to be done for installation of CCTV camera.

Required Tools/Equipment:

- Site for installation
- Site log
- Measuring scale

Practical

Perform drilling operation at a site to install a base plate for a security camera.

Required Tools/Equipment:

- Drilling machine
- Measuring tape
- Spirit level, Marker
- Personal protective equipments such as safety shoes, goggles, mask, helmet and gloves

Practical

Perform mounting of a sensor device on a wall.

Required Tools/Equipment:

- Dilled surface for mounting of sensor
- Sensor installation kit
- Measuring tape, Marker
- Personal protective equipments such as safety shoes, goggles, mask, helmet and gloves

UNIT 2.8: Connecting Microcontroller Boards for Data Transfer and Connecting the Boards

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the connectivity points in Arduino and Raspberry pi
2. List the connectivity options available for microcontroller
3. List the types of cables and connectors
4. Explain how to connect a device to the microcontroller board

2.8.1 Connectivity Points in Microcontrollers

These days smart devices have come up. The connection can be wired (such as Ethernet, telephone or power line) or wireless (such as RF transmission, spread spectrum, cellular, Wi-Fi or Bluetooth). Talking of connectivity in homes, wired connections include telephone lines or power lines with short-range RF acting as the transmission medium. Therefore, microcontrollers might have to transmit/receive messages while interacting with the hardware.

A microcontroller board has a number of connectivity points available for the specific control functions. The following image shows a microcontroller board with different connectivity ports:

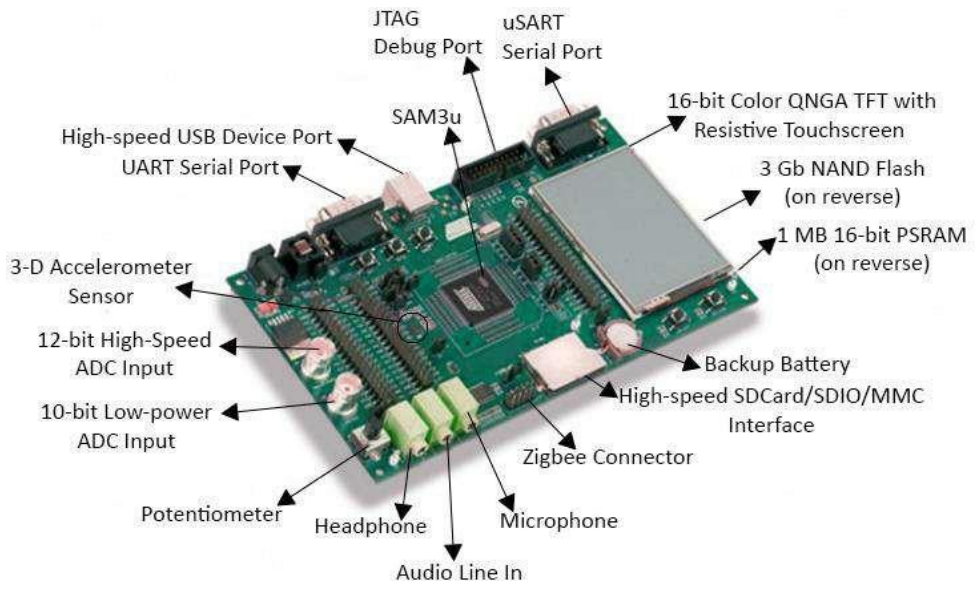


Fig. 2.8.1: A microcontroller board with different connectivity ports

The two common microcontroller boards are:

- Arduino
- Raspberry Pi

Arduino

Arduino is an open-source electronic circuit/board which can be programmed to perform certain action. It has a pre-programmed microcontroller that is coded using programming language in the Arduino development environment. This allows the user to develop and code electronic components.

An Arduino board comprises of digital and analog input/output (I/O) pins which can be connected to other boards/circuits. This opensource board has communication interfaces like Universal Serial Bu (USB) which loads programs from a computer.

The following image shows the pin layout of an Arduino board:

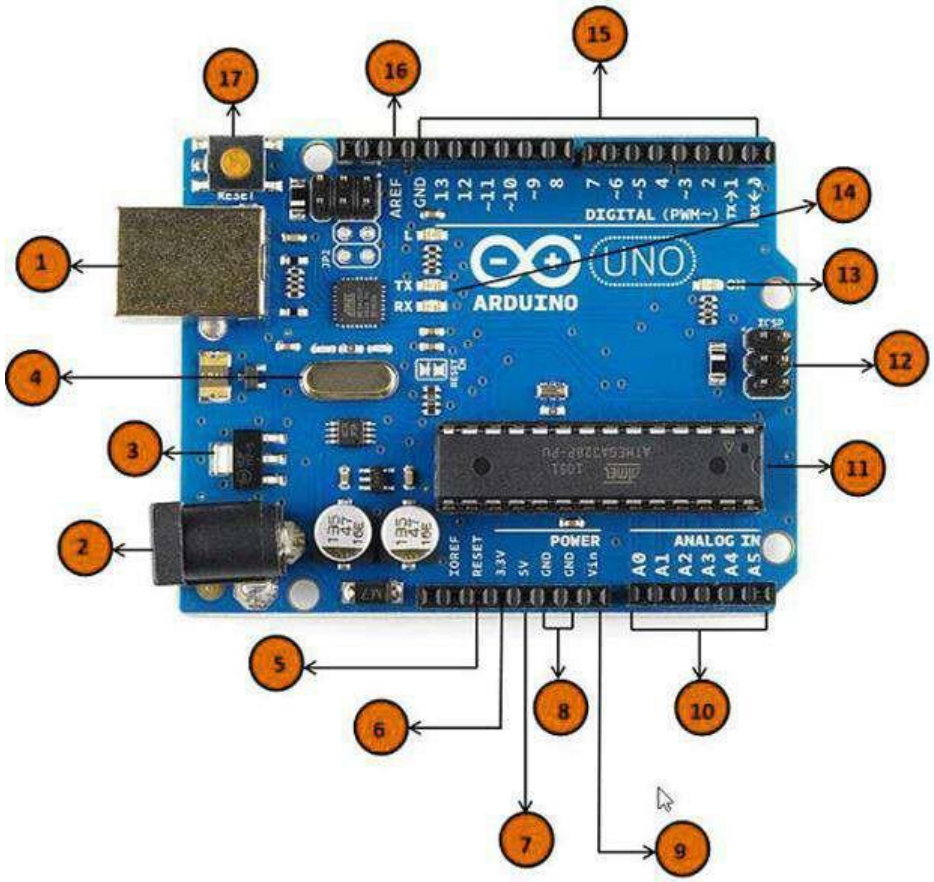


Fig. 2.8.2: Pin configuration of an Arduino board

The various parts labelled in the above image are as follows:

1. Power USB
2. Barrel Jack
3. Voltage Regulator
4. Crystal Oscillator
5. Arduino Reset
6. 3.3V Pin
7. 5V
8. GND
9. Vin
10. Analog Pin
11. Main microcontroller
12. ICSP Pin
13. Power LED Indicator
14. TX and RX LEDs
15. Digital I/O
16. AREF
17. Arduino Reset

These parts have been discussed as follows:

- **Power USB:**

  The computer's USB connecter can be connected to the Arduino board with a USB cable.

- **Barrel Jack:**

  Arduino can also be powered from an AC mains power supply with the Barrel Jack.

- **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:**

  A Crystal oscillator is used to keep time for Arduino board. An Arduino crystal oscillator normally has 16.000H9H printed on the top which indicates that the frequency is 16,000,000 Hertz or 16 MHz

- **Arduino Reset:**

  An Arduino board can be reset to its factory settings. The UNO board can be reset by two methods. By using the reset button (17) on the board or connecting external reset button to the Arduino pin labelled RESET (5).

- **Pins:**
  - 3.3V − Supply 3.3 output volt
  - 5V − Supply 5 output volt
  - Arduino board components work well with 3.3 volt and 5 volt supply
  - GND (Ground) − The GND pins on Arduino to ground the circuit
  - Vin − This pin can be used to power the Arduino board from an external power source, like AC mains power supply

- **Analog Pins:**

  The Arduino UNO board comprises of five 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.

- **Main Microcontroller:**

  Every Arduino board (of AMTEL Company) has its microcontroller which is the brain of the processor. However, the main integrated circuit depends on the configuration of the board.

  Before loading any new program code onto the Arduino Integrated Development Environment (IDE), determine which IC the board has by reading the top of the IC. For more details about the IC construction and functions, refer to the data sheet.

- **In Circuit Serial Programming (ICSP) pin:**

  ICSP (12) is an Atmel Atmega microcontroller, which a tiny programming header for the Arduino having MOSI for master output / slave input, MISO for master input / slave output, SCK for serial clock, RESET, VCC for voltage connection and GND for earthing. It is also known as Serial Peripheral Interface (SPI), which is kind of an "expansion" of the output, and the output device is slave to the master of SPI bus.

- **Power LED Indicator:**

  Power LED indicator lights up when Arduino is connected to a power source. If the light is not turned on then there is some kind of fault with the connection.

- **TX and RX LEDs:**

  On the Arduino board, there are two labels, TX (transmit) and RX (receive), which are placed separately. One is placed at the digital pins 0 and 1, which indicates pins used for serial communication. The other label is the TX and RX led (13). During transmission of data, the TX led flashes randomly depending on the speed of transfer which depends on baud rate specified for the board. On the other hand, for the receiving process the RX light flashes.

- **Digital I/O:**

  Arduino UNO board comes with 14 digital I/O pins (15) 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 at times is used to specify the external reference voltage (between 0 and 5 Volts) as the upper limit for the analog input pins.

Raspberry Pi

Raspberry Pi initially designed for Linux OS is an opensource board which has the primary chip on the Raspberry Pi (a System on a Chip application). This operates components onboard components like CPU, graphics, memory or the USB controller. Since it is an open source board, it can be programmed in any intended way, and also the code can be provided for other users to use or modify.

The Model B+ Raspberry Pi version has:

- 40 GPIO pins
- 4 USB 2.0 ports
- Micro SD card slot
- Lower power consumption
- Better audio output
- Sleek form factor

The following image shows the pin configuration of a Raspberry Pi board:

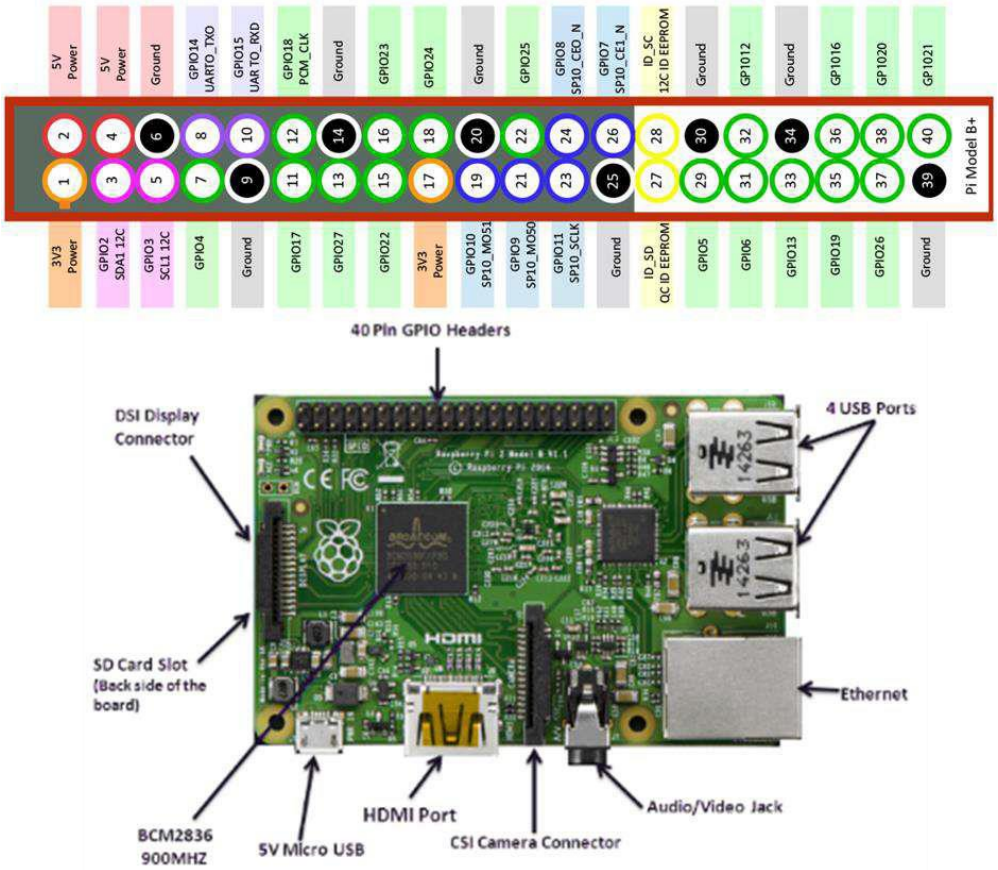


Fig. 2.8.3: Pin configuration of a Raspberry Pi board

2.8.2 Connectivity Options for Microcontroller

Various connectivity options for a microcontroller are as follows:

- Embedded Wi-Fi
- Bluetooth
- Low Power Wide Area Network
- Embedded Wireless
- ZigBee (802.15.4)

Embedded Wi-Fi

Microcontroller units (MCUs) have Wi-Fi modules which include embedded WLAN modules with support for Wi-Fi IEEE 802.11 b/g/n standards. They enable Wi-Fi connectivity on embedded devices without any problem for the user. These Wi-Fi modules are plug and play devices like the embedded WLAN stack, TCP/IP (Network) stack and small-sized security supplicants. It is a self-contained solution actuated by 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.

Bluetooth

Some MCU use Bluetooth connections. These self-contained modules are low-power and used mainly for wearables or IoT devices which need Bluetooth Low Energy IP Stack or radio frequency (RF) experience.

MCUs are tailored for battery-powered applications having 1.8V - 4.3V voltage range, sub-1µA sleep current and sub-3mA / 4mA TX/RX current value. This ensures ultra-low-power connections, using lowest possible electric charge. This means extended battery life by 2 - 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

Low Power Wide Area Network

The technologies for setting up low power WAN's are Long-range Wireless (LoRa) and sig fox. 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 scalable, high-capacity network with low energy consumption. All this is done while maintaining an easy to implement star-based cell infrastructure.

Embedded Wireless

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 2.4 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.

In 2.4 GHz receiver / transmitter, the commands are sent with a signal / data package. A Raspberry Pi or an Arduino board can be equipped with a 2.4 GHz receiver / transmitter to receive commands from a base station and send back data.

RF Identification (RFID)

RFID involves contactless reading and writing of data into an RFID tag's non-volatile memory through an RF signal. Low frequency RFID devices typically consist of a transponder (tag) and reader. The RFID chips are suitable for the smallest devices and require no external components, lowering the tag costs.

2.8.3 Optimization of the Micro Controller

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 requires to perform certain steps for optimising the power consumption in the microcontroller chip. These steps are:

1. Optimise the Pull up Resistor: The resistor value should be optimised to its greatest possible value after 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 least voltage is needed for transmitting the signals; lesser the voltage, less will be 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.

2.8.4 Connecting IP Enabled and Non-IP Enabled Devices

Non-IP Enabled Devices

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

1. The control settings page of the ZigBee device gives an access to control panel which allows to control the devices.
2. The control panel should be accessed for addition of 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, password is required for pairing. If this is so, enter identical passwords on both of the devices.

For connection of the non-IP sensors, a sensor hub is used to process the data from individual sensors and app-ready information is generated. This hub is implemented in a small, low-power microcontroller. The sensors may be discrete devices, fully integrated sensor devices and multiple co-packaged MEMS sensors. For example, on-board sensors may combine accelerometer, gyroscope and magnetometer elements along with a microcontroller that processes the data from the sensor data and makes the fused data available such as rotation vector, linear acceleration or gravity.

IP Enabled Devices

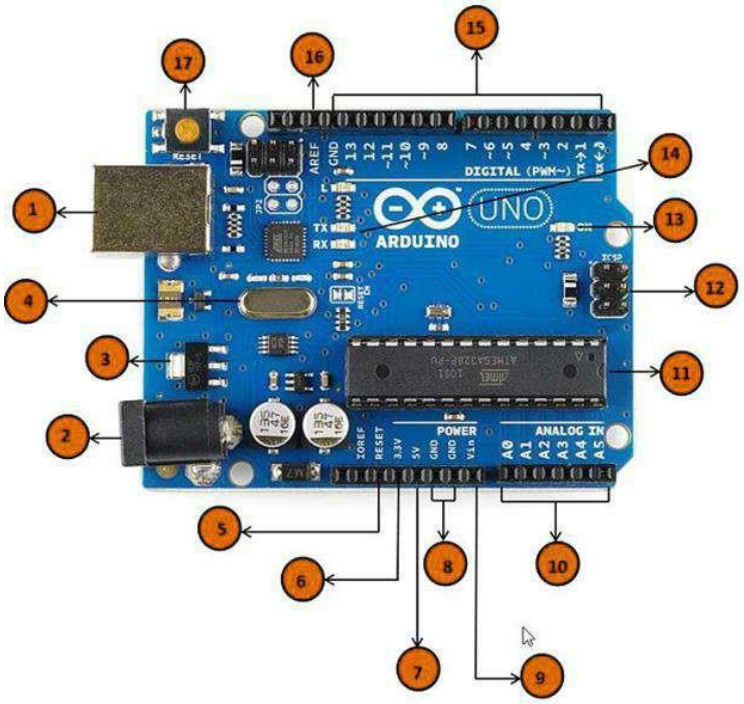
An IP address is needed for connecting IP enabled devices via the Internet. The steps in connecting devices through IP are as follows:

1. The control panel should be accessed from one device.
2. The network and the sharing option should be opened.
3. The LAN, WAN connection across which the device has to be connected should be selected.
4. Then, properties window should be opened and IPv4 option should be selected.
5. "Use the following IP address" should be selected.
6. The IP address 192.168.127.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.

Exercise

1. Write down the components marked in the Arduino board and the function of each component:



Exercise

1. Write down a few points regarding connectivity options of a microcontroller given below:

   - Bluetooth
   - Low Power Wide Area Network
   - Embedded Wireless
   - ZigBee (802.15.4)

Exercise

List down the points for connecting IP enabled and non IP enabled devices.

- IP Enabled devices
- Non IP Enabled devices

2.8.5 Types of Cables and Connectors

There are various types of connectors used for connecting communication cables as shown in the following image:

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. 2.8.4: Different types of connectors

The cables used in connecting the microcontrollers are network cables as well as the cables shown in the following table:

Portable cord		These cords are used to supply power to the PCB's with microcontroller boards. These are basically 9V DC power adaptors and can be used to power sensor, actuators and the microcontroller boards.
Audio-Video (AV)		These cables are used for audio and video signal transmission. These cables are used in Raspberry Pi boards.
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.
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.
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 (DTV), with a single cable. HDMI has support for standard, enhanced or high-definition videos. Multi-channel digital audio support is also there. These are used for Raspberry Pi boards only.

Table 2.8.1 Cables used in connecting microcontrollers

Exercise

1. Name the different types of cables shown in the table and write down their functions.

Image	Name	Feature

UNIT 2.: Installing Suitable Framework

Unit Objectives

At the end of this unit, you will be able to:

1. Execute the steps of connecting Arduino board to the PC

2.9.1 Procedure of Connecting Microcontroller

The microcontroller board needs to be connected to a PC or a laptop. A software is required to be installed on the PC or the laptop for connecting the board.

The data from sensors is fetched by the software program for the microcontroller and then transmitted to the PC with USB cable. The data transmitted is updated every second in this process.

The steps for connecting an Arduino board to the PC are as follows:

- Take the Arduino Uno board and a USB cable as shown in the following image:

Fig. 2.9.1: Arduino board and cable

- Arduino IDE for the operating system can be downloaded from the Internet. (https://www.arduino.cc/download_handler.php?f=/arduino-1.8.5-windows.exe)
- Connect the Arduino board with the USB cable and the USB port of the PC. The following image shows connecting the USB plug to the board:

Fig. 2.9.2: Connecting the USB plug to the board

- Unzip all the files and install the drivers. The following screenshot shows the installation window:

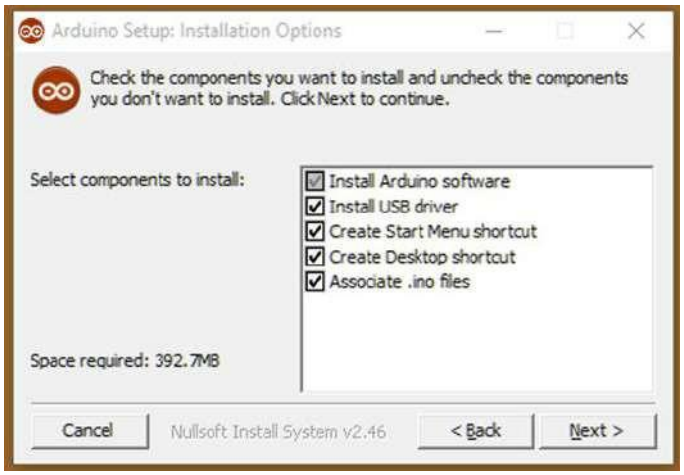


Fig. 2.9.3: Arduino installation window

- Choose the components to install. The following screenshot shows the window for installing components:

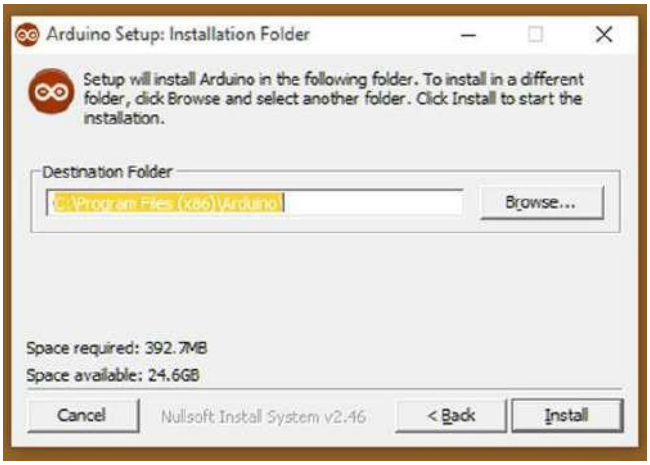


Fig. 2.9.4: Window for installing components

- Choose the installation directory. The following screenshot shows the window for installation directory:

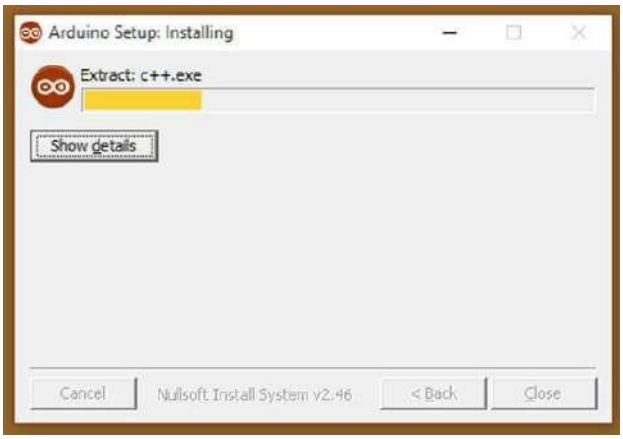


Fig. 2.9.5: Window for installation directory

- The process will extract and install all the required files to execute properly the Arduino Software (IDE).
- Open Arduino Environment Software and Select the Arduino board type under Tools>Boards>Arduino UNO. The following screenshot shows identifying the board:

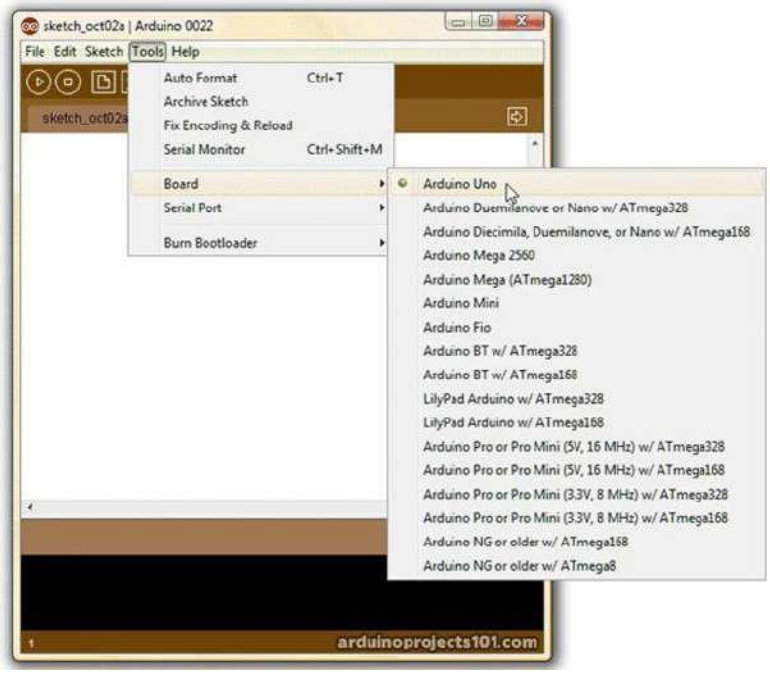


Fig. 2.9.6: Identifying the board

- Then, choose the serial port under Tools>Serial Port>COM 7 (COM # depending on what COM port is free during setup) as shown in the following screenshot:

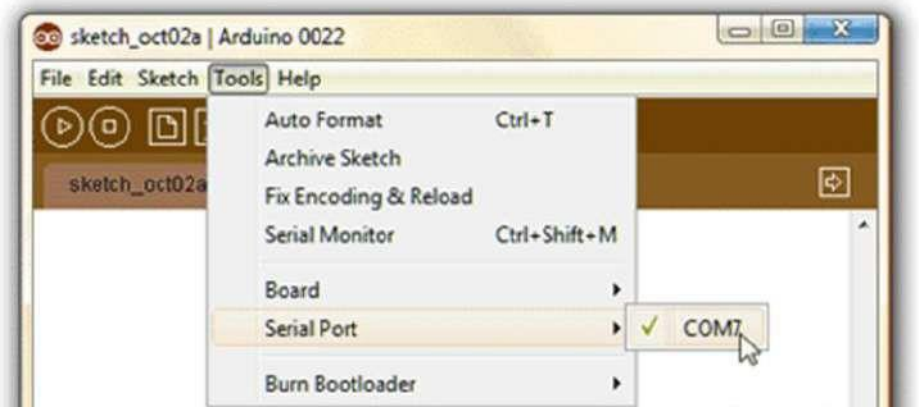


Fig. 2.9.7: Selecting the serial port

- Open an example code by clicking File→Examples→Basics→Blink as shown in the following screenshot:

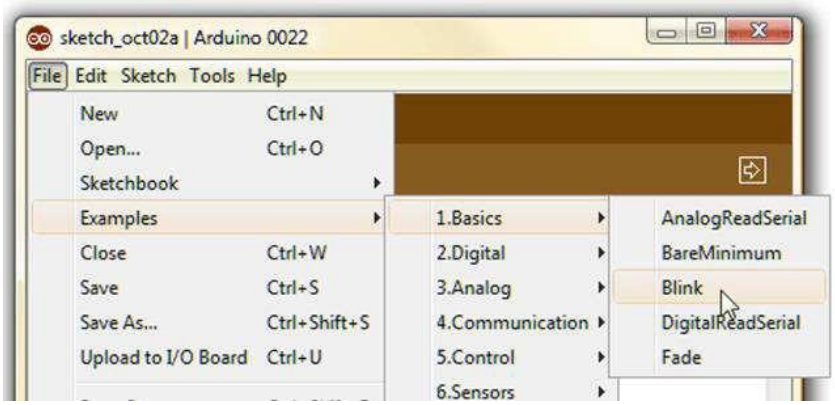


Fig. 2.9.8: Opening a code

- A screen will appear as shown in the following screenshot:

Fig. 2.9.9: Screenshot of the code

- Then, click on upload button to upload the code to Arduino. Wait till the "Done Uploading" message status appears. The following image shows screenshot for uploading code:

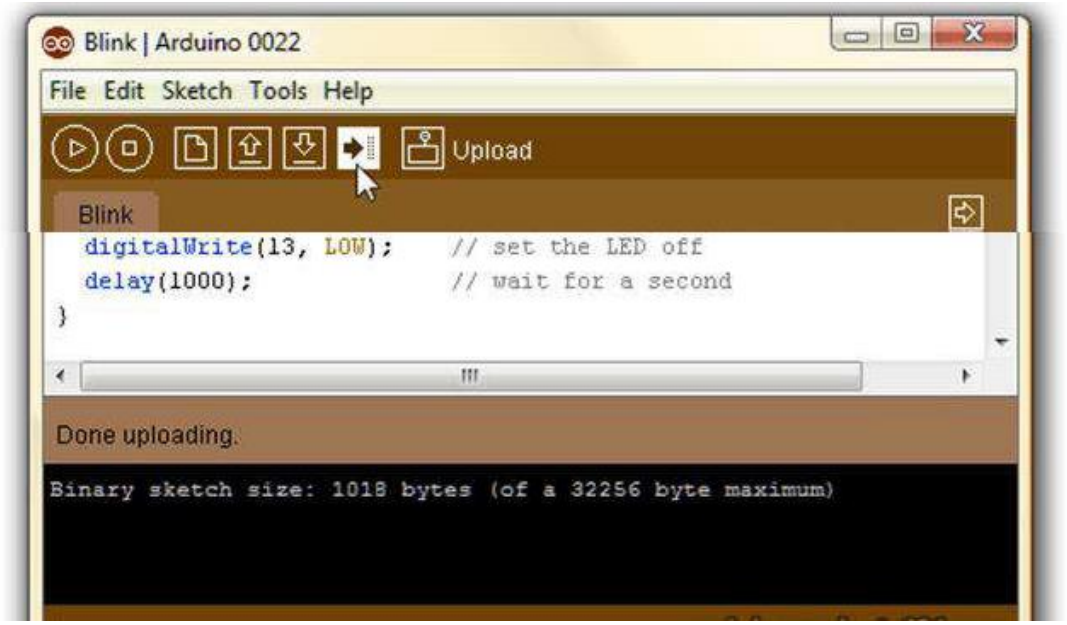


Fig. 2.9.10: Uploading a code

- To check if the computer and the Arduino are communicating, check the blinking of LED. This indicates successful installation of Arduino as shown in the following image:

Fig. 2.9.11: LEDs blinking on the controller board

The steps for connecting a device to the Raspberry Pi microcontroller and making it ready to boot are as follows:

- To start off, place the SD card into the SD card slot on the Raspberry Pi board. The cards and the wires should be connected to the proper port and pins. The ports and pins can be understood by looking at the pin configuration. The following image shows placingthe SD card:

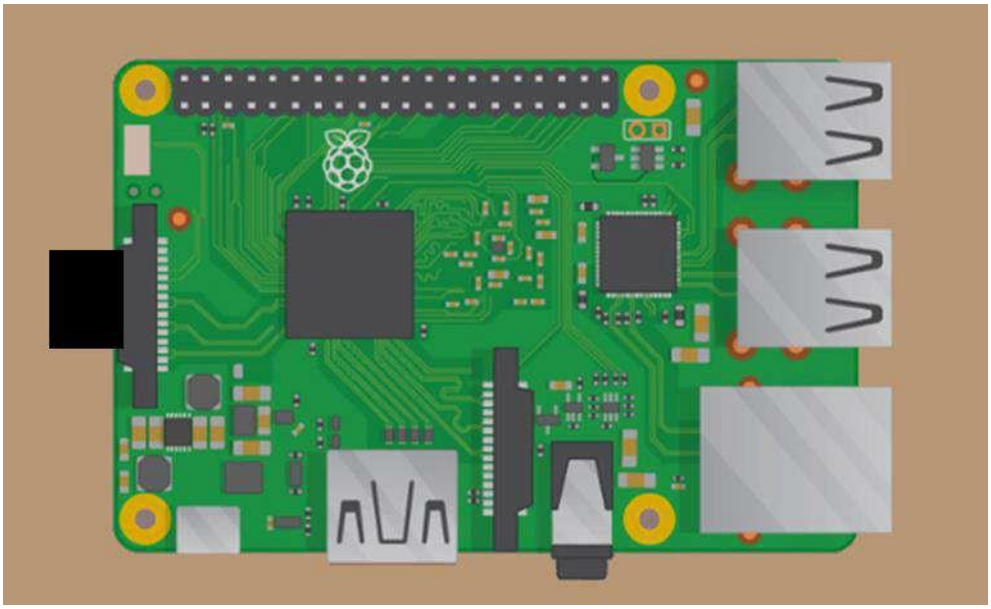


Fig. 2.9.12: Placing the SD card

- Then connect the keyboard and the mouse via the USB ports on the Raspberry Pi as shown in the following image:

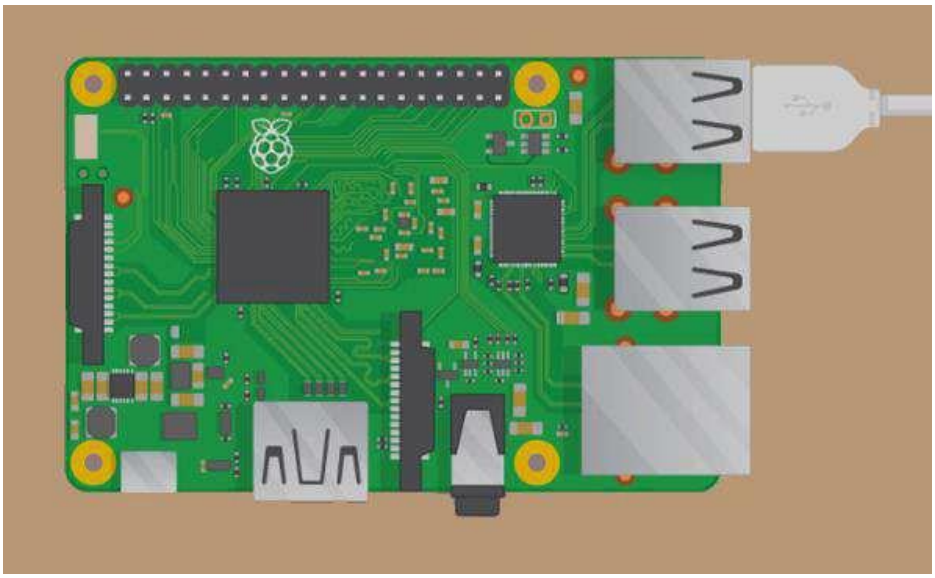


Fig. 2.9.13: Plugging cables to the USB ports

- Turn on the device and choose the right input medium (such as HDMI 1, DVI and so on).

- Then, connect HDMI cable from Raspberry Pi to the device so that the status can be displayed on the monitor of the device. The following figure shows HDMI cables plugging in the board:

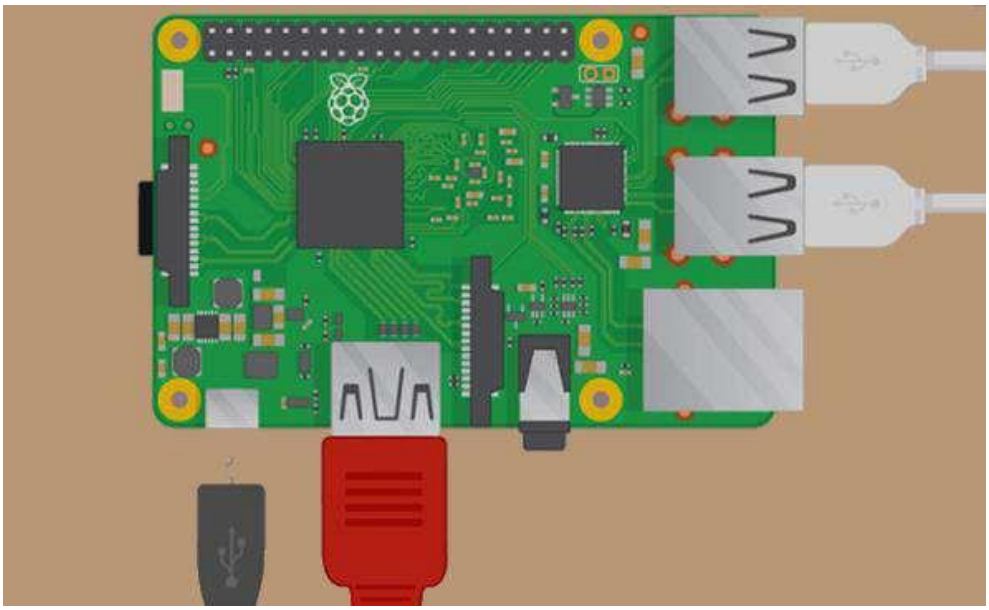
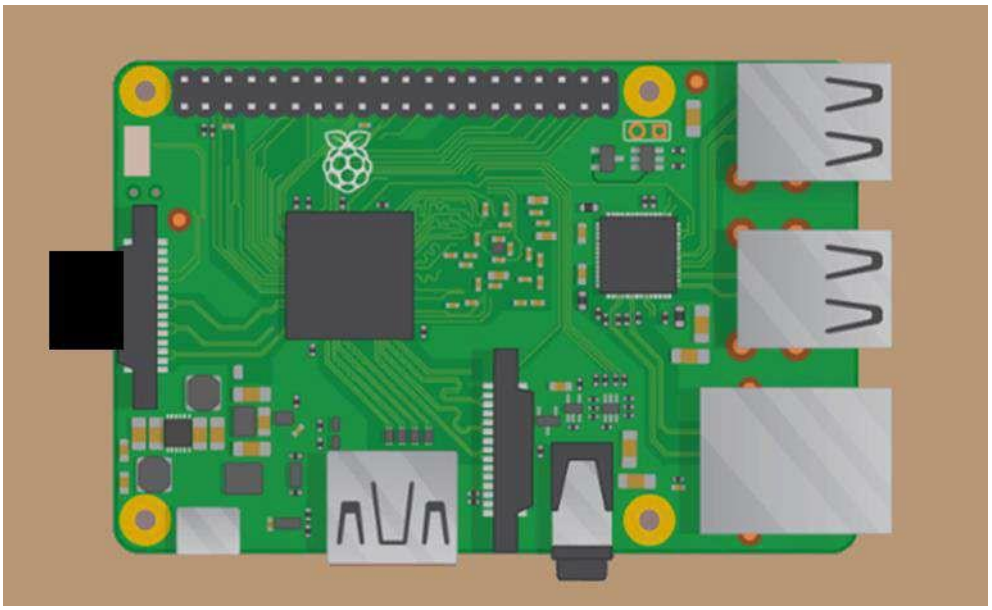


Fig. 2.9.14: Plugging HDMI cables to the board

- For Internet connectivity with Raspberry Pi,plug the Ethernet cable into the Ethernet port, or connect the Wi-Fi dongle to the USB ports. In case of Raspberry Pi 3, there are onboard ports for this.
- When all the cables are plugged, and the SD card is inserted correctly, connect the micro USB power supply. This power up and boots the Raspberry Pi.

Exercise

1. Name the cables that are attached to the Raspberry Pi board and the functions they perform.



UNIT 2.10: Transferring Software Code to On-board Microprocessor and Compiling Code to On-board Microprocessor

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the nodes and gateways
2. Explain the basic coding structure of microcontroller
3. Identify the options to transfer codes
4. Explain the challenges in transferring codes
5. Explain how to compile a code
6. List the types of compilers available

2.10.1 Understanding Nodes and Gateways

To fetch the data or control switch with instruction set, every sensor and actuator is attached to a microcontroller. The microcontroller, sensors, power and radio are collectively known as sensor nodes. A sensor node is a self-contained unit which collects the data generated by the sensors.

The sensor node cannot handle the data locally because of low processing power, memory, and storage. Therefore, the data is transferred to a central location via low-energy radio communication network. The sensors' communication link is determined by the kind of device used such as - ZigBee, Bluetooth Low Energy (BLE), or Power over Ethernet (PoE). IoT gateway is a central hub which behaves like an aggregator of raw data generated by the sensor nodes. The following figure shows nodes and gateway:

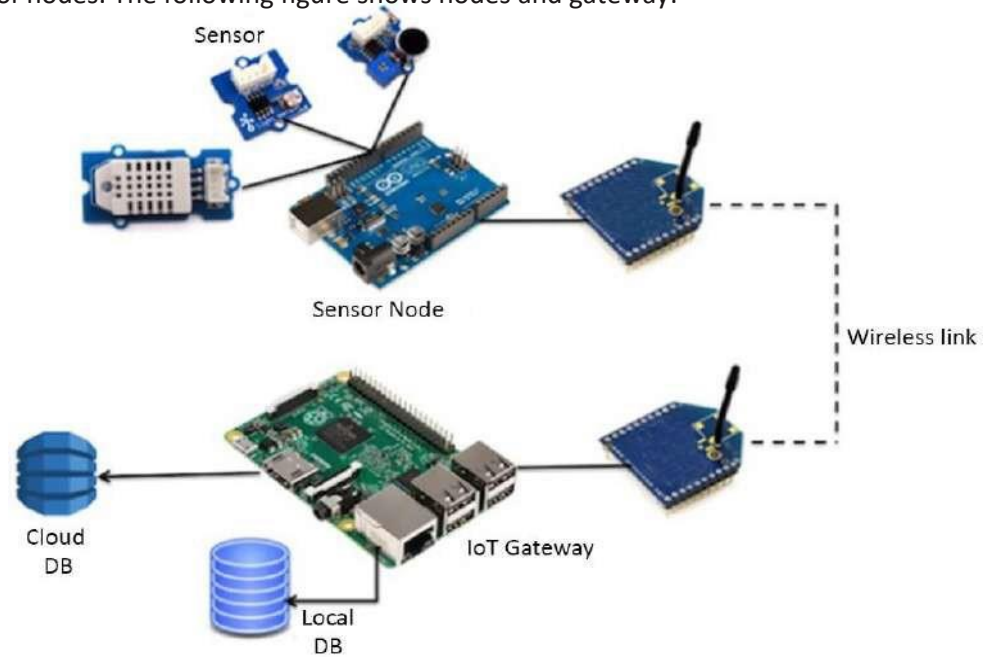


Fig. 2.10.1: Nodes and gateway

Wireless point-to-point or mesh network is easily made with XBee modules by configuring them (to operate in transparent data/API mode) with the standard AT commands. XBee modules have built-in error correction for eliminating any errors for reliable wireless link. They come in plethora of options having support for protocols like ZigBee, Bluetooth and Wi -Fi.

The following figure shows an IoT network:

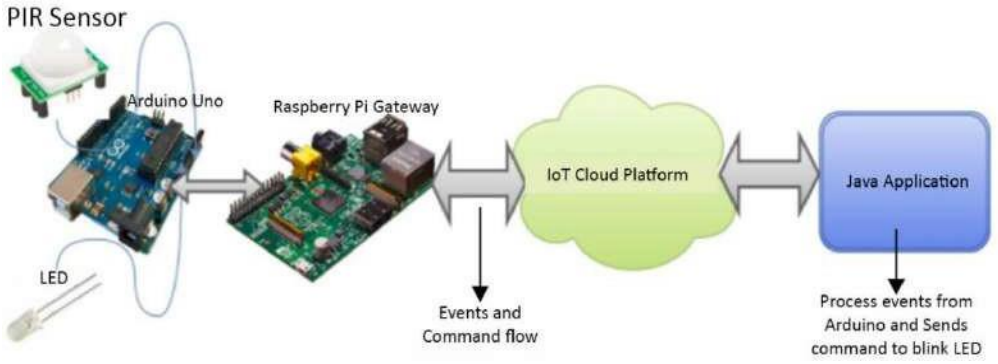


Fig. 2.10.2: An IoT network

The configurations that can be used to demonstrate the gateway support are as follows:

- Raspberry Pi as gateway
- Arduino Uno as device
- Passive infrared (PIR) Motion sensor connected to Arduino Uno
- Internal temperature sensor connected to Arduino Uno
- LED as actuator connected to Arduino Uno

Signal from PIR sensor and the internal temperature sensor are detected by the Arduino Uno and this data is transmitted to the Raspberry Pi. Then the Raspberry Pi Gateway will allocate the data to Watson IoT Platform via MQTT.

2.10.2 Understanding the Code

Programs/codes are first created in the Arduino development environment and then uploaded onto the Arduino board. The code needs to have proper syntax with use of valid command names and correct grammar for each code line. The code compiler will go through the entire code and then flag syntax errors before downloading. These programs are input line by line. Every Arduino program has two functions - setup() and loop().

The instructions in the setup() function are used to initialize the program and are executed when the program starts.

The following screenshot shows a structure of a program in Arduino:

```
void setup()
{
  // commands to initialize go here
}

void loop()
{
  // commands to run your machine go here
}
```

Fig. 2.10.3: Structure of a program in Arduino.

A program has the following elements:

- Statements, also known as commands, end with a semi-colon (;).

  Note: Most of the times the programmer forgets to enter the semi-colon which leads to an error. This error should be checked thoroughly.
- Comments are the notes that follow the code written after "//" on a line. Multi-line block comments begin with "/*" and end with "*/".
- Constants are fixed numbers which can be written as ordinary decimal numbers (integer only), in hexadecimal (base 16) or in binary (base 2).
- Labels - Labels refer to the locations in the code, and they are combination of letters, numbers and underscore (_). The first character of a label should be a letter though. For pin pointing a location, label ends with a colon. The following image shows a code segment with label:

```
repeat: digitalWrite(2,HIGH);
        delay(1000);
        digitalWrite(2,LOW);
        delay(1000);
        goto repeat;
```

Fig. 2.10.4: A code segment with label

- Variables are assigned by declaring in the program, and declaring them is a must. The following image shows the declaration of variables:

```
byte i;
word k;
int length;
int width;
```

Fig. 2.10.5: Declaration of variables

- Symbols redefine the naming and are used for making the code ready for scanning. Symbols are denoted by "#define" command, and they need to be at the start of the program.

The following image shows a demonstration without symbols when an LED is connected to pin 2:

```
void setup()
{
  pinMode(2,OUTPUT);
}

void loop()
{
  digitalWrite(2,HIGH);  // turn LED on

  delay(1000);
  digitalWrite(2,LOW);   // turn LED off
  delay(1000);
}
```

Fig. 2.10.6: Example of symbols

The following table lists some commands of Arduino programming:

pinMode(n,INPUT)	Set pin n to act as an input; one-time command at top of program
pinMode(n,OUTPUT)	Set pin n to act as an output
digitalWrite(n,HIGH)	Set pin n to 5V
digitalWrite(n,LOW)	Set pin n to 0V
delay(x)	Pause program for x millisec, x = 0 to 65,535
tone(n,f,d)	Play tone of frequency f Hz for dmillisec on speaker attached to pin
for()	Loop. Example: For (i=0;i<3;i++){} do the instructions enclosed by {} three times
if (expr) {}	Conditional branch. If expr true, do instructions enclosed by {}
while (expr) {}	While expr is true, repeat instructions in {} indefinitely

Table 2.10.1 Commands of Arduino

2.10.3 Transferring Software Codes

The nodes and the gateways may be connected to the microcontroller board and the software code may be transferred through the following:

- Wi-Fi module
- Bluetooth module
- SD card
- ZigBee modules and so on

The following steps helps to load a software code from the nodes to the microcontroller board:

- With a serial cable interface, connect the kit to the computer.
- Then put the microcontroller in the hardware's socket and push the lock button to ensure proper connection to the board.
- Open the software on the computer. Then, navigate to the menu bar and open File-functions-open-save-setting options.
- Select 'Open' from the drop-down menu and select 'Load file'.
- Then, click 'Load' button to upload hex file into the microcontroller.

Other conventional method to burn a controller is to unplug the circuit, place it on burner and then with an API, load the hex file. However, controllers these days come with In System Programmer (ISP) feature which saves the step of programming a controller without removing the controller from the circuit.

2.10.4 Challenges in Transferring

Some of the challenges in transfer of the codes to the microcontrollers are as listed in the following figure:

Power Supply Error

- While programming a PICAXE microcontroller, there's an error "unable to program". The reason for this could be the wrong/faulty power supply connected to the microcontroller. For example, using a faulty wall adapter when replaced with the correct one results in smooth programming.

Choosing Appropriate Serial Port

- While programming, mention the port to which the programmer is connected. For example, not selecting the correct serial port results in failing to program PIC microcontroller.

Installation of Drivers

- Install the necessary drivers before ensuring proper functioning of the programmer. By default the drivers are installed automatically when programmer is connected for the first time. If it doesn't, download the drivers online. For example, while programming, the Arduino drivers didn't install automatically and the location of drivers had to be specified.

Pull Ups

- Some microcontrollers need pull ups in their circuit before programming. For example, pickaxe microcontroller needs 10k pull up resistor on the serial pin before programming. If this is not done, there's an error.

Microcontroller Undetected by Programming Application

- This indicates problem with power supply check; so recheck the connection and then again connect the programmer to the computer. Now, it should be able to detect the the microcontroller; otherwise there might be a problem in the microcontroller.

Fig. 2.10.7: Challenges in transfer of codes

Exercise

1. Complete the following table by writing the commands in Arduino boards programming.

pinMode(n,INPUT)	
pinMode(n,OUTPUT)	
	Set pin n to 5V
digitalWrite(n,LOW)	
delay(x)	
	Play tone of frequency f Hz for d millisec on speaker attached to pin
	Loop. Example: for (i=0;i<3;i++){} Do the instructions enclosed by {} three times
	Conditional branch. If expr true, do instructions enclosed by {}
while (expr) {}	

2. Write down the steps that help to load a software code from the nodes to a microcontroller board.

_____

_____

_____

_____

2.10.5 Compiling a Code

After the microcontroller board is connected to the sensors, the microcontroller needs to be compiled by a code. This code will enable the microcontroller to work with the sensor. The following steps are the example of a test code which is used to connect a fingerprint sensor and a Raspberry Pi board:

1. Booting up a Raspberry Pi board:
   - While booting up the Raspberry Pi board, configuration tool called "rasp-config" needs to be called. The following screenshot shows the command window for the same:

Fig. 2.10.8: A "rasp-config" command

   - Then, select the keyboard type to "Generic 105 PC" option.
   - Select other option from the "configuration of keyboard" settings.
   - Set up a login id and password for the Raspberry Pi board from the Raspi-config main screen.
   - Finish by accepting all the changes.
   - Then, enter the region for time zone in Rasp-config screen.
   - Finish the process and the configuration is done.
2. Compiling code for a fingerprint sensor:
   - Run one of the sample files:

     python2 /usr/share/doc/python-fingerprint/examples/example_index.py

- A total of 1000 different fingerprints can be stored. The following code will appear which shows the position under which the fingerprint data is stored:

  Shell

  Currently stored templates: 0

  Please enter the index page (0, 1, 2, 3) you want to see:
- If the message appears as:

  "Exception message: The fingerprint sensor port "/dev/ttyUSB0" was not found!" then, check the cabling of the set up.
- For recording fingerprints call the following:

  python2 /usr/share/doc/python-fingerprint/examples/example_enroll.py
- Now, put the finger on the scanner and wait till the finger is scanned properly. And then, put the finger second time for verification for the storage number.
- To check whether the finger is recognized, call the following code:

  python2 /usr/share/doc/python-fingerprint/examples/example_search.py
- Now, put the finger again and check for the following message if the finger is detected successfully:

  Currently stored templates: 2

  Waiting for finger...

  Found template at position #1

  The accuracy score is: 63

  SHA-2 hash of template:
  3aa1b01149abf0a7ad0d7803eaba65c22ba084009700c3c7f5f4ecc38f020851

2.10.6 Types of Compilers

Some common compilers used are as follows:

- **MPLAB XC8 C pic microcontroller Compiler:** The MPLAB XC8 C compiler is the best compiler of top series compilers and it only supports the 8-bit pic microcontrollers such as PIC 10, PIC 12 and PIC 18. It is also known as ANSI C compiler.
- **MPLAB XC16 C pic microcontroller Compiler:** MPLAB XC16 C compiler is a version of MPLAB XC compiler but this version only supports the 16-bit pic microcontroller such as, PIC 24F, PIC 24H, PIC 24E, DSPIC 30F, DSPIC 33F and DSPIC 33E.
- **MPLAB XC 32 C pic microcontroller Compiler:** The MPLAB XC32 C compiler is also a version of MPLAB XC compiler but it is only used for support or to program the 32-bit microcontroller such as PIC32 MZ, PIC32 MX and PIC32 MM.

The following screenshot shows an MPLAB XC 32 C pic microcontroller compiler:

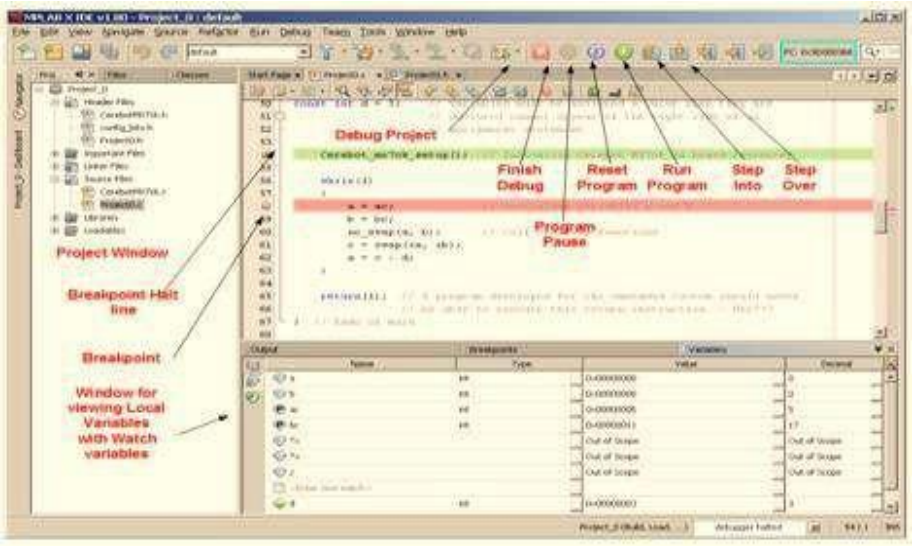


Fig. 2.10.9: MPLAB XC 32 C pic microcontroller compiler

- PIC CSS pic microcontroller Compiler: It has the largest built in functional library such as data type (int1, int32, short, long, float and so on), standard C syntax (if, else, while, do, switch, break and so on) and powerful pre-processor commands for pic microcontroller. It has ready to run examples of programs for user's understanding. It has the facility to migrate from one microcontroller to any type of other pic microcontroller. It has standard C constructs and peripheral drivers with minimum development time. The following screenshot shows a PIC CSS pic microcontroller compiler:

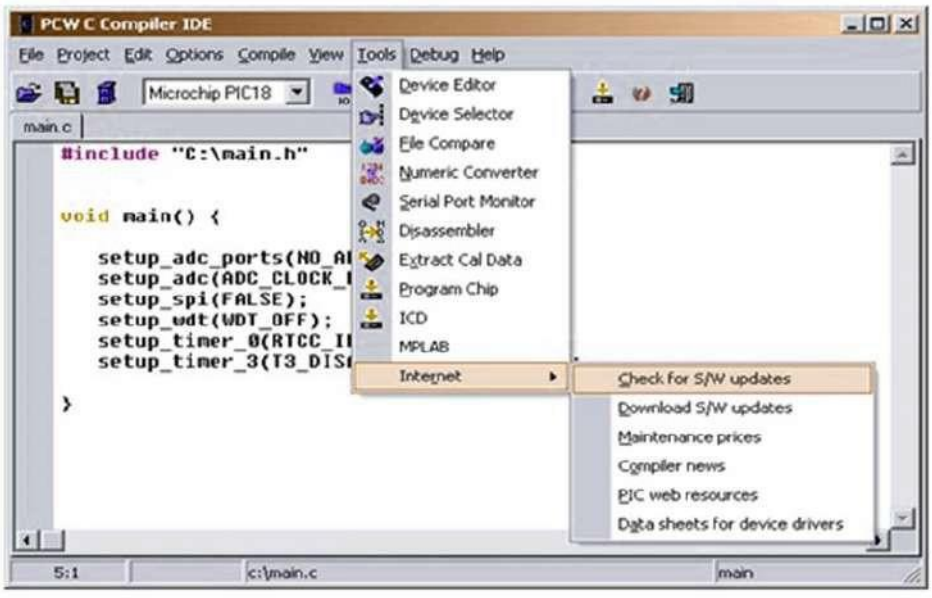


Fig. 2.10.10: PIC CSS pic microcontroller compiler

Exercise

1. Write down the types of compilers used in microcontroller compiling and their features.

UNIT 2.11: Understanding Error Codes and Debug Software

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the ways of debugging a microcontroller code
2. Explain the steps of setting the software in debug mode
3. Interpret the error codes

2.11.1 Introduction

The user may encounter errors and warnings, resulting in bringing the procedure to a halt. Such errors are mostly syntactical in nature and make execution of the code impossible. An attentive and logical approach can help in resolving such situations. Execution of code needs to be completed to go to the next level. Errors can occur on an 8-bit micro (like the PIC16F88) while entering values of about 8 bits and mistakenly putting wrong values. As it requires 8 bit values, putting values lesser or higher than 8 will lead to error prompt. However, to correct the error try adding longer/shorter values, which might initially cause weird results. Once the right value is put, the compilation will automatically start.

There are various ways of debugging a microcontroller. The following figure shows the ways:

In Circuit Emulator(ICU)

- ICU is a special processor allowing access to the internal operation of the processor.

In Circuit Debug (ICD) or PIC Microcontroller

- ICD, also called Background Debug Mode(BDM) lets access through code running in the target processor. The processor with a tiny hardware onboard halts the processor after the program reaches a specific address.

Simulation

- The source code simulator enables doing the complex language code and watching its effect on memory and variables without actually having to look at the assembler code. This enables concentrating on the high level language operation and hence on the problem at hand.
- It cuts the time taken to download and program the target processor.

Serial RS232

- The latest microcontrollers have a built in UART. It is like a free debug tool that requires very less software coding and resources.
- For debug output, the UART output pin (TX) needs to be connected to a suitable level translator circuit.

Liquid Crystal Display (LCD)

- LCD is an easy display output of debugging information. This is specific in case of computing. Showing text display output is its another use.
- The LED indicator shows how healthy a microcontroller is.
- It displays text as 16 characters in length in 2 rows.
- Blinking LED works like a debugging tool to inform that the downloaded code is working fine.
- Incorrectly set parameters on the programming software or compiler may render the code dead.

Pin Debugging

- It is probably the easiest debugging method. All it requires is setting or resetting the pin in the code meant to be monitored.
- It has minimal impact on the code speed or size and can provide the following information:
- Tells if the code is active
- Offers information on the repetition rate
- Provides the routine time length
- To test, all it requires is an oscilloscope or a frequency counter and time measuring tool

Logic Analyser

- This tool is attached to the pins to be observed and captures the waveforms displaying multiple traces on a single display. It uses a trigger module that can be set to activate on combinations of the input signals or on their length. So, one can trigger on specific patterns or on glitches or both.
- The logic analyser can be of great use in examining peripheral operation if a system uses microcontroller for debugging the SPI or I2C buses. Some logic analysers come with built-in support for such protocols.

Fig. 2.11.1: Ways of debugging

2.11.2 Setting Debugging Mode in Microcontroller

The following steps show how to enable debugging using a LabVIEW application:

Step 1: Go to the Project Explorer window and explore Build Specifications option. Right click and select Properties as shown in the following screenshot:

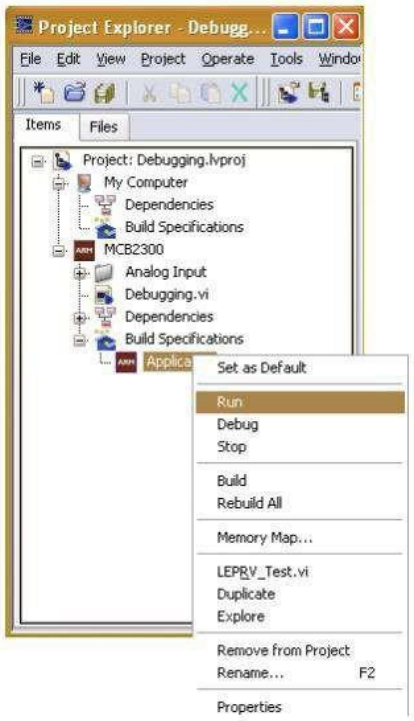


Fig. 2.11.2: Enabling build specifications

Step 2: This will fetch the Build Specification Properties window. Select Application Information from the Category bar as shown in the following screenshot:

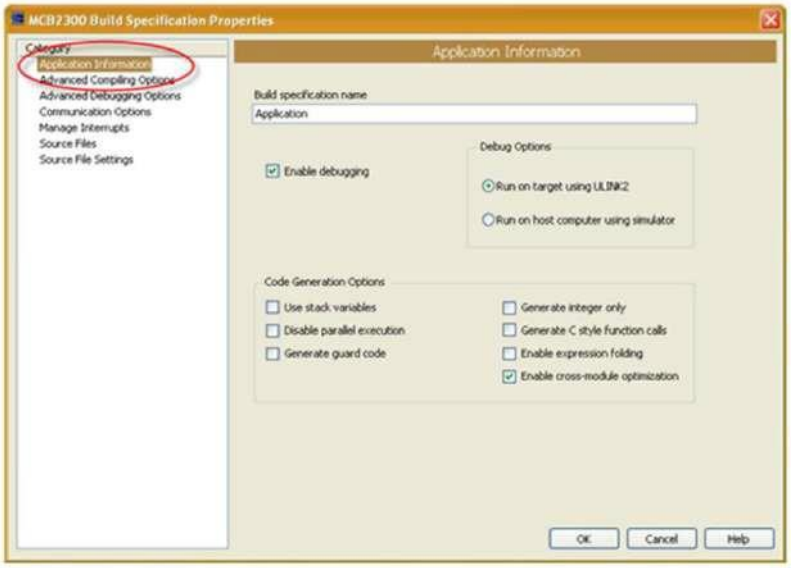


Fig. 2.11.3: Setting build specifications properties

Step 3: Check if the Enable debugging checkbox is selected in the Build Specification Properties window. Under Debug Options, select either Run on target using ULINK2 or Run on host computer using simulator. Choose the first option to debug if hardware is available and code's operation needs to be tested in real environment settings. Go for the second option if no hardware is available or rapid testing needs to be carried out in a simulated mode. The following shows the screenshot for setting debug options:

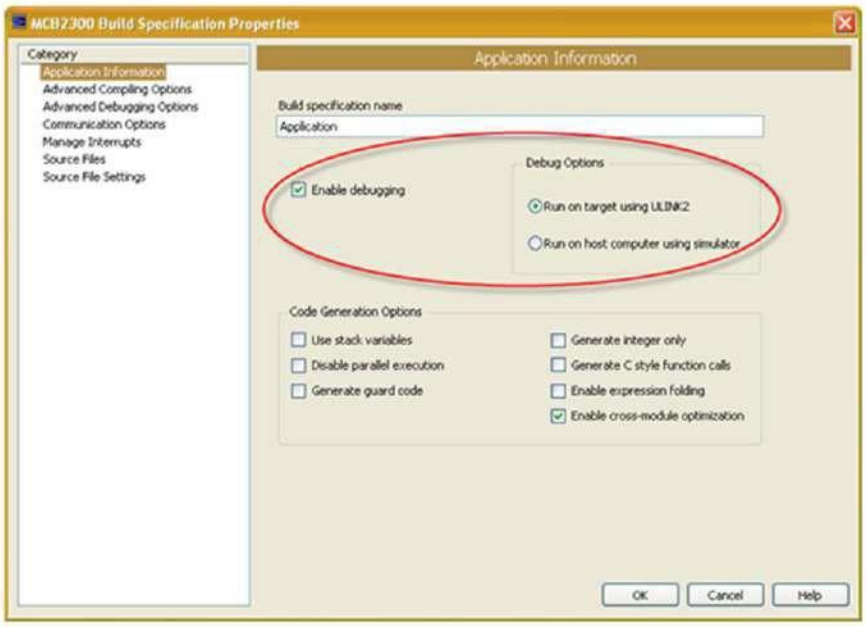


Fig. 2.11.4: Setting debug options

Step 4: Now, select Advanced Debugging Options from the Category bar on the left. Under Debug Mode, the following options are listed – 1) Serial port 2) TCP port 3) USB ULINK2 JTAG. The following screenshot shows options for setting communications:

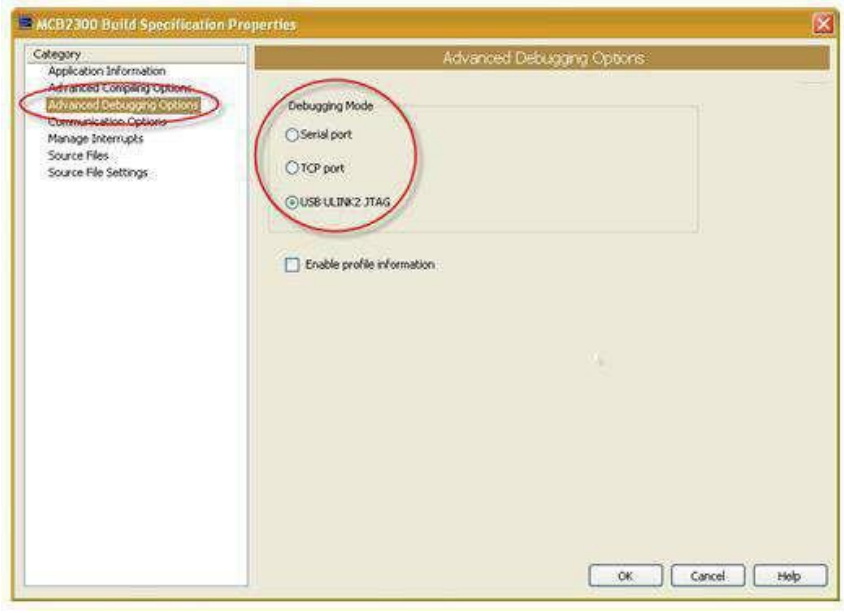


Fig. 2.11.5: Setting communication options

Step 5: Click the OK button situated on the right bottom. This will enable debugging. Now, go back to the Project Explorer window, right-click the Application and select Run. The following screenshot shows running of application:

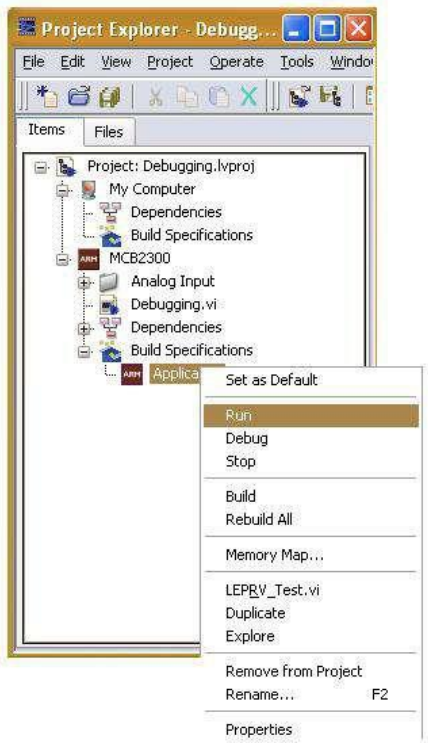


Fig. 2.11.6: Running the application

2.11.3 Understanding and Interpreting Error Codes

Generally, compile time errors and warnings are caused by incorrect syntax or wrong variables or functions. The error prevents completion of compile process, resulting in formation of no binary file. However, the warning does not prevent the binary from being created, but reviewing it is important as the intended task will not be achieved through the code.

The following screenshot shows Arduino compiler error message:

Fig. 2.11.7: Arduino compiler error messages

The common errors are as follows:

- "Identifier undefined" errors due to missing variables and interfaces
- Missing semicolons ";". Semicolons are a must at the end of each line
- Missing quotes of brackets, "",(),[] or {}. These are used in pairs to contain various types of statement. An error will occur if they are not used in correct pairings

Running Verify/Compile command will fetch a number of compiler errors in the dialog box.

The following image shows a Java code segment:

```
1  /*--- Blink an LED  ---//
2  //Associate LEDs with an Arduino Digital pin.
3  //The Arduino already has a built-in LED that we can use on D
4  int ledPin = 23;  \\We're using Digital Pin 23 on the Arduino
5
6  void setup();
7  {
8     pinMode(ledPin OUTPUT);    //Set up Arduino pin for output
9  }
10
11 loop()
12 (
13    /The HIGH and LOW values set voltage to 5 volts when HIGH
14    digitalWrite(ledPin, high); //Setting a digital pin HIGH t
15    delay(1000):  //Get the microcontroller to wait for one se
16    digitalWrite(ledPin. LOW);  //Setting the pin to LOW turns
17    Delay(1000);  //Wait another second with the LED turned of
18    }
19 }
```

Fig. 2.11.8: A Java code segment

Upon compilation of the code, the errors as shown in the following table may appear:

Line	Error Message	Interpretation
Line 1 /*— Blink an LED —//	Uncaught exception type:classjava.lang.RuntimeException java.lang.RuntimeException: Missing the */ from the end of a /* comment */	The error in line 1 is because of wrong usage of comment styles. The comment should end with "*/" instead of "//". Hence the correct code is: /*— Blink an LED —*/
Line 4 Error intledPin = 23; \\We're using Digital Pin 23 on the Arduino.	error: stray '\' in program	The line uses "\\" characters to begin a comment rather than "//" characters. The correct line is: intledPin = 3; //We're using Digital Pin 3 on the Arduino.
Line 6 Error void setup();	error: expected unqualified-id before '{' token	The error is occurring because of usage of the semicolon (;). Remove the semicolon as shown below: void setup()

Line	Error Message	Interpretation
Line 8 Error 'void setup()': pinMode(ledPin OUTPUT); //Set up Arduino pin for output only.	error: expected `)' before numeric constant/home/myDirectory/ Desktop/myPrograms/arduino - 0015/hardware/cores/arduino /wiring.h:102: error: too few arguments to function 'void pinMode(uint8_t, uint8_t)' At global scope:	The error is because of missing comma between ledPin and OUTPUT. The correct code should be like: pinMode(ledPin, OUTPUT); //Set up Arduino pin for output only.
Line 11 Error loop()	error: expected constructor, destructor, or type conversion before '(' token	As no value is not being returned, so the keyword voidin front of the function name needs to be added. The correct code is: void loop()
Line 13 Error /The HIGH and LOW values set voltage to 5 volts when HIGH and 0 volts LOW.	error: expected primary-expression before '/' token	This line should be a comment telling what the program is for. The error is occurring because of only one slash character "/" instead of two "//". Add another slash character. //The HIGH and LOW values set voltage to 5 volts when HIGH and 0 volts LOW.
Line 14 Error digitalWrite(ledPi n, high); //Setting a digital pin HIGH turns on the LED.	error: 'high' was not declared in this scope	Programming in C language considers upper and lower case letters differently. To fix this error, use upper case letters in case of 'high' and recompile. Example: digitalWrite(ledPin, HIGH); //Setting a digital pin HIGH turns on the LED.
Line 15 Error delay(1000): //Get the microcontroller to wait for one second.	error: expected `;' before ':' token	This statement is ending with a colon character ":". However, a semicolon ";" should be used in this case. It can be fixed by simply replacing colon with the semicolon and recompiling. delay(1000); //Get the microcontroller to wait for one second.

Line	Error Message	Interpretation
Line 17 Error Delay(1000); //Wait another second with the LED turned off.	error: 'Delay' was not declared in this scope	An error may occur simply using lower or upper case. Like in this case – the error is caused by using upper case character for the letter "d" in delay. User lower case and try again. delay(1000); //Wait another second with the LED turned off.
Line 18 Error } }	error: expected declaration before '}' token	An extra character may cause an error. An extra curly brace at the end of this program is a good example. Remove it to fix the error.

Table 2.11.1 Common errors in Arduino

Exercise

1. Write down the interpretation for the given code and message used for debugging a microcontroller.

Code and Message	Interpretation
E2483: Array dimension 'specifier' could not be determined	
E2509: Value out of range	
E2100: Invalid template declarator list	
E2249: = expected	

2. Write down the ways to debug a microcontroller board.

_____

_____

_____

_____

UNIT 2.12: Functioning of Microcontroller and Attached Devices

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the steps to check the microcontroller functions
2. Describe how to use the Emulator to check the proper functioning of the devices
3. Manage the communication hurdles

2.12.1 Understanding the Basic Framework

It is very important to understand the basic framework of any system. Otherwise, the connections cannot be made in an efficient way. The technician must understand the location of the installation points of the gateways and the devices, so that the installations and connections are made properly. The following image shows the security system of a

Fig. 2.12.1: Home security system

There are motion detector sensors, fire or smoke alarm sensors, water level sensors and temperature sensors installed in the house. The technician needs to install the sensors and connect them to the main system through the network connections available. He/she needs to understand the compatibility of the software and its versions to install the whole framework in the monitoring system.

2.12.2 Checking Functioning of Microcontrollers

Ensure that the correct input signals are being applied to the microcontroller from each sensor and that the correct output signals from the microcontroller will drive the output circuitry in the expected manner.

However, in some cases where a part of hardware is powered or controlled by a microcontroller using another microcontroller, testing that section is comparatively easier.

The following figure shows the steps to check the functioning of the Raspberry Pi microcontroller:

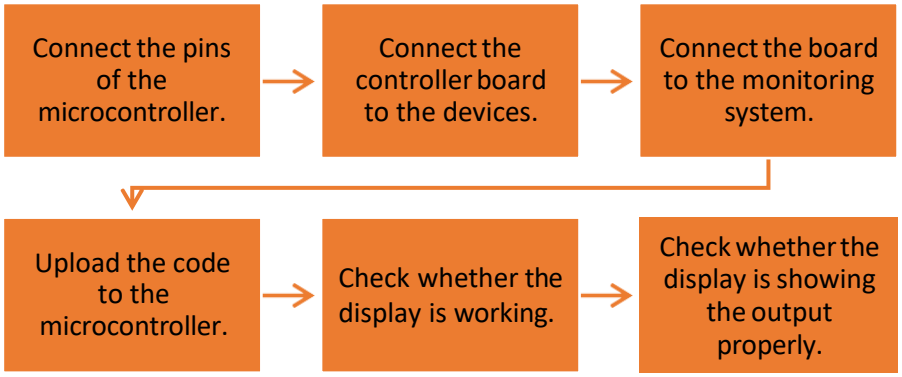


Fig. 2.12.2: Steps to check the functioning of a microcontroller

The steps to run a complete board test are as follows:

Step 1: Usually the controller board comes preloaded with test software. This is to eliminate need of software installation process. All it requires is connection to the system. Once the connection is established, access the serial terminal as shown the picture, set the baud rate at 9600 and reset the controller. A test menu (shown in the picture) will appear. Select fields as shown in the figure and follow the procedure to test all the peripherals. The following screenshot shows the test menu of the terminal:

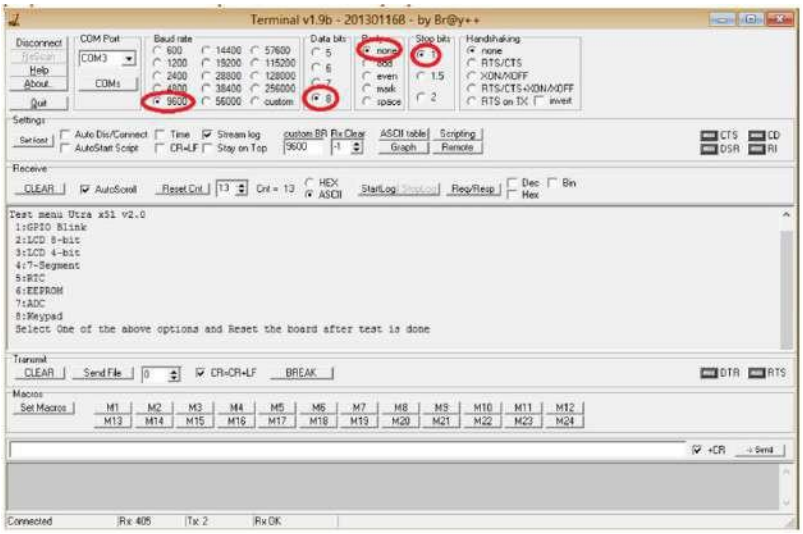
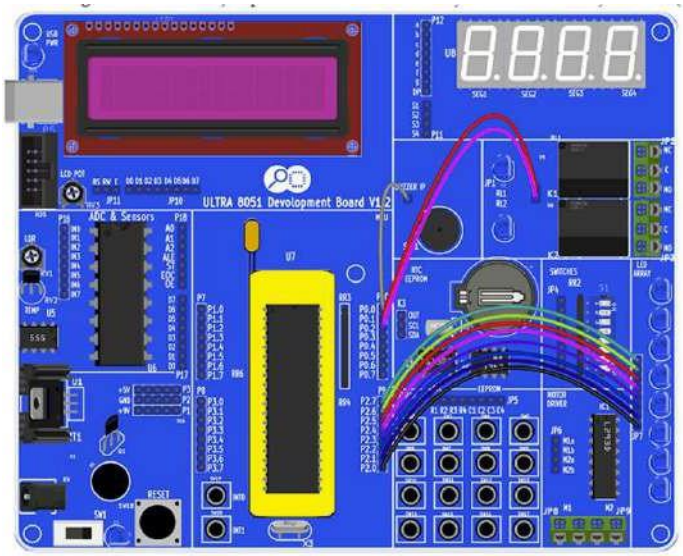


Fig. 2.12.3: Test menu of the serial terminal

Step 2: General-purpose input/output (GPIO) Test: To perform this test, try connecting LEDs, buzzer and relays to port pins and check if LEDs are blinking, buzzer is giving a beep sound and relay is chattering. However, the Rx, Tx pins will not blink because they are controlled by CP2102 (Usb2Serial). The following image shows the connectivity and the screenshot of the terminal window:



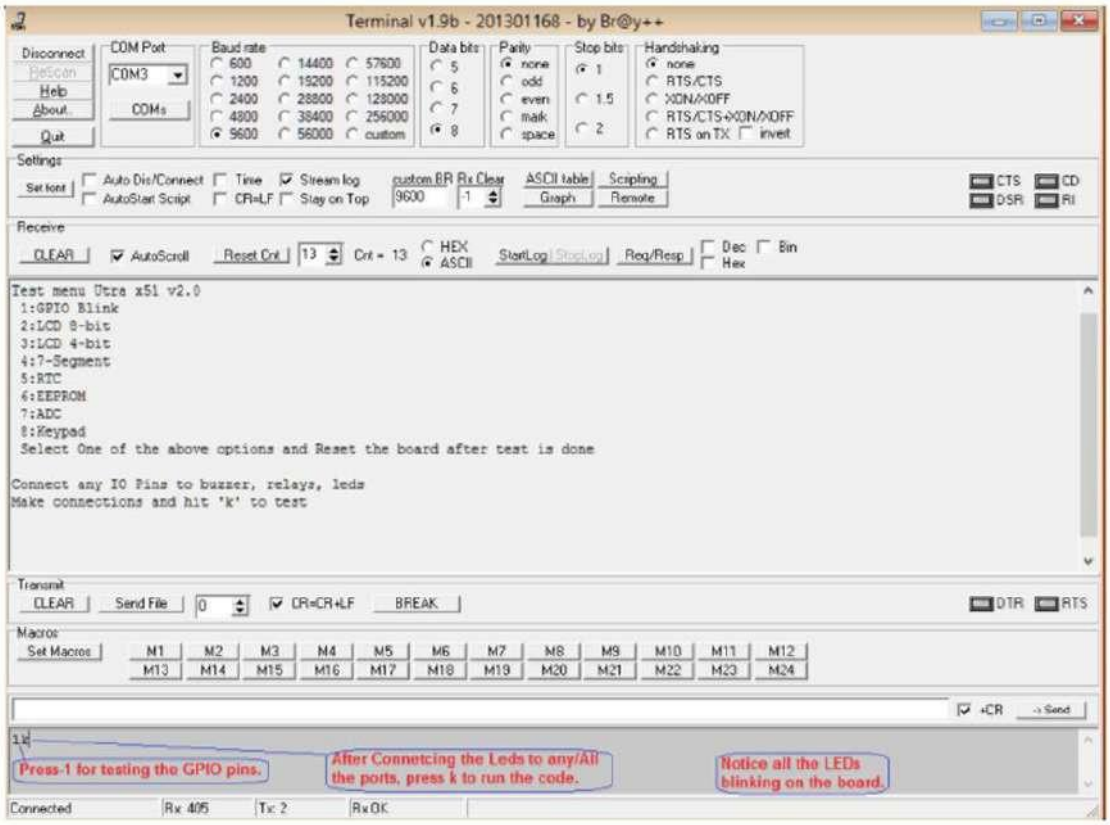


Fig. 2.12.4: Connectivity and the screenshot of the terminal window

The steps of the test are as follows:

- Press 1 to test GPIO pins
- Press k key to run the code after connecting LEDs to the ports
- Check if all LEDs are blinking or not

Step 3: LCD 8-bit Test: Connect the LCD pins. The following image shows the pin layout for the sample board:

RS	RW	EN	D0	D1	D2	D3	D4	D5	D6	D7
P0_0	P0_1	P0_2	P2_0	P2_1	P2_2	P2_3	P2_4	P2_5	P2_6	P2_7

Fig. 2.12.5: Sample LCD pin layout

The following image shows the LCD connection and the output:

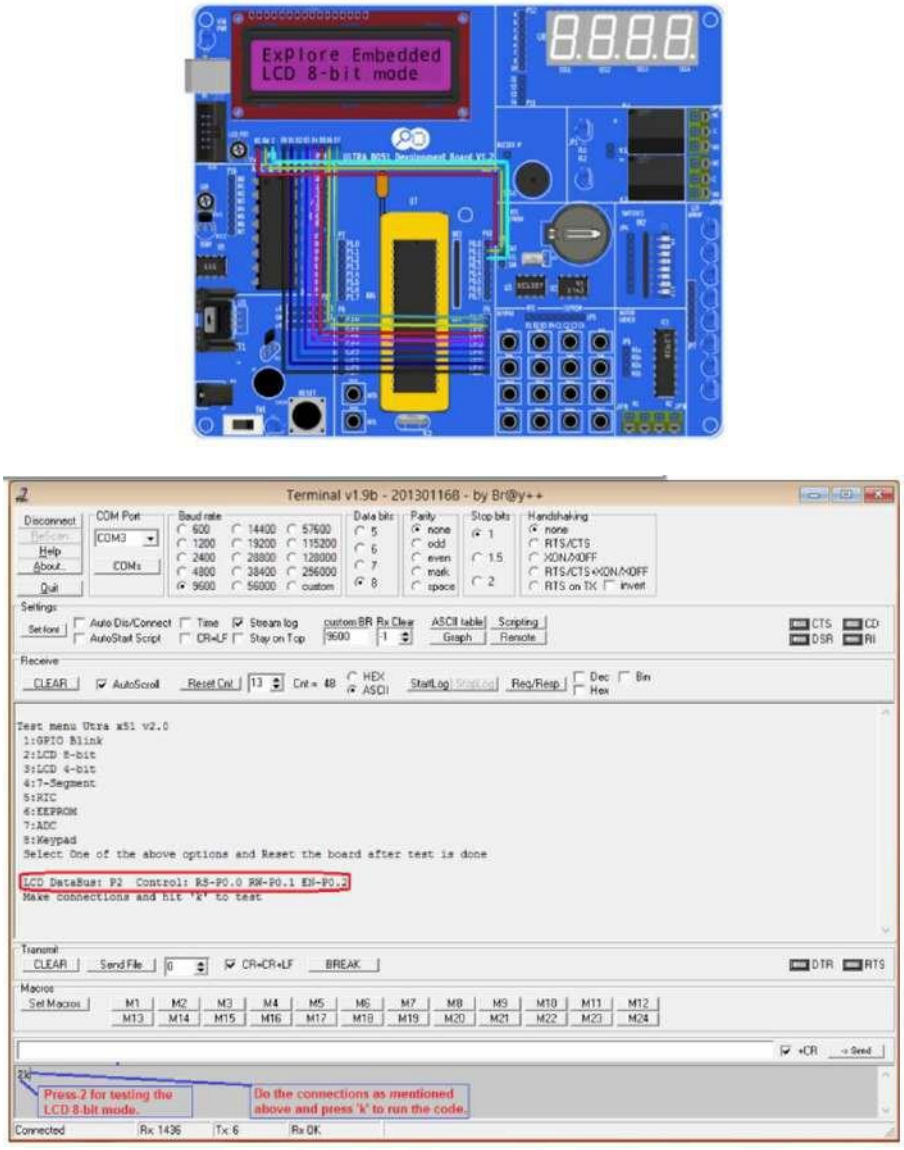
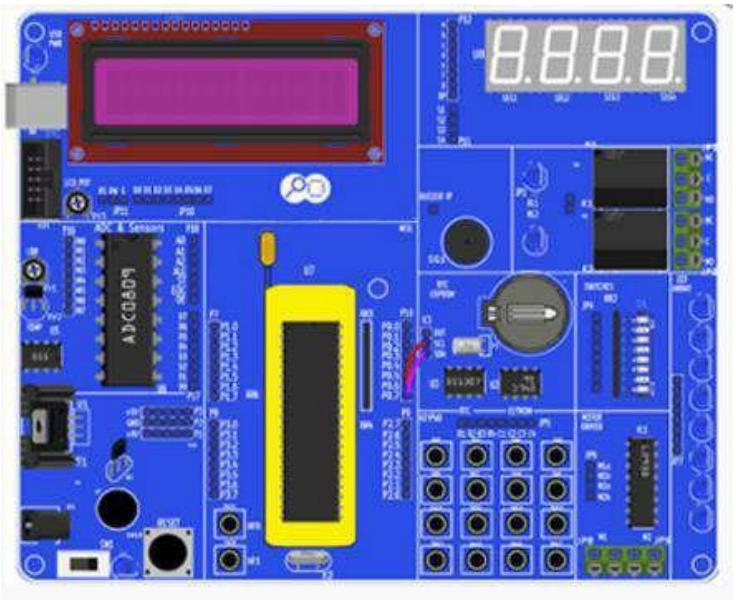


Fig. 2.12.6: LCD connection and the output

The steps of the test are as follows:

- Test LCD 8-bit mode by pressing '2' key
- Establish connection as said before, followed by pressing 'k' to run the code

Step 4: Real-Time Clock (RTC) Test: The RTC pins are connected to P0 (SCL-P0.6, SDA-P0.7). The following image shows the RTC test and the output:



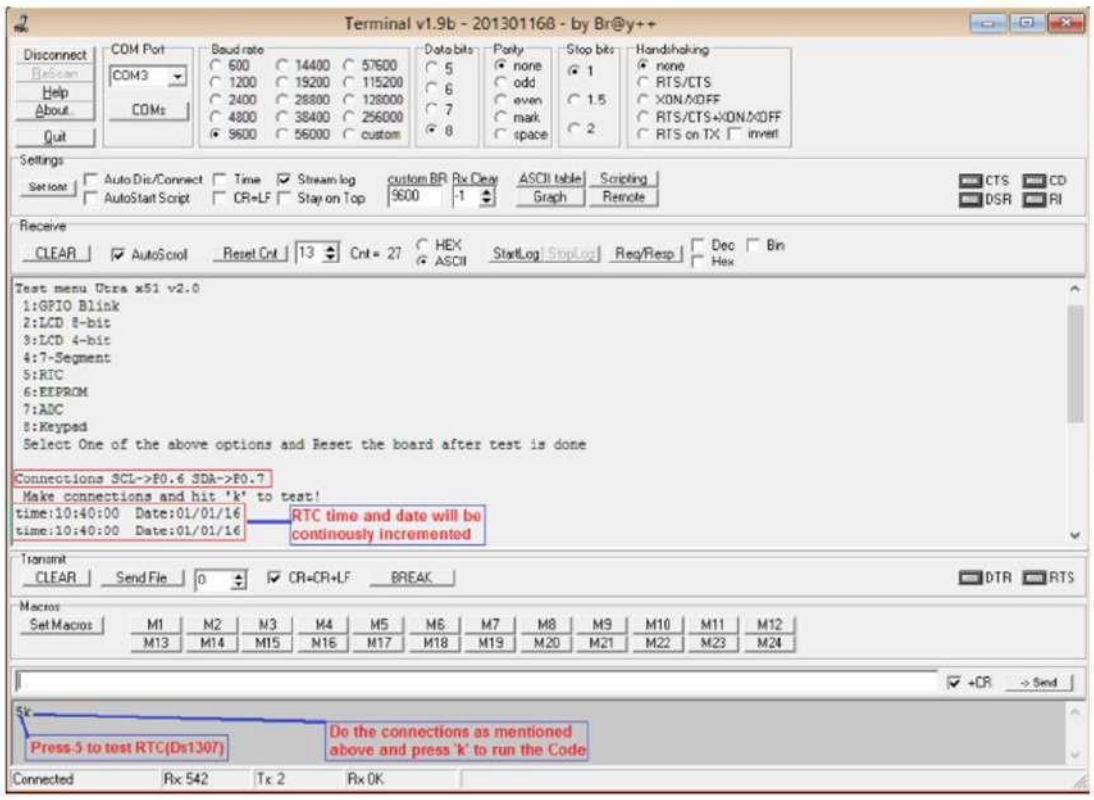


Fig. 4.7.7: RTC test and the output

The steps of the test are as follows:

- Press key 5 to run LCD 8-bit mode test
- Establish connections as stated before followed by pressing 'k' key to run the code
- After pressing 'k' key, there will be an increase in RTC time and date

Step 5: Analog-to-digital converter (ADC) Test: The board houses temperature sensor, Pot and LDR. Values these sensors read and collect are sent on Universal asynchronous receiver-transmitter (UART). Set all connection like before and press 'k' key to run the code. The following screenshot shows the output:

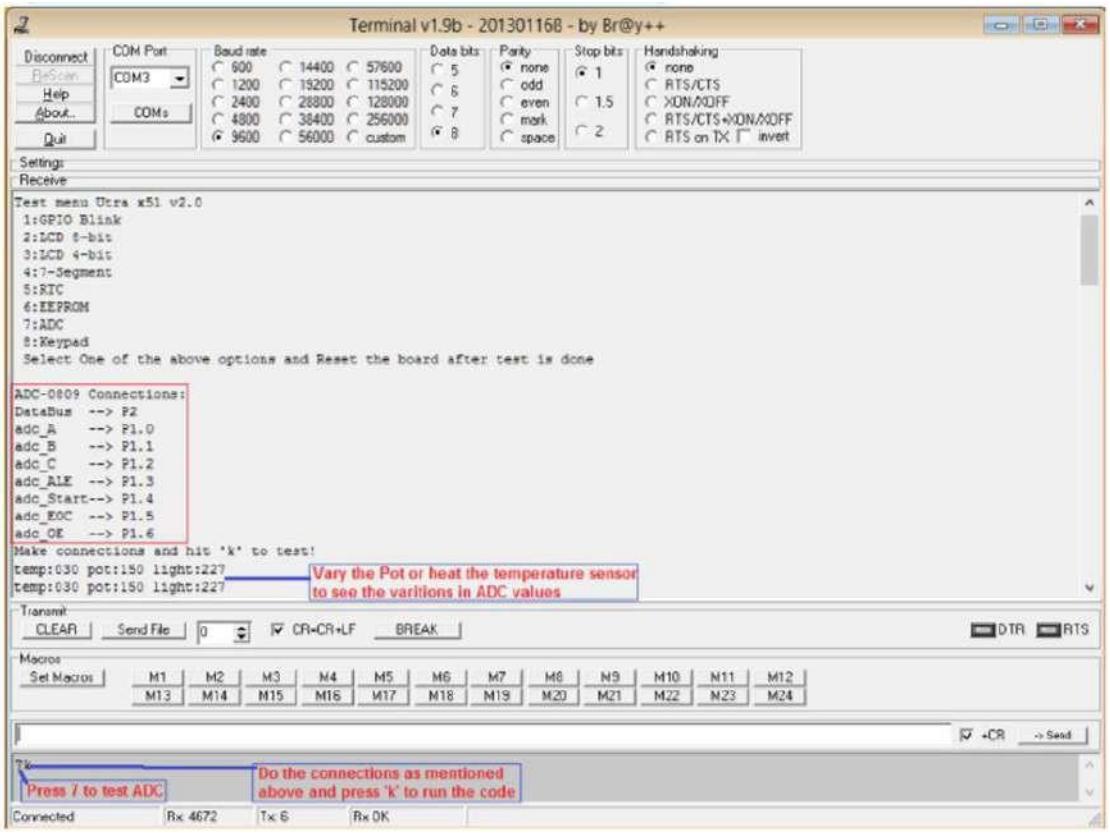


Fig. 2.12.8: ADC test and the output

Step 6: Keypad Test: Follow same procedure to set the connections and press 'k' key using the Hex keypad to run the code and check the output.

The following screenshot shows the output:

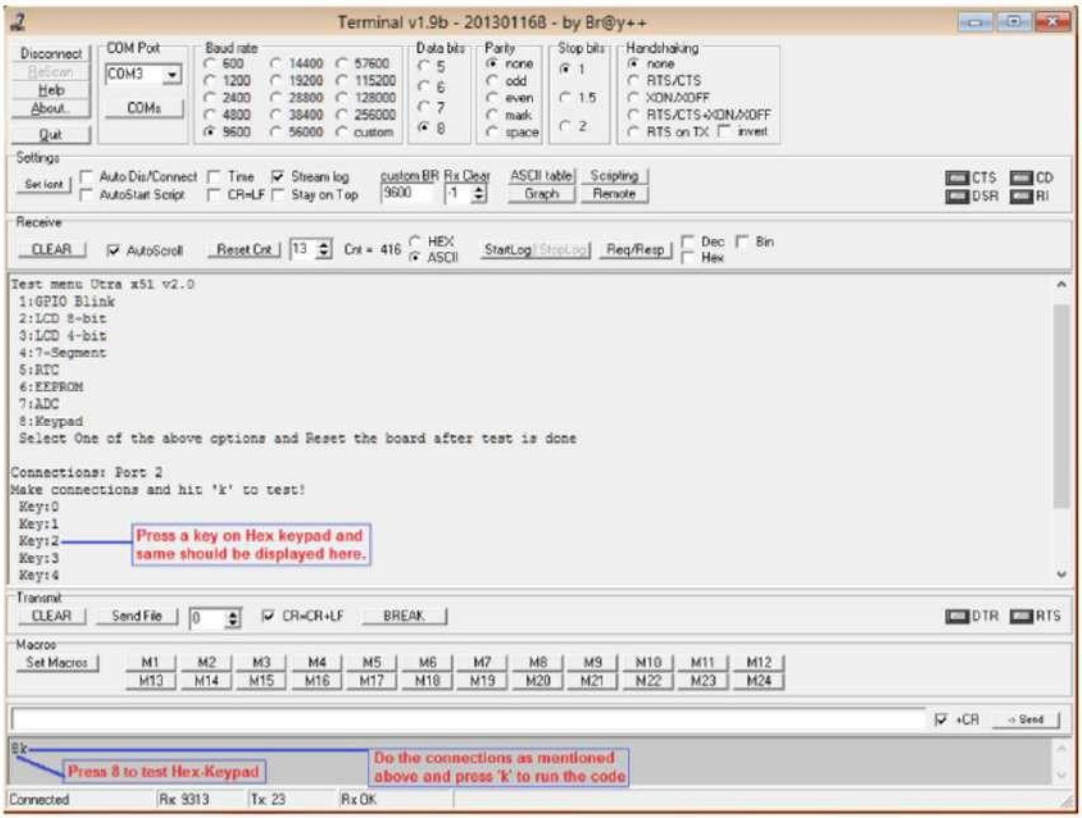


Fig. 2.12.9: Keypad test output

2.12.3 Checking Connectivity

The microcontroller board should be connected to the network through Ethernet, LAN or Wi-Fi connection. Then, the connection should be tested to see whether it is working properly or not. The procedure to be followed to test the device's connectivity to the network is as follows:

Step 1: Connect the device to the network.

Step 2: Choose Test Management Network and press Enter key.

Step 3: Type IP address or another DNS host name.

Step 4: Press Enter key to perform the test.

2.12.4 Using Emulator to Check Functioning of Devices

An emulator is a hardware that functions like a microcontroller. It is used as a debugging tool, owing to its functionality and efficiency. Functionality of an emulator is always non-intrusive in nature, which means emulation doesn't affect the resources or I/O pins present on the microcontroller in any way.

The following figure shows the connection of an emulator:

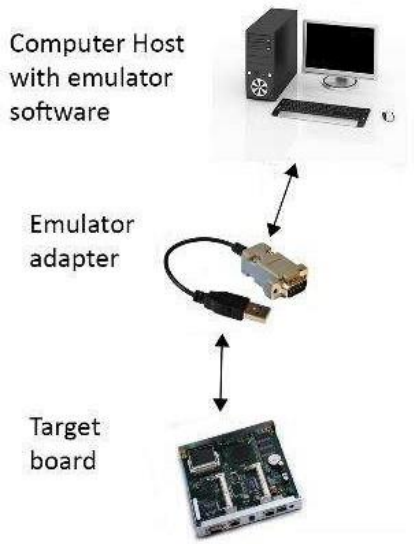


Fig. 2.12.10: Connection of emulator

The following interactions can be enabled if the target devices have built-in sensors like accelerometer, compass, light, or proximity sensors:

- Change application settings, based on the current light conditions
- Change the screen orientation (from portrait to landscape) as the device is flipped
- Change alert mode in case of an incoming call. Example: Flip the device screen towards the tabletop to silence the device
- Enable movement or gesture detection. Example: A security camera with motion detection is used
- Change the orientation of a map based on the device compass orientation

Applications utilizing sensor module in the emulator can be easily tested. The sensors view contains controls to set the values.

The following image shows the sensors module in an emulator:

Fig. 2.12.11: Sensor module in an emulator

The steps for emulation of an Arduino are as follows:

Step 1: Open the design software for simulation and place the components of the circuit as shown in the following screenshot:

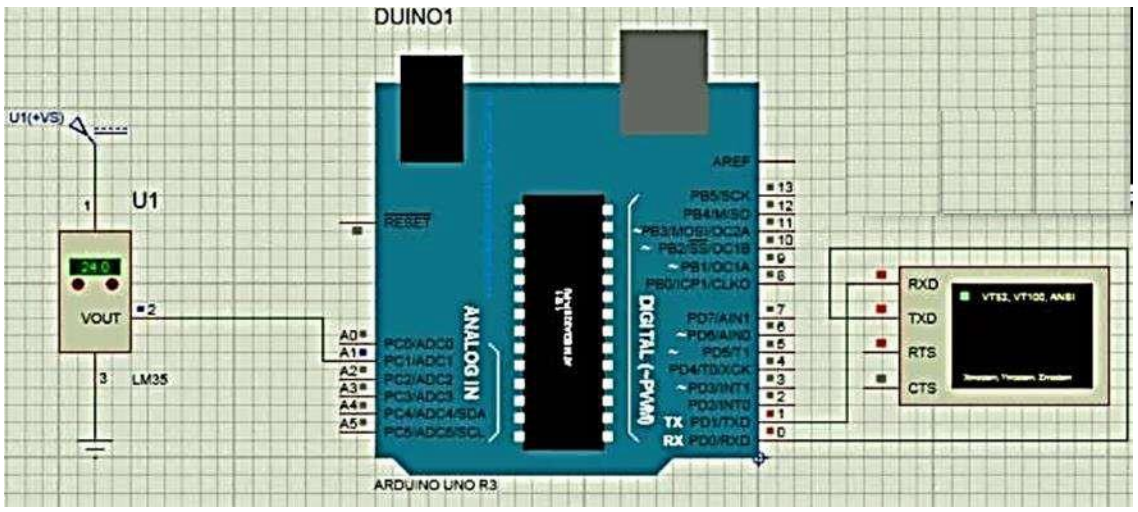


Fig. 2.12.12: Designing the circuit

Step 2: Save the design and open the code in the application for the Arduino coding as shown in the following screenshot:

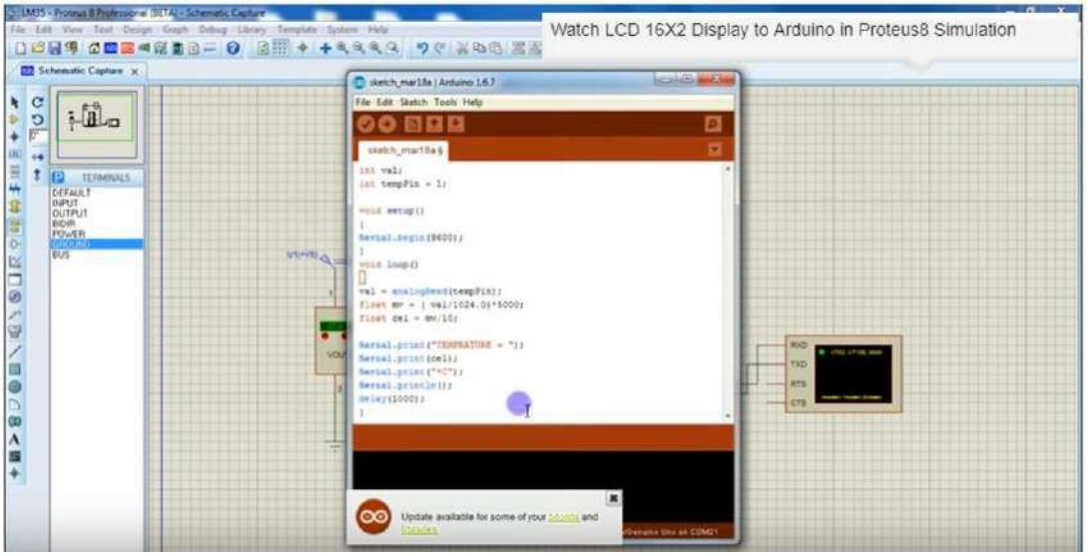


Fig. 2.12.13: Arduino code

Step 3: Compile the code and save it as shown in the following screenshot:

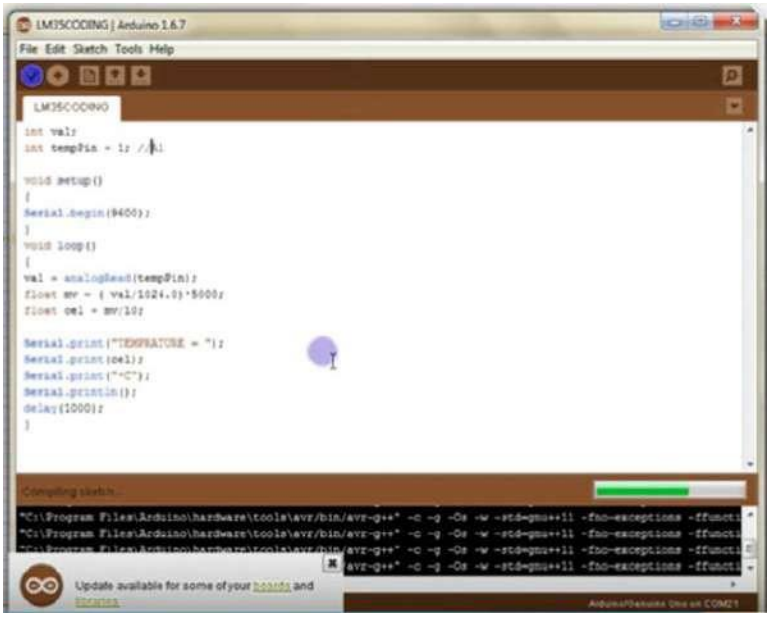


Fig. 2.12.14: Compiling the code

Step 4: Double click the Arduino board and the Edit component window appears, as shown in the following screenshot:

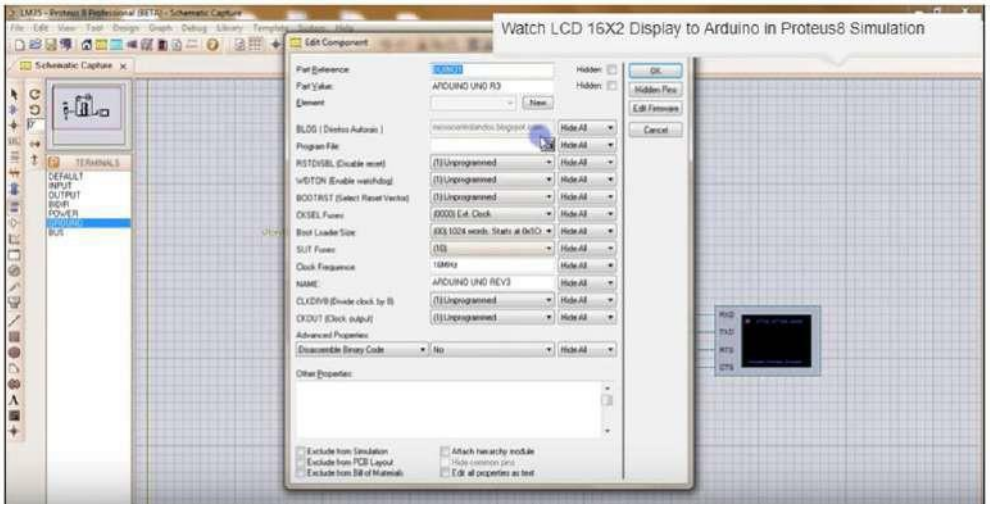


Fig. 2.12.15: Edit component window

Step 5: Browse the Arduino code and run. A virtual terminal with output will appear, as shown in the following screenshot:

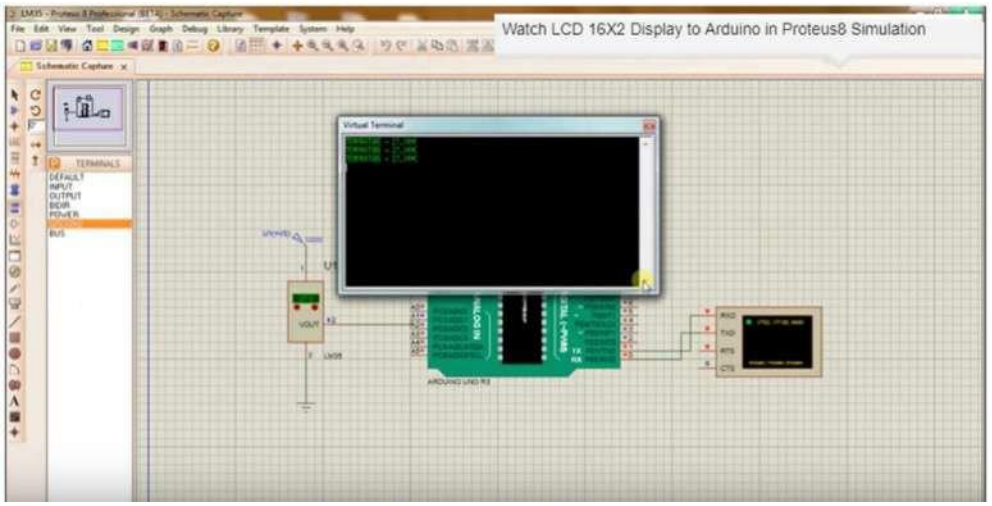


Fig. 2.12.16: Virtual terminal window with output

2.12.5 Removing Communication Hurdles

There may be some problems with connecting the devices to the monitoring system. The technician should take care of the communication problems between the devices and the gateways. The communication hurdles may be there because of various reasons that are as follows:

- The devices are not in the line of sight.
- The Ethernet is not connected properly.
- There is no network connection available.
- The devices are not in range of the network connection.

The technician should check if all the connections are made properly. He/she must ensure that the devices are installed in accurate places and the range of connectivity is proper. I t should also be checked that the software and the hardware are compatible to each other.

Exercise

1. Write down the interactions that can be enabled if the microcontroller is connected with an accelerometer or with gyroscopic sensors.

_____

_____

_____

_____

2. Write down the steps to check the functioning of a Raspberry Pi microcontroller.

_____

_____

_____

_____

Practical

Install and run a program on a Raspberry Pi board.

Required Tools/Equipment:

- Raspberry Pi board
- Connecting cables
- Computer system
- Raspberry Pi framework

Practical

Install and run a program on an Arduino board.

Required Tools/Equipment:

- Arduino board
- Connecting cables
- Computer system
- Arduino Uno framework

Practical

Install an Arduino Uno software on a windows OS and configure for a fingerprint sensor.

Required Tools/Equipment:

- Arduino board
- Connecting cables
- Computer system with windows OS
- Arduino Uno framework

Practical

Debug a Raspberry Pi board microcontroller.

Required Tools/Equipment:

- Raspberry Pi board
- Connecting cables
- Computer system
- Raspberry Pi framework

Practical

Perform cabling connection of a Raspberry Pi microcontroller board.

Required Tools/Equipment:

- Raspberry Pi board
- Connecting cables
- Computer system
- Raspberry Pi framework

Practical

Perform steps in optimising power consumption in a microcontroller board.

Required Tools/Equipment:

- Raspberry pi board
- Multimeter
- Personal protective equipments
- Signal tester
- Network with Ethernet cable
- Oscillator, diode and resistor of different values

Practical

Connect Arduino board to PC.

Required Tools/Equipment:

- Arduino board
- Laptop/Computer system with latest configuration and internet connection
- HDMI, USB, Type C, power cable for Arduino board
- PPEs (safety gloves, ESD band, safety shoes)

Practical

Connect Raspberry pi board to a system to boot the board.

Required Tools/Equipment:

- Raspberry pi board
- Laptop/Computer system with latest configuration and internet connection
- HDMI, USB, Type C, power cable for Arduino board
- SD card
- PPEs (safety gloves, ESD band, safety shoes)

Practical

Perform a connectivity check on an Arduino board.

Required Tools/Equipment:

- Make sure that all the network and power cables are connected properly
- Open the utility tool for Arduino testing on laptop
- Choose Test Management Network and press Enter key.
- Type IP address or another DNS host name.
- Press Enter key to perform the test

Practical

Perform emulation of an Arduino board.

Required Tools/Equipment:

- Arduino board connected with all cables
- Laptop/Computer system with latest configuration and internet connection
- Arduino design software installed on computer
- HDMI, USB, Type C, power cable for Arduino board

Key Learning Outcomes

At the end of this module, you will be able to:

1. Identify the prerequisites for initialization of nodes and gateways
2. Explain the configuration of edge appliances
3. Identify the steps of node and gateway initialization
4. Describe how to check connectivity
5. Explain the execution scenarios of software
6. Identify the prerequisites for software installation
7. Explain the challenges with launching software
8. Explain the data transfer indicators
9. Compare data transfer on various networks
10. Explain different data transfer failure scenarios
11. List the steps to connect to a network remotely
12. Identify the steps to connect to short range networks
13. Explain the configuration of a router
14. Describe controlling of devices by connecting hub
15. Explain the bypassing of a hub
16. Explain the types of data transfer
17. Identify various data transfer modes
18. Explain how to control the data transfer

UNIT 2.13: Initializing Nodes and Gateways

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the prerequisites for initialization of nodes and gateways
2. Explain the configuration of edge appliances
3. Identify the steps of node and gateway initialization
4. Describe how to check connectivity
5. Explain the execution scenarios of software

2.13.1 Prerequisites for Initialization

Initialisation of a node and gateway means configuring the IoT devices and routers with a username and a password. Before initialising the nodes and gateways, the technician needs to perform complete installation of the IoT setup. This involves dealing with IoT devices such as installing an IoT camera, installing a router and establishing a working Internet connection.

For example, an IoT camera can be set up along with the IoT framework and then, finally a node gateway can be initialized, using the steps as shown in the following figure:

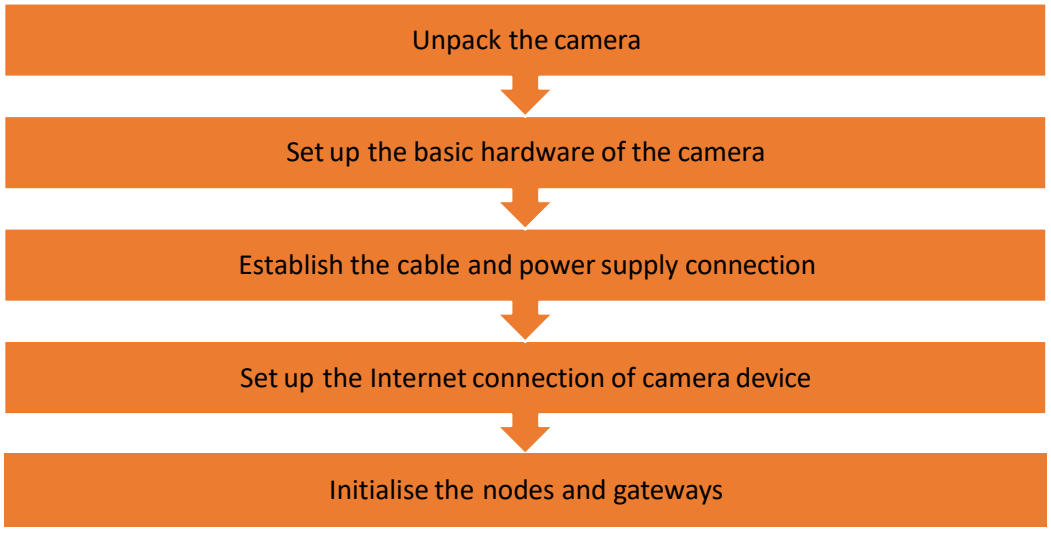


Fig. 2.13.1: Prerequisite steps for an IoT camera device installation

2.13.2 IoT Device Installation

In the process of installation of an IoT camera, certain steps need to be performed.

Unpack the Camera

As a part of the installation kit, the technician will get the camera and its accessories in the package. The person will need to perform the following steps:

1. Check the specification of the installation kit with the order copy before unpacking.
2. Remove the packaging with suitable tool (utility knife).
3. Check whether the device and its accessories in the package is complete and not damaged.
4. Dispose the packaging waste as per the working instructions.

Set Up the Basic Camera Hardware

After unpacking, setting up of the basic hardware needs to be done. This includes mounting of camera and camera stand. The following steps show the basic hardware setting up steps:

1. Connect the camera by sliding it on the stand.
2. Mount the screws and secure them tightly.

   The following figure shows the camera hardware assembly:

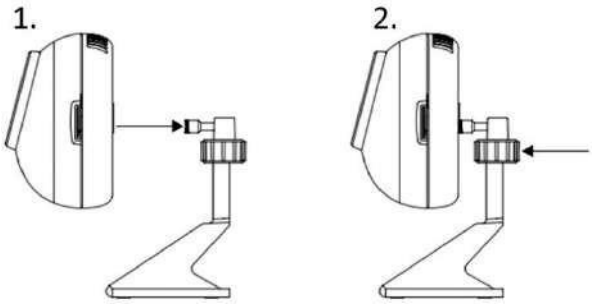


Fig. 2.13.2: Camera hardware set up

If the camera needs to be mounted on the wall, then the following steps need to be done:

1. Find a proper place on the wall where the camera can cover the surveillance area properly.
2. Next, mark and drill pilot holes aligned to the camera's bottom stand.
3. Put the wall anchor in the holes and secure the bottom stand of the camera with screws.
4. Attach the camera to the camera stand.

The following figure shows the mounting of a camera on wall:

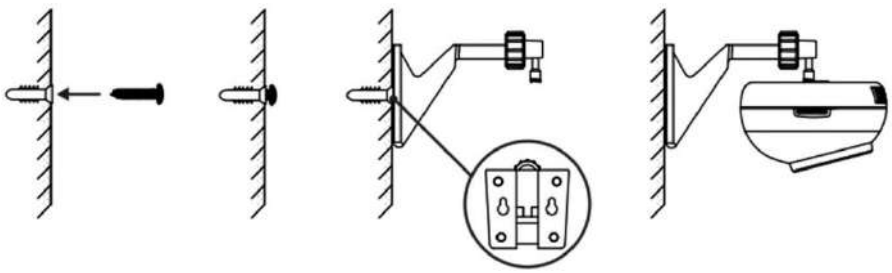


Fig. 2.13.3: Mounting of camera on a wall

Establish the Cable and Power Supply Connection

Next, the power cable and power supply connection needs to be done. The following steps are done for completing the cable connection:

1. Check the specification of power adaptor. Generally, the power adaptor that is provided is of 12 v/1 A power. The following image shows an adaptor with the power labelling on it:

Fig. 2.13.4: Power adaptor specification

2. Connect the power adaptor end located at the back of the camera to the power supply port.
3. Then, connect the power supply plug to a nearby power supply port. The connection of the power adaptor is shown in the following figure:

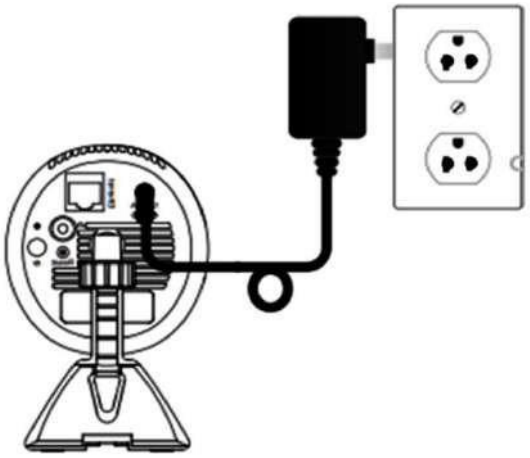


Fig. 2.13.5: Power adaptor connection

Set Up the Internet Connection of Camera Device

To make the IoT camera work over the wireless Internet connection through Wi-Fi, the camera needs to be connected with the router. As per the requirement of customer/site, there can be a pre-installed wireless Internet connection already present on the site or the technician has to perform installation of a router for wireless Internet connection.

In case a pre-installed wireless Internet connection is available, the following steps should be performed to complete a wireless setup automatically:

1. Check that the wireless Internet connection over the router device is working properly.
2. Ensure that the camera is placed within the range of the router.
3. Press the WPS (Wi-Fi Protected Setup) button on the gateway or router for 1-5 seconds so that the WPS LED starts blinking.
4. Then press the WPS button on the back of the camera, so that the LED indication for Wi-Fi starts blinking and turns green. The following figure shows the steps of automatic connection of router and camera:

Fig. 5.1.6: Automatic connection of router and camera

If the automatic connection does not work, then perform manual connection using a utility tool, such as EnViewer, provided by the IoT camera manufacturer in the CD given with the packaging. In this example, EnViewer Finder by EnGenius is being used. The following are the steps to be performed to connect the camera manually:

1. Switch on the laptop/desktop, wait till the system start up completes and ensure the window starts running.
2. Insert the utility tool disc in the disc drive and run the disc. The following are the steps to run the disc:
   - Open “My Computer” from the start menu.
   - Right click on the disk drive and then select “Run the disc as administrator”.
   - Follow the installation steps to complete the installation of the tool.
3. After completing the installation, perform the following steps to run the tool:
   - Go to the computer desktop’s home screen.
   - Open run the window by pressing “window” and “R” on the keyboard.
   - Type the name of the tool and press “Enter”.
4. In the tool window, find the camera connected to the router network in the list given. If the camera is not visible in the list, click the refresh button to view it. The camera will show the host name, IP (Here, IP of the camera is taken as 192.168.0.101) and its version in the camera row of the list.

The following screenshot shows the camera listed in the utility tool:

Fig. 2.13.7: Screenshot showing the camera listed in the utility tool

5. Select the camera from the list and enter the username and the password in the column given on the top right corner and then click next for configuration shown in the above image. The default username and the password are given in the camera packaging or in the user manual. The following image shows the username and the password on a camera packing:

Fig. 2.13.8: Username and password on camera packing

6. Click the network tab given in the options in the utility tool and select the mode of connecting the camera with the network. The following screenshot shows the modes of network connection:

Fig. 2.13.9: Screenshot showing the modes of network connection

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

Manual: In this option, an IP address needs to be provided in the TCP/IP section. Make sure that the IP is not used by some other network.

The following screenshot shows the manual network setup wizard:

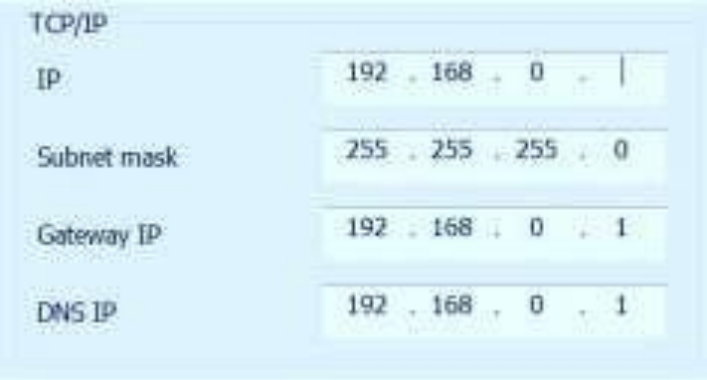


Fig. 2.13.10: Screenshot showing the manual network setup wizard

Point-to-Point Protocol over Ethernet (PPPoE): The camera can be directly connected with the modem using the PPPoE protocol when the Internet service is using the PPPoE Internet protocol. For this, the service provider needs to be contacted to get the relevant details. The router uses the same PPPoE protocol setting; only the username and the password are required. The following screenshot shows the window for setting up the PPPoE protocol:

Fig. 2.13.11: Screenshot showing the window for setting up the PPPoE protocol

This will successfully add the camera to the wireless Internet connection. The technician is provided with a router in the configuration kit, depending upon the requirement of the job, whether a wireless Internet connection is available on the site or the technician has to install a router device to create a wireless Internet connection.

Install the Router

To install a router for a wireless Internet connection at a site, the technician has to perform the steps as shown in the following figure:

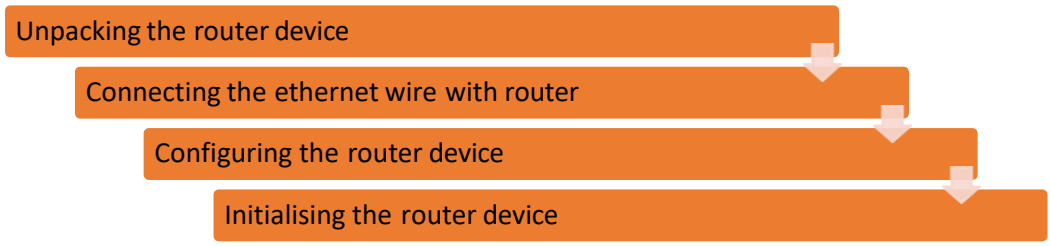


Fig. 2.13.12: Router installation steps

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. He/she would need to perform the following steps:

1. Match the specification of the router with the requirement of the camera. The following table lists some of the specifications which need to be checked with the camera:

Interface	RJ45
Wi-Fi	802.11 b/g
Secured access	WPA/WPA2-PSK and WEP
Data transmission rate	Up to 54 mbps

Table 2.13.1 Specifications to be checked

2. Unpack the router, then check the accessories and devices for any damage. The following list shows the items provided in the packaging:
   - Router device
   - RJ 45 cable
   - Power adaptor
   - Product manual

Connecting the Ethernet and Power Cable with Router

After unpacking, place the router at a position which is suitable for a clear line of sight with the devices, such as a camera as per the example, that need to be connected. After positioning of the router, the Ethernet and the power cable of the router needs to be connected to the power source using the following steps:

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.

The following image shows the LED indicator on a router:

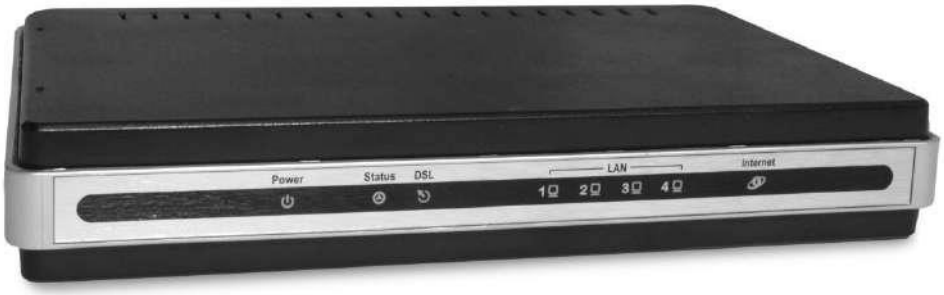


Fig. 2.13.13: Router LED indicator

2. 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. The following image shows the power and Ethernet cable connection with router:

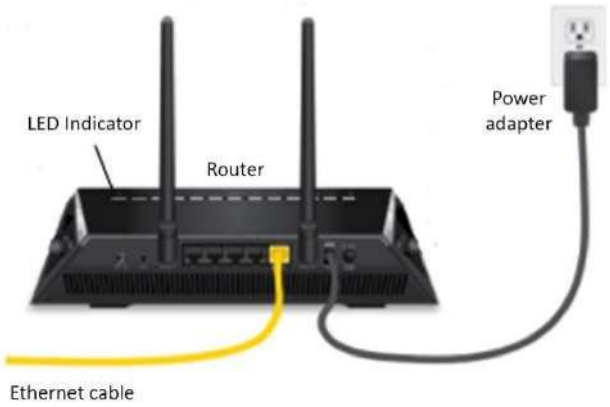


Fig. 2.13.14: Power and Ethernet cable connection with router

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. The following steps then need to performed:

1. Open a web browser on the computer and then enter the IP address for the router which is given on the product manual in the address bar. For example, consider 192.168.0.1 as the IP address of the router. The following screenshot shows this step:

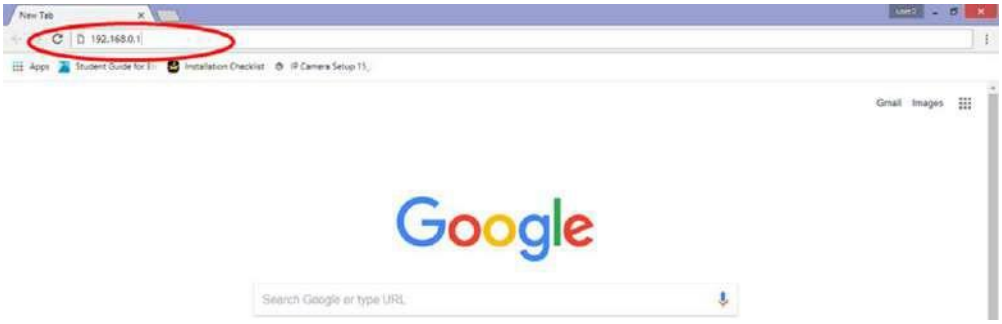


Fig. 2.13.15: IP address for router configuration

2. Then, enter the default username and password given in the router manual or within the packing in the window that opens. The following screenshot shows the window:

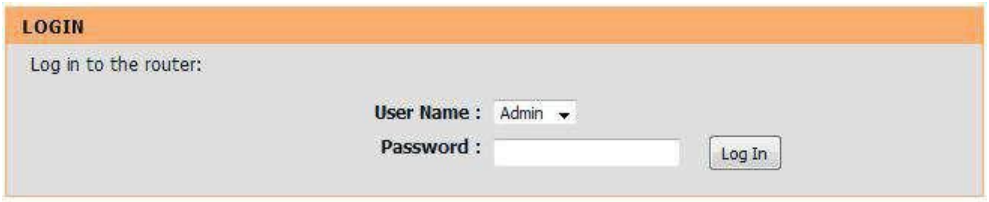


Fig. 2.13.16: Window for router configuration

After completing the hardware set up of the IoT device and connecting it with the Internet, the final step is to initialise the node devices and the gateway routers. The initialisation 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.

2.13.3 Node Initialization

While using a node or a device for the first time, it is required to set a login and a password for the system default user. This is also known as initialisation of nodes (IoT devices). This will make the system secure and configured.

For example, for an NVR based camera set up, initialisation through a network video recorder (NVR) software is mentioned, in which the NVR device is initialised with the router. The following image shows an NVR device:

Fig. 2.13.17: Front and back view of an NVR

The following steps should be followed in establishing the connection between an NVR device, a camera and a router:

Step 1: Unpack the NVR device and connect the device with the router using an Ethernet cable. The following figure shows the connection of an IoT camera, a router and an NVR device set up:

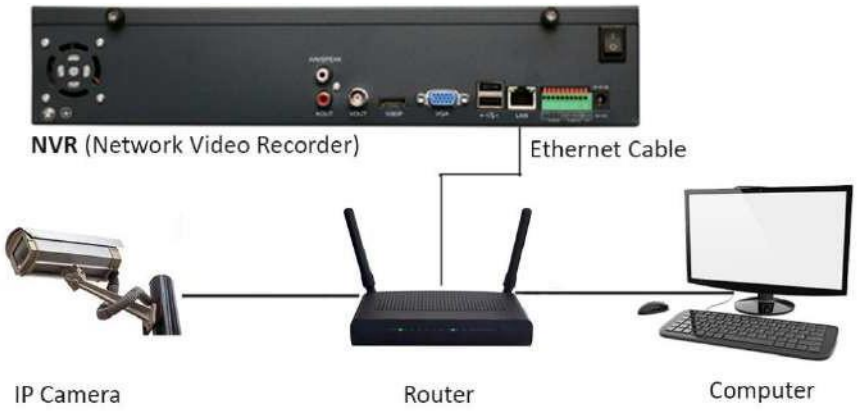


Fig. 2.13.18: NVR device connection with router and camera

Step 2: Power on the NVR device and let it boot into the initialization interface. The following image shows the power indicator of an NVR device:

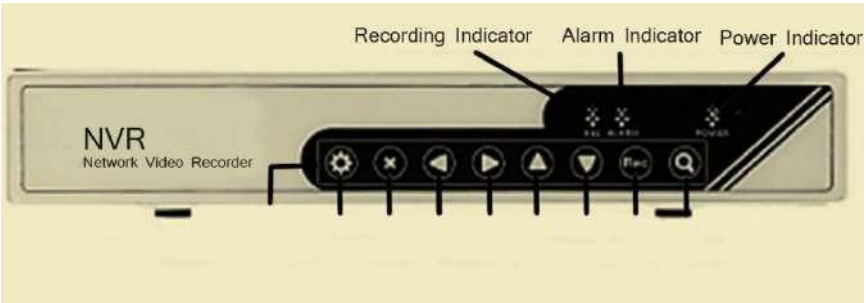


Fig. 2.13.19: NVR device indicators

Step 3: The NVR software is given with the NVR device or it can be downloaded from the Internet. For example, the following link is used to download the NVR software for Genius Vision camera set up:

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

Step 4: Install and run the NVR software on a computer system connected to the same network with which the NVR device and the IP camera are connected.

Step 5: Configure the default login details for the camera. The following screenshot shows the device login screen of an NVR software on a computer system:

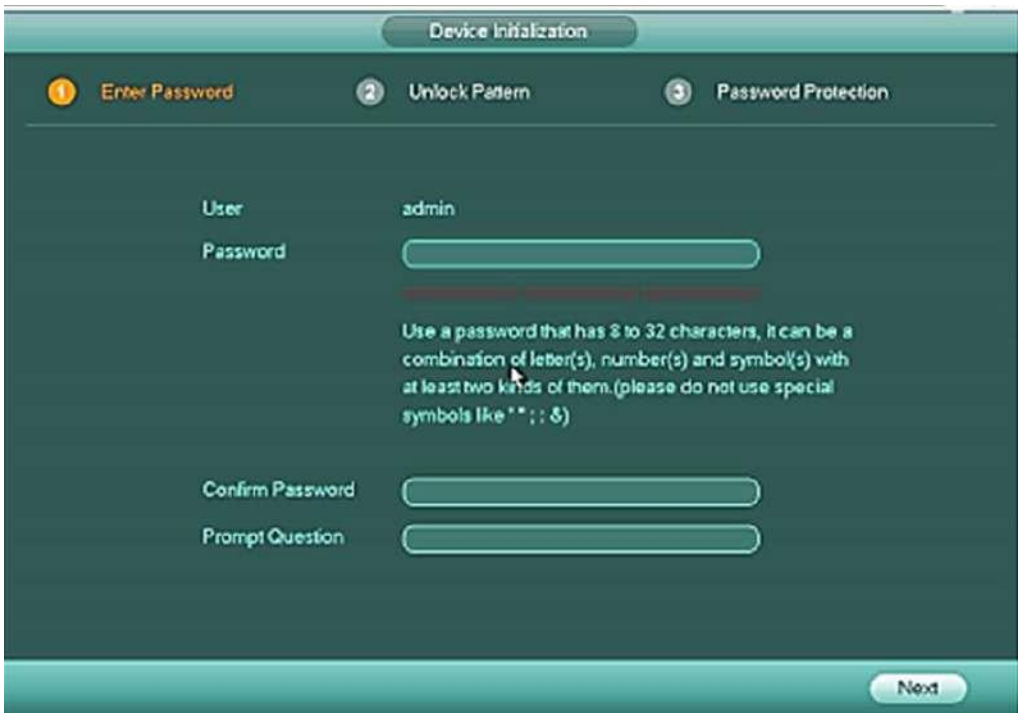


Fig. 2.13.20: Device login screen

Step 3: For initialization of camera device, connected through the same LAN, launch the interface on the desktop and check the connected device list.

The following screenshot shows the screenshot of the list of devices connected to the network:

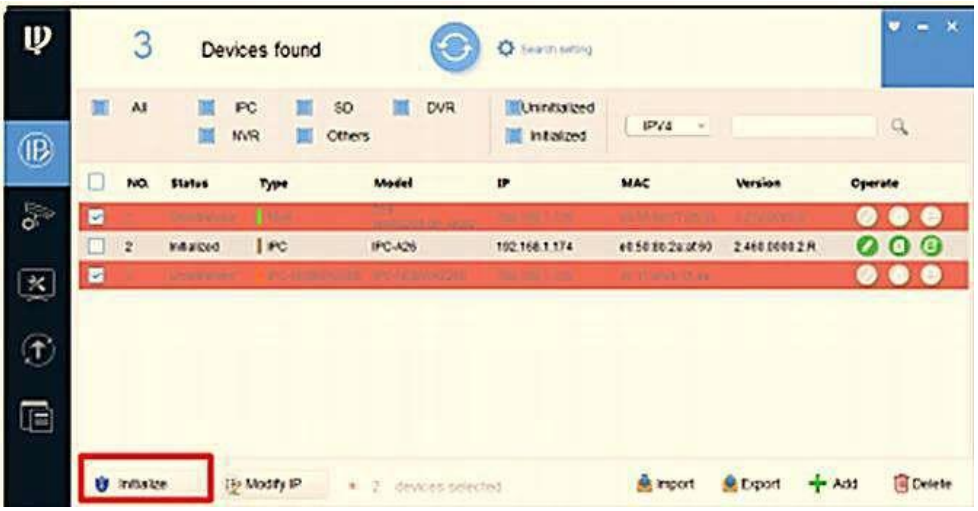


Fig. 2.13.21: Screenshot of list of devices connected to the network

Step 4: Select the uninitialized camera device from the list and enter the initializing interface by clicking on the "Initialize" button.

The following screenshot shows the initializing interface:

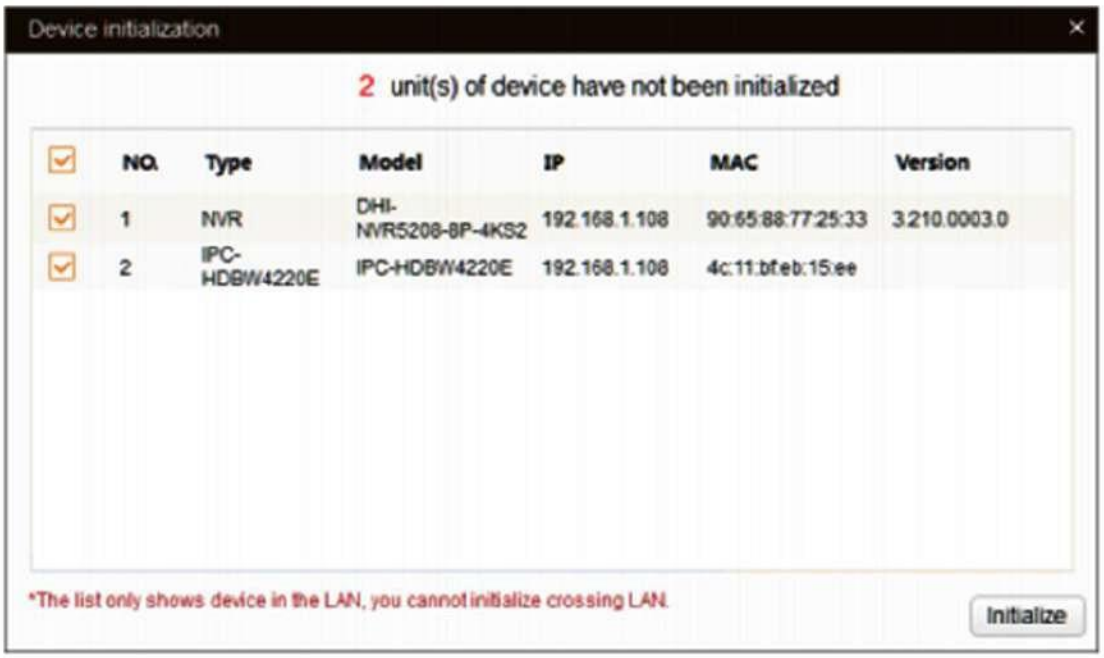


Fig. 2.13.22: Initializing interface

Step 5: Select the devices and click "Initialize" and set the initialization parameters. The following screenshot shows setting up of password of the device:

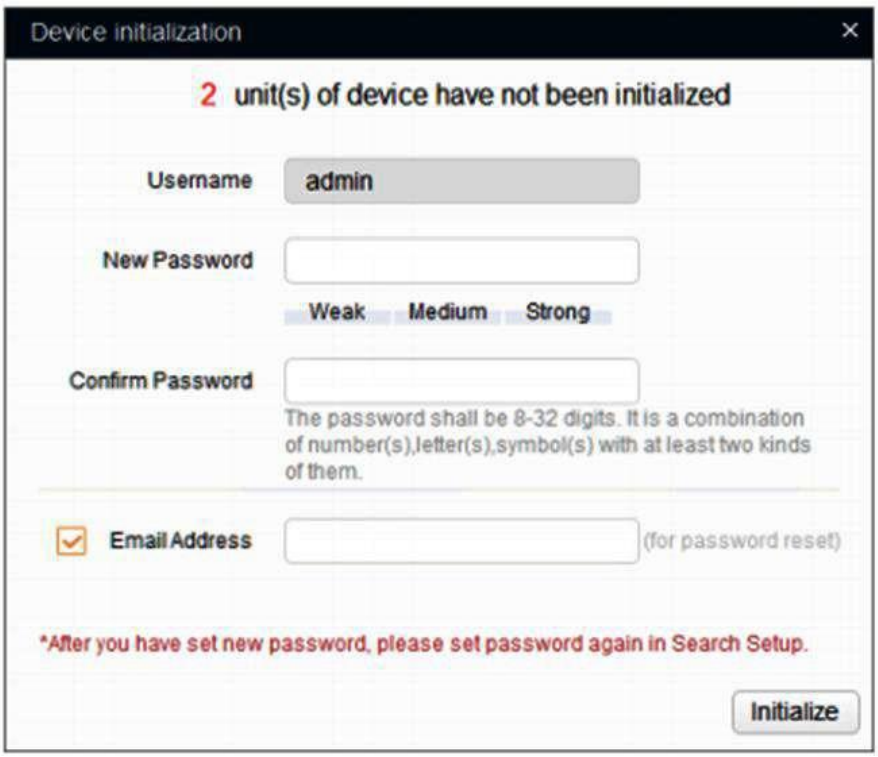


Fig. 2.13.23: Setting up of password of the device

The following screenshot shows the detected devices after initialization:

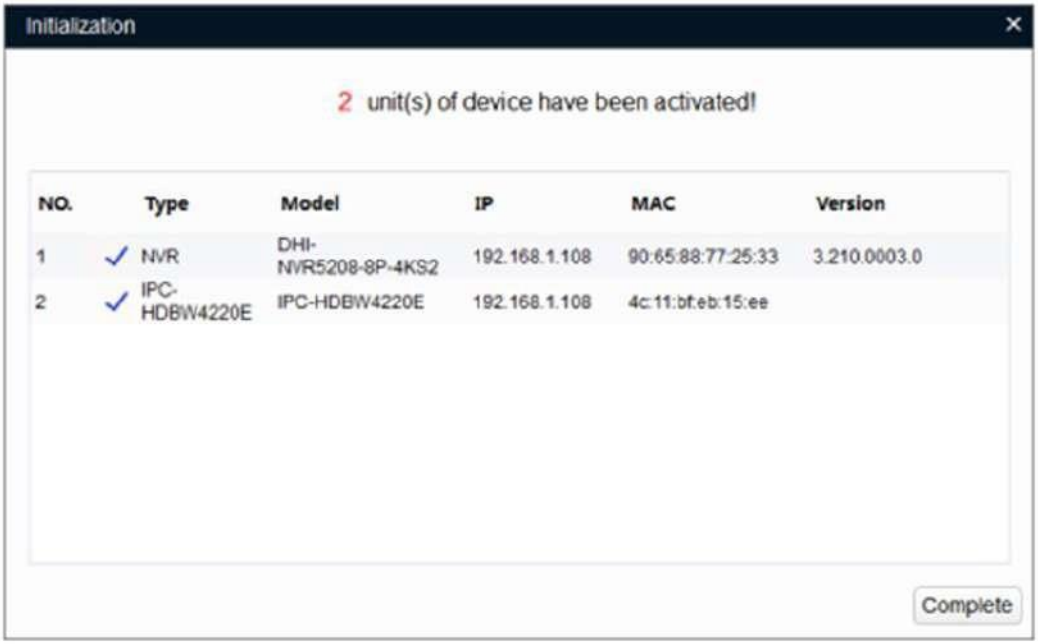


Fig. 2.13.24: Detected devices after initialization

2.13.4 Gateway Initialization

The gateway or router needs to be initialised to establish the Internet connection between the network provider and the gateway, that is, the router installed on the location. For example the steps for initializing a D-Link router are as follows:

Step 1: Connect the power adapter to the back panel of the router.

Step 2: Insert the Ethernet cable to the router and the computer system. The window as shown in the following image will open:

Fig. 2.13.25: Router setup

Step 3: Configure the Internet connection and set up a password. The following screenshots show the configuration of Internet connection and password:

Fig. 2.13.26 (a): Internet connection configuration window

Fig. 2.13.26(b): Password setup window

Step 4: Check the setup details as shown in the following screenshot:

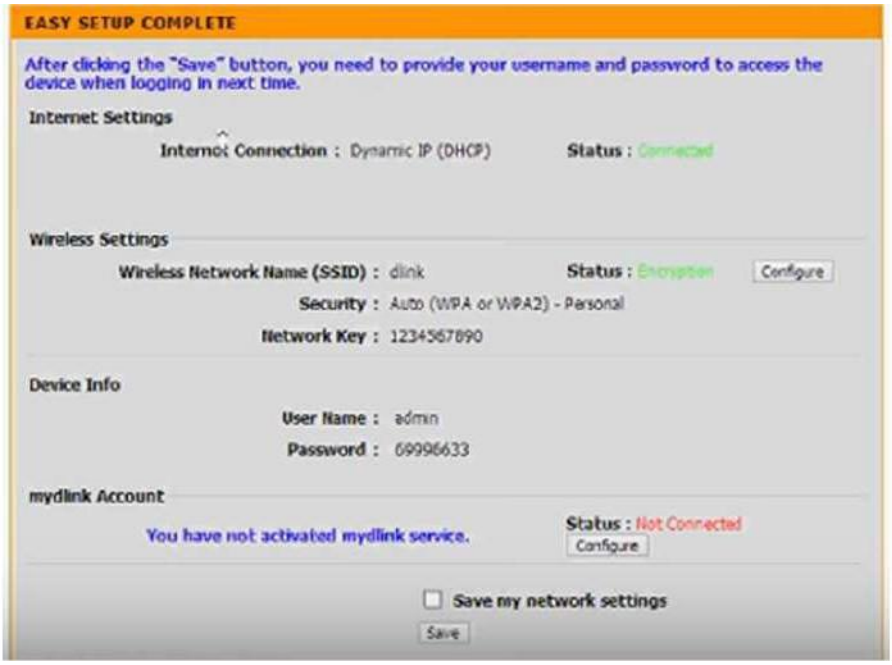


Fig. 2.13.27(a): Router configuration

Step 5: Open the Internet browser and type the default gateway address at the address bar. Login to the account and the router details' window will open. The following images show the screenshots of router settings:

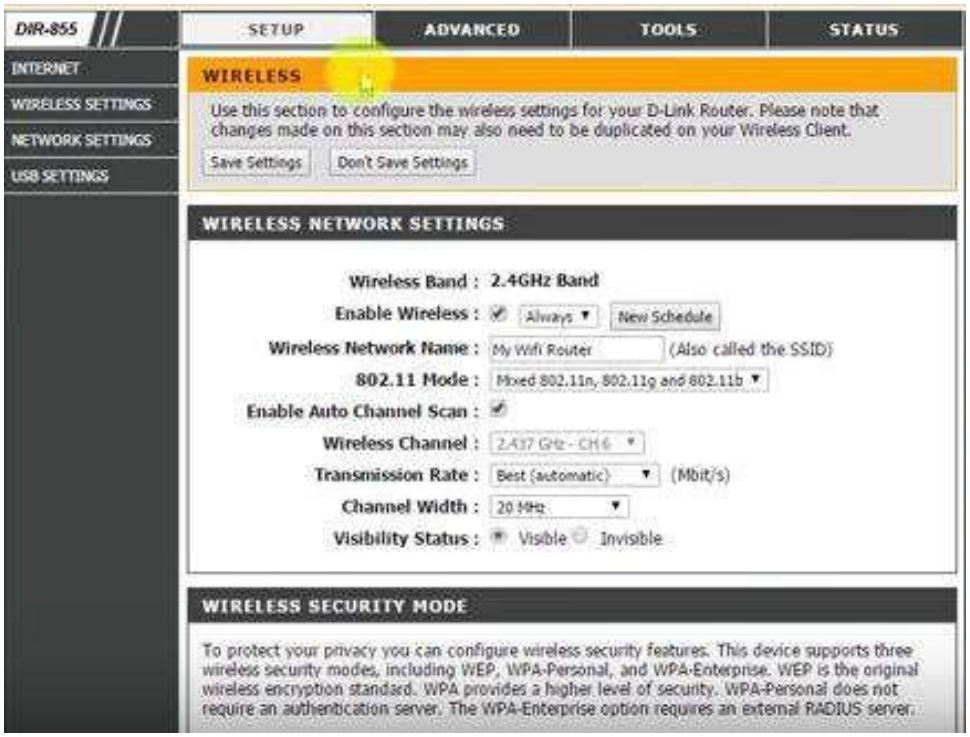


Fig. 2.13.27(b): Screenshot of router settings

Fig. 2.13.27(c): Screenshot of router settings

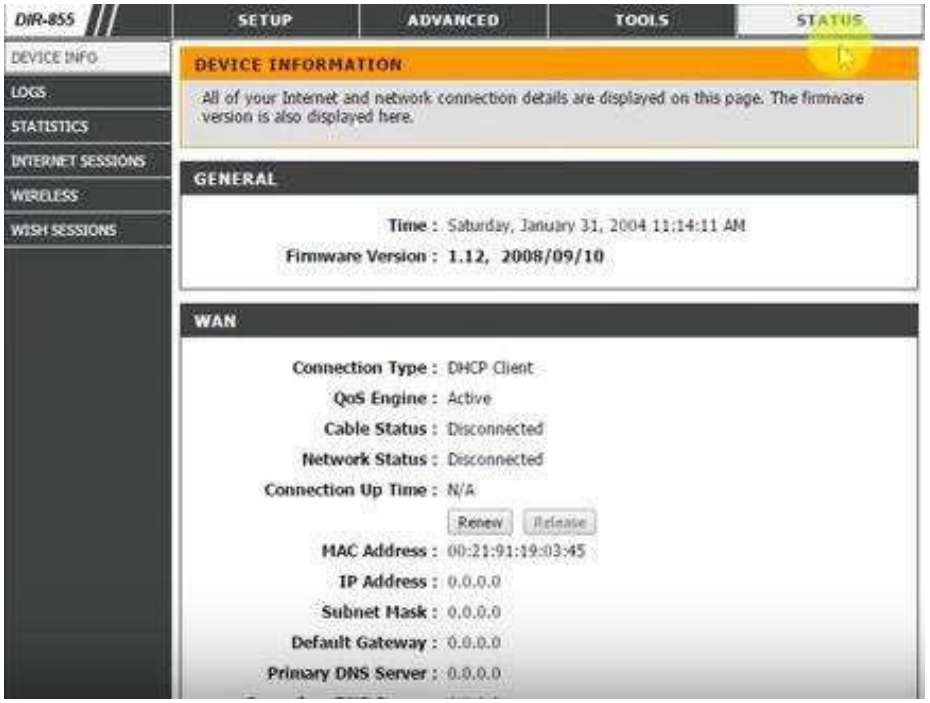


Fig. 2.13.27(d): Screenshot of router settings

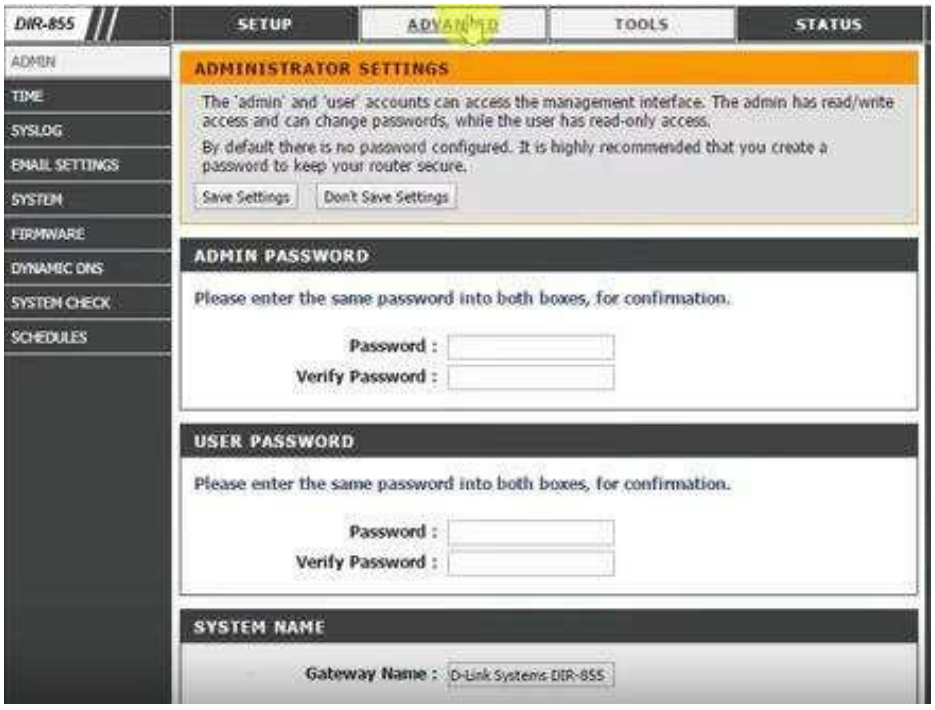


Fig. 2.13.27(e): Screenshot of router settings

2.13.5 Connectivity Checks

After initialising 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.

To test the network connectivity the steps given below are to be followed:

Step 1: Open command prompt and type “ipconfig” and press enter. It shows the connection details and ensures that there is no problem in network connection.

Step 2: Type “ping <gateway address>” to check there is no loss of packets and the router is working well.

To check the connection of the devices to the gateway, the steps given below are to be followed:

Step 1: Launch the IoT device software installed on the laptop or desktop and open the default webserver page.

The following images show the screenshot of the 6lowPAN Border router details along with the system information, sensors connected, network status and so on:

Fig. 2.13.28(a): Screenshot of Internet settings

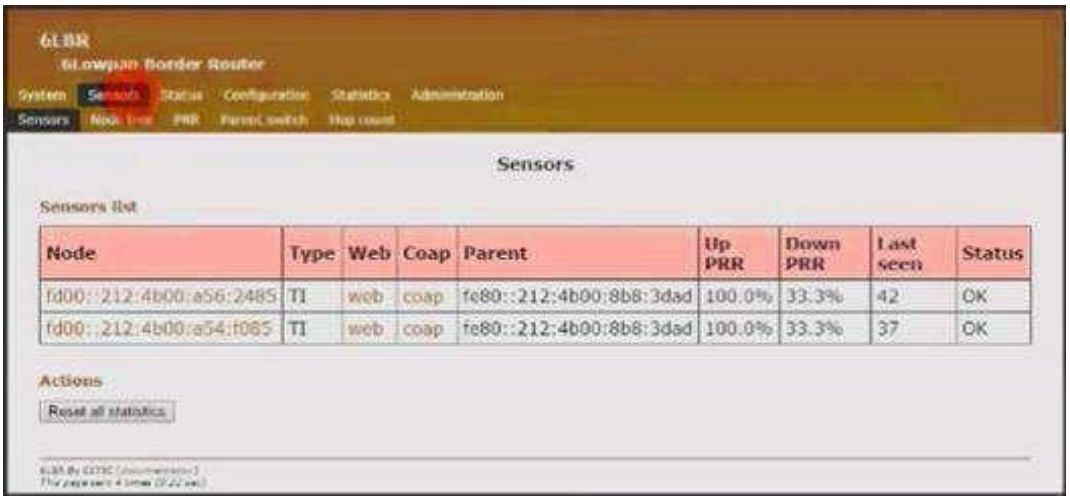


Fig. 2.13.28(b): Screenshot of list of sensors connected

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.

To connect a physical device to the gateway and to test the connectivity, the steps given below are to be followed:

Step 1: To do so in Microsoft Azure suite, click on the devices to check the device parameters.

The following screenshot shows the connected devices in the Microsoft Azure window:

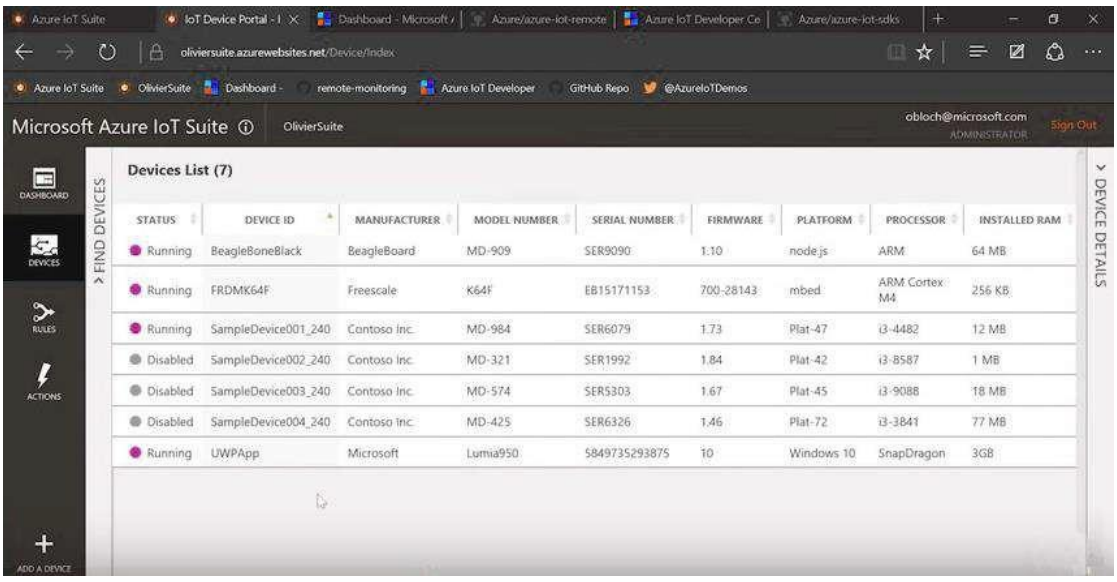


Fig. 2.13.29: Screenshot of Microsoft Azure window

Step 2: Click on "Add New" as shown in the following image:

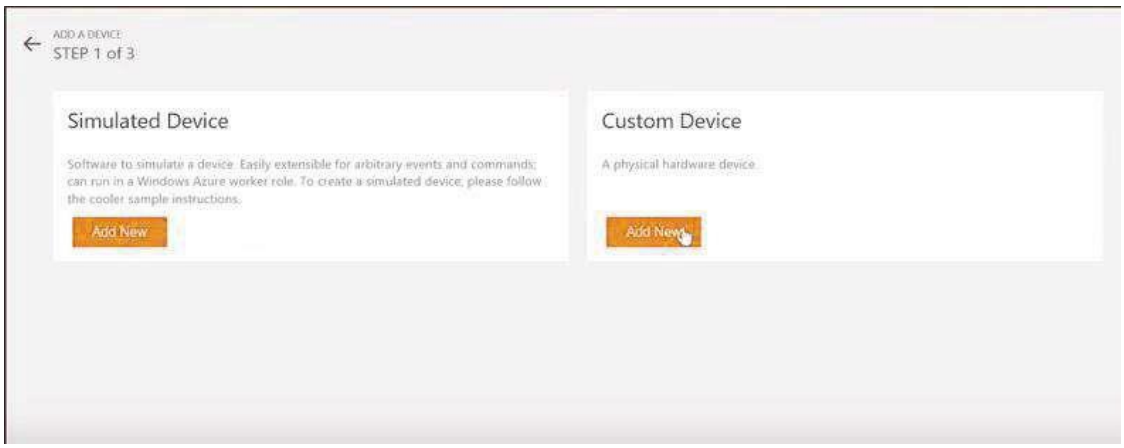


Fig. 2.13.30: Add new device

Step 3: Define the device ID as shown in the following image:

Fig. 2.13.31: Defining device ID

Step 4: Configure the device ID and IoT hub name as shown in the following image:

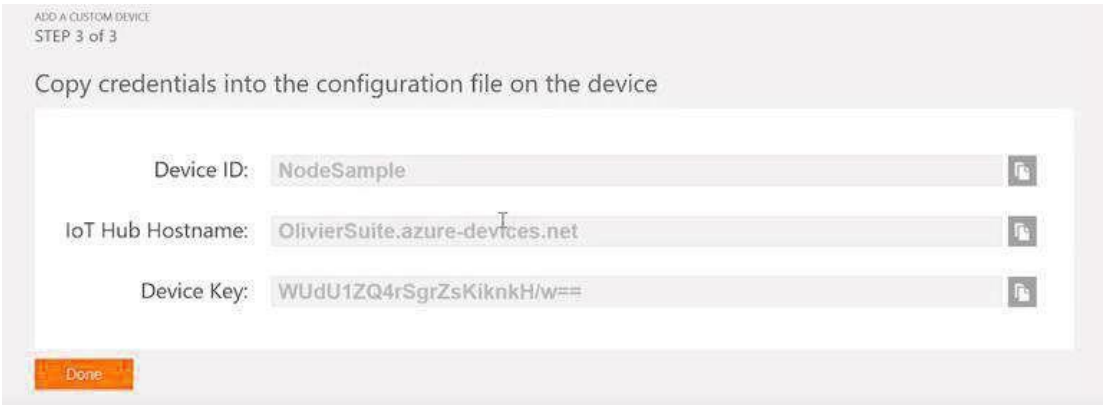


Fig. 2.13.32: Configuring the device ID and IoT hub name

Step 5: Set the command for the device as shown in the following image:

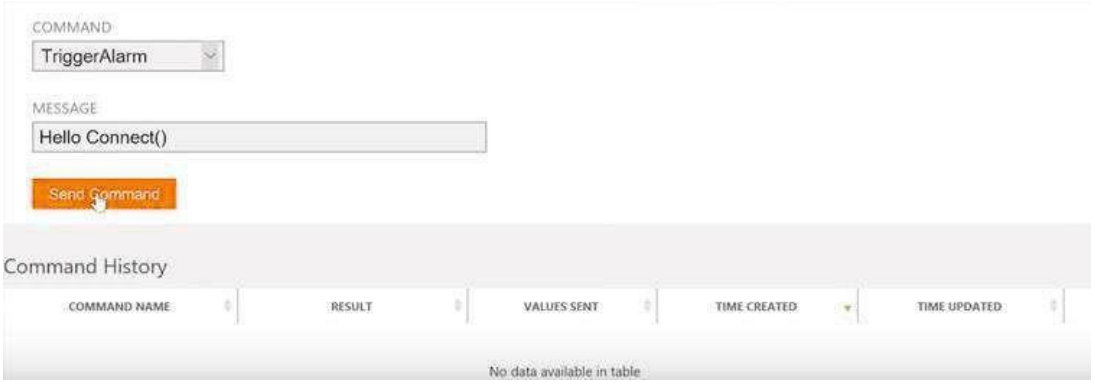


Fig. 2.13.33: Setting command for the device

Step 6: Check whether the device is functioning according to the command as shown in the following image:

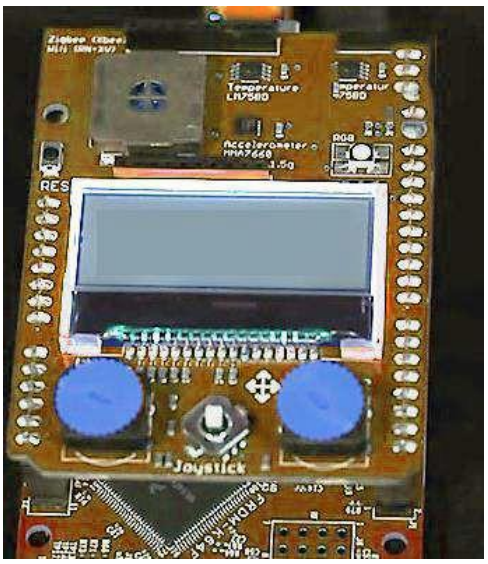


Fig. 2.13.34: Checking whether the device is functioning according to the command

2.13.6 Software Execution Scenarios

After initialisation of node devices and gateway (routers), the execution of the software is done. The last step involves executing the software and the device is connected to the communication channel. Take the example of an IoT camera device which needs to be connected with a ZigBee communication channel.

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

1. Connect a USB cable to the ZigBee coordinator on the camera device and the computer system. The following figure shows the connection:

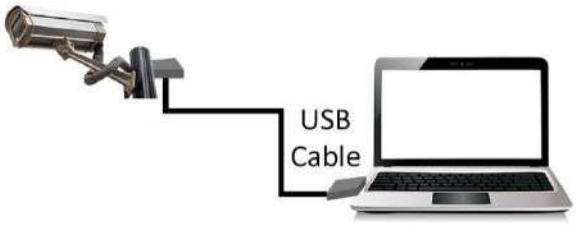


Fig. 2.13.35: Connection between camera and laptop with a USB cable

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

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

3. 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 follows:

   http://ncd-base-station.software.informer.com/

4. Run the Base Station software for setting up the device. The following screenshot shows the selection window for setting up Base Station:

Fig. 2.13.36: 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. The following screenshot shows the device selection window:

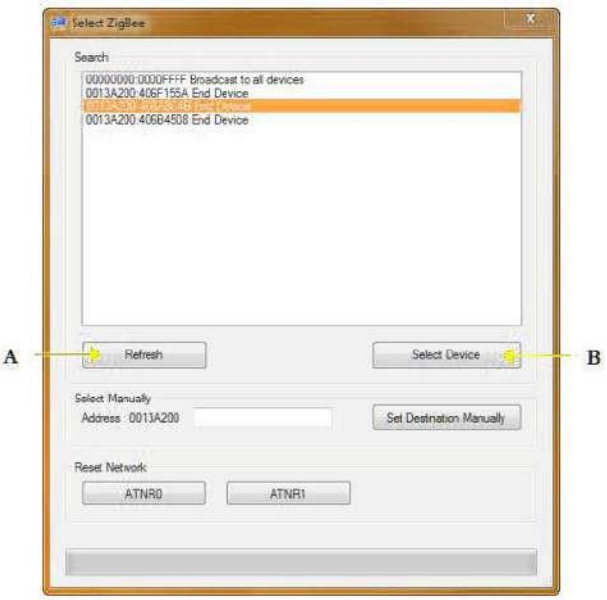


Fig. 2.13.37: Device selection window

- 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. The following screenshot shows the NCD configuration window:

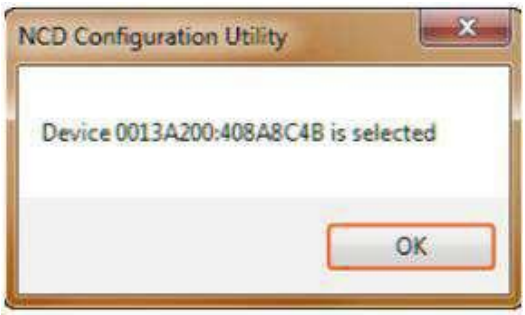


Fig. 2.13.38: NCD configuration window

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. The following screenshot shows the command option window:

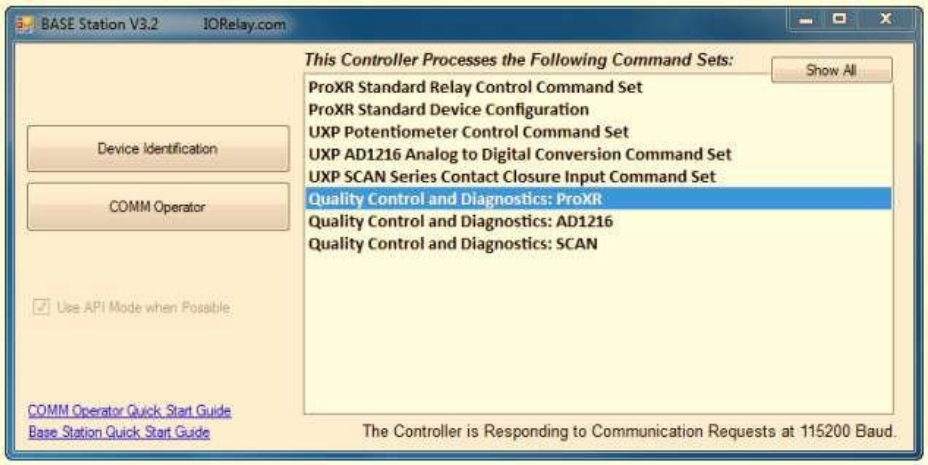


Fig. 2.13.39: Command option window

Exercise

1. Write down the modes of network selection in setting up an IoT camera device.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____
   g. _____
2. Write down the steps in gateway initialization.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
3. Write down the connectivity checks to be performed while connecting devices to the gateways.
   a. _____
   b. _____
   c. _____

UNIT 2.14: Launching the Software on Nodes and Gateways

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the prerequisites for software installation
2. Explain the challenges with launching software

The prerequisites for the software to function on the devices and the gateway are as shown in the following figure:

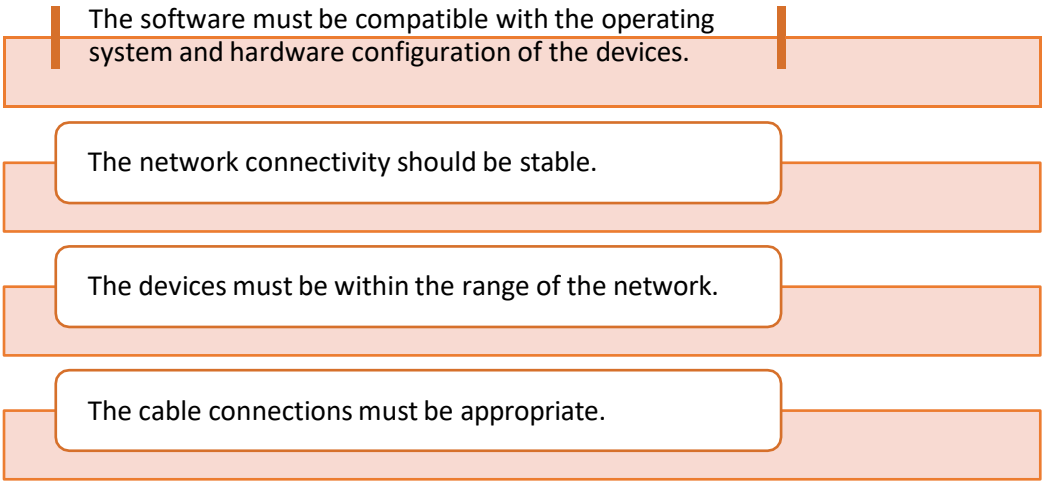


Fig. 2.14.1: Launching prerequisites

Software Launching Challenges

The various challenges are as follows:

1. Hardware-Software Compatibility

The IoT infrastructure is coupled with various hardware and software components. The software applications may not function effectively if there is a compatibility issue between the components.

2. Device Interaction

It is mandatory that the hardware and software communicate with each other in real time. Backward compatibility as well as upgrade issues create a challenge for the framework.

3. Network Availability

The data should be communicated extremely fast all the time; a stable network connection is always a need. The software interface will display the results accurately if there is a strong network available.

Exercise

1. Write down the prerequisites for the software to function on the devices and the gateway.

_____.

_____.

_____.

_____.

UNIT 2.15: Confirming Communication and Establishing Connectivity

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the data transfer indicators
2. Compare data transfer on various networks
3. Explain different data transfer failure scenarios
4. List the steps to connect to a network remotely
5. Identify the steps to connect to short range networks

2.15.1 Data Transfer Using the Indicators

The lights on the devices such as gateways, routers and so on help in determining the status of the device's operation. All the communication/data transfer using onscreen I/O streams or appropriate LED indications are checked as per the system test manual. The following table lists the different indicators on a device:

	Solid	**Blinking**	**Off**
Battery	Battery is good	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

Table 2.15.1 Different indicators on

2.15.2 Data Transfer Comparison Scenarios

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

	ZigBee	Bluetooth LE	Z-Wave	NFC	Wi-Fi
IEEE Specification	802.15.4	802.15.1	ITU -T	ISO 13157	802.11 a/b/g
Frequency Band	868/915 MHz; 2.4 GHz	2.4 – 2.5 GHz	908.42 MHz	13.56 MHz	2.4 GHz; 5 GHz
Network Type	WPAN	WPAN	WPAN	P2P	WPAN
Power Consumption (mA)	40	12.5	2.5	50	116
Nominal Range (m)	10	50	30	.05	100
Max. Signal Rate	250 kbps	305 kbps	40-100 kbps	424 kbps	54 Mbps

Table 2.15.2 Comparison between the data transfer over various networks

There are various tools to check the network speed and data transfer rates. In Windows OS, it can be checked by clicking the “Ethernet” option and going to the “Properties”. The following screenshot shows a status of an Ethernet network:

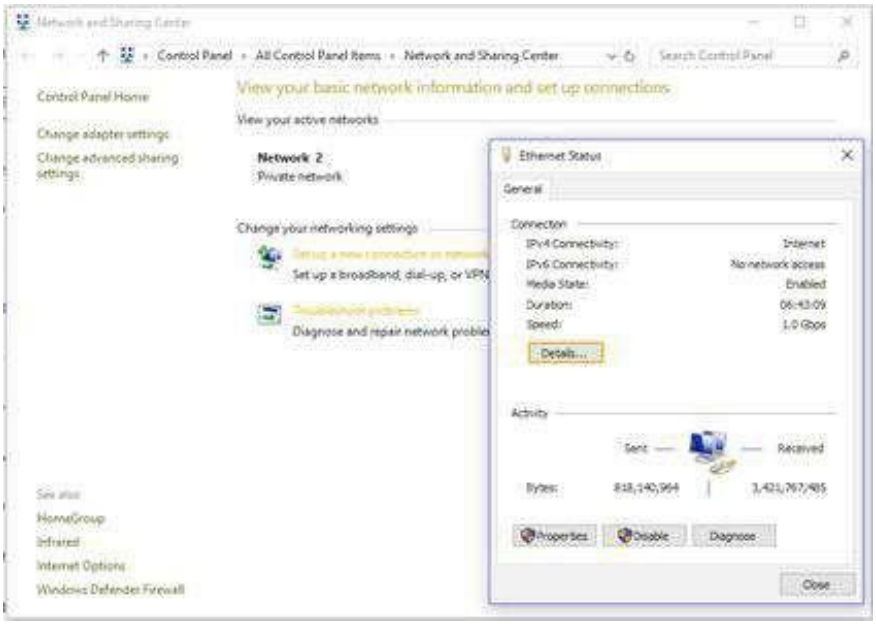


Fig. 2.15.1: Network status

There are various software available, which can test the network speed and statistics. Some of the software are as follows:

LAN Speed Test (Lite):

It is used for measuring the LAN speed by copying a file from a computer to another one on the same network.

The location of the destination device is browsed and the Start Test button is clicked to run the test. The following screenshot shows a Lite window:

Fig. 2.15.2: Lite window

LANBench:

It is used to test the network which is using TCP only. The LANBench application should be run on both the computers; server and client. The server requires the Listen button to be clicked, while the client side requires the configuration details such as the server's IP address, packet size, test duration, connection and transfer mode. The following screenshot shows a LANBench window:

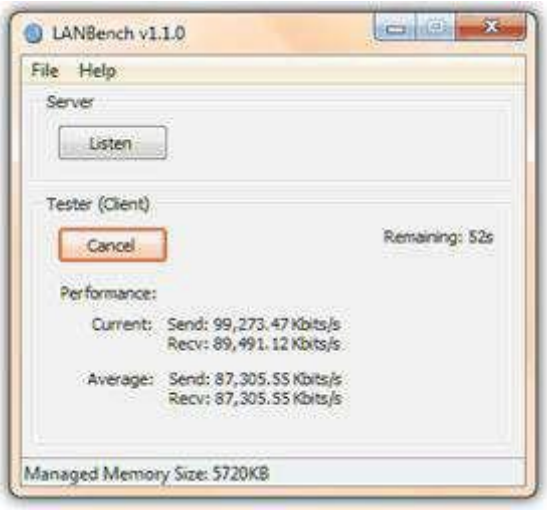


Fig. 2.15.3: LANBench window

2.15.3 Data Transfer Failure Scenarios

Data transfer failure can occur due bad network connection or improper connection and configuration. The following table lists some scenarios of data transfer failures:

Issue	Cause / Solution
Transferring data from a computer to cloud takes longer than expected time.	• Computer does not include a Gigabit Ethernet adapter. • Network or the hardware does not support Gigabit. • There is Wi-Fi local network overhead or line of sight is between devices and distance. • A network hub is being used instead of a switch. • Data transfer speed is affected by data protection software, Anti-Virus, Malware Protect. • There is a large multi-terabyte data set. • The device is connected to a faulty USB port or a faulty or low quality USB cable.
Device is not in range of network.	• Use an Ethernet cable to connect the computer. • A direct connection is better than a wireless one; related to performance and transfer speeds. • If an Ethernet connection is possible, disable the Wi-Fi network.
Faulty network hardware causes performance issues. It causes mismatch in network speeds.	• USB 3.0 or higher port along with a high-quality USB cable should be used. • Faulty and outdated networking devices shouldnot be used.
Network hubs can cause auto-negotiation mismatches, network packet collisions and packet drops.	• Network hubs should be replaced with Gigabit switches.
Outdated firmware can affect network performance.	• Network equipment firmware must be updated and outdated hardware should be replaced.
Data transfer over 2.4 and 5 GHz Wi-Fi bands is much slower than wired Ethernet.	• Direct connection using Ethernet cable is better than the wireless one. • If an Ethernet connection is not possible, connect using the 5 GHz band.
3rd party applications contribute to network traffic by scanning and downloading content.	• Ensure 3rd party applications are not indexing or virus scanning.
Backup functions consume CPU, memory and disk access resources and decrease data transfer rates.	• Stop the backup functions while transferring content.

Table 2.15.3 Scenarios of data transfer failure

Exercise

1. Complete the given comparison table for the different types of communication channels used in IoT.

	ZigBee	Bluetooth LE	Z-Wave	NFC	Wi-Fi
IEEE Specification					
Frequency Band					
Network Type					
Power Consumption (mA)					
Nominal Range (m)					
Max. Signal Rate					

Exercise

1. Write down the cause and the solution for the given issues which happen during data transfer failure between devices.

Issue	Cause / Solution
Faulty network hardware cause performance issues. It causes mismatch in network speeds.	
Network hubs can cause auto-negotiation mismatches, network packet collisions and packet drops.	
Outdated firmware can affect network performance.	
Data transfer over 2.4 and 5 GHz Wi-Fi bands is much slower than wired Ethernet.	
3rd party applications contribute to network traffic by scanning and downloading content.	

2.15.4 External Connectivity

External connectivity is required for an IoT framework to provide access to the remote users to the central site. For this, a connectivity method allowing site-to-site as well as remote client connectivity must be deployed. The connectivity can be established between the gateway and the local Wi-Fi router or 3G/4G connectivity options. (Preconfigured in the uploaded software on gateway microcontroller)

Connecting to the Network Remotely

To access a router or any device remotely, the following steps must be followed:

Step 1: Open the web browser and enter the router address. The default address is 192.168.0.1. For any device, such as a surveillance camera, enter the device's IP address. The following screenshot shows the default IP address at the address bar:

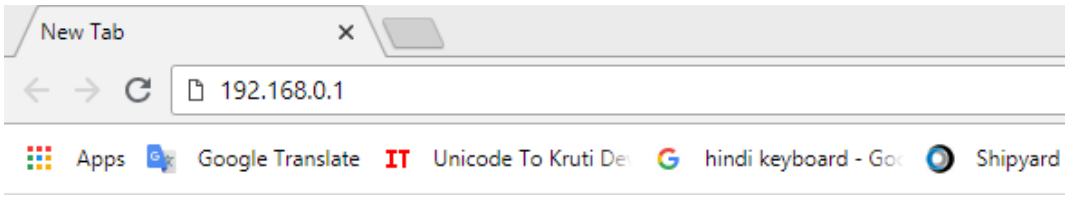


Fig. 5.4.1: IP address at address bar

Step 2: An authentication window will appear. Enter the user ID and the password in the window as shown in the following screenshot:

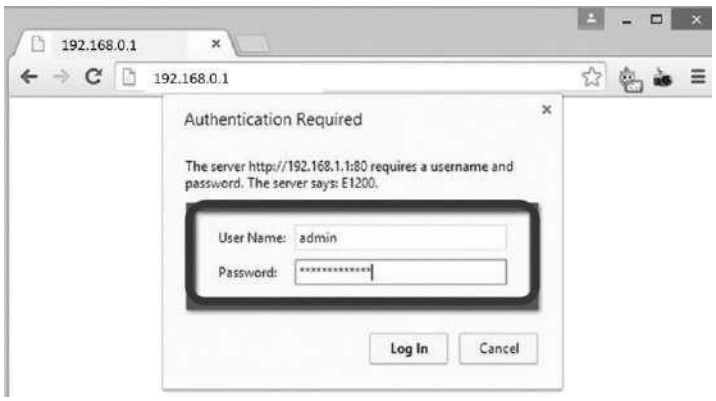


Fig. 2.15.4: Authentication window

Step 3: Check the network status and the details on the window as shown in the following screenshot:

Fig. 2.15.5: Network status window

Step 4: Enter the security settings details and enable the security option suitable, as shown in the following screenshot:

Fig. 2.15.6: 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 the following screenshot:

Fig. 2.15.7: 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 the following screenshot:

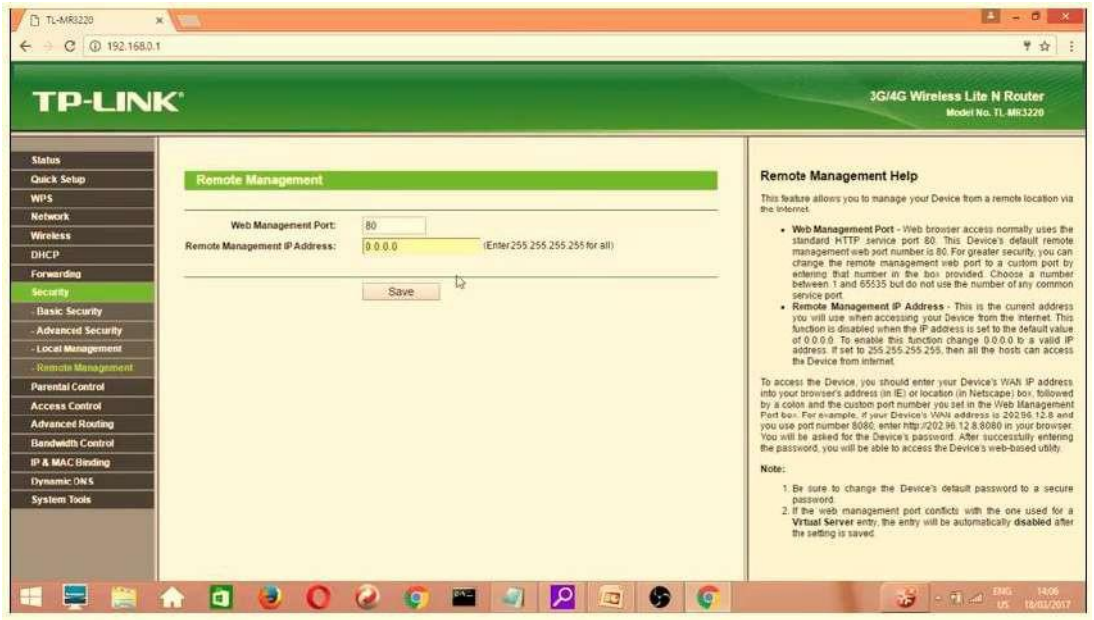


Fig. 2.15.8: Remote management settings for denying any access

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. The following screenshot shows accessing the camera remotely:

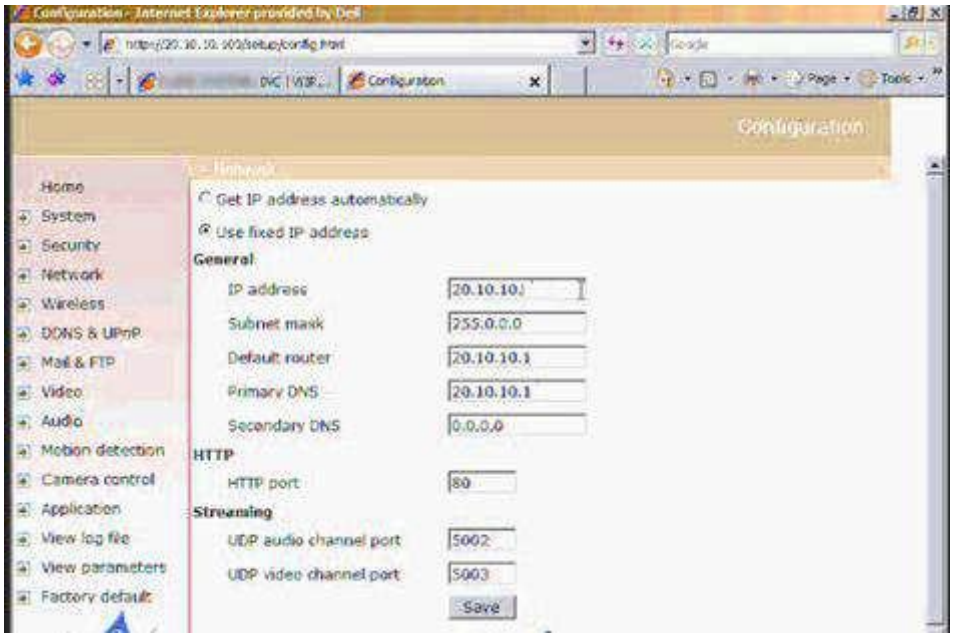


Fig. 2.15.9: Accessing the camera remotely

Connecting to Different Short Range Wireless Networks

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

Connecting to Bluetooth Network

The steps to connect a Raspberry Pi to another system via Bluetooth are as follows:

Step 1: Connect a Bluetooth module to the Raspberry Pi and open the interface for the Raspberry Pi in the system. The following screenshot shows the interface window:

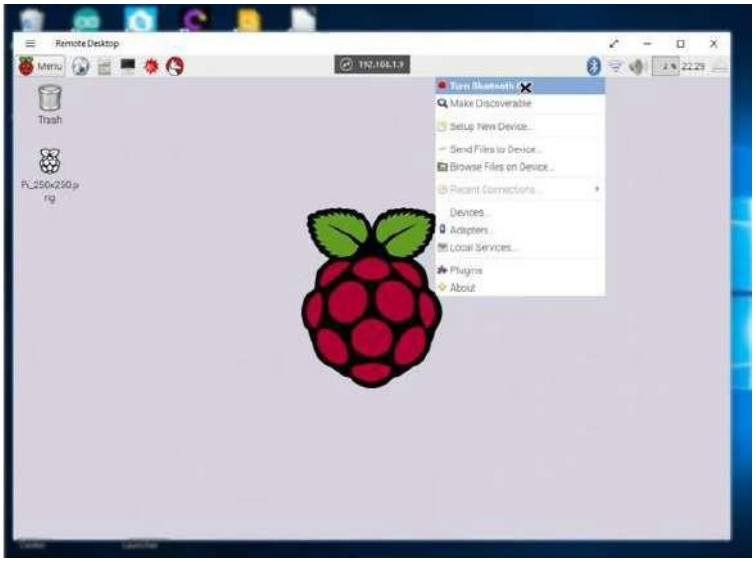


Fig. 2.15.10: Raspberry Pi interface window

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

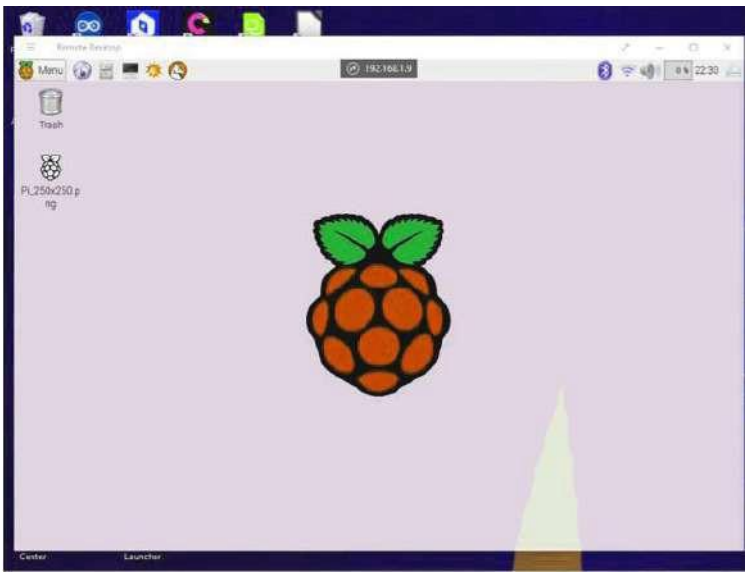


Fig. 2.15.11: Turning Bluetooth on

Step 3: Open the devices window and search for Bluetooth devices as shown in the following screenshot:

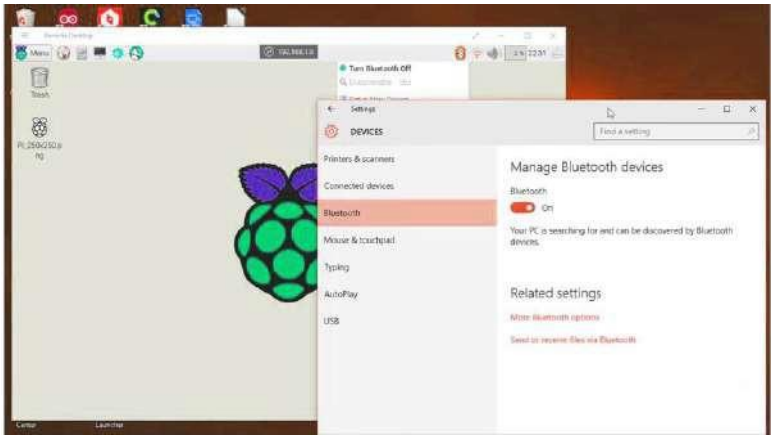


Fig. 2.15.12: Searching for Bluetooth devices

Step 4: Check for the Raspberry Pi and pair the devices as shown in the following screenshot:

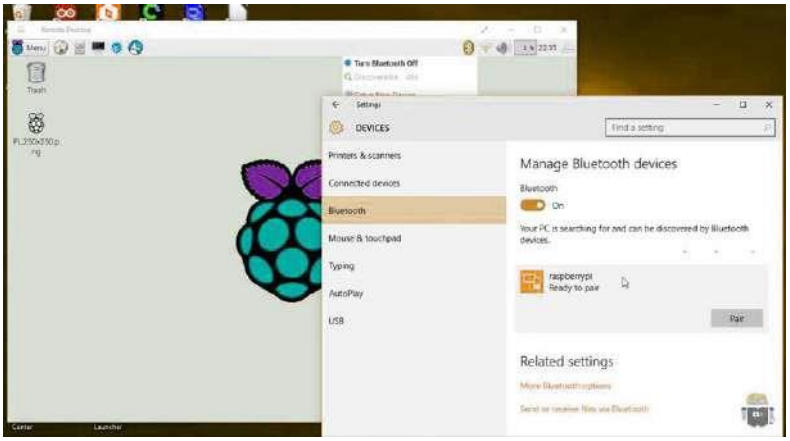


Fig. 2.15.13: Pairing the Bluetooth devices

Step 5: Check whether the passcodes are matching and confirm the pairing as shown in the following screenshot:

Fig. 2.15.14: Checking the passcodes

Step 6: Click on the "Send/Receive files" for file sharing as shown in the following screenshot:

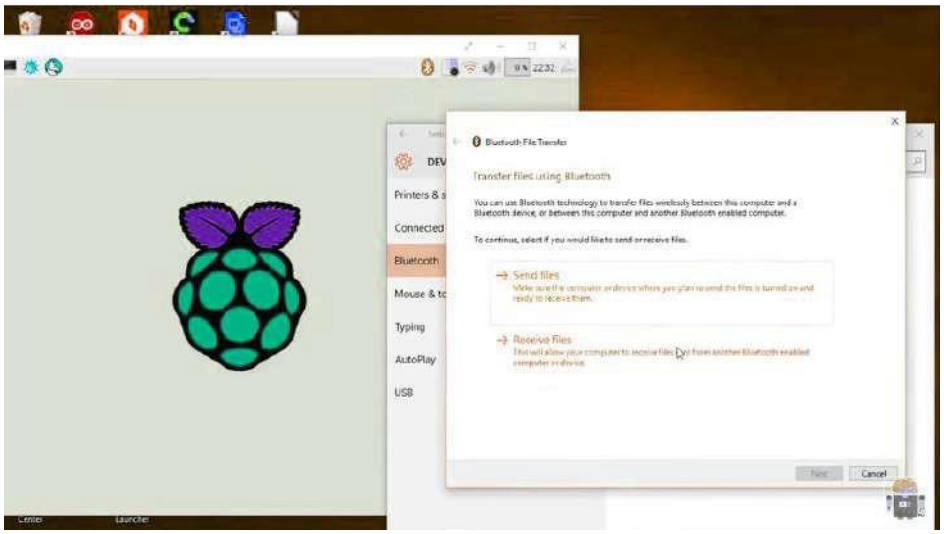


Fig. 2.15.15: Sharing the files

Connecting to ZigBee Network

The steps are as follows:

Step 1: Connect the XBee modules to the Arduino.

Step 2: Install the software of the XBee modules in the system. The following screenshot shows the XCTU interface window as an example of the ZigBee interface:

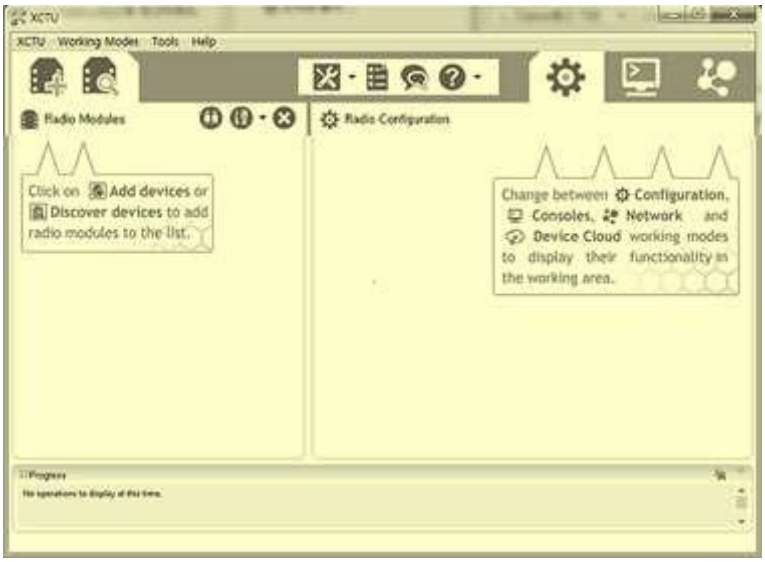


Fig. 2.15.16: XCTU interface window

Step 3: Search for radio modules in the options and a window with the serial port of the devices will appear as shown in the following screenshot:

Fig. 2.15.17: Devices with serial port

Step 4: Select the serial port of the device that needs to be added and set port parameters as shown in the following screenshot:

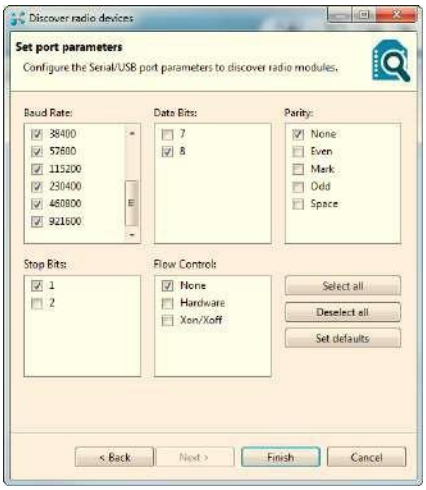


Fig. 2.15.18: Device port parameters

Step 5: Click on "Finish" and a window depicting the discovered radio modules will appear as shown in the following screenshot:

Fig. 2.15.19: Discovered radio modules

Step 6: Configure the module as shown in the following screenshot:

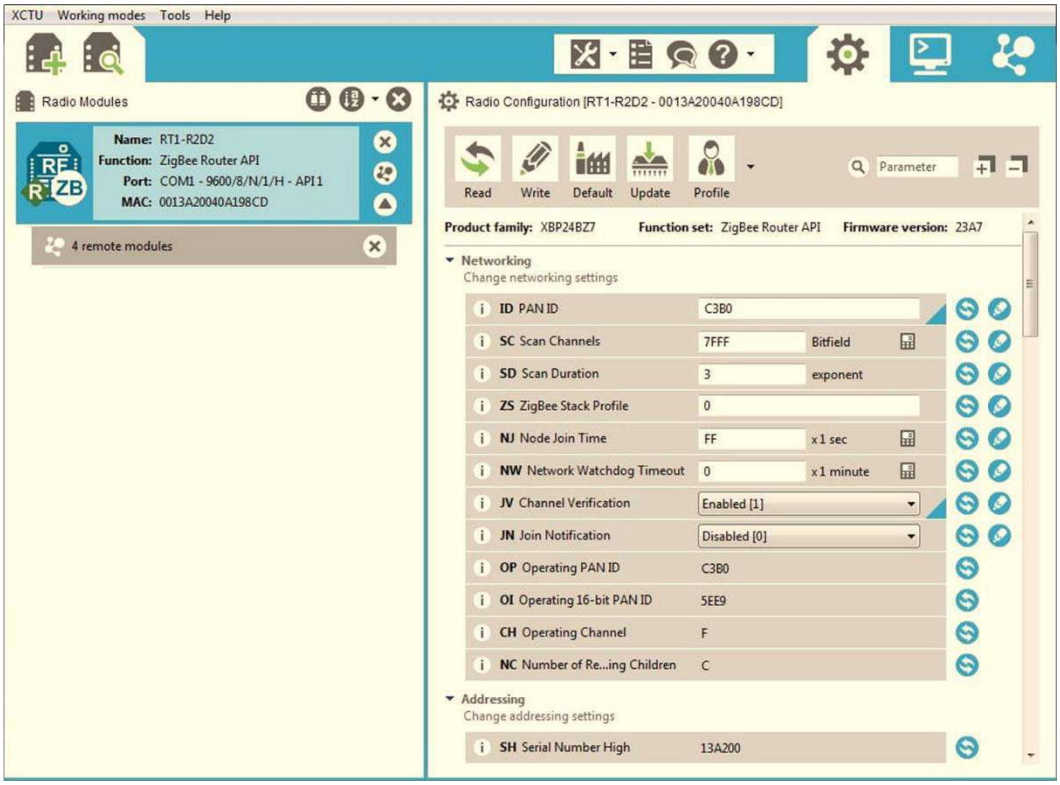


Fig. 2.15.20: Configuring the radio module

Exercise

1. Write down the steps involved in connecting a Bluetooth using a Raspberry Pi framework.

   a. _____

   b. _____

   c. _____

   d. _____

   e. _____

   f. _____

UNIT 2.16: Controlling Edge Appliances and Hubs and Checking for data transfer and Confirming from the server end

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the configuration of a router
2. Describe controlling of devices by connecting hub
3. Explain the bypassing of a hub
4. Explain the types of data transfer
5. Identify various data transfer modes
6. Explain how to control the data transfer

2.16.1 Configuring a Router

Router is the main stake of a network; therefore, properly configuring the router ensures that the data is encrypted, and security is boosted. Proper router configuration also ensures secure connectivity of all devices in a network and provides restrictive access if necessary. The following image shows configuration of a router:

Fig. 2.16.1: Configuring a router

Configuring a router is a five-minute task and can be achieved easily by performing the following steps:

1. Using Ethernet cables, connect the router to a modem by its WAN / WLAN ports and to a computer using one of the LAN ports on the router.
2. Access the router configuration page using a web browser on the computer. Open a web browser and enter its IP address in the browser's address bar. Mostly the IP address is http://192.168.1.1, but with some manufactures this may vary slightly. Generally, a router would have its default address mentioned in the manual, or it can even be looked up online from the manufacturer's website.
3. If the configuration address is correct, the configuration page will appear. This page will require username and password to access; type in the username and the password to arrive at the configuration setting page. The router comes with default username and password, which would be mentioned in the manual, or might be printed on the router itself. For most routers, the default username is "admin" and the password is either "admin" or "password."

4. After gaining access on the router's management page, click on Network > WAN and change WAN connection type to PPPoE. Now, enter the PPPoE username and the password provided by the ISP. Click save; the router should begin to connect to the Internet and may take a while. Wait for a few minutes and check the WAN on the configuration page. If the WAN shows the IP address, then it implies that the router and the modem have been successfully connected.
5. On the way out from the configuration page, ensure to change the default username and password of the router.

2.16.2 Controlling Devices by Connecting to a Hub

A hub is a hardware device that connects the devices on a network and helps to control the devices by connecting them to a hub. A smart home hub is an ideal example of the hub. The devices on a home automation network might include thermostats, lights, door locks, appliances, motion sensors and so on that are connected to the hub. The following figure shows a hub device:

Fig. 2.16.2: A hub in a network set up

These devices have sensors/actuators embedded in them to facilitate smart controls and communications, monitor environmental elements and schedule as well as control tasks. Unlocking doors, activating lights and turning heat on/off when the user is detected within a specified distance from the home are some good examples of tasks accomplished by these devices.

How Does a Hub Work?

In simple words, a hub is a less expensive and less complex way to connect multiple devices on a network. Data travels in a network in packets and a hub forwards these data packets out to all the devices connected to it through built-in multiple ports. As a hub disseminates data packets to every device on the network, each device connected to the hub receives that packet. As a result, each device coupled in a shared network receives a percentage of the available network bandwidth, slowing down a network.

Furthermore, a hub is a junction where the data comes from various devices and is disseminated ina single or multiple direction/s. A hub might or might not have a built-in switch to figure out in which direction the collected data needs to be forwarded.

The following image shows multiple device connected to a hub:

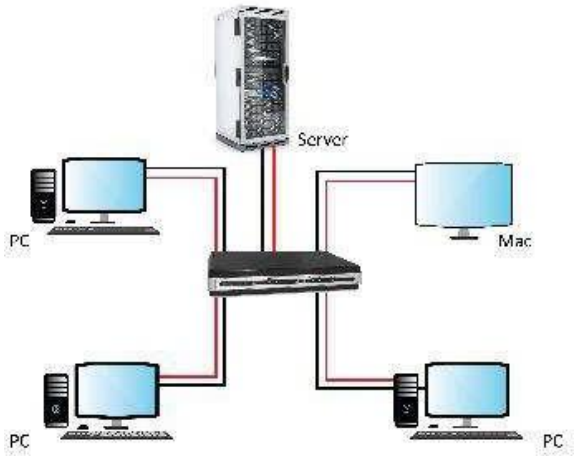


Fig. 2.16.3: Multiple devices connected to a hub

2.16.3 Bypassing the Hub

A network hub is the most basic networking device designed to connect a host of computers and networking devices together. However, unlike a switch or a router, the network hub has some limitations. It does not have routing tables, and neither is it intelligent enough to broadcast information across different connections, which can be a security risk. Moreover, a hub cannot detect network errors; most it can do is detect collision errors. Thus, if more control over the network is desired, specific VPN connection has to be configured or parental filtering is needed in place; consider bypassing the hub and connecting directly to a router. The following image shows a network hub connected to multiple networking devices:

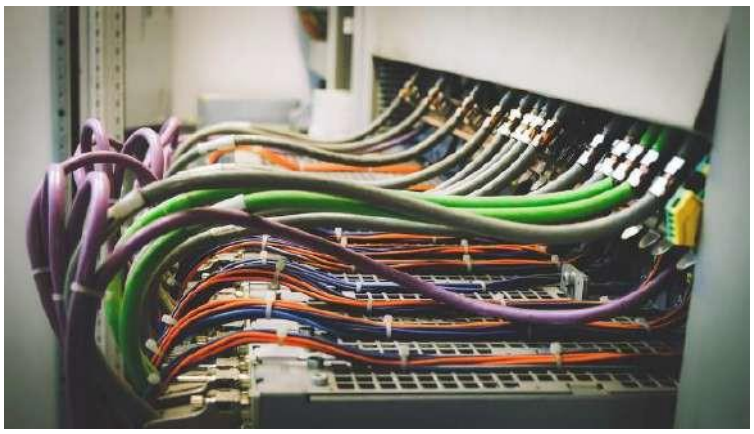


Fig. 2.16.4: Network hub connecting multiple networking devices together

To add a new router, the network hub will have to be put into a Bridge Mode. This would enable the information to pass through the hub without restrictions, allowing the user to control data according to the need from the new hardware equipment.

2.16.4 Configuring the Bridge Mode to Bypass the Hub

- Connect to the router by entering its IP address in the browser's address bar. In most cases it will be https://192.168.1.1.
- Login using the default username and password – generally, the username will be "admin" and the password will be "admin" or "password." The default username and password would be mentioned in the router's manual, or might be printed on the router itself.
- Next, click on Network and disable DHCP. Save.
- Reconnect and remove the username and the password. Save again.

The router should now be in Bridge Mode. The data will now pass directly to the new router.

Exercise

1. Write down the steps in configuring a Bridge Mode to bypass a hub.

   a. _____

   b. _____

   c. _____

   d. _____

2. Write down the steps involved in configuring a router.

   a. _____

   b. _____

   c. _____

   d. _____

   e. _____

2.16.5 Types of Data Transfer

Data transfer refers to the transmission of data from one device to another. There are generally four types of data transfer. The following figure shows the types of data transfer:

Fig. 2.16.5: Types of data transfer

Interrupt Transfer

Input devices that are used as human interfaces such as keyboards, mouse and so on, generally use this. The detected input signals are handled as interrupt requests. In case of USB, the processes, as interrupt requests, are initiated by the host. The host periodically "polls" the input device, to reflect the keyboard inputs to the screen so that the user is not irritated. The method with which the host transfers the data periodically is referred to as "Interrupt transfer."

Bulk Transfer

Image input, printing and storage devices such as digital cameras, printers, scanners and so on are required to transfer large volumes of data without any loss. Bulk transfer facilitates highly reliable data transfers. The rate of transfer depends on the availability of the bus. Hence, it is not suited for applications requiring strict management of the data transfer rate.

Isochronous Transfer

Real time data transfer is required for the audio and video devices. Such devices must be capable of transferring a certain quantity of data on a periodic basis. USB uses frames for dividing time into units, for the data transfers to be executed.

The main concept is to transfer a constant amount of data over each time period, maintaining a consistent flow of time.

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.

2.16.6 Data Transfer Mode

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 shown in the following images:

- **Simplex:** Communication is unidirectional. Data can be sent in one direction only, from the sender to the receiver.

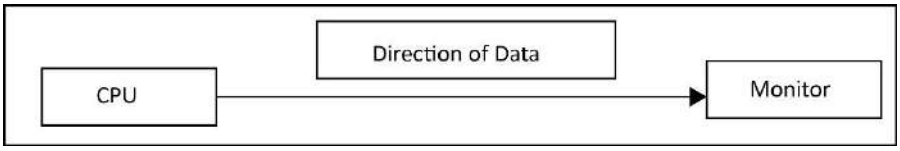


Fig. 2.16.6: Simplex mode

- **Half Duplex:** Data can be sent in both directions but not at the same time.

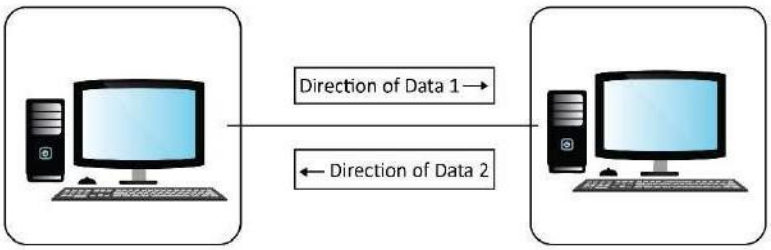


Fig. 2.16.7: Half duplex mode

- **Duplex:** Data can be sent in both directions simultaneously. A device can send as well as receive data, for example a telephone network.

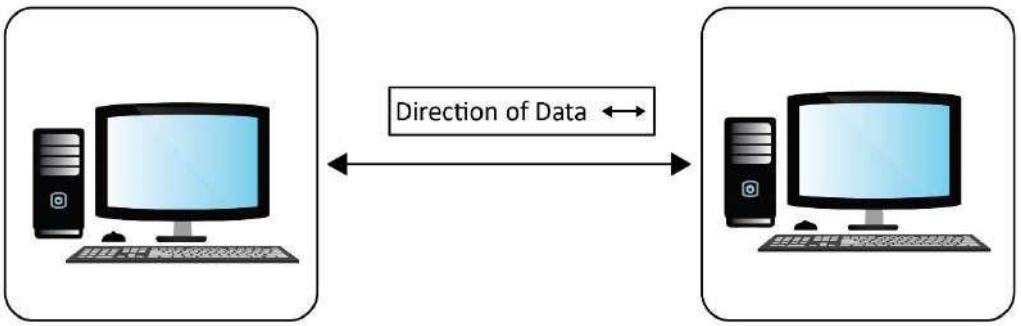


Fig. 2.16.8: Duplex

2.16.7 Controlling the Data Transfer

Data transfer can be controlled by changing the baud rate of the Arduino or the Raspberry Pi. The following image shows the baud rate of a set up:

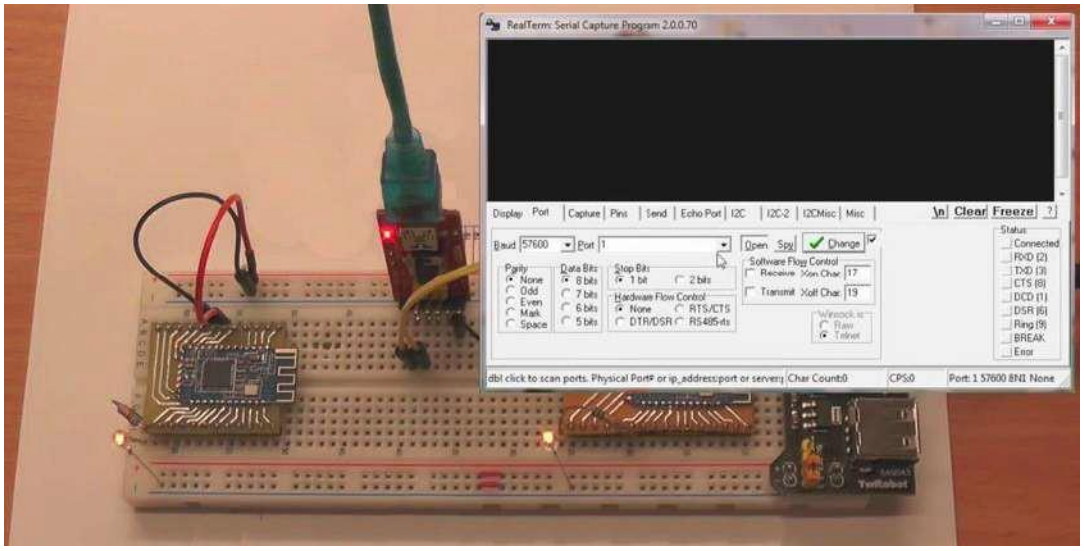


Fig. 2.16.9: Baud rate of a set up

To control the data transfer rate for a router, the following steps should be followed:

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. The following image shows the wireless settings for TP-Link:

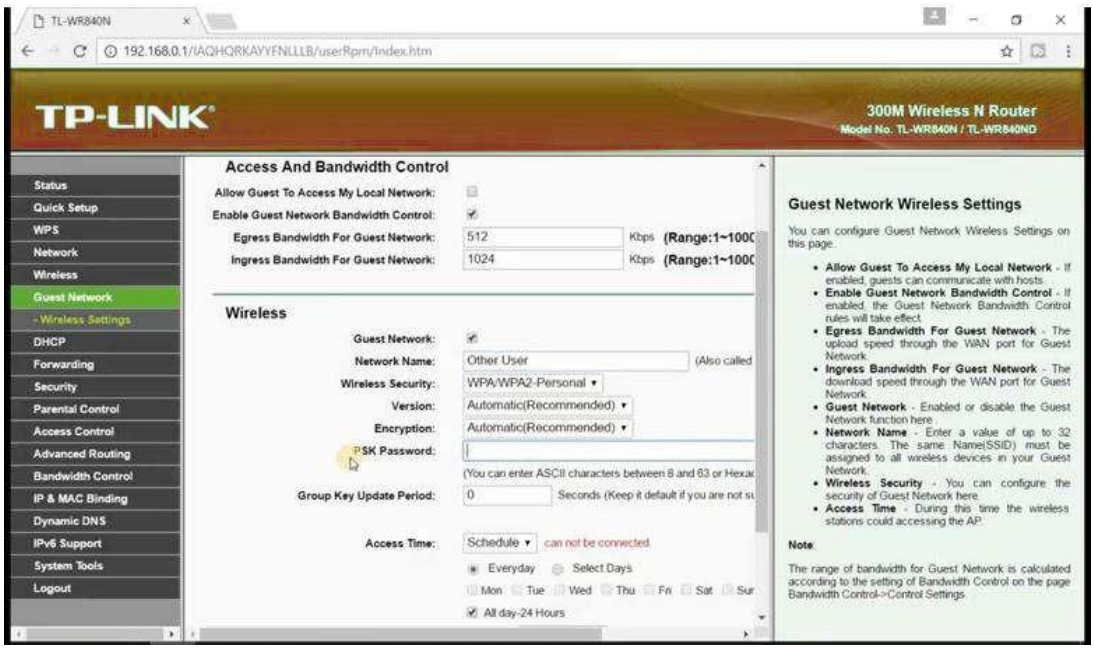


Fig. 2.16.10: Wireless settings for TP-Link

Exercise

1. Write the types of data transfer and their features.

   a. _____

   b. _____

   c. _____

   d. _____

Practical

Perform a Zigbee gateway installation for a smart home set up.

Required Tools/Equipment:

- Ethernet and power cable
- Wi Fi router set up
- ZigBee gateway connection app
- IoT device to control switches

Practical

Perform a Raspberry Pi board Bluetooth network configuration.

Required Tools/Equipment:

- Raspberry Pi board with Bluetooth configuration
- Computer system with Raspberry Pi framework installed
- USB cable for connection.

Practical

Perform a Raspberry Pi serial console connection over Bluetooth.

Required Tools/Equipment:

- Mobile device with Bluetooth configured
- Raspberry Pi board with Bluetooth configuration
- Power supply to Raspberry Pi board

Practical

Perform the prerequisite steps involved for setting up router and IoT camera device installation.

Required Tools/Equipment:

- Site for IoT device installation
- IoT camera installation kit
- Router installation kit
- Tool kit

Practical

Perform the steps involved in connecting an IoT camera and router by automatic and manual connection.

Required Tools/Equipment:

- Router installed with internet connection
- IoT camera
- Computer system with latest configuration

Practical

Perform the steps involved in installation of a router.

Required Tools/Equipment:

- Router installation kit
- Ethernet cable with internet connection
- Computer system with latest configuration

Practical

Perform the steps for configuring a router after installation.

Required Tools/Equipment:

- Router
- Ethernet cable with internet connection
- Computer system with latest configuration

Practical

Establish connection between NVR, camera device and router to initialise the nodes.

Required Tools/Equipment:

- NVR installation kit
- Computer system with latest configuration and internet connection
- Router and Ethernet cable

Practical

Configure a router to connect a sensor device remotely to the network.

Required Tools/Equipment:

- Router with active internet connection
- Laptop/computer system

Practical

Perform the steps to control the data transfer rate of a router.

Required Tools/Equipment:

- Router with active internet connection
- Laptop/computer system

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

3. Level 1 Troubleshooting of IOT

Telecom Sector Skill Council

Unit 6.1 - Testing Connectivity between Devices
Unit 6.2 - Checking Connectivity between Devices
Unit 6.3 - Checking On-board Memory Storage Card
Unit 6.4 - Testing Working of Connectivity Modules
Unit 6.5 - Checking the On-board Power Supply
Unit 6.6 - Checking Communication Link Performance Matrix
Unit 6.7 - Checking Data Transfer from Gateway to Server
Unit 6.8 - Checking Communication between Devices
Unit 6.9 - Setting Connectivity Credentials
Unit 3.10 –Project on Humidity and Temperature Sensing Device
Unit 3.11 – Project on Air Pollution Sensing Device
Unit 3.12 – Organizational Processes and Standards Unit 3.13 –Project Handling Concepts and Applications
Unit 3.15 – Record Maintenance
Unit 3.16 –Record Performance/Test Results
Unit 3.17 – Maintain Records and Process Documents

Key Learning Outcomes

At the end of this module, you will be able to:

1. Identify the types of IOT testing
2. Explain connectivity of IoT devices
3. Explain the IoT test approaches
4. List the IoT test challenges and IoT testing tools
5. Describe testing pin configuration
6. Explain the different ways of connecting the IoT gateway to the nodes
7. List the tools to verify networking connectivity
8. Explain the role of event viewer and hardware in verifying network connectivity
9. Explain the role of local connectivity
10. List the steps to check on-board memory storage card for storing node data in Raspberry Pi
11. Explain the two ways to store data locally for the Arduino boards
12. List the parameters to check working of on-board Wi-Fi or a 3G, 4G connectivity module
13. Explain the role of range, bandwidth, Intermittent connectivity and security
14. List the steps to run Wireshark
15. Explain the checking of on-board power supply
16. Demonstrate checking of power supply at different hardware configurations
17. List the parameters affecting the performance matrix of node and gateway connections
18. Explain the role of Maximum transmission unit (MTU), data loss, delay and reliability
19. Identify the basic troubleshooting steps to check the data transfer between the gateway and the server
20. Identify the Secure Internal Communication (SIC) ports
21. Explain the checking of SIC and gateway connectivity
22. Identify the steps for loading software and testing the communication between devices
23. Explain starting a node, checking active links and establishing a session
24. Describe securing of devices using the MQTT protocol
25. Explain device authentication based on user id/password
26. Explain device authentication based on one time password (OTP)

UNIT 3.1: Testing Connectivity between Devices

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the types of IOT testing
2. Explain connectivity of IoT devices
3. Explain the IoT test approaches
4. List the IoT test challenges and IoT testing tools
5. Describe testing pin configuration

3.1.1 Types of IoT Testing

The complex architecture of IoT systems and their unique characteristics mandate various types of tests across all system components. To ensure that the scalability, performance and security of IoT applications is up to the mark, certain tests are recommended, which are as shown in the following figure:

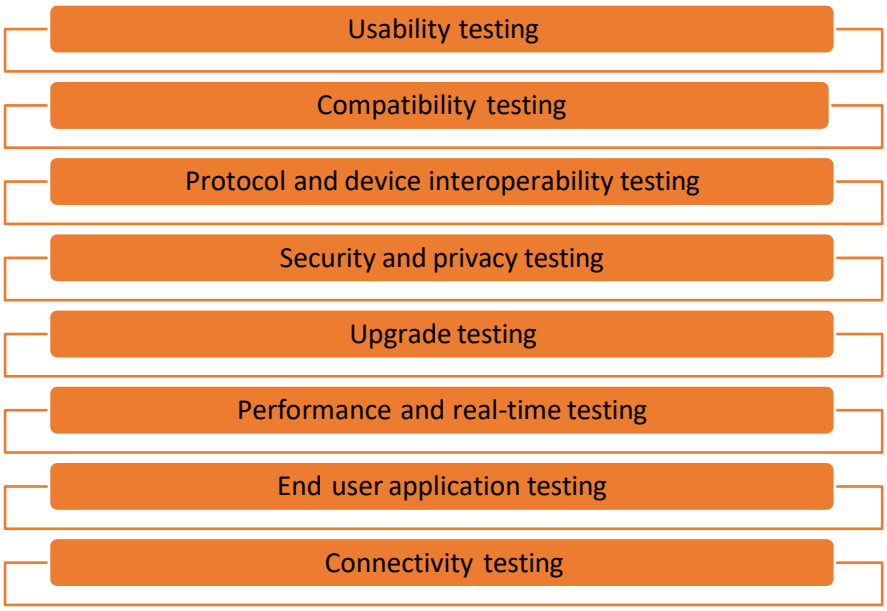


Fig. 3.1.1: Types of testing in IoT

Some basic points to remember for usability are:

1. The usability of each of the devices should be ensured.
2. The devices should be portable so as to be conveniently moved into different segments and areas.
3. The equipment should be smart enough to push not only the notifications but also the error messages, warnings and so on.
4. The system should have an option to log all the events to provide clarity to the end users. If it is not capable of doing that, the system should push those as well to a database to store them.

5. The notifications should be shown and handling of the display should be done properly in the devices [computers/mobile devices].
6. Usability in terms of displaying data, processing data and pushing job tasks from the devices should be tested thoroughly.

Some basic points to remember for compatibility testing are:

1. The complex architecture of an IoT system makes compatibility testing a must.
2. Testing items such as, multiple operating system versions, browser types along with respective versions, generations of devices and communication modes [for e.g. Bluetooth 2.0, 3.0] is necessary for IoT compatibility testing.

Some basic points to remember for protocol testing are:

1. As IoT comprises of various protocols, it needs to pass through multiple regulatory/compliance checkpoints.
2. It is essential to ensure that such a scenario does not arise where the product passes through all the testing steps but fails in the final compliance checklist [testing performed by regulatory body].
3. It is better to practice to meet the regulatory requirements in the starting of the development cycle itself.
4. The same should be made a part of the testing checklist. By doing this, it is ensured that the product is certified for the regulatory checklist as well.

Some basic points to remember for IoT security are:

1. The biggest security challenge of IoT is that it is data centric, where all the devices/systems connected together operate based on the data that is available.
2. When it comes to the data flow between devices, there is always a chance that the data can be accessed or read while getting transferred.
3. From a testing standpoint, it is to be checked if the data is protected/encrypted when getting transferred from one device to the other.
4. Wherever there is a user interface (UI), ensure that there is a password protection on it.

Some basic points to remember for upgrade testing are:

1. IoT is a combination of multiple protocols, devices, operating systems, firmware, hardware, networking layers and so on.
2. When an upgrade is performed, be it for the system or for any of the involved items as stated above, thorough regression testing should be carried out/strategy should be adopted, so as to overcome upgrade related issues.

Some basic points to remember for performance testing are:

1. As per the performance of the system, the testers need to ensure that the IoT system is scalable.
2. When the technicians carry out testing, it should be done for 2-10 testing platforms at a time and it should be ensured that the data is propagated to 10-20 devices.
3. As testers, the technicians need to make sure the system performs the same even though the added data is propagated.
4. The technicians should also test the monitoring utility to display the system usage, power usage, temperature and so on.

Some basic points to remember for end user/pilot testing are:

1. As far as the IoT is concerned, pilot testing is a must.
2. Testing only in a lab makes sure that the product/system works appropriately. But, this may backfire badly when exposed to real-time conditions/steps/scenarios.
3. During pilot testing, the system is exposed to a limited number of users in the real field. They use the application and give feedbacks on the system.
4. These comments come in handy to make rectifications so that the application becomes robust enough for production deployment.

Some basic points to remember for connectivity are:

1. As it is an Internet based solution, connectivity plays a vital role.
2. The system has to be available all the time and should have seamless connectivity with the stakeholders.
3. As per connectivity, two things are very important to test;
    - Maintaining connectivity, transferring data and receiving job tasks from the devices should be seamless when the connection is up and running.
    - The other condition that needs testing is the connection down scenario. It does not matter how robust the system and the network are; there are chances that the system will go offline. Being a tester, the technician should test the offline conditions as well. Once the system is not available on the network, there has to be an alert which can prompt the technician or the user to rectify any issue. On the other hand, there has to be a mechanism in the system which can store all the data in it during the offline period. Once the system comes online, all that data should get propagated. Data loss should not be there in any condition.

IoT Testing Challenges

There are many challenges a tester faces in IoT.

Hardware-Software Mesh

IoT is an architecture which is closely coupled among various hardware and software components. It is not only the software applications that makes the system but also the hardware ones; sensors, communication gateways and other parts too play a vital role.

Only functionality testing does not help in completely certifying the system to be as per standards. There is always a dependency of the hardware and the software on each other in terms of the environment, data transfer and so on. So, it becomes a tedious job as compared to testing a generic system [only a software/hardware component].

Device Interaction Module

As this is an architecture between different set(s) of hardware and software, it becomes mandatory that they talk to each other in real time/near real time. When they both integrate with each other, things such as security, backward compatibility and upgrade issues becomes a challenge for the testing team.

Real-time Data Testing

It has already been established that a pilot testing/regulatory testing is mandatory for a system such as this; however, it is very tough to get data for doing pilot test of an IoT device. Being in the testing team, getting regulatory checkpoints or getting the system deployed in the pilot is very difficult for the technician. The step becomes even tougher if the system is related to healthcare as per the example. So, this stays as a big challenge for the testing team.

User Interface (UI)

IoT is spread across devices belonging to every platform [iOS, Android, Windows, and Linux]. Testing it on certain devices can be done but testing it on all possible devices is almost impossible. The possibility of the UI being accessed from a device which is not owned or simulated cannot be ignored. That is a challenge which is tough to overcome.

Network Availability

Network connection plays a vital role, as IoT is all about the data being communicated at faster speeds all the time. The IoT architecture has to be tested in all kinds of network connectivity/speeds. To test this, virtual network simulators are mostly used to vary the network load, connectivity, stability and so on.

IoT Testing Tools

There are various tools which are used during testing of IoT systems. They can be classified based on the target as follows:

Software:

1. Wireshark**:** This is an open source application used to monitor the traffic in the interface, source/destination host addresses and so on.
2. Tcpdump**:** This does a similar job as that of the Wireshark except, this does not have a graphical user interface (GUI). This is a command line base dutility which helps the user in displaying the TCP/IP and other packets that are transmitted or received over a network.

Hardware:

1. Joint Test Action Group (JTAG) Dongle: This is similar to a debugger in PC applications. This helps in debugging the target platform code and shows the variable step by step.
2. Digital Storage Oscilloscope: This is used to check various events with time stamps, glitches in power supply and signal integrity check.
3. Software Defined Radio: This is used to emulate receiver and transmitter for a large range of wireless gateways.

3.1.2 Testing PIN Configuration

The connectivity of the microcontroller board with the sensor can be tested by testing the PIN configuration of the microcontroller. Testing for PIN configuration of microcontroller with a sensor is done to detect the proper functioning between the sensor and the microcontroller.

An example of a sound sensor module can be taken, which is used to detect sound intensity. These sensors are used for security, switches and other types of monitoring devices. The accuracy of the sound sensor can be adjusted as per the usage. The sound sensor basically uses a microphone which provides input to an amplifier. Then, the input goes to the peak detector and buffers. Whenever a sensor detects a sound, a voltage signal is processed and sent to a microcontroller, which performs the necessary action.

Specifications

The specifications for a sound sensor and a microcontroller are given as follows:

- Operating voltage: 3.3 V-5V
- Output model: digital switch output (0 and 1, high or low level)
- Mounting screw hole
- PCB size: 3.4 x 1.6 cm
- PIN configuration
- VCC: 3.3 V-5V DC
- GND: Ground
- DO: Digital output
- AO: Analog output

Schematic Diagram

The following figure shows the schematic diagram of a sound sensor and a microcontroller:

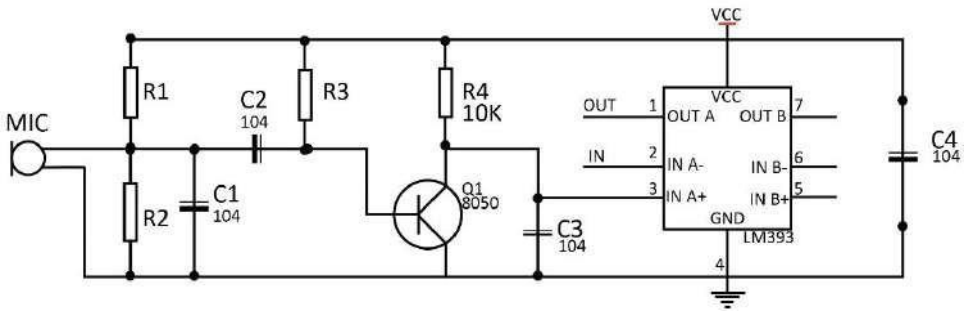


Fig. 3.1.2: Schematic diagram of sound sensor and microcontroller

Wiring Diagram

The following image shows the wiring diagram of a sound sensor and a microcontroller:

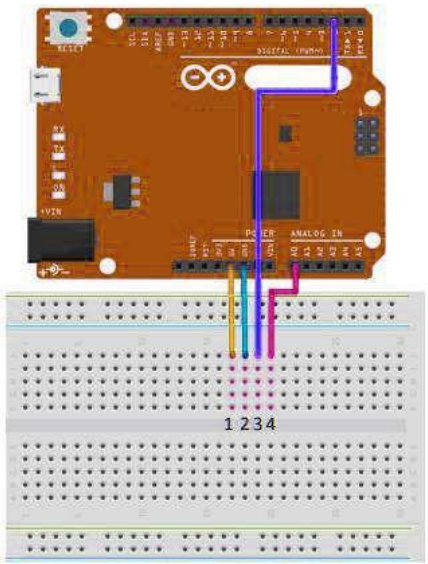


Fig. 3.1.3: Wiring diagram of sound sensor and microcontroller

Sample Sketch

The sample sketch is as follows:

```
void setup(){
    Serial.begin(9600);
    pinMode(2, INPUT);
}
void loop()
{
if(digitalRead(2) == 0) Serial.println("no sound detected");
else Serial.println("sound detected");
delay(250);
}
```

Test Procedure

Components Used:

- Microcontroller (any compatible Arduino)
- Sound sensor module
- 1 Pin M-M connectors
- Breadboard
- USB cable

1. As per the wiring diagram, connect the components by using an M-M pin connector.
2. Connect the VCC pin to the 3.3V or 5V power supply and GND pin to the ground. DO pin and AO pin are connected to digital I/O pin and analog pin respectively.
3. Insert the sample sketch into the Adruino IDE after connecting the pins.
4. Connect the ports from microcontroller to the computer by using the USB cables.
5. Look for the results in the serial monitor.

Test Results

The following image shows the module when it is not subjected to sound:

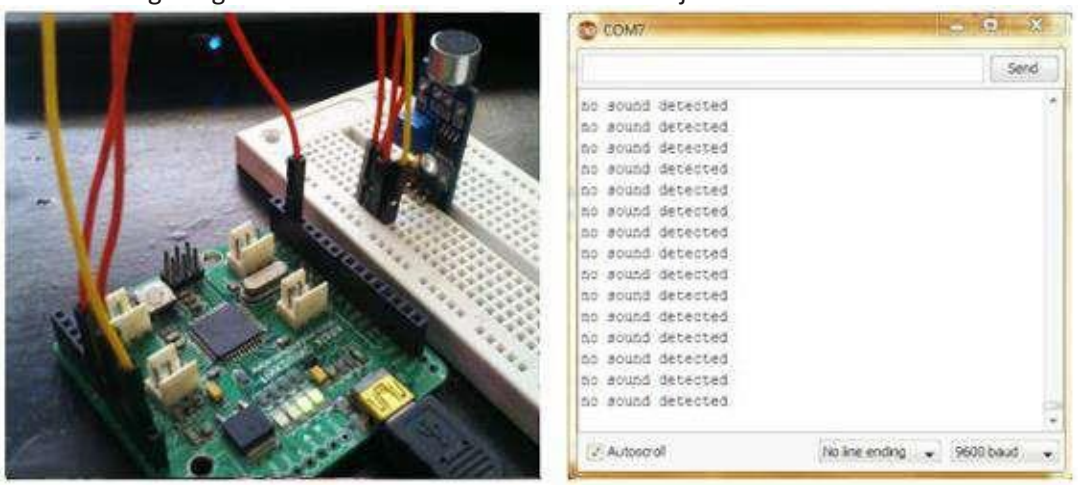


Fig. 3.1.4: Test results when sound is not detected

The following image shows the module subjected to sound, where the red LED lights up when the sound is detected:

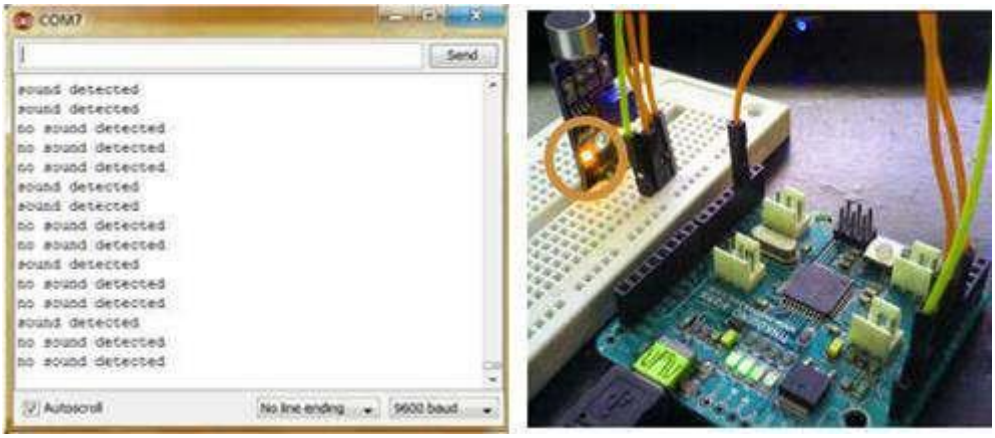


Fig. 3.1.5: Test results when sound is detected

Exercise

1. List the types of testing required in IoT.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____
   g. _____
   h. _____

2. Write down some basic points to remember for end user/pilot testing in IoT.
   a. _____
   b. _____
   c. _____
   d. _____

UNIT 3.2: Checking Connectivity between Devices

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the different ways of connecting the IoT gateway to the nodes
2. List the tools to verify networking connectivity
3. Explain the role of event viewer and hardware in verifying network connectivity
4. Explain the role of local connectivity

3.2.1Node Gateway Connectivity

There are different ways by which an IoT gateway can extend connectivity to nodes. Some of which are:

- Via IoT Gateways
- Directly – IoT Nodes

Via IoT Gateways

Nodes can connect to the IoT via a gateway. The nodes themselves are not IP-based and thus cannot directly connect to the Internet/WAN. Rather, they use either wired or wireless PAN technology to connect to the gateway with a less expensive and less complex mode of connectivity. The gateway maintains an IoT agent for each node that manages all data to and fro from the nodes. In this case, application intelligence can also be located in the gateway. The following figure shows nodes connected to the IoT via a gateway:

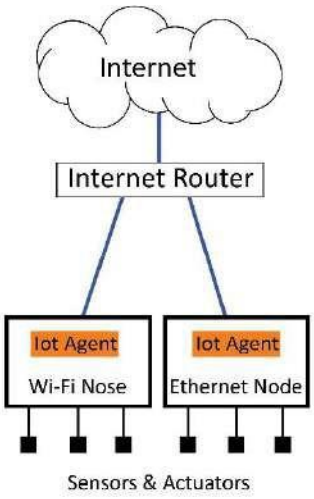


Fig. 3.2.1: Node connectivity via IoT gateway

Directly – IoT Nodes

Nodes can connect directly to the Internet using a WAN connection such as Wi-Fi or Ethernet. The gateway serves primarily as a router; in fact, it can be simply a router when nodes have their own IoT agent and autonomously manage themselves.

The following figure shows nodes connected directly to the Internet using a WAN connection:

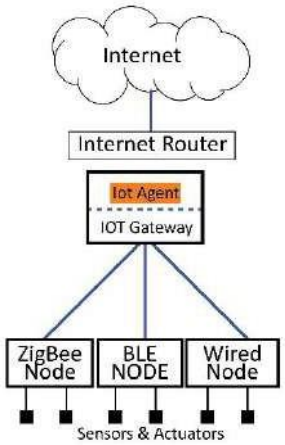


Fig. 3.2.2: Node connectivity directly to IoT gateways

Network Connectivity

Identifying and diagnosing active directories' issues is required for verifying network connectivity. This results in diagnosis of various network issues along with the suggestions. The following areas are examined to determine the network functioning problem:

Event Viewer

It is the most useful tool to identify networking problems, directory services and the solutions of the problems. It also categorises the errors for easy analysis. Check the event log to see if in the directory service there is any occurrence of indicator of future problems. Check the system log folder and analyse the type of error warning lists. Visit the event properties page for each error warning to view the description and the data returned. Click the words and translate the hexadecimal code to decimal in the Data box. If there is a number in the event column for the error code, use the net helpmsg command to get the description of the error.

Example:

If the starting four digit of 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 command prompt:

nethelpmsg<message number in decimal>

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

Hardware

In hardware network hub, cables, devices and so on are checked for their functionality. For example, if in the network dial-up connection property in the control panel, the connection icon is marked with a red 'X', this means that the network cable is disconnected. Check the server operation guide to check hardware functionality.

Check the network adaptors and drivers' functionality through the control panel. Also, the hardware wizard on the hardware tab of the system properties in the control panel can be used. To check whether a device is working properly, select the device from the device box. Click finish and the trouble shooter starts as Add/Remove hardware wizard exits. Each device property can be examined by double clicking the device icon. Generally, tab status of each device is displayed. Click the trouble shooter to check if the device is not working properly.

Local Connectivity

Check the local area connection for verifying the network connectivity. Ensure that the devices reconnected to the network and the IP addresses are correct. This can be done by using IPConfig command-line tool. This tool can be used to view or modify the IP configuration details in the computer. IPConfig can also be used to register the computers' entire DNS service with the DNS dynamic update.

The steps to configure IP details are as follows:

1. Open the command prompt, type ipconfig and press ENTER
2. In the output look for the following:
   - IP address
   - Default gateway
   - DBCP server
3. Use ping tool to get the network connectivity between default gateway and DHCP server.

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

1. Open the command prompt, type the following for ping the loopback address:

   127.0.0.1

   If it fails, then verify that the computer was restricted, after TCP/IP was installed and configured.
2. Ping the IP address of the computer.

   If the ping command fails then restart the computer to check the computer with TCP/IP installed and configured.
3. Ping the IP address of default gateway.

   If the ping command fails, verify the default gateway IP and check the router.
4. Ping the IP address of remote host.

   If the ping fails, check the correctness of remote host IP address; see that it is operational and the router between the host and the remote computer is operational.
5. 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.

The following example is for an unsuccessful TCP/IP configuration for the local area network. The disabled components are in bold text. The IP address is not displayed as the absence of IP address shows that the local area network is not properly connected:

- ipconfig /all

  Windows 2000 IP Configuration

  Host Name SERVER1

Primary DNS Suffix ..... reskit.com
Node Type . . . . . : Hybrid IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No DNS Suffix Search List. ..... reskit.com
server1.reskit.com
Ethernet adapter Local Area Connection:
Media State .....Cable Disconnected
Description .....3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)
Physical Address. . . . . : 00-10-5A 99-F7-15

The following is an example for network connectivity available in a network with IP address displayed:

- ipconfig /all
  Windows 2000 IP Configuration
  Host Name Server1
  Primary DNS Suffix ..... reskit.com
  Node Type . . . . . : Hybrid IP Routing Enabled. . . . . : No WINS Proxy Enabled. . . . . : No DNS Suffix Search List. ..... reskit.com
  Server1.reskit.com
  Ethernet adapter Local Area Connection: Connection-specific DNS Suffix. : Server1.reskit.com
  Description .....3Com EtherLink XL 10/100 PCI TX NIC (3C905B-TX)
  Physical Address. . . . . : 00-10-5A-99-F7-15 DHCP Enabled ..... No IP Address. . . . . : 172.25.128.19 Subnet Mask.....: 255.255.252.0
  Default Gateway . . . . . : 172.25.128.1DNS Servers .....: 172.26.128.19
  Primary WINS Server .....: 172.25.254.203

Exercise

1. Write the steps to configure IP details.
   - _____
   - _____
   - _____

2. Write the steps to test TCP/IP connectivity by using the ping command.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____

UNIT 3.3: Checking On-board Memory Storage Card

Unit Objectives

At the end of this unit, you will be able to:

1. List the steps to check on-board memory storage card for storing node data in Raspberry Pi
2. Explain the two ways to store data locally for the Arduino boards

3.3.1 Checking the Storage

Arduino boards do not have built-in storage devices. Raspberry Pi boards come with a Secure Digital (SD) drive and can accept USB-based storage devices where data can be stored. The steps which could be used to check the on-board memory storage card for storing node data in Raspberry Pi are as follows:

1. Open a new command line/terminal session as shown in the following image:

Fig. 3.3.1: New command line

2. Run the command “Df” and press enter.
3. This will display the total disk usage for the SD card in columns as shown in the following image:

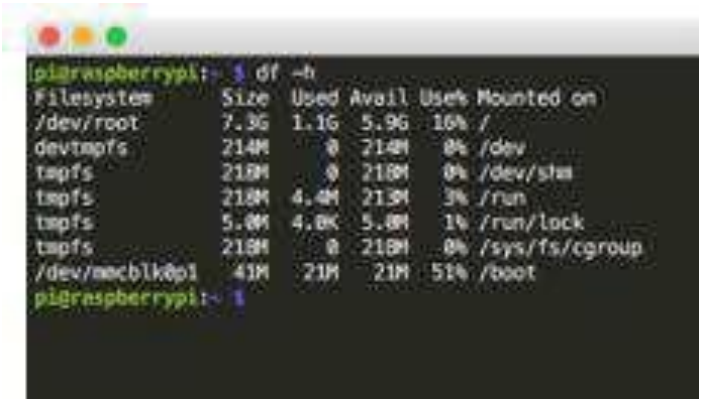


Fig. 3.3.2: Total disk usage

4. To make it more readable, add the -hflag (Df-h), which will add G and M units for gigabytes and megabytes.

3.3.2 Local Storage Options for the Arduino

Although the Arduino has no on-board storage devices, there are two ways to store data locally for the Arduino. It can be stored in a special form of non-volatile memory or on an SD card, hosted via either a special SD card shield or an Ethernet shield (most Ethernet shields have a built-in SD card drive).

Note: Some of the communication protocols can be used to send data to other devices. For example, the serial interface can be used to write data to a serial device.

Exercise

1. Write the steps to check on-board storage card on a Raspberry Pi board.
   - _____
   - _____
   - _____
   - _____

UNIT 3.4: Testing Working of Connectivity Modules

Unit Objectives

At the end of this unit, you will be able to:

1. List the parameters to check working of on-board Wi-Fi or a 3G, 4G connectivity module
2. Explain the role of range, bandwidth, Intermittent connectivity and security
3. List the steps to run Wireshark

3.4.1 Checking the Network

The following parameters should be considered to check the working of an on-board Wi-Fi or a 3G, 4G connectivity module at the nodes:

- Range
- Bandwidth
- Intermittent connectivity
- Security

Range

Networks can be described in terms of the distances over which data is typically transmitted by the IoT devices attached to the network. The wireless devices have a software utility which monitors the signal strength and the transmission, such as light indicators of green, yellow or red colour. When the indicator is green that means the signal is good and strong. As the distance moves away from the router or access point, the strength of the signal goes low and the indicator turns yellow. When the signal strength drops to the weakest point then the indicator turns red.

Test the packet loss

1. For windows, click start button and enter "cmd' in the search field section. Then, press ENTER.
2. Type the ping followed by an IP address and then press ENTER. The following are some common ping commands:
   - Ping 127.0.0.1: This is a "loopback ping" in which if the loopback step fails, then the TCP driver might be corrupted, the network adaptor might not be working or IP might have been interfered by another service.
   - Ping: This will ping IP address of a local computer of a remote server or any client that receives the IP address to verify that it is reachable. An example is, ping 192.168.1.1 which is default IP address of NETGEAR router.
   - Ping: This command will test the Internet connectivity and DNS functionality, for example, ping google.com.

Bandwidth

Bandwidth, or the amount of data that can be transmitted in a specific period of time, limits the rate at which data can be collected from the IoT devices and transmitted upstream. The following factors need to be considered:

- The volume of data that each device is generating
- The number of devices that are deployed in a network
- The way the data is being sent; as a constant stream or in intermittent bursts, as the bandwidth that is available will need to cope with the peak periods

For testing the bandwidth, an IPERF tool can be used. The following steps are performed to test the bandwidth using the iperf tool:

1. Start the iperf server on the desired port. The following image shows the method to start iperf on a server:

Fig. 3.4.1: Method to start iperf on a server

2. This can be done from the client end by connecting the server port, tweaking more connections and reporting parameters as shown in the following image:

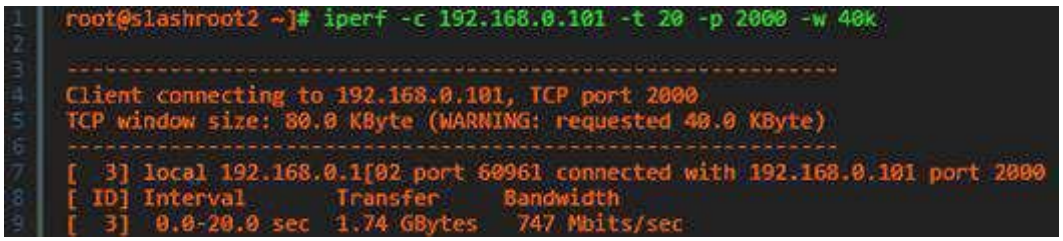


Fig. 3.4.2: Connections and reporting parameters

The options used in commands are as follows:

- -t option used in the command given above gives data transfer for 20 seconds.
- -p option tells the client to connect the port 2000 on the server.
- -w will specify desired window size value, as the window size tuning improves the TCP transfer rate to a certain extent.

The iperf shows the transfer rate at an interval of 1 second for the whole 10 second transfer.

Intermittent Connectivity

Firstly, it is required to check whether the issue is in wired or wireless network. This can be done by performing the following step:

1. Continuously ping the Google's public DNS (8.8.8.8) and the router simultaneously from the terminals of the laptop. If packet loss is found in both the IPs, then there must be an issue in the wireless connection. If the packet loss is only on 8.8.8.8, then there should be an issue with the wired connection.

After finding the fault in the wire/wireless connection, the following steps should be performed:

1. Check the configuration.
2. Misconfiguration in IP address, subnet mask and gateway can lead to syncing failure and this will make the testing difficult. Include DNS access and Internet connection via router to avoid any further issue.

Wireshark- Packet Capture

Wireshark is a tool which is used to troubleshoot network issues. The following steps are performed to run the Wireshark:

1. Download and install the Wireshark
2. Open the Wireshark on the system
3. Click the gear icon on the top of the window
4. Make sure that the monitor mode is enabled for en0 interface as shown in the following screenshot:

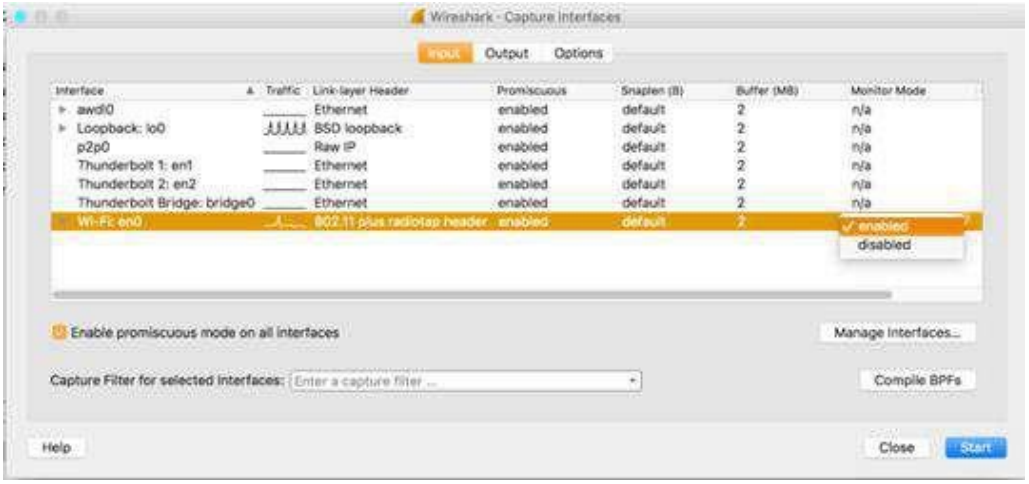


Fig. 3.4.3: Wireshark screenshot

5. Click on the close icon and restart the Wireshark
6. Start capture on en0, which is a beacon, control and management frame interspersed with data frames

Security

Security is always a priority; so ensure to select networking technologies that implement end-to-end security, including authentication, encryption and open port protection. For example, IEEE 802.15.4 includes a security model that provides security features that include access control, message integrity, message confidentiality and replay protection; which are implemented by technologies based on this standard, such as ZigBee.

Exercise

1. Write the steps involved in testing the packet loss in network.
   a. _____
   b. _____
2. Write the factors to be considered for testing the bandwidth of an IoT network.
   a. _____
   b. _____
   c. _____

UNIT 3.5: Checking the On-board Power Supply

Unit Objectives

At the end of this unit, you will be able to:

1. Explain the checking of on-board power supply
2. Demonstrate checking of power supply at different hardware configurations

3.5.1 Check the On-board Power Supply

The Raspberry Pi is powered by a +5.1V micro USB supply. Exactly how much current (mA) the Raspberry Pi requires is dependent on what is connected to it.

Typically, the model B uses between 700-1000Ma depending on what peripherals are connected; the model A can use as little as 500mA with no peripherals attached. The maximum power the Raspberry Pi can use is 1 Amp. If a USB drive needs to be connected that will take the power requirements above 1 Amp, then connect it to an externally-powered USB hub.

The power requirements of the Raspberry Pi increase as use of the various interfaces on the Raspberry Pi is increased. The GPIO pins can draw 50mA safely, distributed across all the pins; an individual GPIO pin can only safely draw 16mA. The HDMI port uses 50mA, the camera module requires 250mA and a keyboard and a mouse can take as little as 100mA or over 1000mA. Check the power rating of the devices which have to be connected to the Pi and purchase a power supply accordingly.

Monitor the voltage across RPi under different setups to see whether the power supply is indeed within 4.75 to 5.25V when operating. To achieve that, measure the board using multimeter on TP1 and TP2. The following image shows the location of TP1 and TP2 on board:

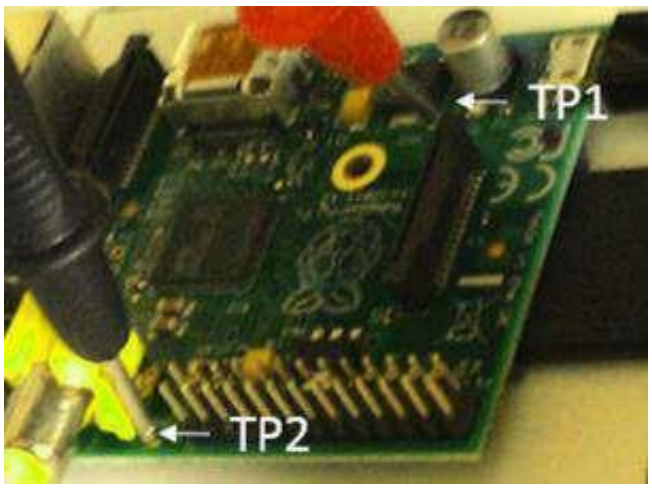


Fig. 3.5.1: TP1 and TP2 on board

Check the power supply at different hardware configurations:

- Normal Mode + WLAN + LAN; The following image shows the power supply testing in normal mode + WLAN + LAN:

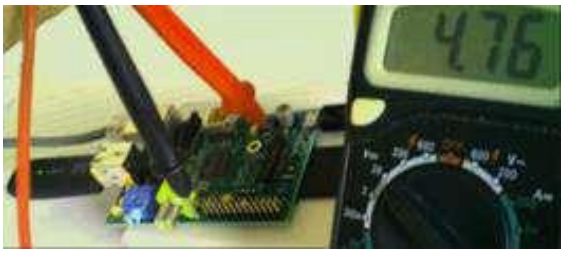


Fig. 3.5.2: Power supply testing in normal mode + WLAN + LAN

- Normal Mode + WLAN; The following image shows the power supply testing in normal mode + WLAN:

Fig. 3.5.3: Power supply testing in normal mode + WLAN

- Normal Mode + LAN + USB Keyboard + Mouse; The following image shows the power supply testing in normal mode + LAN + USB keyboard + mouse:

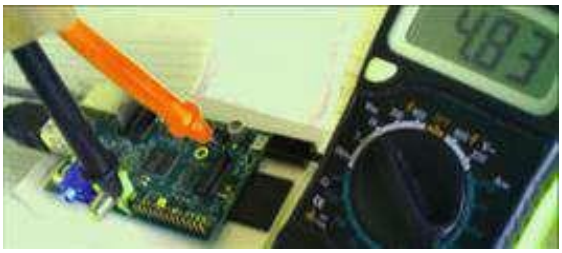


Fig. 3.5.4: Power supply testing in normal mode + LAN + USB keyboard + mouse

- Normal Mode + LAN; The following image shows the power supply testing in normal mode + LAN:

Fig.3 .5.5: Power supply testing in normal mode + LAN

- Normal / Idle Mode; The following image shows the power supply testing in normal / idle mode:

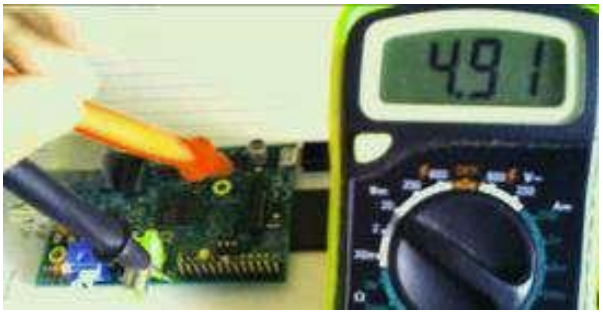


Fig. 3.5.6: Power supply testing in normal / idle mode

- Power Down Mode; The following image shows the power supply testing in power down mode:

Fig. 6.5.7: Power supply testing in power down mode

Exercise

1. Write the different types of hardware considerations for IoT hardware power testing.
   a. _____
   b. _____
   c. _____
   d. _____
   e. _____
   f. _____

UNIT 3.6: Checking Communication Link Performance Matrix

Unit Objectives

At the end of this unit, you will be able to:

1. List the parameters affecting the performance matrix of node and gateway connections
2. Explain the role of Maximum transmission unit (MTU), data loss, delay and reliability

3.6.1 Performance Matrix Parameter

Parameters which affects the performance matrix of node and gateway connections are:

- MTU
- Data loss
- Delay

MTU

In computer networking, the MTU is the size of the largest network layer protocol data unit that can be communicated in a single network transaction. Fixed MTU parameters usually appear in association with a communications interface or standard. Some systems may decide MTU at connection time.

Check the best value of MTU for the Internet:

1. Open the command prompt window. Input command "ping -f -l xxxx192.168.0.1".

   Note: xxxx stands for the value of MTU. The best value of MTU then needs to be attained according to the results
2. If the result "packet needs to be fragmented but DF set." appears, it means that the value is too big. Decrease the value and test again. The following screenshot shows checking of MTU:

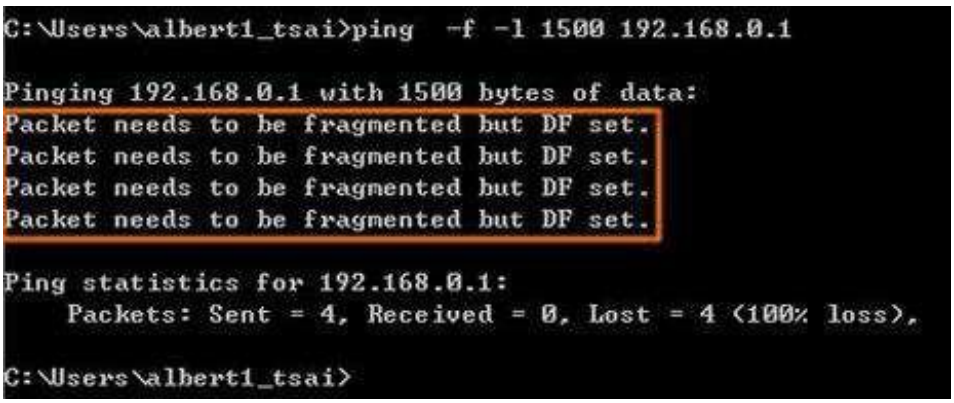


Fig. 3.6.1: Checking MTU

3. If the result comes out as below, it means that the value is suitable:

   Reply from 192.168.0.1: bytes=xxxx time=xxxms TTL=xxx

4. To find the best value of MTU, increase the value and test againuntil a best value is found, which will not cause the packet to be fragmented. The following screenshot shows unfragmented packets:

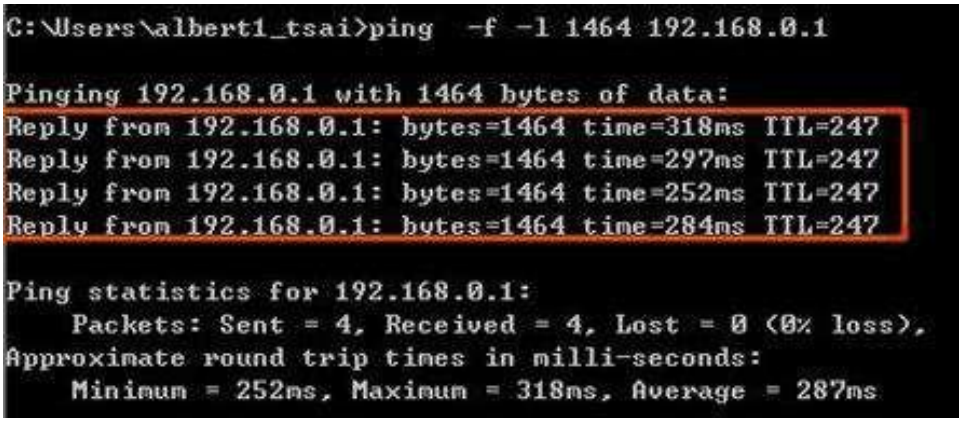


Fig. 3.6.2: Unfragmented packets

5. Since the reality value of MTU should include 20 bytes for IP header and 8 bytes for ICMP header, it needs to add 28 bytes into the result which is obtained from the previous step.

Data Loss

Data loss is an error condition in information systems in which information is destroyed by failures or neglect in storage, transmission or processing. Information systems implement backup and disaster recovery equipment and processes to prevent data loss or to restore lost data.

Check Data Loss

1. Begin the packet loss test. Open Windows menu to locate the command processor.
2. Identify the IP address of the gateway.
3. Now, ping the IP of the gateway.

   The following screenshot shows the pinging gateway IP:

Fig. 3.6.3 Pinging gateway IP

4. To test the packet loss, ping a website from the network; for example, google.com. The following screenshot shows pinging of google.com:

Fig. 3.6.4 Pinging google.com

5. It will provide the network latency reported as round trip time (RTT) in milliseconds (ms). The following screenshot shows round trip time:

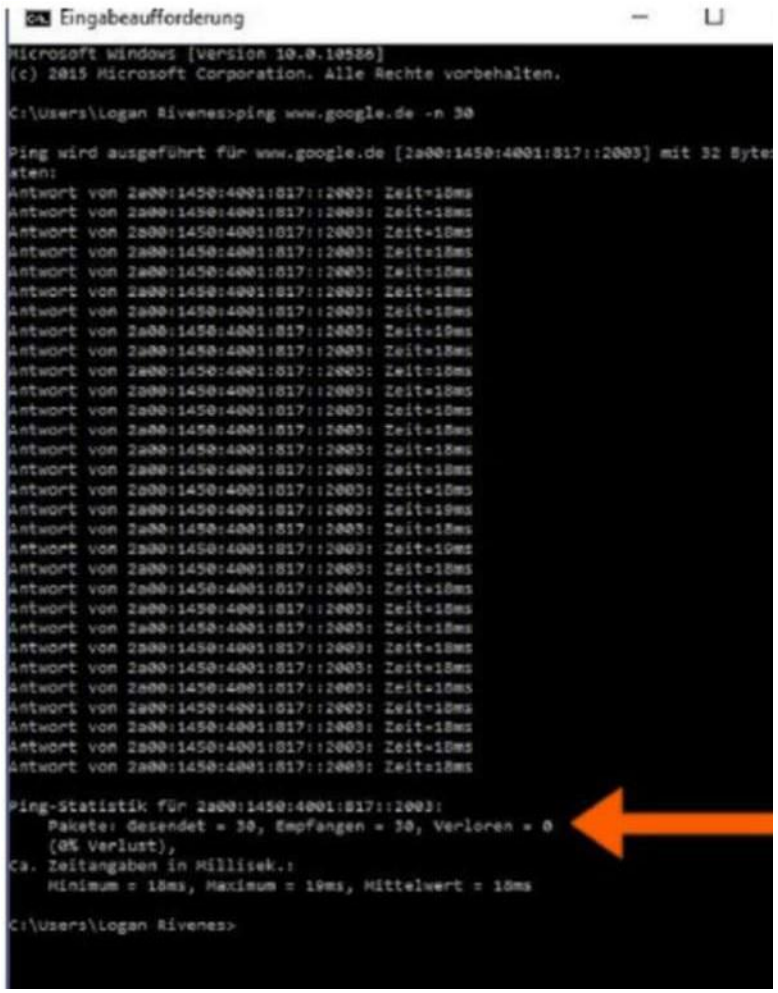


Fig. 3.6.5 Round trip time

Delay

The delay of a network specifies how long it takes for a bit of data to travel across the network from one node or endpoint to another. It is typically measured in multiples or fractions of seconds. Delay may differ slightly, depending on the location of the specific pair of communicating nodes.

Test Delay in Network

1. Enter the commands for testing network and Internet latency directly at the command line.
2. Run a Ping loopback test. The Ping loopback test will test the computer's connection to verify that there are no local hardware problems causing the network or Internet latency issue.
3. Type "Ping 127.0.0.1 -n 20". This IP address is the same for nearly all built in network connections. The "-n 20" extension will send 20 packets of data before terminating the test.
4. View the statistics. The time it took for the packet of data to travel locally should be less than 5ms and there should be zero packet loss.
5. Run Ping to a remote server. Now that it has been verified that the local port is working, Ping remote servers to test the latency.
6. Normal latency varies by the type of connection from 5ms - 40ms for cable modem, 10ms - 70ms for DSL, 100ms - 220ms for dial-up and 200ms – 600ms for cellular. The distance to the remote server also adds to latency.
7. Type "Ping" followed by the IP address or site URL to be pinged and press Enter.
8. View the report. As the test pings the remote address, it will report back the results; the final number after the "time = "is the time it took, in milliseconds, for the packet to travel to the remote site and back to the computer.
9. Run Traceroute test. The traceroute test will show the path that the data travels from the computer to the remote server and any delay in that path. This can be helpful in determining the source of network or Internet delays.
10. Type "tracert" followed by the IP address or site URL to route and press Enter.
11. View the results. As the test traces the path, it will display each address along the way and the time it took for a data packet to travel and acknowledge receipt for each "hop" along the path. The more "hops" or other devices the data packet needs to route through, the more delay will be experienced.

Exercise

1. Write down the steps to check the data loss in a network.

   a. _____

   b. _____

   c. _____

   d. _____

   e. _____

UNIT 3.7: Checking Data Transfer from Gateway to Server

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the basic troubleshooting steps to check the data transfer between the gateway and the server
2. Identify the Secure Internal Communication (SIC) ports
3. Explain the checking of SIC and gateway connectivity

3.7.1 Data Transfer from Gateway to Server

The connection between the gateway and the server can be done by performing afew basic steps and checking the ports. The steps performed in checking the data transfer between the gateway and the server are as follows:

Basic Troubleshooting Steps

These include the following steps:

- Ensure that the gateway and the security management server are connected properly.
- Check whether the server and the gateway are using the same SIC activation key.
- Ensure that the date and the time of the operating system is accurate. If the security management server and the remote gateways are in two different time zones then the remote gateway needs certification validation.
- Ensure that the connection between the security management server and the remote gateway are allowed, if the security management server is behind any other gateway.
- Check whether the security management server's IP address and name are present in the host file on the gateway.
- If the IP address of the security management server undergoes static network address translation (NAT) by the local security gateway, thenadd a public IP addressof the security management server to the host file on the remote gateway to resolve to its hostname.
- Then, restart the Check point daemon(CPD) with the commands as follows:

  #cpwd admin stop-name CPD-path "$CPDIR/bin/cpd_admin" -command "cpd_admin stop"

  #cpwd_admin start –name CPD –path "$CPDIR/bin/cpd" –command "cpd"
- Based on sk33764, using the command line of the gateway, type: fwunloadlocal. This will remove the security policy from the security gateway server and allow all the traffic through it.

After basic troubleshooting, the technician should perform the basic connectivity check to make sure the gateway and the server are connected properly.

Checking Connectivity

Before performing the connectivity check, make sure that the SIC ports are open. The SICports are:

- Port 18209: this port is used for communication between the VPN-1/Firewall-1 Module and the certificate authority (status, issue, revoke).
- Port 18210: This port is used to pull certificate from the CA.
- Port 18211: This port is used by the cpd daemon on the module to receive the certificate (when clicked on the initialize in the policy editor).

To check if the SIC is listening to its network ports on the check point device (can be security gateway server or security management server), the following commands are used:

- For Windows:
  - Open the CMD and execute:

    >netsat –na | findstr 18211
- For Linux:
  - #netsat –na | grep 18211
- The output should be:

  TCP 0.0.0.0”18211 0.0.0.0:0 LISTENING

A NAT device will not be affected between SMatCenter server and security gateway, on the basis of a check point enabled entity which communicated by using the SIC. This is because the protocol is based on certificates and SIC names which are not the IPs.

To check if the gateway is listening to the smartcenter server to get the certificates, the CPD debugs the output which should be as follows:

[CPD ID]@cpmodule[Date] Get SIC KeyHolder: SIC certificate read successfully

[CPD ID]@cpmodule[Date] SIC initialization started

[CPD ID]@cpmodule[Date] get my sicname from the registry:

Read the machines sic name: CN=member_1,0=cpmodule..6vxoys

[CPD ID]@cpmodule[Date] Initializes sic infrastructure

[CPD ID]@cpmodule[Date] SIC certificate read successfully

[CPD ID]@cpmodule[Date]nInitialised SIC authentication methods

Exercise

1. Write the types of SIC ports that need to be checked while testing the network connectivity.

   a. _____

   b. _____

   c. _____

UNIT 3.8: Checking Communication between Devices

Unit Objectives

At the end of this unit, you will be able to:

1. Identify the steps for loading software and testing the communication between devices
2. Explain starting a node, checking active links and establishing a session

3.8.1 Test for Node and Gateway Software

After the final set up of nodes and gateways, the technician needs to check the communication between the devices by running the software at the nodes and gateways. The following are the steps performed in loading the software and testing the communication between the devices:

1. Start the Node

Click on the Start Node on the SNA Node operations toolbar to start the local node. Then, to start the node, specify the configuration on it. Select the files that are configured and click open. After some time, the node will start and establish all the defined links.

2. Check that the Links are Active

As the nodes starts, active nodes will appear with names which were specified earlier. To check if the links are active, perform the following steps:

1. Locate the host resource icon which is on the left side of the SNAnode operation window. Select the "+" icon to expand the list of resources.
2. Click the connections (for CPI-C and APPC configurations, click peer connections).
3. Click on the details icon on the toolbar, to get the details about the displayed links.

3. Establish a Session

To establish a session in a configuration, the clients have to establish a session through the gateway to the host. The configuration specified by the client needs to tell the gateway's network address information, such as the token ring address for the gateway' stokenring card.

For AnyNet socket over the SNA, use the following ping application to reach another socket over SNA node in the network:

Ping IP address

If this comes successfully, then a test frame will be received which will indicate that packets were transmitted to the remote node and then they return. Ping application or any other socket application can also be used to reach the local node from another socket over SNA node which is in the same network. Then, run the application on that node only after specifying the local nodes Any Net socket over the SNA IP address.

Exercise

1. Write down the steps taken to check the links in an IoT network.

   a. _____

   b. _____

   c. _____

UNIT 3.9: Setting Connectivity Credentials

Unit Objectives

At the end of this unit, you will be able to:

1. Describe securing of devices using the MQTT protocol
2. Explain device authentication based on user id/password
3. Explain device authentication based on one time password (OTP)

3.9.1Securing Devices

After completion of the installation of IoT devices with all the connection tests done, the last step is to secure the entire network and the device.

Device security ensures that only trusted set of devices are used to access the network and the devices which can break the trust or application can be blocked from sending any type of command to the network or accessing any data. A device simulator program that demonstrates the security mechanism is discussed as follows:

- User ID/Password authentication
- OTP authentication
- Server unique authentication
- Message payload authentication

The following screenshot shows a device simulator:

Fig. 3.9.1: Device simulator

Authenticating with a User Name and Password

The MQTT protocol provides username and password field in the CONNECT message for the authentication of any device. A client should send a user name and password to connect to any MQTT broker.

The user name is a Unicode Transformation Format 8-bit (UTF-8) encoded string and the password is a binary data, each of which has a 65535 byte max. The MQTT protocol which does not encrypt the user name or password unless any transportation encryption is used, is sent in clear text format. The following screenshot shows sample coding for username and password in MQTT:

```
try {
    MqttClient securedClient = new MqttClient(broker, clientId, persistence);
    MqttConnectOptions connOpts = new MqttConnectOptions();
    connOpts.setCleanSession(true);
    connOpts.setUserName(userName);
    connOpts.setPassword(password.toCharArray());
    System.out.println("Connecting to broker: "+broker);
    securedClient.connect(connOpts);
    System.out.println("Connected");
} catch(MqttException me) {
    System.out.println("reason "+me.getReasonCode());
    System.out.println("msg "+me.getMessage());
    System.out.println("loc "+me.getLocalizedMessage());
    System.out.println("cause "+me.getCause());
    System.out.println("excep "+me);
    me.printStackTrace();
}
```

Fig. 3.9.2: User name and password fields in MQTT

Authenticating with OTP Authentication

In MQTT provided authentication mechanism, the IoT application needs to implement additional security to identify any device which tries to connect. An OTP based authentication approach is developed for these situations. This is useful for protecting the device from improper use by eliminating any kind of risk occurring due to unauthorised users gaining access to it.

When the OTP authentication is enabled, the device sends an OTP request to the IoT broker application after startup by using a normal MQTT messaging. The following image shows the flow diagram of OTP authentication system:

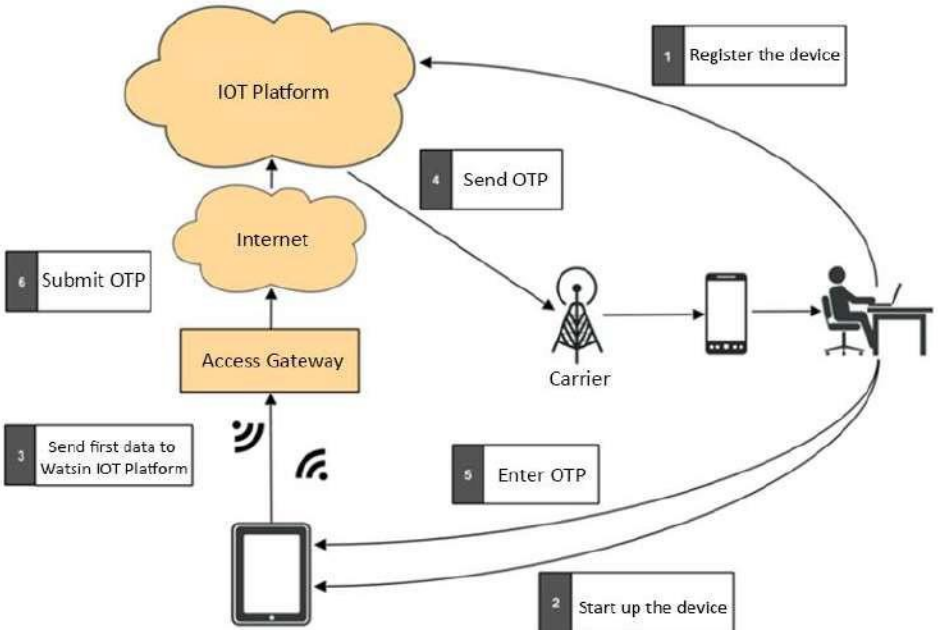


Fig. 3.9.3: OTP authentication system

A code shows how OTP authentication can be turned on or off by using any of the devices' properties. The code is shown in the following image:

```
    // Create the request for OTP
    JSONObject idObj1 = new JSONObject();
    try {
        idObj1.put("event", "server_otp_request");
        idObj1.put("deviceId", deviceIdentifier);
    } catch (JSONException e1) {
        System.out.println("Exception occurred");
        e1.printStackTrace();
    }
    new SendMessageToServer("server_otp_request", idObj1).start();
    System.out.println("otp request sent....");
}
```

Fig. 3.9.4: Code for OTP authentication in MQTT

The IoT app then generates an OTP, which is sent to the device owner separately by sending the notification to the device. The following screenshot shows the OTP generation code in MQTT:

```
otp = IOTSecurityUtil.generateOTP();

JSONObject jsonObj = new JSONObject();
try {
    jsonObj.put("cmd", "server_otp_response");
    jsonObj.put("otp", otp);
    jsonObj.put("appid", strAppId);
    jsonObj.put("time",
    new SimpleDateFormat("yyyy-MM-dd HH:mm:ss").format(new Date()));

 // Server starts a timer of 5 mins during which the
 // OTP is valid.
    task = new TimeOutTask();
    t = new Timer();
    t.schedule(task, 30000000L);

} catch (JSONException e) {
    e.printStackTrace();
}
System.out.println("Sending otp  -  " + otp);

// Publish command to one specific device
// iot-2/type/<type-id>/id/<device-id>/cmd/<cmd-id>/fmt/<format-id>
new SendMessageToDevice(strDeviceId, "server_otp_response", jsonObj)
        .start();
```

Fig. 3.9.5: Code for OTP generation in MQTT

After the OTP is generated, the OTP is entered into the device which sends it to the broker app. This app validates the OTP sent by the device and sends a success/failure (in case of incorrect OTP or timeout situation) message to the device. Then the device can retry OTP authentication based on a retry count from the configuration.

If the OTP authentication is not successful even after a retry, the application shuts down. Otherwise if OTP authentication is not enabled, the device will skip OTP authentication after startup.

The following screenshot shows the code for validation of OTP authentication:

```
    if (receivedOTP.equals(otp)) {
        if (task.isTimedOut) {
        // User took more than 100 seconds and hence the OTP is invalid
        System.out.println("Time out!");
        otpValidated = false;
        otpTimeOut = true;
        } else {
        System.out.println("OTP validated..");
        otpValidated = true;
        otpTimeOut = false
        }
    } else {
        System.out.println("Incorrect OTP..");
        otpValidated = false;
        otpTimeOut = false;
    }

    JSONObject otpRespObj = new JSONObject();
    try {
        otpRespObj.put("cmd", "server_otp_validate");
        otpRespObj.put("isOTPValid", String.valueOf(otpValidated));
        otpRespObj.put("isTimeOut", String.valueOf(otpTimeOut));
        otpRespObj.put("appid", strAppId);
        otpRespObj.put("time", new SimpleDateFormat(
                        "yyyy-MM-dd HH:mm:ss").format(new Date()));
    } catch (JSONException e) {
        e.printStackTrace();
    }
    System.out.println("Result of OTP validation -  " + otpValidated);
    // Publish command to one specific device
        new sendMessageToDevice(strDeviceId, "server_otp_validate",
        otpRespObj).start();

}
```

Fig. 3.9.6: Code for OTP validation in MQTT

Exercise

1. Mention the methods of authentication of any IoT set up.

   a. _____

   b. _____

Practical

Check the on-board memory storage card for storing node data in Raspberry Pi.

Required Tools/Equipment:

- Raspberry pi board with memory card inserted
- USB cable
- Computer system with Raspberry pi framework

Practical

Run and capture data loss by using Wireshark in a network.

Required Tools/Equipment:

- Computer system with an established Internet network
- Wireshark set up on the computer

Practical

Perform test delay in a network.

Required Tools/Equipment:

- Computer system
- Internet network connection

Practical

Perform test of a microcontroller board for a sound sensor compatible to Arduino board.

Required Tools/Equipment:

- Arduino board
- Sound sensor
- Board connecting wires
- Laptop/computer system with latest configuration
- Arduino IDE on system
- 1 Pin M-M connectors
- Breadboard
- USB cable

Practical

Perform bandwidth test of a network using IPERF tool.

Required Tools/Equipment:

- Gateway/Router with established internet network
- Laptop/computer system with latest configuration
- IPERF tool installed on the system

Practical

Perform the steps to troubleshoot network issues using Wireshark tool.

Required Tools/Equipment:

- Gateway/Router with established internet network
- Laptop/computer system with latest configuration

Practical

Perform the steps to check the best value of maximum transfer unit for an internet connection.

Required Tools/Equipment:

- Gateway/Router with established internet network
- Laptop/computer system with latest configuration

Practical

Perform the steps to check delay between IoT devices installed.

Required Tools/Equipment:

- Gateway/Router with established internet network
- Laptop/computer system with latest configuration
- An IoT device such as camera or sensor installed

Practical

Perform the steps in checking the data transfer between gateway and server.

Required Tools/Equipment:

- Gateway/Router with established internet network
- Laptop/computer system with latest configuration

Practical

Perform the steps in loading the IoT camera device software and testing communication between devices.

Required Tools/Equipment:

- Installed IoT camera device
- Laptop/computer system with internet connection
- IoT camera device software installed on computer

UNIT 3.10: Project on Humidity and Temperature Sensing Device

3.10.1 Scenario

Prepare an IoT project for humidity and temperature device which obtains information of the surrounding environment and uploads the data in cloud network.

3.10.2 Application

This device can be installed in cold storage to obtain the humidity and temperature readings anytime from anywhere. This would help in analysing the change in temperature and humidity and its effect on the stored material.

3.10.3 Objective

The objective is to set up IoT hardware for obtaining humidity and temperature information from a sensor which will be analysed on cloud platform through wireless Internet.

3.10.4 Requirements

- DHT-11 sensor
- Thing Speak platform
- Arduino MCU
- ESP8266 Wi-Fi module

3.10.5 Block Diagram of the Setup

The following image shows a block diagram for the complete IoT framework for the humidity and temperature sensing system:

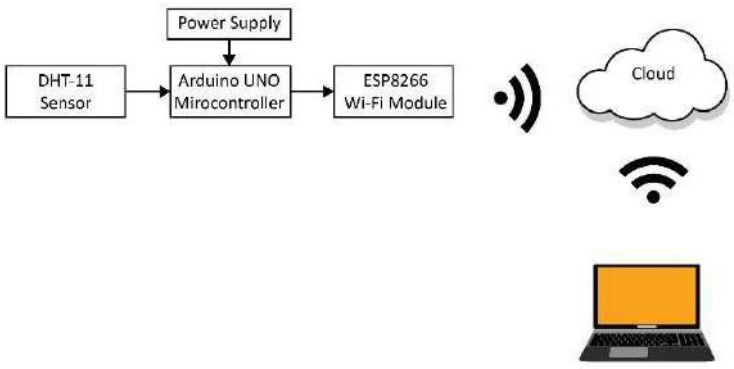


Fig. 3.10.1: Block diagram for the

3.10.6 Circuit Diagram

The circuit for the project is built on Arduino MCU, DHT11 sensor and ESP8266 Wi-Fi module connected together. The following image shows the circuit diagram connections:

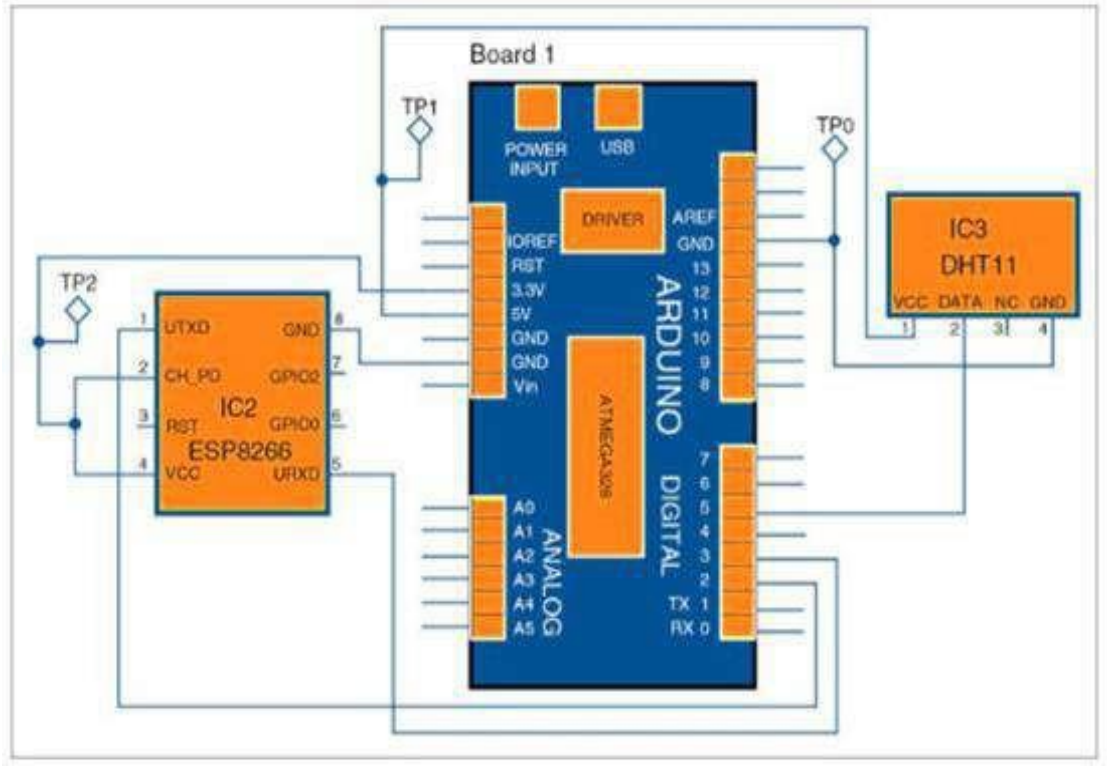


Fig. 3.10.2: Circuit diagram of humidity and temperature monitoring using Arduino with

3.10.7 Basic Working

The DHT11 sensor senses the temperature and humidity of the surrounding and then it sends the data to digital pin 5 of the Arduino MCU. From there the temperature and humidity values are sent to the cloud. These values are sent at regular intervals of time through the ESP8266 Wi-Fi module. Then from the cloud, the data can be taken by using ThingSpeak platform through Internet.

3.10.8 Construction of Project

1. Login to the Think Speak by registering. Use the following link for the same:
   http://thingspeak.com
2. After completing the registration, login to the account and create a new channel by providing humidity and temperature in the fields.

The following screenshot shows the same:

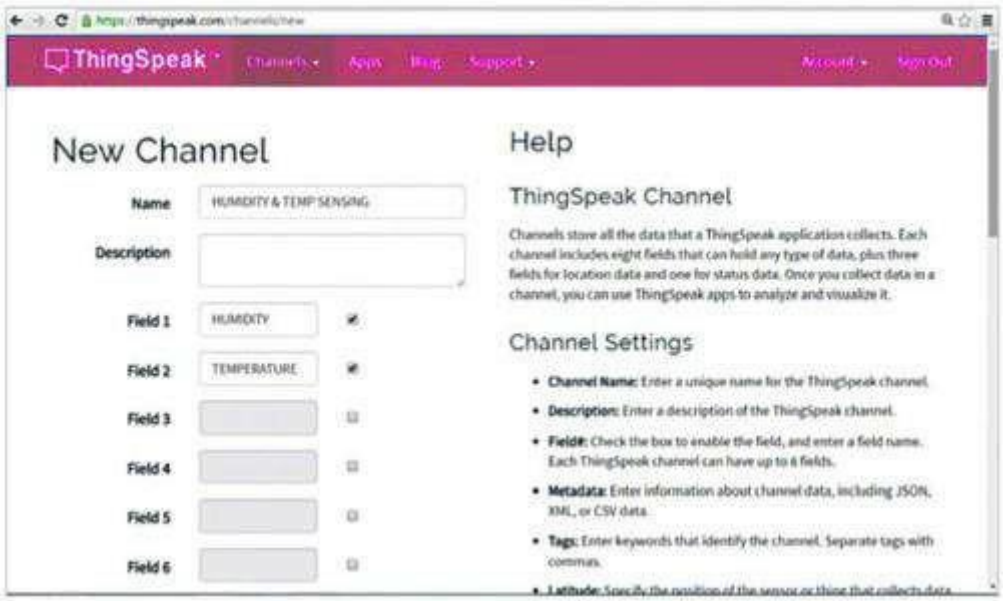


Fig 3.10.3: Filling fields in the Think Speak platform

3. After creating a new channel, it will create the following two API keys:
   - Write API key
   - Read API key
4. Replace the given line in the program with write API key:

   String apiKey = "NTIM1RXET6YVUVWF";
5. Now, provide the Wi-Fi host name and password of the network in the two lines given in the program (IoT.ino):

   String Host_Name = "Jonah";

   String Password = "2569696";
6. Now, the program is verified with the Wi-Fi setup.
7. Compile the sketch/program provided in the kit and upload it to the Arduino MCU through Arduino IDE.
8. After uploading the sketch, the temperature and humidity value can be taken by logging in to the Think Speak account.

UNIT 3.11: Project on Air Pollution Sensing Device

3.11.1 Scenario

Prepare an IoT project for air pollution measuring device which obtains information about air pollution through any smart phone.

3.11.2 Application

This device can be installed in public places like parks and local markets so that it can daily access the pollution, temperature and humidity parameters of the environment. This information can be accessed by people through their smart phones so that they get the information about the pollution level of any area they want while sitting in their homes.

3.11.3 Objective

The objective is to set up the hardware for IoT enabled air pollution meter which monitors air quality on a smartphone using a third-party app.

3.11.4 Requirements

- Arduino board with Arduino shield
- A smartphone with latest android version
- Blynk application available for android phones
- Voltage regulators 7805 (IC1 and IC2),
- Temperature and humidity module DHT11
- Gas sensor MQ135 and PM2.5/PM10 sensor

3.11.5 Block Diagram of the Setup

The following figure shows a complete block diagram of the IoT framework for the air pollution meter:

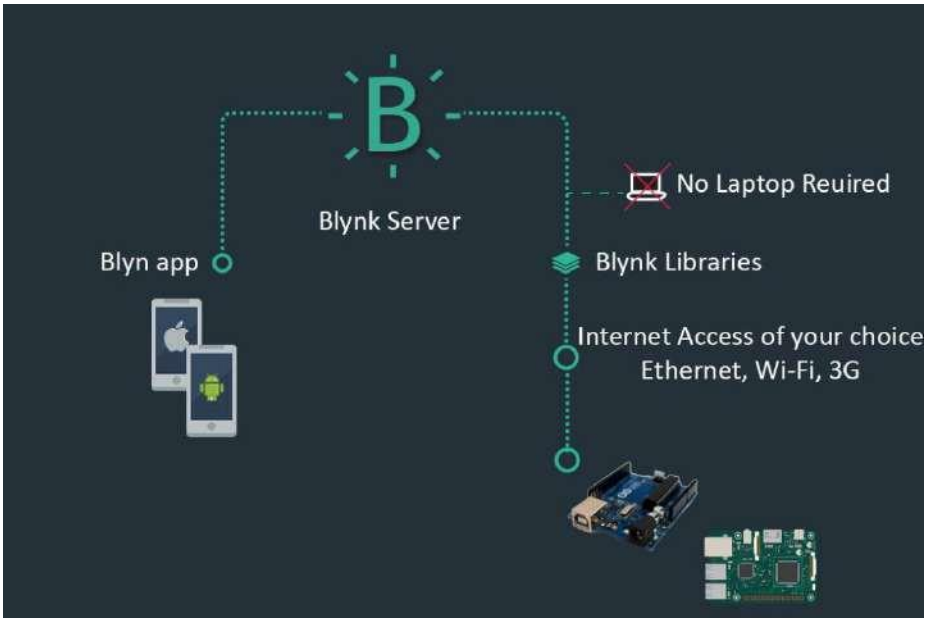


Fig. 3.11.1: Block diagram for IoT framework for the air pollution

3.11.6 Circuit Diagram

The components in the set-up are connected with each other. The main part is the Arduino Uno board with Arduino shield.

The voltage regulators 7805 (IC1 and IC2) are connected with CON7. The temperature and humidity module DHT11 is connected to CON3. The output of the gas sensor is connected to analogue input pin A3 of the Arduino Uno board through CON2. The PM2.5/PM10 sensor is connected to CON1 and this sensor is connected to UART port (TX and RX) of the Arduino Uno board. Connector CON4 is used for connecting 230V AC mains which drives the lamp connected to CON5 and fan connected to CON6. A 12V battery is connected to CON7, which is regulated to 5V using 7805 regulators (IC1 and IC2).

The following image shows the circuit diagram for the same:

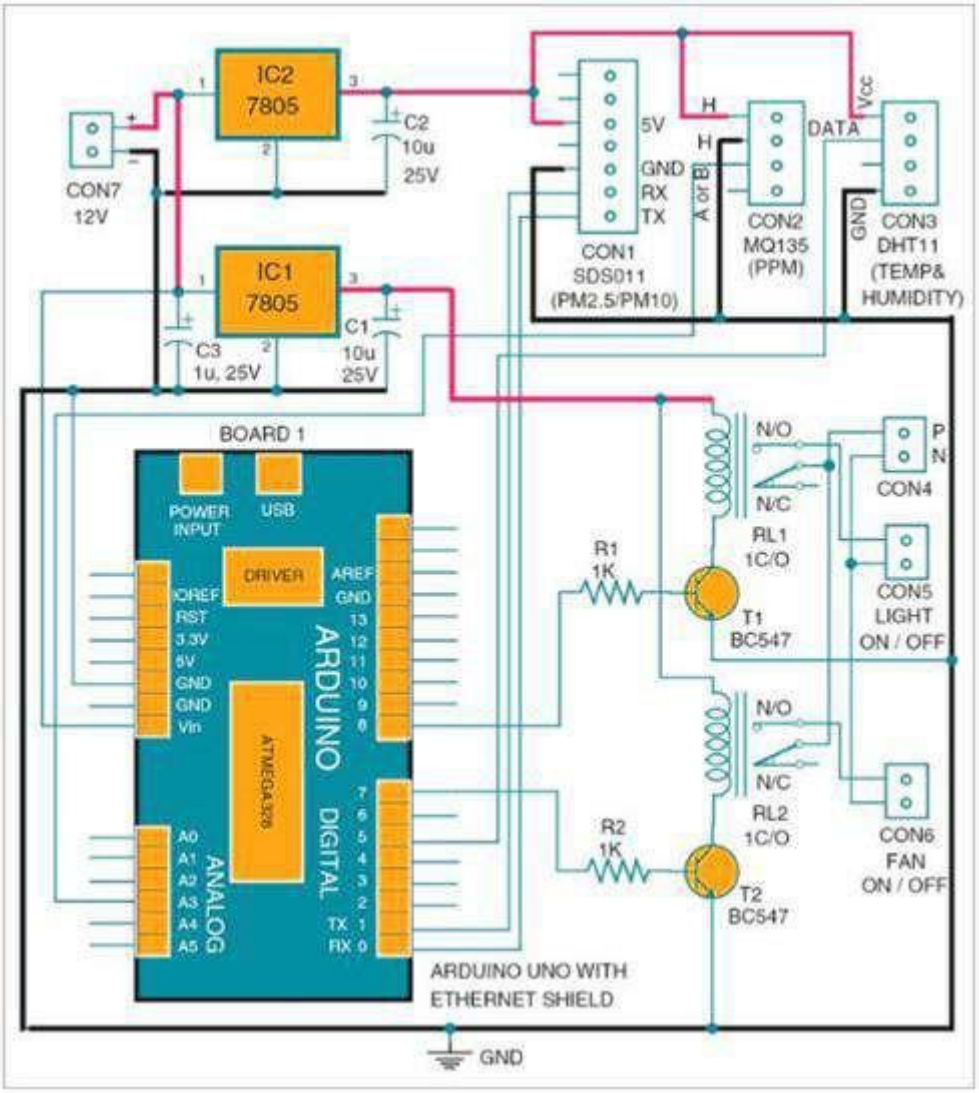


Fig. 3.11.2: Circuit diagram for the air pollution monitoring IoT set-up

3.11.7 Construction of Project

1. Mount the Ethernet shield on the Arduino Uno board and then connect Board1 to a computer by using a USB cable.
2. In Arduino sketch ethernetcient.ino, change the IP address with the systems IP in IPAddress.
3. Compile and upload the code into Arduino Uno from Arduino IDE.
4. Now, compile ethernetserver.ino sketch and upload it to Arduino Uno board. Change the IP address with the systems IP in IPAddress.
5. Navigate to Ethernet shield's IP address.
6. Connect the android mobile with the Wi-Fi.
7. Download and install Blynk app from Google Play Store.

8. Create a new Blynk account. The following image shows the screen for creating a new Blynk account:

Fig.3.11.3: Creating a new account in Blynk

9. After logging into your account, start by creating a new project by giving it a name. The following image shows the screen for creating a new project:

Fig. 3.11.4: Creating a new project window

10. Select the hardware model which is used. Select Arduino Uno in this case. The following image shows the screenshot for selecting hardware:

Fig. 311.5: Selecting the hardware

11. Click email button to send a token to the email address for registration. This token will be used in auth[] = "token" in pollution.ino file. The following image shows the token generation screen of the Blynk:

Fig. 3.11.6: Typical authorisation token

12. Download the Blynk library (Blynk_v0.3.4.zip) and include the library in Arduino IDE. Then compile and upload pollution.ino code to Arduino board. The link for the library file is given below:

    https://github.com/blynkkk/blynk-library/releases/tag/v0.3.4

13. After completing the above steps press Create in the app. The following image shows the screen for the same:

Fig. 3.11.7: Pressing Create button

14. Tap anywhere on the screen to open the widget box and add widgets. The following image shows the screen for widget box window:

Fig. 3.11.8: Widget box window

15. Add the LCD, LED, on/off switch, pushbuttons and RTC widgets. The following image shows the screen for the LCD screen widget:

Fig. 3.11.9: LCD widget setting

16. Now, run the project by pressing Play. The following image shows the play screen and play mode on the app:

Fig. 3..10: Play button and play mode

Key Learning Outcomes

At the end of this module, you will be able to:

1. Define organisational processes
2. Identify the elements and steps of an organisational process
3. Explain the importance of organisational processes
4. Identify the hierarchy in an organisation
5. Explain different project handling concepts
6. List the steps of an IoT project implementation process
7. Explain what is decision making
8. Identify the steps involved in decision making
9. Explain the techniques used in decision making
10. List the advantages of decision making
11. Identify the steps involved in a problem solving process
12. Identify business records
13. Explain the methods of record maintenance
14. Explain the importance of record maintenance
15. Explain the significance of recording performance
16. Analyse a technician's role in recording performance
17. Identify methods used in recording performance
18. Explain the importance of documentation
19. Explain global format system used for documentation
20. List the steps of document processing
21. List the qualities required to do documentation
22. Explain the importance of communication skills
23. Explain the methods to improve reading skills
24. Explain the methods for improving writing skills
25. Explain the methods to develop interpersonal skills
26. List the special safety policies for women
27. Explain methods to improve women safety
28. Explain the need of relaxation policies for women

UNIT 3.12: Organisational Processes and Standards

Unit Objectives

At the end of this unit, the participants will be able to:

1. Define organisational processes
2. Identify the elements and steps of an organisational process
3. Explain the importance of organisational processes
4. Identify the hierarchy in an organisation

3.12.1 Introduction

Every working individual is a part of an organisation and hence needs to adhere to and follow certain processes made by the organisation. An organisational process involves understanding, categorizing, and assigning work to the best suited employee for the task. Therefore, a technician working in IoT installation and devices' configuration needs to follow the processes within an organisation.

Well-developed organisational processes ensure that team members are assigned responsibilities and tasks based on their skills, experience and individuality. If the organisational processes are not well planned, they might have a negative impact on the organisation's overall efficiency and productivity.

The main aim of an organisational process is to increase productivity and efficiency in a group of people, whether they are technicians, supervisors or managers. Such groupshave their own role and responsibility at work.

3.12.2 Importance of Organisational Processes

In any organisation, multitalented people work together towards a single goal. Hence, the processes induce team work which further increases efficiency. Some points highlighting the significance of processes are:

- Categorization based on the experience and the talents, which creates pyramid structure and well-defined roles
- Elimination of duplication of work/responsibilities and thus, decrease in errors while assigning tasks
- Proper co-ordination among team members to solve problem(s), thus making employees aware of the hierarchies and procedures
- Recognition of individual talents and capabilities for appraisals and promotions; this approach develops mental satisfaction and encourages an employee to perform better and more efficiently
- Ensuring security of a position/designation; thus an employee remains less worried about the future

3.12.3 Elements of Process

An organisational process has three common basic components which are as shown in the following figure:

Unity	Team Work	Delegation of Work
In an organisation, people work towards a common goal. Steps to reach desired goals are decided by the manager and conveyed to the employees. People follow common rules, policy and strategy.	In an organisation, different people work in a team to reach the common purpose. People with different skill sets put in their individual effort to attain success. Team leader and other high authorities encourge and guide the employees.	In an organisation, people are classified based on their skill sets and put in a group. For example, the Human Resources team recruits and supports the employees. The Technical team works on technical related issues.

Fig. 3.12.1: Organisational elements

3.12.4 Steps of Organisational Process

An organisational process has five major steps to bring effectiveness. Therefore, as a technician to work effectively in a team, a person needs to perform the steps as shown in the following figure:

Fig. 3.12.2: Organisational process

The steps are:

- **Analysing the Target:** Recognition and classification of the activities used for reaching the goal is done. Higher authorities playa vital role in planning the steps and actions that help to accomplish the goal.

- **Create a Strategy:** Strategies are created by the manager and the team leads to achieve a goal effectively and efficiently.
- **Categorise the Work:** Activities and steps are categorised, based on the importance. These steps are organized to reach the goal in a short/specific duration. This stage finalizes the flow and the frame of the work to be carried out by the people in the organisation.
- **Assign and Give Authorisation:** This is a process to determine the people to be involved in an activity. This is a very important step, because it regulates the work process efficiency and time.
- **Co-ordinate and Have Perfect Relationships:** It is important to maintain a healthy relationship with the people in an organisation. The organisational process should respect the employees and give them freedom to work.

3.12.5 Common Organisational Structure

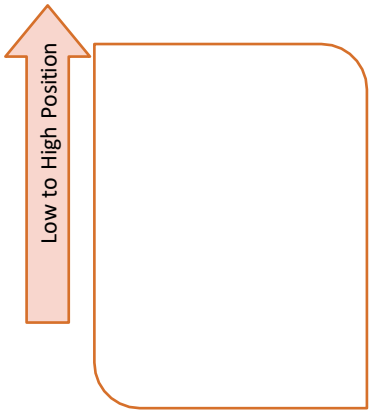
In an organisation, people are divided in a group based on their skill set, educational qualification and work experience. Managers work closely with other employees, such as technicians, to carry out multiple activities for reaching a common goal.

The layout of a general organisational structure is as shown in the following figure:

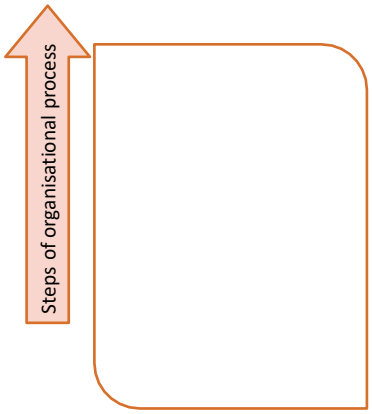
Fig. 3.12.3: Organisational

Exercise

1. Arrange the following personnel in an ascending order as per their position in an organisation:
   Manager – Trainee - Team-lead – Technician - CEO



2. Arrange the following steps as per the correct order:
   Analysing the target - Co-ordinate and have perfect relationships - Categorise the work - Create a strategy - Assign and give authorisation



UNIT 3.13: Project Handling Concepts and Applications

Unit Objectives

At the end of this unit, the participants will be able to:

1. Explain different project handling concepts
2. List the steps of an IoT project implementation process

3.13.1 What are Projects?

A project connects all the work processes into one system. In a growing telecom industry, multi-functional units come together to form a single solution for all the problems. Therefore, team integration plays an important part in achieving goals for IoT projects.

IoT projects are complex because they involve decision making, smart approach and development of complex programme(s) and tools.

3.13.2 Project Handling

As a technician, one would be required to possess some project handling skills as shown inthe following figure:

Cost

Prior to starting a project, analyse its cost and be aware of cost of tools and methods needed for the project.

Feature and Performance

Analyse whether the tools used are effective and easily available. Try to go with preffered brands that have high performance record in the market.

Smart Strategy

Devise a plan and its associated steps to solve a problem or an issue quickly.

Fig. 3.13.1: Project handling

3.13.3 Project Implementation Process

IoT projects are complex and require many activities and planning to be done. The following figure lists the details of a typical project implementation process:

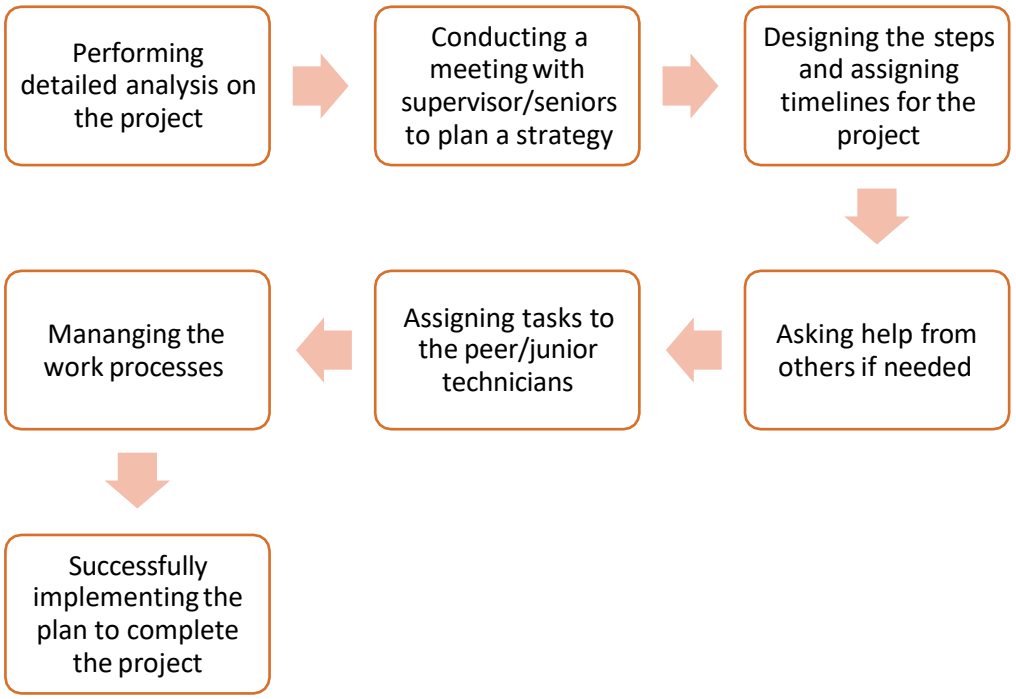


Fig. 8.2.2: Project implementation process

Exercise

Mark the following, True or False:

1. Project management reduces the cost of project.
2. It is very important to create a strategy to start a project.
3. Project management is not beneficial for the employees.

UNIT 3.14: Record Maintenance

Unit Objectives

At the end of this unit, the participants will be able to:

1. Identify business records
2. Explain the methods of record maintenance
3. Explain the importance of record maintenance

3.14.1 Business Records

IoT is all about integrating hardware, software, infrastructure and network. This information is stored in a database or in a cloud platform. Most of the information which is generally stored by a technician includes, plans, client data, tools and strategies.

It is important for a record system to be simple, consistent and easily available.

3.14.2 Methods to Store Records

There are two methods named electronic and manual that are used for storing records as shown in the following table:

Electronic method	Manual method
• It is a method which uses computer based techniques to store any information. • Word and excel files is a common example • It is very simple and effective method. • It can be stored in soft and hard copies both	• It is a traditional method. • The person uses paper, pen, file and other stationary items to store the information. • It is cost effective. • This is less secure as it is prone to accidents like fire.

Fig. 3.14.1: Methods to store

3.14.3 Importance of Storing Records

Maintaining correct business records plays a significant role in the following ways:

- To schedule the work and to make service related appointments
- To store the operational process, product and technology
- To provide reference of previous work to curb possible error in future
- To check the billing and other costs involved during any project
- To check the profit earned by any particular project

- To reduce complications occurring at the time of fixing
- To identify and rectify the drawbacks
- To remove confusions during work by providing reference material
- To keep business and the process on track

Exercise

Fill in the blanks:

1. Common methods to store the data are _____and _____
2. IoT integrates hardware, software _____and _____

UNIT 3.15: Recording Performance/Testing Results

Unit Objectives

At the end of this unit, the participants will be able to:

1. Explain the significance of recording performance
2. Analyse a technician's role in recording performance
3. Identify methods used in recording performance

3.15.1 Recording Performance

Each organisation should have a proper communication system with the clients and the technicians to resolve any errors and to improve the quality of the service.

There are of tools available to alert technicians in case of an error.

After the deliverance of the service, as a technician it is important to schedule a maintenance and performance check. This helps in preventing the future occurrence of errors.

At times, some errors at the technician's end may cost a monetary loss to the client. Such errors should be avoided to uphold the client's trust and the quality of the service.

3.15.2 IoT Services

Some key points about IoT services are:

- Advanced technologies, smarter infrastructure and automation tools have increased the need of IoT services in all organisations.
- If an organisation has derived their work strategy, development and technologies, they are in need of IoT solutions to enable their work plans and operating models.
- IoT services can help in designing a work plan in solution development and in delivery.
- IoT can create a cloud platform which can connect all the operations in an organization including infrastructure, hardware and software tools.

3.15.3 Role of a Technician

Role of a technician includes the following tasks:

- Install efficient and high-quality devices.
- Schedule a visit to a client site to check the performance of the device(s).
- Make use of automation tools.
- Place an alarm system which can signal during error occurrence.

3.15.4 Methods to Record Performance

A technician should follow certain methods to record the performance of his/her service which are as listed in the following figure:

Make Use of Real-time Data

- Use real-time sensors at client's premises to monitor them constantly.
- Get an updated data feed from sensors to be used to check quality and performance of the service.
- Make a presentation or graphic representation from the data feed, if required.

Make Use of Automated Alerts

- Use alert systems for checking the operational conditions of services which need significant attention, for example, Internet downtime and temperature change.
- Ensure that alert system is connected to the mobile of the person who will need an alert in case of error in any operational conditions.
- Reach the client'S site in case of any operational problem, preferably on immediate basis.

Ensure Automated Ticket

- Set a system or tool that can create and send the tickets automatically.
- Ticket system eliminates middle men which require cost and time.
- Make sure the ticket system is easily accessible to clients.

Forecast the Problems or Errors

- Forecast the problems and solve them on regular basis.
- Ensure reduction of errors and downtime at the very first place by forecasting errors.

Make Use of Efficient Tools like Proximity Manager

- Use tools like proximity manager that can come handy during errors. These tools often suggest the possible way to resolve a problem by analysing past history and help in fetching the solution.

Fig. 3.15.1: Methods to record performance

Exercise

Fill in the blanks:

1. Each organisation needs to have proper _____with client and technician to minimize error.
2. After service, technician should do_____check at client's place.
3. Give one example of things that every technician should have:_____
4. _____is one of the technician's role.
5. _____tool is used for issue resolving by analysing previous history.

UNIT 3.16: Maintain Records and process Documents

Unit Objectives

At the end of this unit, the participants will be able to:

1. Explain the importance of documentation
2. Explain global format system used for documentation
3. List the steps of document processing
4. List the qualities required to do documentation

3.16.1Documentation

Nowadays, laptops, computers and mobile devices play a vital role in documentation. So, it is mandatory for every technician to be mobile phone and computer proficient.

Technicians should document the following information:

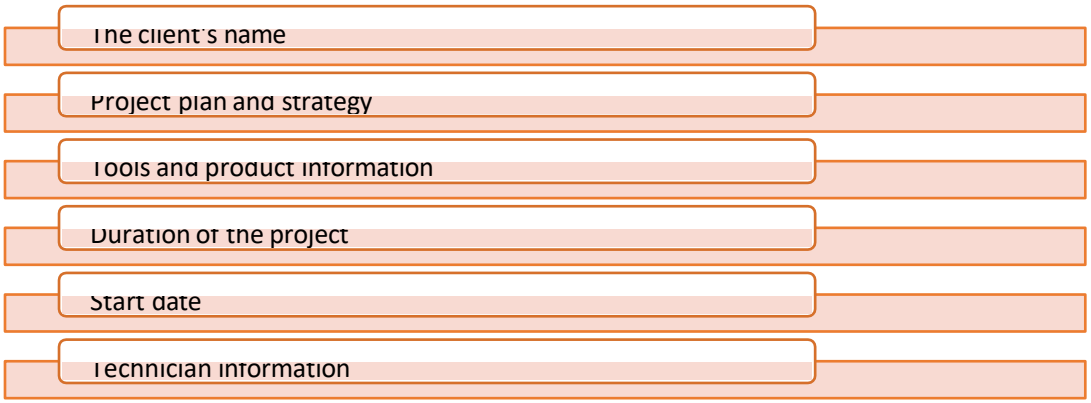
- Service request from client
- Strategy used and followed
- First visit date
- Product used and their cost
- Errors
- Services
- Bills
- Service operation visits

Tools are available to capture the above information and document them automatically.

3.16.2 Document Format

Any document should have information about the work process, the tools used, the involved technician and the client.

The general format used in documentation is as listed in the following figure:



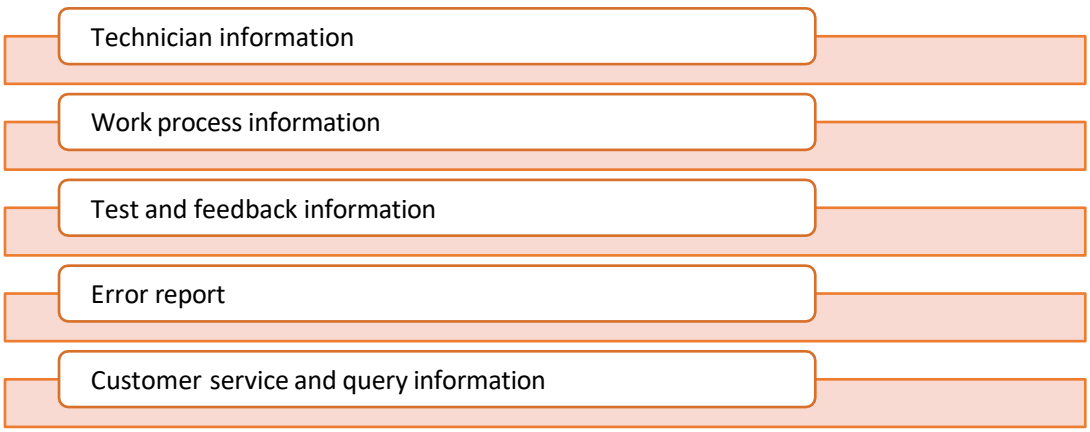


Fig. 3.16.1: Document format

3.16.3 Document Processing

Document processing is a procedure used to convert all information into digital form. The steps that are followed when processing a document are as shown in the following figure:

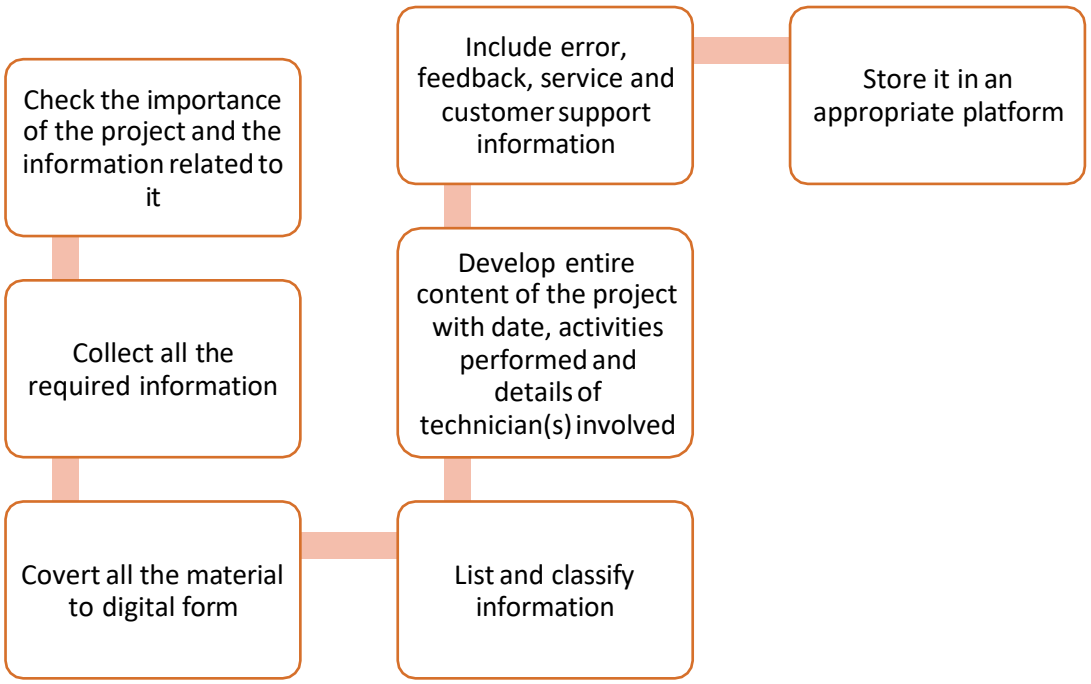


Fig. 3.16.2: Document processing

Tools and devices that can be used in document processing are:

- Laptop or Desktop
- Scanner
- Software Tools

3.16.4 Qualities for Record Maintenance

Records are maintained on high security systems. A skilled person such as a technician is appointed to maintain such records. This person should have the following quali ties:

- Should be able to understand all the tools and sources related to maintenance
- Should be in a position to take decisions appropriate for maintaining and processing records
- Should be aware of legal and privacy statements
- Should track all the day-to-day activities
- Should be able to protect the documents and be aware of the possible threats
- Should be able to furnish the required records
- Should be able to classify important and unimportant information

Exercise

Write the answers in brief:

1. What are the tools used in document processing?

   _____

2. Give two examples of the things that a technician needs to document.

   _____

3. Give two qualities of a person who is involved in record maintenance.

   _____

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

4. Organise work and resources as per health and safety standards

Telecom Sector Skill Council

Unit 4.1 – Workplace health and Safety
Unit 4.2 – Different types of health hazards
Unit 4.3 – Importance of Safe working practices
Unit 4.4 – Reporting safety hazards
Unit 4.5 - Waste Management
Unit 4.6 - Organizations' Focus on Greening of Jobs

TEL/9101

Key Learning Outcomes

At the end of this module, you will be able to:

2. Explain about the work place health and safety
3. Differentiate various health hazards
4. Demonstrate various first aid techniques
5. Importance of safety at workplace
6. Understand Basic hygiene Practices and hand washing techniques
7. Explain the need for social distancing
8. Understand the reporting of hazards at workplace
9. Explain e-waste and process of disposing them
10. Explain Greening of jobs

UNIT 4.1: Workplace health & safety

Unit Objectives

At the end of this unit, you will be able to:

1. Understand about workplace health and safety
2. Explain tips to design a safe workplace
3. Explain precautions to be taken at a workplace

4.1.1 Safety: Tips to Design a Safe Workplace

Workplace health and safety policy defines the best possible work conditions and safety for the employees. Employees have a right to feel safe in their workplace. Hence the organizations create and follow legal standards and ensure a hazard-free workplace.

Every organization is obligated to ensure that the workplace follows the highest possible safety protocol. When setting up a business some tips to remember:

- Use ergonomically designed furniture and equipment to avoid stooping and twisting
- Provide mechanical aids to avoid lifting or carrying heavy objects
- Have protective equipment on hand for hazardous jobs
- Ensure presence of emergency exits and they are easily accessible
- Set down health codes and ensure they are implemented
- Follow the practice of regular safety inspections in and around the workplace
- Get expert advice on workplace safety and follow it
- Get regular inspection of electrical wiring and also the electrical switches and gadgets
- Install fire extinguishers and fire alarms.

4.1.2 Precautions to be taken while at work

Every employee is obligated to follow all safety protocols put in place by the organization.
All employees must make it a habit to:

1. Immediately report unsafe conditions to the supervisor
2. Recognize and report safety hazards that could lead to slips, trips and falls
3. Report all injuries and accidents to the supervisor
4. Wear the correct protective equipment when required
5. Learn how to correctly use equipment provided for safety purposes
6. Be aware of and avoid actions that could endanger other people
7. Always be alert
8. Educate the employees about the first/emergency exits on the floor, and also where the fire extinguishers are kept.

Tips

- Be aware of what emergency number to call at the time of a workplace emergency
- Practice evacuation drills regularly to avoid chaotic evacuations

UNIT 4.2: Different types of Health hazards

Unit Objectives

At the end of this unit, you will be able to:

7. Understand the health hazards
8. Demonstrate First Aid Techniques

4.2.1 First Aid

Illness, injuries, and pain are part of human life. This can happen anyway. Every individual is prone to illness and injuries at any time and anywhere.
In case of any of these, some kind of immediate medical attention or treatment is needed to reduce the discomfort, pain, and deterioration of the condition. The medical attention that is given at the first instance before seeking professional medical help is called "First Aid". First aid is the immediate and temporary treatment given to the victim of an accident or sudden illness while awaiting the arrival of "Medical Aid". First Aid means providing the initial treatment and life support for people with an injury or illness. However, First Aid has its limitations and does not take the place of professional medical treatment. Proper early assistance given by First Aider helps in saving the life of a patient.
Illness and injuries can happen anywhere, be at home, the workplace, or in the market place. Whatever safety measures we adopt, we are all prone to illness sometime or the other.
Some common injuries and their rescue techniques:

4.2.1 First Aid Techniques

- 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.

Click/Scan this QR code to access the video on First Aid at workplace

Fig. 4.2.1a: Clean cut or wound

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.

Fig. 4.2.1b: apply hydrogen peroxide or iodine

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.

Fig. 4.2.1c: 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

For Burns:

11. Immediately put the burnt area under cold water for a minimum of 10 minutes
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
14. Before sterile dressing application, remove jewellery (if any)
15. It is better to leave the burned area open
16. Do not apply any medication or ointment
17. Breaking a blister – it is an absolute no-no!

Fig. 4.2.1d: Put Burnt Area under Water

For Broken Bones and Fractures

1. **Protruding bone must be left alone**

18. If a bone has broken through the skin, it must not be pushed back into place.
19. The area must be covered with a clean bandage and immediate medical attention must be sought.

2. **Bleeding must be stopped**

20. Steady and direct pressure must be applied with a clean piece of cloth for 15 minutes and the wound must be elevated.
21. If a blood soaks through, one must apply another cloth over the first and seek immediate medical attention.

3. **Swelling must be controlled**

22. The RICE (Rest, Ice, Compression and Elevation) therapy must be applied to control and reduce swelling.
23. Rest the injured part by having the person stay off of it.
24. 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.

For Heart Attack/Stroke

4. Think FAST. Face: is there weakness on one side of the face? Arms: can they raise both arms? Speech: is their speech easily understood? Time: to call Emergency helpline
5. Immediately call medical/ambulance helpline or get someone else to do it

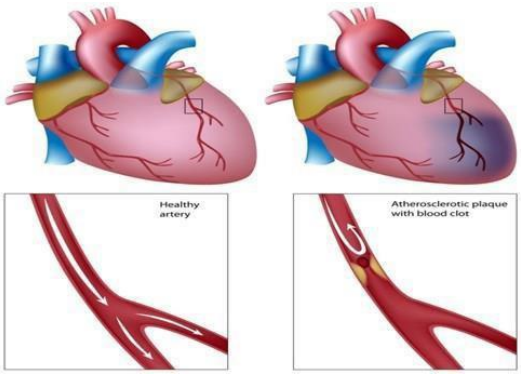


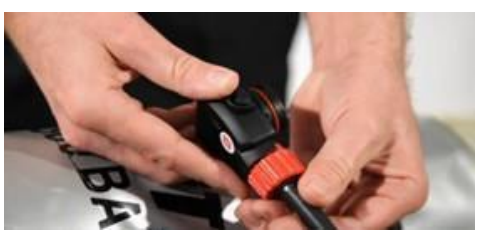
Fig 4.2.1e: Anatomy of Heart Attack

For Head Injury

6. Ask the victim to rest and apply a cold compress to the injury (e.g. ice bag)
7. If the victim becomes drowsy or vomits, call Medical helpline or get someone else to do it

Steps of using breathing apparatus:

Check the parts of the breathing apparatus thoroughly.



Check the bypass knob (red). Close it if you see it open. After this, press the reset button (area above bypass nob – black)

Inspect the facemask to see that it is undamaged.

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.

After wearing the breathing apparatus tighten shoulder straps and fasten the waist belt.

The cylinder valve should be opened slowly to inspect the pressure gauge.

Make sure that 80% of the cylinder is full.

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.

Breath in and normally to see if you can breathe normally or not.

Now insert a finger sidewise of the facemask for easy outward airflow.

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.

Normally Breathe to vent system
Listen for a whistle alarm while observing the pressure gauge
at 55 bar (+/-5 bar)

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.

Fig. 6.2.1f: 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.

Fig. 6.2.1g: 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 Specially Abled Persons

9. **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 to evacuation site if possible.
6. Use a sturdy chair, or a wheeled one, to move the person to an enclosed stairwell
7. Notify emergency crew of their location

4.2.2 Importance of Fire Safety Drills

Fire drills are indispensable in any workplace or public building for rehearsing what to do in the event of a fire. They are also a lawful obligation under the Fire Safety Order of 2005 and all workers in a company must partake. Here's how to get the most out of your fire practice.

Why have fire drills?

There are numerous reasons why fire drills are vital; first of all, fire drills are a chance to practice evacuation techniques to make sure all staff are acquainted with them. The staff will vacate the building quickly and therefore in a real life situation panic will be decreased, as everyone will know what they need to do. Fire drills are also beneficial for testing escape methods to assess their efficiency.

During fire drills, checks can also be carried out on alarm systems to make certain they are working properly and that emergency exits are passable. Overall fire drills help increase safety, so that you will be best equipped if a real fire does happen.

How often?

Ideally there should be two fire drills a year, although this may vary according to the workplace and after checking the firm's risk assessment. If there are people who work in shifts, suitable preparations should be made to ensure all staff partake in at least one fire drill per year and to educate them as to how to handle the situation.

Should you inform staff beforehand?

There are arguments for and against making people conscious of fire drills before they take place. Some people contend that not notifying staff gives an element of surprise, so that people take drills more sincerely. However, this can also have the reverse effect in a real fire, as on overhearing the alarm people may reason that it's only a drill.

The benefit of notifying all staff of fire drills in advance is that initially, they will not panic, which circumvents potential injuries that could be instigated in a rush to exit a building. Furthermore, if the alarm sounds, lacking a prior warning, there will be no uncertainty as to if it is a drill or not and people will act correctly. In public places such as shopping centres, it is prudent to make members of the public alert when a drill is about to happen.

UNIT 4.3: Importance of Safe Working Practices

Unit Objectives

At the end of this unit, you will be able to:

- Explain Basic Hygiene Practices
- Understand the importance of Social Distancing
- Demonstrate the safe working practices

4.3.1 Basic Hygiene Practices

We are living in an environment with millions of germs and viruses. And our body can be a breeding space for these microbial organisms. They grow and multiply and cause many diseases which sometimes can prove to be fatal for the human beings. These disease-causing microbial organisms kill over 17 million people every year. Some simple hacks and little changes of basic personal hygiene habits can bring amazing changes to all of us. We can prevent contracting these diseases if we follow these hygiene practices every day.

Personal Hygiene

Personal hygiene is all about managing your body hygiene, essentially caring for your well-being incorporating some physical hygiene habits. Also, there are mental health benefits as well, as they affect each other immensely.

What are good personal hygiene habits?

Good personal hygiene includes but not limited to-

- Take regular shower
- Maintain oral hygiene
- Wash your hands frequently
- Wash your genitals
- Keep your clothes and surrounding dry and clean

  These habits should be practiced on a regular basis, at home, at work, basically where you are!That's the whole idea of preventing your body system collapse over a tiny microbes

Personal Hygiene Practices at Home

Your home should be the most comfortable and convenient for you to keep up your personal hygiene level to a standard, yet, we find ourselves procrastinating over hygiene issues when we are at home. Even though some of these tasks barely take a minute.

1. Take Regular shower

Do not wait up to feel the dried sweat in your body to feel the urge to take shower, make it a routine, you have the choice to either take them before you head to work or after the long day or even before you head to sleep, whichever one suits your routine. Make sure to rinse your body thoroughly, especially the genitals and underarms as they produce more sweat and are more prone to fungal activities.

2. Wash your hands frequently

We use our hands to do our most physical acts, from picking up the keys, browsing through our phones, cooking or eating to attending our pets. While we agree and accept the importance of washing hands before eating and after visiting the toilet, it is also ***important to wash our hands*** with soap or sanitizer every now and then. The pandemic covid-19 which crippled the life all over the world has taught us an important lesson that sanitizing our hands regularly is the only way we can avoid transmission of the disease. Use ***alcohol based sanitizer*** to wash hands well to prevent the spread of communicable diseases

Click/Scan this QR code to access the video on Hand washing techniques

4.3.1 - 7 steps for Handwashing

3. Maintain oral hygiene practices

It is very important to take care of the teeth and gum, to prevent tooth decay and bad odour. Just brushing them twice a day is not enough, but using fluoride toothpaste and brushing properly is very essential. And wash it well with water to remove any food particles that is stuck in the gap in between the teeth. It is advised to wash the teeth everyday twice to maintain healthy teeth and gum.

- **Nails and hairs hygiene**

The cleanliness of nails and hair is also very important. They store dirt and grease. And even the microbes could be in there stuck and spreading. If the nail is not clean they can cause severe food poisoning, as we use our hands to eat food. Trim the nails once in a fortnight and wash hair at least twice a week with a shampoo to keep them healthy

- **Nose and ears hygiene**

Wherever we are most likely to breathe in some pollutants, and most of the particles are bound to be stuck in the nasal hair. So, rinse the nose and ear with warm water once you return from outside.

- **Wear fresh and clean clothes**

Changing into neat and clean clothes will prevent many infectious diseases. It will also give the mental effect immediately and it will boost the mind. Wash clothes with a good detergent every day and dry it in the sun. This will ward off any microbes attached to the clothes. If possible, Dettol can be used while rinsing which is an anti-disinfectant.

- **Food hygiene**

You can get severely sick from food-borne diseases, as most of your foods are raw, purchased from outside, they risk being cross-contaminated with harmful microbes. Food hygiene is basically the idea of better storage, handling, and preparation of food to prevent contamination and to prevent food poisoning.

4.3.2 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, feaces, saliva, skin (through touch) and using 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 spread it to others, the symptoms and 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 the 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.

As communities reopen and people are more often in public after the pandemic, the term "physical distancing" (instead of social distancing) is being used to reinforce the need to stay at least 6 feet from others, as well as wearing face masks. Historically, social distancing was also used interchangeably to indicate physical distancing which is defined below.

However, social distancing is a strategy distinct from the physical distancing behaviour.

What is self-quarantine?

Self quarantine was imposed on people who have been exposed to the new covid-19 and who are at risk for getting infected with the virus were recommended to practice ***self-quarantine***. Health experts advised the self- quarantine for 14 days or two weeks. Two weeks provides enough time for them to know whether or not they will become ill and be contagious to other people.

self-quarantine was also recommended for people who have recently returned from traveling to a part of the country or the world where COVID-19 was spreading rapidly, or if a person has knowingly been exposed to an infected person.

Self-quarantine involves:

- Using standard hygiene and washing hands frequently
- Not sharing things like towels and utensils
- Staying at home
- Not having visitors
- Staying at least 6 feet away from other people in your household

Once your quarantine period has ended, if the symptoms are not there, then the person may return to normal routine as per doctor's advice.

What is isolation?

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.

4.3.2 Complete
PPE Kit

Disposing off the PPE Kits

The PPE kits are worn by health workers and doctors who are attending to patients with highly infectious diseases and who are kept is isolation in order to arrest the spread. They have to wear it every time they go near the patient and have to remove it once their duty is over. Most of the PPE components are used for single use, however the face mask and goggles can be reused provided they are sanitised properly. The PPE kits have to be disposed off safely as they might have contaminants stuck to them and they may infect the healthy person if they are not discarded properly. The health workers may be all the more vulnerable to contact the disease.

4.3.3 Safe Workplace Practices

Every company has the provision of 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 are:

Supplies and Accessories in the First Aid Box

Splint

Elastic wraps

Latex gloves

Adhesive tape

Wound cleaning agent

Blanket

Scissors

Tweezers

Triangular bandages

Gauze roller bandage

Adhesive bandages

Gauze pads

Antiseptic cleansing wipes

Burn cream or gel

Eyewash liquid

CPR Kit

Chemical hazards are 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)

Now, where there are 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 Poison control unit gives 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

Click/Scan this QR code to view the video on CPR techniques

Fig. 4.3.3: CPR

- In case the victim's breathing has stopped, give CPR (Cardiopulmonary resuscitation)
- 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.

Exercise

- Burnt area should be kept under _____ for a minimum of 10 minutes
- _____exits should be easily accessible in case of fire.
- _____or _____must be applied to the wound to reduce the risk of infection
- The RICE which is_____,_____,_____ and _____therapy must be applied to control and reduce swelling.

UNIT 4.4: Reporting Safety Hazards

Unit Objectives

At the end of this unit, you will be able to:

- Discuss the process of reporting in case of emergency (safety hazards)
- Understand methods of reporting hazards

4.4.1 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 same.

The general highlights of the Organizational Reporting Protocol, commonly known as the 6Cs, are:

- **Communicate First**
  - The first source of information during 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:

While identifying and reporting a hazard / potential threat / potential risk, one must describe the following:

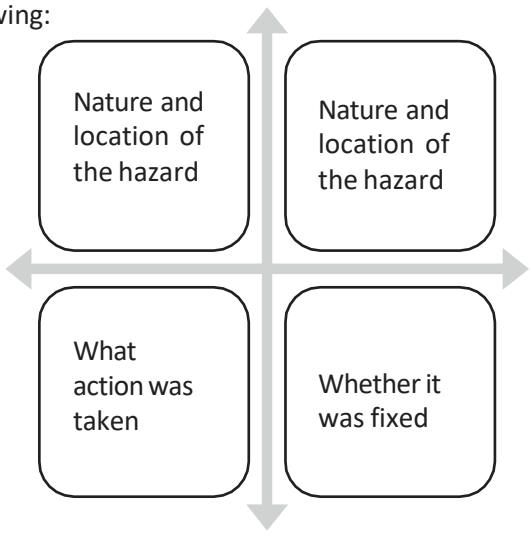


Fig. 4.4.1a: Describing hazard matrix

Part A: To be completed by the Worker Details Required:

2. Name of Worker
3. Designation
4. Date of filling up the form
5. Time of incident / accident
6. Supervisor / Manager Name
7. Work Location / Address
8. Description of the hazard / what happened (Includes area, task, equipment, tools and people involved)
9. Possible solutions to prevent recurrence (Suggestions)

Part B: To be completed by the Supervisor /

Manager Details Required:

10. 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:

11. Actions taken / Measures adopted (Identify and devise actions to prevent further injury, illness and casualty)

Action	Responsibility	Completion 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 are caused by the following:

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:

Fig 4.4.5: Sample form of reporting hazards

UNIT 4.5: Waste Management

Unit Objectives

At the end of this unit, you will be able to:

5. Understand what is e-waste
6. Understand the concept of waste management
7. Explain the process of recycling of e-waste

4.5.1 Introduction to 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 on the technological features of electronic products is forcing consumers to discard their old electronic products very quickly, which, in turn, adds to 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.

Click/Scan this QR code to view the video on e-waste Management

4.5.2 What is E-Waste?

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 off 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.

4.5.3 Electronic goods/gadgets are classified under three major heads:

White goods: Household appliances,

Brown goods: TVs, camcorders, cameras etc.,

The complete process is carried out as per the government guidelines.

4.5.4 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

4.5.4 E-waste Management Process (contd.)

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

4.5.5 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 material, like paper, corrugated cardboard (OCC), glass, plastics 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 favorable influence on the world where we live.

Recycling will greatly help us to save both the environment and us from pollution. If we take immediate action, we can control this, as the quantity of waste we are accumulating is increasing all the time.

4.5.6 Colour codes of waste collecting bins

Waste collecting bins colour code

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 is the plastic waste, 0.17 million tonnes is the biomedical waste, 7.90 million tonnes is 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 of 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 color bin system was suggested. Green bin for wet waste and blue for dry waste. However, there is a drawback in that system. People do through the sanitary napkins and children's diaper along with wet waste causing the contamination of things. Hence the government has come up with three colored garbage collection bins.

4.5.6 Tricolored Bins

1. **Green Bin**

The green coloured bin is used to dump biodegradable waste. This bin could be used to dispose off 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.

2. **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/thermocol (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.

4.5.7 Waste disposal methods:

6. Incineration: Combusting waste in a controlled manner to minimize incombustible matter like waste gas and ash.
7. Waste Compaction: Waste materials are compacted in blocks and are further sent away for recycling.
8. Landfill: Waste that can't be recycled or reused can be thinly spread out in the low-lying areas of the city.
9. Composting: Decay of organic material over time by microorganisms.
10. Biogas Generation: With the help of fungi, bacteria, and microbes, biodegradable waste is converted to biogas in bio-degradation plants.
11. Vermicomposting: Transforming the organic waste into nutrient-rich manure by degradation through worms.

4.5.8 Sources of Waste

8. **Construction waste** – waste coming from construction or demolition of buildings.
9. **Commercial waste**- waste from commercial enterprises
10. **Household waste**- garbage from households is either organic or inorganic
11. **Medical or clinical waste** -wastes from the medical facilities- like used needles and syringes, surgical wastes, blood, wound dressing
12. **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.
13. **Industrial waste**-The waste from manufacturing and processing industries like cement plants, chemical plants, textile, and power plants
14. **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
15. **Mining waste**- chemical gases emitted in mine blasting pollutes the environment. And the mining activity greatly alters the environment and nature.
16. **Chemical waste**-waste from the chemical substance is called chemical waste.
17. **Radioactive waste**: radioactive waste includes nuclear reactors, extraction of radioactive materials, and atomic explosions.

4.5.9 Sources of Pollution

All these above-mentioned waste 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 .

4.5.10 Types of Pollution

Types of Pollution	Detail/Pollutants involved
Air pollution	11. Solid particles and gases mixed in the air cause air pollution 12. Pollutants: emissions from the car, factories emitting chemical dust, and pollen
Water pollution	1. 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 unfit for consumption. 2. Pollutants that contaminate the water are discharges of untreated sewage, and chemical contaminants, release of waste and contaminants into 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.

UNIT 4.6: Organizations' focus on the Greening of jobs

Unit Objectives

At the end of this unit, you will be able to:

- Understand the concept of ESG
- Explain the different factors of ESG

4.6.1 What is 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 hat 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.

4.6.2 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 are critical.

The factors are divided into three categories; environmental, social, and governance. Knowing about these factors come a long way in designing the effective ESG policy.

Environmental

Environmental factors relate to a business's impact on the environment. Examples include:

5 Usage of renewable energy
6 Effective waste management
7 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:

8 diversity and inclusion
9 proper work conditions and labor standards
10 relationships with the community

Governance

Governance factors relate to the company policies for effectively running it. They include:

11 tax strategies
12 structure of the company
13 relationship with stakeholders
14 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.

Exercise

1. ESG stand for _____, _____, _____.
2. Governance factors include _____, _____, _____, _____.
3. The three causes of air pollution _____, _____ and _____.
4. Mining waste includes_____.
5. Landfill is a _____.
6. _____,_____ and _____ coloured bins are used for disposing the waste.
7. The plastics cans are trashed in _____coloured bin.
8. _____,_____and _____ are considered as e-Waste
9. _____ part of e-waste is recycled and used again
10. **E-waste is made up of hazardous substances like _____,_____,_____ and _____**

Skill India
कौशल भारत - कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

Telecom
Sector
Skill
Council

5. Communication and Interpersonal Skills

Unit 5.1 – Interaction with supervisors, peers, customers and differently abled persons.

Unit 5.2: Explain the importance of developing sensitivity towards disabled persons

TEL/9102

Key Learning Outcomes

At the end of this module, you would be able to

- Understand what is communication and the importance of communication in the workplace
- Understand effective communication and communicate effectively for success
- Discuss types of communication -verbal and non-verbal
- Communicate at workplace
- Communicate effectively with superiors
- Communicate effectively with colleagues and customers using different modes viz face-to face, telephonic and email communication
- Understand the hurdles for effective communication
- Conduct professionally at work place
- Respect differences in gender and ability
- Communicate effectively with person with disabilities
- Respect for disable people

UNIT 5.1: Interaction with supervisor, peers and customers

Unit Objectives

At the end of this unit, you will be able to:

- Understand the importance of communication
- Understand types of communication

5.1.1 Why is Communication Important?

- Communication Skills are more important than ever, for all fields of endeavor.
- Whatever the role a person is holding in the organization, having a firm grasp of effective communication will undoubtedly be a key role in the individual's as well as the organization's success
- Oftentimes, people with excellent technical skills don't get promoted to higher roles because of their inability to communicate effectively
- Hence one fundamental skill everybody should be proficient along with the technical skill is ***Communication Skills***
- Effective communication helps us to build rapport with the customer both internal and external and help us *resolve issues* and *conflicts* easily and quickly.

5.1.2 What is Communication?

1. Communication is the process of sending and receiving information among people.
2. It is imparting or exchanging of information by speaking, writing, or using some other medium
3. The purpose of communication is to convey your thoughts and opinions to others.
4. Communication is said to be successful only when both the sender and the receiver perceive it in the same way.
5. In your personal and professional life, you would be communicating with the following people-
    - Colleagues
    - Customers
    - Friends
    - Parents
    - Relatives

5.1.3 Effective Communication

Effective communication is the process of delivering messages to a target audience in a way that guarantees satisfactory reception and understanding. If the communication is effective, both the sender and the receiver will share the same information at the end of the process. Effective communication is about more than just exchanging information. It's about understanding the emotion and intentions behind the information

5.1.4 Effective Communication for Success

Effective Communication is critical to a business's success. From top to bottom, among colleagues, from subordinates to superiors, and from the organization to the outside, several messages are delivered daily. All the people must communicate these messages properly. Content, language, remarks, tone of voice, and non-verbal communication are elements that affect the effectiveness of messages

Clear and effective communication will

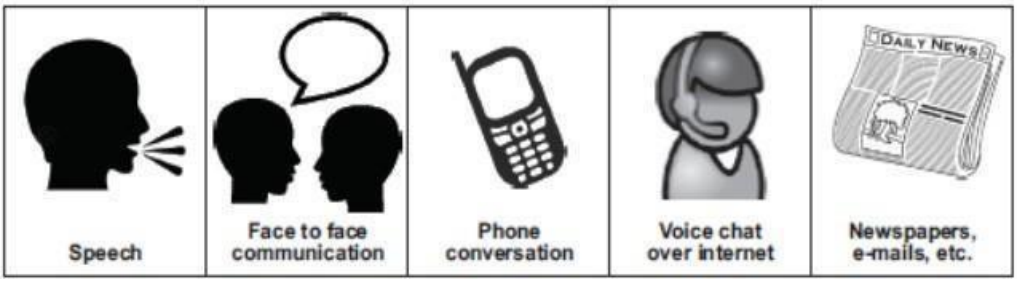
- Increase customer satisfaction
- Bring more business to the company
- Increase productivity among team members

5.1.5 Types of Communication

Communication has been divided into two types:-

1. Verbal Communication
2. Non-Verbal Communication

Verbal communication takes place when people exchange words with each other, either spoken or written. It includes the **choice and use of words and language to convey a message**. Examples of verbal communication are face-to-face conversation, telephonic conversation, and a speech or presentation.



Click/Scan this QR code to access the video on Types of Communication

Speech has certain characteristics which will affect the message that is being spoken:

4 Volume – loud speech may sound bossy, very quiet speech cannot be heard.

5 Tone – use warm tones without sounding over-friendly. Cool tones are very unwelcoming.

6 Pace – fast speech is not easy to follow. Speak at a reasonable pace so that the other person has a chance to understand.

Correct body language also plays an important role in effective communication. For example, a warm smile accompanying 'Have a nice day' or looking directly at the person who is being spoken to give a positive image of the organisation.

Non –Verbal Communication

Non-verbal communication includes the overall body language of a person. There are two kinds of non-verbal communication:

Signs and symbols: for example pictures, or notices, or signboards, or even photographs, sketches and paintings. Here are some examples of different signs and symbols:

Gestures and expressions: hand signs, facial expressions, body postures or body language that can help to convey a message. You can learn to communicate better with others if you learn to recognise some of these.

Facial expressions - A smile or a frown

Gestures - movements of hands and body to help explain or emphasize the verbal message **Body posture -** how we stand or sit. Maintain a good posture. When you are talking to a colleague or guest, remember to stand up straight, look professional and be positive. Do not slouch, lean against something or fidget with equipment or your hands.

Orientation - whether we face the other person or turn away

Eye contact - whether we look at the other person and for how long

Proximity - the distance we are from a person

Head nods - for encouragement, indication of agreement or disagreement

Appearance - dress and grooming

Non-verbal aspects of speech - tone and pitch of voice

These non-verbal clues are important as they can be used to improve the quality of communication. They can be used to reinforce any verbal communication; for example, leaning forward and looking at the person you are speaking to and smiling naturally. Your expressions, posture and appearance must be appropriate and should tell the guest that you are professional, competent and willing to help.

5.1.6 Communication at workplace

In every situation, while interacting with people, we make use of both verbal and Non-Verbal Communication. It is the key to the success of any organization. Be it communication with customers, supervisors, or peers. In today's scenario having technical skills alone is not enough to get the work done, but communication skill is also equally important. Completing the task must require the support of the whole team, and without proper communication, it cannot happen. Effective Communication helps managers to perform their jobs and responsibilities and it serves as a foundation for planning.

5.1.7 Communication with supervisors

Effective and open communication within a team will build a common purpose among team members that will allow them to reach their goals. Team leaders know that group communication enhances organizational efficiency. The team members should always follow the communication guidelines. Some of the points to remember while interacting with supervisors:

1. Be aware of the communication guidelines of the organization.
2. Understand and interpret clearly, the work requirements from the supervisor.
3. Keep the supervisor informed about the progress of the task assigned.
4. Participate in all the discussions which call for decision-making, and provide facts and figures
5. Give/ accept suggestions during the discussions.
6. Accept the feedback positively and work towards rectifying errors if any. Make sure the same mistakes are not repeated.

5.1.8 Communication with colleagues & customers

- The main responsibility of a Customer Care Executive is to handle customers' concerns.
- Interaction with colleagues/peers is also equally essential and it enhances productivity in the workplace.
- Be polite in speaking to your peers at the office.
- Value other people's time as much as you value your own.
- Before you begin discussing something, ask your coworker if it is the right time to talk, and give a true picture of how much time you expect to take. Always start the conversation
- Communication with colleagues/customers can be through face-to-face, telephonic, or email.
- Keeping a few points in mind while communicating will make the interaction pleasant

Click/Scan this QR code to view the video on communication with customers and colleagues

5.1.9 Face-to-face Communication

This is an important medium of oral communication, wherein two or more persons talk to each other and see each other physically. This form of communication is direct or straight. Things to remember while you are communicating face to face

- Adjust the tone of voice, don't be too loud
- Make eye contact
- Use appropriate language
- Maintain adequate distance
- Acknowledge, nod during interaction
- Use appropriate non-verbal gestures to communicate with persons with disabilities

Benefits of face-to-face communication

- Instant feedback
- Information conveyed clearly
- Build rapport

5.1.10 Telephonic Communication

Another widely adopted mode of communication is through the telephone. This is the person- to-person conversation where nobody sees others but hears each other and interacts instantly. Nowadays mobile phones are becoming more popular along with landlines as a mechanical media of oral communication.

The following suggestions are recommended to follow while making telephone calls-

- Make the call at the appropriate time
- Provide details about your identity like name, company, department, etc.
- Discuss the purpose of the call
- Think about the tone of your voice
- Listen carefully
- Speak clearly
- If you don't understand something, ask
- Use please, thank you, sorry wherever necessary
- Follow the organization's policies and procedures while interacting on the telephone.

Click/Scan this QR code to view the video on Effective Telephone Communicaiton

5.1.11 Email Communication

Email or Electronic mail is a method of exchanging messages using electronic media. The official or business communication between colleagues or inter-department communication usually happens through email. The advantage of email is you can send communication to many people at the same time.

Points to remember in email communication

- Be clear and concise
- Keep the content short and to the point
- Avoid using jargon and short forms
- Re-read the message, before sending it for grammar and spelling mistakes
- The subject line should describe the main mail content
- Use readable font size (don't keep it too small)
- Add signature at the bottom of the mail body
- Check the attachments for viruses before sending

5.1.12 Importance of timely completion of tasks

Time is a major factor that evaluates **the success or failure of a project**. Even when the whole team has done a wonderful job and produced high-quality results, with half the cost allotted to the project, everything will be a waste if it was not delivered on time. Any deviation from the timeline will call for a penalty and sometimes may result in losing the project and eventually the customer. so adhering to the timeline is important when it comes to any organization who are into products and services.

Benefits of adhering to timelines:

- Increased and improved customer satisfaction
- Increased productivity and efficiency of the individual
- Team feels motivated
- Sense of adhering to the SLA's and Standard Operating Procedures
- Shows the commitment toward the work and the organization
- Good word of mouth from the customers

5.1.13 Standard Operating Procedure

A ***Standard Operating Procedure (SOP)*** is a standardized process that outlines a set of detailed instructions to help workers perform complex tasks properly and safely. The main objective of standard operating procedures is to develop an effective quality system and comply with industry-specific regulations and standards. Failure to follow SOPs can cause significant errors in operations and services.

For a mobile repairing center, the SOP defines the different process of operations, namely handling customer, repairs, sales and interaction among the staff within the repair center.

SOP also clearly defines the responsibility of each and every designated person in the organisation and what is expected from them. It further defines what the various levels of engineers will handle with respect to the handsets coming for repair.

The escalation matrix specifies how the different levels escalate the issue to the next level and adhere to the timelines for repair and communication to the customer.

SOP is created keeping in mind the customer satisfaction as a main motive.

Each and every person in the organisation is expected to read the SOP thoroughly and work accordingly. Because every customer when they go for purchasing a product, one of the main things they see is the post-sales Support. If they find the brands deliver good service support then they don't mind even spending few extra moneys.

5.1.14 Escalation Matrix

Escalation matrix is made up of several levels of contact based on the specific problem at hand. This is being followed by all who are working on that product and have to adhere to the service guidelines. And the problem has to be closed at a minimum turnaround time, and for any reason the repair is taking time proper reason has to be mentioned and notified to all the people concerned including the customer.

5.1.15 Escalation Mechanism

Customer service is a very important aspect of a typical service industry. Giving committed service to customers every time and on time is very crucial for the success of the brand. In recent times, customers do research on how the after-sales support of a product is, and based on that rating they will decide which brand to buy. If the customer service is not good, they will not go for that product even though the product is very good. Hence customer service is a second important aspect of a product and services organization.

For electrical home appliances, the customer logs a complaint and the service engineer is sent to the
site for looking into the problem and repairing.

For electronic devices like mobile phones and tablets, the customer is expected to take the product to their service center to get it checked and repaired.

The resolution time matters a lot, as mobile phones have become an indispensable device for people. Their business cannot function without that. Hence too much downtime is also not good. Once at the service center, the technicians at L1 level look for the problem and try to resolve it. If it's beyond their area of resolution the same is escalated to the next level. Every organization has ***Standard Operating Procedures*** clearly state the workflow for the repair of the smart phones. Every individual working there must be aware of the same and adhere to the deadline for faster service and enriched customer satisfaction.

5.1.16 Escalation through CRM

Customer Relationship Management is a software, through which most of these companies who are into customer service, manage their customers. The customer details are entered in the system and also the services which are logged against a particular customer. This is the automated system, which takes a particular action after a period of time. For example, if a service request is assigned to an engineer for rectifying a problem of a client, and if the engineer does not update the status of the service in the system within a specified period of time, the problem is automatically escalated to the next level for resolution. Then the new engineer who is responsible for resolving pick it and try to find a solution. This system helps to maintain a track of a particular problem and the current status which will help the organization in effectively managing the customer queries. The complete escalation route is mentioned in the SOP and the same is implemented through the CRM software. This eases the manual escalation procedure which is time consuming and slow.

5.1.17 Escalation issues at work

Whether an issue arises among team members or with customers, sometimes the severity of the circumstance requires an escalation to management. Understanding how to approach an escalation can help you better find a solution when conflicts arise. We explore what it means to escalate an issue in the workplace and provide tips for how to do so successfully.

What does it mean to escalate an issue at work?
Escalating an issue in the workplace is the process of bypassing those involved by contacting upper/senior management. It involves raising awareness of the context to the right people in order to resolve a challenging situation. Typically, escalation occurs when there is an issue that the current staff working on the problem can't resolve and requires assistance from those with more authority and resources

When should you escalate an issue at work?
Deciding when to escalate an issue depends on the amount of risk it can bring to the company. Because escalating an issue can lead to difficult meetings and cause disruptions in work, you should reserve them for issues that truly require escalation. You can often avoid escalating an issue by solving the problem with the individual first.
However, some issues require support from those with higher authority. Consider escalating an issue at work when:

- You have already tried other strategies but that did not work.
- Resolving may incur additional cost to the company or the customer, while rectifying the
  problem.
- Because of the non-availability of certain parts the repair work is taking longer than usual.
- The engineer broke another part while repairing a part. So escalation is required to get the approval to replace the broken part by the company.

5.1.18 Hurdles for Effective Communication

Following are factors contribute to communication not being effective.

Stress and out-of-control emotion. When you are stressed or emotionally disturbed, you're more likely to misread other people and send confusing non-verbal signals. Calm down before continuing the conversation.

Lack of focus. You can't communicate effectively when you're multitasking. If you're checking your phone, planning what you're going to say next, or daydreaming, you're almost certain to miss nonverbal cues in the conversation. To communicate effectively, you need to avoid distractions and stay focused.

Inconsistent body language. Nonverbal communication should support what is being said, not contradict it. If you say one thing, but your body language says something else, your listener will likely feel that you're being dishonest. For example, you can't say "yes" while shaking your head no.

Negative body language. If you disagree with or dislike what's being said, you might use negative body language to ignore the other person's message, such as crossing your arms, avoiding eye contact, or tapping your feet. You don't have to agree with, or even like what's being said, but to communicate effectively and not put the other person on the defensive, it's important to avoid sending negative signals.

Unit 5.2: Explain the importance of developing sensitivity towards disabled persons

Unit Objectives

At the end of the unit, you will be able to

- Respect differences in genderand ability
- Communicateeffectively with person with disabilities
- Respectpeople with disability at work

5.2.1 Communication with Disabled Person

A **disability** is any condition that makes it more difficult for a person to do certain tasks or interact with the people around them (socially or materially). These conditions, or defects, may be cognitive, developmental, intellectual, mental, physical, sensory, or a combination of multiple conditions. Defects may be present from birth or can be acquired during a person's lifetime. Often, disabled people are excluded from full participation in any activity." But things are changing; every organization has allotted some percentage of employees from this section of the society. They are also allowed to exhibit their skills in a few jobs which they can perform without putting their life at risk

General tips for communication with disabled people

1. Speak to them as you would speak to anyone else in a soft and low tone.
2. Respect the person first, not their disability. For example, use the term 'a person with disability' rather than 'a disabled person'.
3. Do not use phrases such as 'suffers from' and 'crippled' rather the phrase should be 'people who use a wheelchair' rather than 'wheelchair bound.
4. Don't drag or push a person's wheelchair, and don't move their crutches or walking stick without their permission. It has to be in their personal space.
5. When talking to a person who is in a wheelchair, try to sit in such a way you could reach their eye level. This would not strain them much, to lift their head and talk.

5.2.2 Communicating with people with a hearing impairment

Keep these points in mind while interacting with people with a hearing problem

- Draw the person's attention before you speak. Give a gentle tap on their shoulder, a wave of some other visual signal to the person's attention
- Stand in front of the person and maintain eye contact
- Don't cover the mouth while talking. They can figure out what is being said by just looking at the lip movement
- Speak at a normal pace don't speak fast or slow
- Choose the words wisely
- Use short sentence

5.2.3 Respect people with disability

Learn the proper way to act and speak around someone with a disability.

1. Do not use offensive or derogatory words like 'handicapped', 'crippled', and retarded etc.
2. Don't criticize or blame them. Don't shout at them or use abusive language
3. Talk slowly with a low tone. Pause while talking
4. Avoid excessive whispering, joking and laughing unnecessarily
5. Assuming things about them or their situation.
6. Don't make jokes about their condition or be sarcastic
7. Don't look down upon them because of their disability
8. Appreciate them for their efforts and work, and motivate them to perform better

5.2.4 Safety at workplace for people with disability

Disabilities of all types affect employees and can pose various mental or physical challenges. In many situations, a disability may impact the amount of time it takes for an employee to complete a task or get from one part of a facility to another. Some disabilities may be known while others remain unknown to an employer.

Health and safety legislation should not prevent disabled people from finding or staying in employment so it should not be used as an excuse to justify discrimination against them.

Disabled people and those with health conditions, including mental health conditions, should be given the opportunity to both get into and stay in work.

Responsibilities of an employer towards disabled people

The employer is responsible for the health, safety and welfare of all of their employees, whether they have a disability or not.

Disability is not always obvious so one might not realise a worker is disabled or they might choose not to tell you, particularly if their disability has no impact on their ability to do their job.

Workers do not have to tell anybody unless they have a disability that could foreseeably affect the safety of themselves or anyone else connected to their work. If they do not reveal and there are no obvious indicators of any disability, then the organization are not under any obligation to make workplace adjustments.

Periodically, consult with the employees (whether directly or through their representatives) on issues relating to health and safety. These discussions reflect good safety practice because employees have day-to-day understanding of the job, so they are likely to have good ideas on keeping themselves and others safe.

5.2.5 Workplace adaptations for people with disability

Few changes in the workplace to make it a safe place for the disable people will go a long way in the employee satisfaction for an organisation.

Workplace Adaptations

Workplace should be easily accessible for these people with special needs. One major compliance concern deals with accessibility. For example, if workplaces have been adjusted or created more accessible entrances and exits to their facilities, allowing more independence for persons in wheelchairs, would be a great idea. Other subtle changes may include the width of bathroom stalls, hand rails inside the stalls and long ramps instead of stairs. The path of travel that employees take should never be obstructed; there should be no barriers to prevent someone from getting to safety in an emergency.

Workstations easily can be adapted to follow this universal design. Many companies now use slide- out keyboard trays and monitors on swinging arms to allow employees to adjust to their needs.
Desks can accommodate wheelchairs in place of regular chairs, and general work spaces can be lowered to allow easier access. The main goal is to remove all barriers and allow everyone to concentrate more on completing their tasks.

The biggest challenge with universal design is accommodating the multitude of challenges that different disabilities present. Not all disabilities are the same, and not all will present the same challenges for employees. Some employees may have issues with their right hand while others have issues with their left. For some, it may involve not being able to stand or sit. Some may need low lighting, while others need bright lighting. Designing a facility to accommodate all is always going to be a challenge.

Complying with government guidelines can be more difficult in regards to employees with disabilities. This difficulty lies with ensuring that employees are aware of all hazards in the workplace. Multiple disabilities will create multiple reasons that may keep employees from recognizing hazards. Employees with impaired vision, for example, must have other means of identifying hazards. This may be remedied with audible alarms or touch-activated devices that warn employees not to go in an area. Other employees may have difficulties reading and may benefit from shapes or colors to further identify hazardous areas. For workers who lack hearing ability, employers can utilize signs to demonstrate hazards or use flashing strobes to identify when employees need to evacuate an area and head to safety.

Every organization has to make few adaptations in order to make it a better place to work even for people with disabilities. It should provide an environment where they feel they are safe and can carry out their work rather than worrying about their safety.

Exercise

1. What are the three points you will focus on when you talk to people face to face?

_____

_____

_____

Fill in the blanks

1. Before sending the mail it's important to check the _____and _____of the content.

2. When you interact through phone, provide your identity details like _____,_____ and _____

3. Add your _____at the bottom of your mail.

4. The Customer Care Executive is mainly responsible for handling _____.

Notes

Annexure

Chapter No	Unit No	Topic Name	Page No	QR Code
1	1.1	Applications of Internet of Things	11	Click the QR code to view the video the concept of IoT
2	1.1	Applications of Internet of Things	13	Click the QR code to view the video on working of IoT
3	1.1	Applications of Internet of Things	13	Click the QR code to view the video on smart parking using IoT
4	2.11	Understanding Edge Devices	51	Click the QR code to view the video on edge devices
5	**2.3**	IoT Cloud Framework	92	Click the QR code to view the video on data management

Annexure(contd.)

Chapter No	Unit No	Topic Name	Page No	QR Code
5	4.3	Importance of safe working practices(First Aid Techniques)	329	Click/Scan this QR code to view the video for First Aid at work place
6	4.3	Importance of safe working practices	338	Click/Scan this QR code to view the video on Hand Washing techniques
7	4.3	Importance of safe working practices	345	Click/Scan this QR code to view the video on CPR Techniques
8	4.5	Waste Management	349	Click/Scan this QR code to view the video on Waste Management
9	5.1	Types of Communication	363	Click/Scan this QR code to view the video on Types of Communication
10	5.1	Types of Communication	366	Click/Scan this QR code to view the video communication with Customer and colleagues
11	5.1	Types of Communication	**368**	Click/Scan this QR code to view the video on Effective Telephone Communication

Chapter No	Topic Name	QR Code
12	Employability Skill	Click/Scan the QR code to access e-Book onEmployability Skills

Skill India
कौशल भारत - कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
National
Skill Development
Corporation
Transforming the skill landscape

Click/Scan this QR code to access e-Book

Telecom
Sector
Skill
Council

Address: Estel House, 3rd Floor, Plot No:-126 Sector 44,
Gurugram, Haryana 122003
Email : tssc@tsscindia.com Web : www.tsscindia.com
Phone : 0124-22222222

₹