NCVET
कौशल गुणवत्ता प्रगति

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
RE IMAGINE FUTURE

Telecom Sector Skill Council

Participant Handbook

Sector
Telecom

Sub-Sector
Network Managed Services

Occupation
Network Operation and Maintenance

Reference ID: **TEL/Q6210,** Version **5.0**
NSQF Level **4**

Telecom Technician-IoT Devices/Systems

This book is sponsored by
Telecom Sector Skill Council
Estel House, 3rd Floor, Plot No: - 126, Sector-44
Gurgaon, Haryana 122003
Phone: 0124-2222222
Email: tssc@tsscindia.com Website:
www.tsscindia.com

Disclaimer

The information contained herein has been obtained from sources reliable to Telecom Sector Skill Council. Telecom Sector Skill Council disclaims all warranties to the accuracy, completeness or adequacy of such information. Telecom Sector Skill Council 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 shall be responsible for any loss whatsoever, sustained by any person who relies on this material. The material in this publication is copyrighted. No parts of this publication may be reproduced, stored or distributed in any form or by any means either on paper or electronic media, unless authorized by the Telecom Sector Skill Council.

> 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 SKILL COUNCIL

for

SKILLING CONTENT : PARTICIPANT HANDBOOK

Complying to National Occupational Standards of

Job Role/ Qualification Pack: **"Telecom Technician - IoT Devices/Systems "** QP No. **"TEL/Q6210, NSQF Level 4.0"**

Date of Issuance: 8th May 2025

Valid up to*: 30th April 2028

**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 Sector Skill Council)

Acknowledgements

Telecom Sector Skill Council (TSSC) 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 has 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. TEL/N6234: Install and configure IoT devices at customer premises
2. TEL/N6236: Perform level 1 troubleshooting of IoT devices
3. TEL/N9105: Follow sustainable practices in telecom infrastructure installation
4. DGT/VSQ/N0101: Employability Skills (30 Hours)

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


Notes


Practical

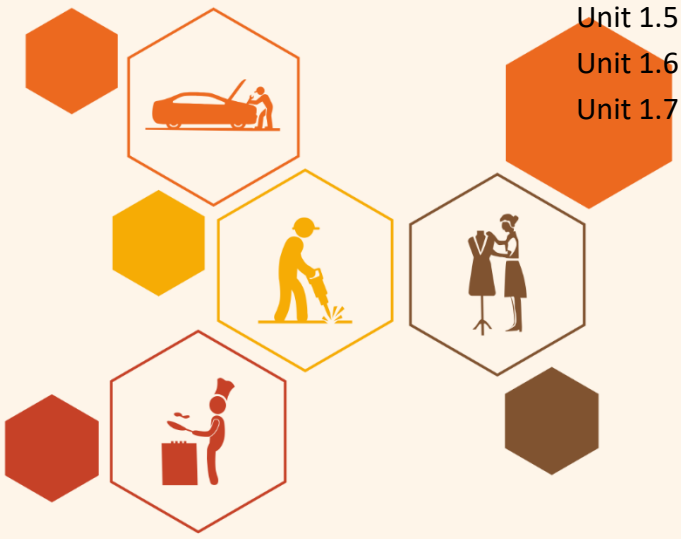

Unit Objectives

Table of Contents

Table of Contents

1. Introduction to the Sector and the Job Role of a Telecom Technician-IoT Devices/Systems

Telecom Sector Skill Council



TEL/N6234

Key Learning Outcomes

By the end of this module, the participants will be able to:

1. Explain the importance of Telecom Sector.
2. Discuss the roles and responsibilities of a Telecom Technician - IoT Devices/Systems.

UNIT 1.1: Introduction to Telecom Sector and Role of a Telecom Technician - IoT Devices/Systems

Unit Objectives

By the end of this unit, the participants will be able to:

1. Explain the significance of the telecom sector in the manufacturing and assembly of IoT devices and systems.
2. Elucidate the key skills and technical expertise required for a Telecom Technician specializing in IoT devices and systems.
3. Describe the challenges faced in assembling and testing IoT devices and systems in the telecom sector.
4. Determine the impact of precision and quality control in the assembly of IoT devices and systems for telecom applications.
5. Discuss the roles and responsibilities of a Telecom Technician in ensuring efficient and high-quality prodsuction of IoT devices and systems.
6. Discuss the applications of IoT in smart cities, healthcare, Industry 4.0, and agriculture.

1.1.1 Introduction to Telecom Industry

The Indian telecom industry has been one of the fastest-growing sectors in the country, striving to tap almost every potential customer with its services. Today, owning a mobile device is a basic necessity, and the demand for seamless connectivity continues to rise.

With the rapid expansion of the Information Technology (IT) sector, the telecom industry in India has experienced a major boom, leading to continuous market growth. Since the Indian population has become highly dependent on telecom services—and with several companies operating both in India and overseas—the sector often faces challenges in maintaining smooth operations amidst growing customer expectations. This study aims to provide insights into the current telecom sector and the measures being taken to enhance customer relationships.

Post-1991 liberalisation, privatisation, and globalisation, the Indian telecom market has become highly competitive, with multiple players operating simultaneously. In such an environment, companies are keen to understand customer perceptions of mobile services to refine their strategies and capture market share.

India remains the world's second-largest telecommunications market. As of March 2025, the total telephone subscriber base stood at around 1,200 million, with an overall tele-density of 85%. The internet subscriber base reached approximately 944 million, while broadband subscriptions grew to over 935 million wireless and about 45 million wired users by mid-2025.

- **Sector growth and infrastructure expansion:** Telecom infrastructure continues to expand rapidly, with the number of towers and mobile base transceiver stations (BTS) steadily increasing. This expansion has helped improve connectivity and service quality, especially in urban regions, though rural areas still face gaps.
- **Policy targets and initiatives:** The Government has launched the National Broadband Mission 2.0 (2025–30), aiming to provide optical fibre connectivity to all Gram Panchayats and key institutions, with at least 95% uptime, and to raise average fixed broadband speeds to 100 Mbps by 2030. In parallel, the Draft National Telecom Policy 2025 sets ambitious goals such as achieving 100% 4G coverage, 90% 5G coverage, 80% tower fibreisation, broadband access to 100 million households, and the rollout of 1 million public Wi-Fi hotspots by 2030.

Fig. 1.1.1: Telecom Industry

Subscriber trends and market dynamics:

By May 2025, India's total telecom subscriber base reached about 1,207 million. Reliance Jio and Bharti Airtel together accounted for nearly all new subscriber additions, while Vodafone Idea and BSNL continued to lose market share. By June 2025, the total wireless subscriber base stood at approximately 1,171 million, driven largely by urban growth, though rural subscriptions showed a slight decline.

1.1.2 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:

Fig. 1.1.2 Wireless interconnection of devices via Internet

1.1.3 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. 1.1.3 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:

Fig. 1.1.4 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:

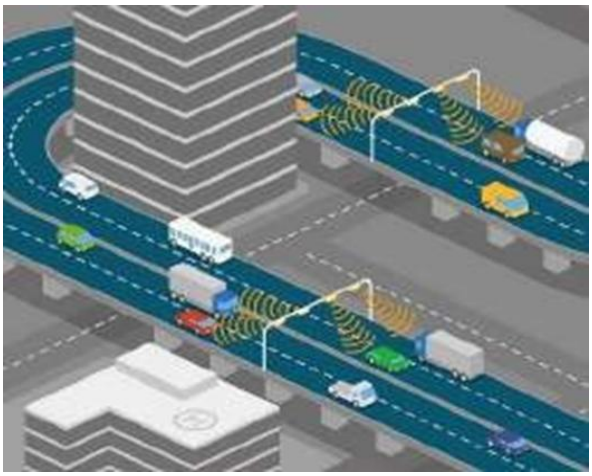


Fig. 1.1.5 Wireless connectivity for managing and controlling traffic

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. 1.1.6 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. 1.1.7 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. 1.1.8 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. 1.1.9 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. 1.1.10 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. 1.1.11 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.

1.1.4 Significance of the Telecom Sector in the Manufacturing and Assembly of IoT Devices and Systems

The Telecommunication (Telecom) sector plays a pivotal role in the development, manufacturing, and deployment of Internet of Things (IoT) devices and systems. IoT relies on seamless connectivity, data transmission, and communication protocols, all of which are enabled and standardized by the telecom industry. Without robust telecom infrastructure and sectoral innovations, IoT devices would lack the essential backbone for interoperability, scalability, and global deployment.

1. Role of Telecom Sector in IoT Ecosystem

a. Connectivity Backbone

- IoT devices require constant connectivity for data collection, transmission, and real-time monitoring.
- Telecom operators provide 2G/3G/4G/5G, Narrowband IoT (NB-IoT), LTE-M, and satellite communication services that form the backbone of IoT systems.
- These networks enable communication across diverse IoT applications such as smart homes, industrial automation, healthcare monitoring, and autonomous vehicles.

b. Standardization and Protocols

- The telecom sector ensures global standardization of communication protocols (e.g., 5G NR, NB-IoT, LoRaWAN, LTE Cat-M1).
- This facilitates interoperability among IoT devices manufactured by different vendors.
- Standards reduce production costs, accelerate innovation, and ensure reliability in IoT deployments.

c. Spectrum Allocation and Regulation

- Telecom authorities allocate and regulate radio frequency spectrum essential for IoT device communication.
- Manufacturing and assembly of IoT systems must comply with telecom regulations to ensure non-interference, safety, and cross-border operability.

2. Impact on Manufacturing and Assembly of IoT Devices

a. Design Considerations

- IoT device design is influenced by telecom-enabled factors such as:
  - Chipset integration for LTE, 5G, or NB-IoT compatibility.
  - Low-power modules for extended battery life in remote sensors.
  - Antenna design for optimal connectivity in diverse environments.
- Manufacturers must collaborate with telecom providers to ensure devices are network-ready.

b. Component Integration

- Telecom advancements drive demand for modems, communication modules, and SIM/eSIM technologies in IoT devices.
- The assembly process requires precise integration of these components to achieve seamless network connectivity.
- Example: Smart meters or industrial sensors use NB-IoT modules embedded during assembly.

c. Production Scalability

- With global telecom networks enabling billions of connections, manufacturers must design IoT devices for mass production and large-scale deployment.
- Telecom-enabled Over-the-Air (OTA) updates influence assembly by requiring devices to support upgradable firmware.

Quality Assurance and Testing

- Telecom sector standards necessitate rigorous network compliance testing during manufacturing.
- Devices undergo validation for latency, throughput, signal strength, roaming capability, and security compliance.
- Collaboration with telecom testing labs ensures devices are market-ready.

3. Sectoral Influence on IoT Growth

a. Industrial IoT (IIoT)

- Telecom-enabled 5G ultra-reliable low-latency communication (URLLC) supports automation, robotics, and predictive maintenance in manufacturing plants.
- IoT assembly lines increasingly adopt real-time telecom-enabled monitoring systems to optimize production.

b. Smart Cities and Infrastructure

- IoT devices for traffic management, waste monitoring, and energy grids depend on telecom operators for connectivity.
- Manufacturers align device specifications with telecom infrastructure in target regions.

c. Consumer Electronics

- Smart home devices (CCTV, smart speakers, wearables) require Wi-Fi, 4G/5G, or Bluetooth integration, shaped by telecom technologies.
- Assembly processes must ensure compatibility with telecom-driven ecosystems such as 5G-enabled smart homes.

d. Global Supply Chain Integration

- Telecom networks enable real-time logistics monitoring using IoT trackers.
- In manufacturing and assembly units, telecom-powered IoT solutions ensure supply chain visibility and quality control.

4. Future Significance

- 5G and Beyond: Ultra-fast 5G and upcoming 6G technologies will enable high-bandwidth, low-latency IoT applications like autonomous vehicles and smart factories.
- Edge Computing & Telecom Synergy: Integration of edge computing with telecom networks will influence device architecture, requiring new designs and assembly methods.
- Sustainability in Manufacturing: Telecom-enabled IoT will optimize energy efficiency, predictive maintenance, and waste reduction in assembly plants.
- Security and Compliance: Telecom operators will drive cybersecurity frameworks for IoT devices, requiring manufacturers to incorporate advanced encryption modules.

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. 1.1.11 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.

1.1.4 Significance of the Telecom Sector in the Manufacturing and Assembly of IoT Devices and Systems

The Telecommunication (Telecom) sector plays a pivotal role in the development, manufacturing, and deployment of Internet of Things (IoT) devices and systems. IoT relies on seamless connectivity, data transmission, and communication protocols, all of which are enabled and standardized by the telecom industry. Without robust telecom infrastructure and sectoral innovations, IoT devices would lack the essential backbone for interoperability, scalability, and global deployment.

1. Role of Telecom Sector in IoT Ecosystem

a. Connectivity Backbone

- IoT devices require constant connectivity for data collection, transmission, and real-time monitoring.
- Telecom operators provide 2G/3G/4G/5G, Narrowband IoT (NB-IoT), LTE-M, and satellite communication services that form the backbone of IoT systems.
- These networks enable communication across diverse IoT applications such as smart homes, industrial automation, healthcare monitoring, and autonomous vehicles.

b. Standardization and Protocols

- The telecom sector ensures global standardization of communication protocols (e.g., 5G NR, NB-IoT, LoRaWAN, LTE Cat-M1).
- This facilitates interoperability among IoT devices manufactured by different vendors.
- Standards reduce production costs, accelerate innovation, and ensure reliability in IoT deployments.

c. Spectrum Allocation and Regulation

- Telecom authorities allocate and regulate radio frequency spectrum essential for IoT device communication.
- Manufacturing and assembly of IoT systems must comply with telecom regulations to ensure non-interference, safety, and cross-border operability.

2. Impact on Manufacturing and Assembly of IoT Devices

a. Design Considerations

- IoT device design is influenced by telecom-enabled factors such as:
  - Chipset integration for LTE, 5G, or NB-IoT compatibility.
  - Low-power modules for extended battery life in remote sensors.
  - Antenna design for optimal connectivity in diverse environments.
- Manufacturers must collaborate with telecom providers to ensure devices are network-ready.

b. Component Integration

- Telecom advancements drive demand for modems, communication modules, and SIM/eSIM technologies in IoT devices.
- The assembly process requires precise integration of these components to achieve seamless network connectivity.
- Example: Smart meters or industrial sensors use NB-IoT modules embedded during assembly.

Production Scalability

- With global telecom networks enabling billions of connections, manufacturers must design IoT devices for mass production and large-scale deployment.
- Telecom-enabled Over-the-Air (OTA) updates influence assembly by requiring devices to support upgradable firmware.

d. Quality Assurance and Testing

- Telecom sector standards necessitate rigorous network compliance testing during manufacturing.
- Devices undergo validation for latency, throughput, signal strength, roaming capability, and security compliance.
- Collaboration with telecom testing labs ensures devices are market-ready.

3. Sectoral Influence on IoT Growth

a. Industrial IoT (IIoT)

- Telecom-enabled 5G ultra-reliable low-latency communication (URLLC) supports automation, robotics, and predictive maintenance in manufacturing plants.
- IoT assembly lines increasingly adopt real-time telecom-enabled monitoring systems to optimize production.

b. Smart Cities and Infrastructure

- IoT devices for traffic management, waste monitoring, and energy grids depend on telecom operators for connectivity.
- Manufacturers align device specifications with telecom infrastructure in target regions.

c. Consumer Electronics

- Smart home devices (CCTV, smart speakers, wearables) require Wi-Fi, 4G/5G, or Bluetooth integration, shaped by telecom technologies.
- Assembly processes must ensure compatibility with telecom-driven ecosystems such as 5G-enabled smart homes.

d. Global Supply Chain Integration

- Telecom networks enable real-time logistics monitoring using IoT trackers.
- In manufacturing and assembly units, telecom-powered IoT solutions ensure supply chain visibility and quality control.

4. Future Significance

- 5G and Beyond: Ultra-fast 5G and upcoming 6G technologies will enable high-bandwidth, low-latency IoT applications like autonomous vehicles and smart factories.
- Edge Computing & Telecom Synergy: Integration of edge computing with telecom networks will influence device architecture, requiring new designs and assembly methods.
- Sustainability in Manufacturing: Telecom-enabled IoT will optimize energy efficiency, predictive maintenance, and waste reduction in assembly plants.
- Security and Compliance: Telecom operators will drive cybersecurity frameworks for IoT devices, requiring manufacturers to incorporate advanced encryption modules.

1.1.5 Key Skills and Technical Expertise Required for a Telecom Technician Specializing in IoT Devices and Systems

Introduction

The rapid convergence of telecommunications and Internet of Things (IoT) technologies has transformed the modern digital ecosystem. Telecom Technicians specializing in IoT play a critical role in installing, configuring, troubleshooting, and maintaining communication networks that enable seamless machine-to-machine (M2M) interactions. Their expertise lies not only in traditional telecom infrastructure but also in the integration of IoT-enabled devices, sensors, gateways, and cloud platforms. To effectively manage these complex systems, a Telecom Technician requires a robust blend of technical know-how, problem-solving skills, and domain-specific knowledge.

1. Networking and Connectivity Skills

- Strong understanding of network protocols such as TCP/IP, UDP, MQTT, CoAP, and HTTP/HTTPS.
- Expertise in wireless communication standards including 4G/5G, NB-IoT, LTE-M, Wi-Fi, LoRaWAN, Zigbee, and Bluetooth Low Energy (BLE).
- Ability to configure and troubleshoot routing, switching, and firewalls for IoT device connectivity.
- Familiarity with IP addressing, DNS, DHCP, and VPNs to ensure secure and reliable data transmission.

2. IoT Device Configuration and Management

- Hands-on experience in installing, calibrating, and maintaining IoT sensors, gateways, and edge devices.
- Knowledge of device provisioning, firmware updates, and over-the-air (OTA) upgrades.
- Proficiency in using IoT platforms for device registration, authentication, and lifecycle management.

Telecommunication Systems Expertise

- In-depth understanding of cellular network infrastructure (base stations, core network, SIM/eSIM technologies).
- Skills in signal measurement and analysis tools for assessing connectivity quality.
- Competence in optical fiber, copper cabling, and RF technologies relevant to IoT deployments.

4. Cloud and Edge Computing Knowledge

- Familiarity with major IoT cloud platforms such as AWS IoT Core, Microsoft Azure IoT Hub, Google Cloud IoT, and IBM Watson IoT.
- Understanding of edge computing architectures for local data processing and reduced latency.
- Ability to configure IoT data flow between devices, edge nodes, and cloud servers.

5. Cybersecurity Awareness

- Knowledge of IoT-specific security protocols, encryption standards, and authentication mechanisms.
- Ability to implement secure network configurations to prevent vulnerabilities and breaches.
- Awareness of compliance standards like ISO/IEC 27001, GDPR, and NIST cybersecurity frameworks relevant to IoT ecosystems.

6. Data Handling and Analytics Basics

- Competence in data collection, logging, and monitoring tools for IoT systems.
- Understanding of basic analytics dashboards, KPIs, and performance metrics.
- Familiarity with data visualization tools for interpreting IoT device outputs.

7. Troubleshooting and Diagnostic Skills

- Proficiency in using network analyzers, spectrum analyzers, and diagnostic software tools.
- Systematic approach to fault detection, root-cause analysis, and issue resolution in IoT-enabled telecom systems.
- Ability to interpret technical documentation, schematics, and system logs.

8. Programming and Scripting Knowledge

- Basic understanding of Python, C, or JavaScript for device-level programming and automation.
- Familiarity with API integration, SDKs, and IoT communication libraries.
- Knowledge of automation scripts for network testing and device management.

9. Soft Skills and Professional Attributes

- Strong problem-solving and analytical abilities to work in dynamic IoT environments.
- Collaboration and communication skills to coordinate with engineers, developers, and clients.
- Adaptability and continuous learning mindset to keep pace with evolving IoT and telecom technologies.

1.1.6 Challenges in Assembling and Testing IoT Devices and Systems in the Telecom Sector

1. Hardware Compatibility Issues

- IoT devices often come from different manufacturers with varying design standards.
- Incompatibility between sensors, gateways, and telecom infrastructure can delay assembly and integration.
- Ensuring mechanical and electrical compatibility during assembly requires precision and testing.

2. Complexity of Multi-Protocol Communication

- Telecom IoT ecosystems use diverse protocols such as NB-IoT, LTE-M, 5G, Wi-Fi, Zigbee, LoRaWAN, and Bluetooth.
- Testing interoperability across these protocols is challenging and time-intensive.
- Protocol mismatch may lead to signal loss, reduced coverage, or inconsistent data transmission.

3. Scalability Concerns in Testing

- Telecom operators often deal with thousands or millions of IoT devices.
- Testing at small scale may not reflect real-world network congestion, latency, or bandwidth limitations.
- Simulating large-scale IoT deployments to evaluate performance is resource-intensive.

4. Power Management and Energy Efficiency

- Many IoT devices are battery-operated, requiring low-power optimization.
- Testing battery life under real telecom conditions (signal fluctuations, data bursts) is complex.
- Inefficient power management can reduce device lifespan, increasing maintenance costs.

5. Cybersecurity and Data Privacy Risks

- IoT devices are highly vulnerable to hacking, malware, and data breaches.
- Testing must ensure robust encryption, authentication, and secure firmware updates.
- Compliance with telecom and data protection regulations (e.g., GDPR, ISO standards) adds complexity.

6. Firmware and Software Integration

- IoT devices rely on embedded firmware and software updates.
- Bugs during firmware installation or over-the-air (OTA) updates can disrupt large-scale deployments.
- Compatibility with telecom network management systems (NMS) needs rigorous validation.

7. Environmental and Reliability Testing

- Telecom IoT devices often operate in harsh environments (outdoor base stations, industrial zones).
- Assembling and testing must account for temperature extremes, dust, humidity, and vibration.
- Reliability testing requires extended test cycles, delaying time-to-market.

8. Latency and Quality of Service (QoS) Testing

- Telecom IoT applications (e.g., smart grids, connected vehicles) require ultra-low latency and high reliability.
- Testing latency across multiple network layers (device, edge, cloud, core telecom infrastructure) is technically demanding.
- Maintaining QoS guarantees while scaling is a significant challenge.

9. Supply Chain and Standardization Gaps

- Lack of universal standards for IoT device assembly and testing creates fragmentation.
- Dependence on global supply chains for chips, sensors, and modules often causes delays.
- Inconsistent standards lead to integration and certification bottlenecks in telecom deployments.

1.1.7 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

1.1.8 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:

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. 1.1.14: 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:

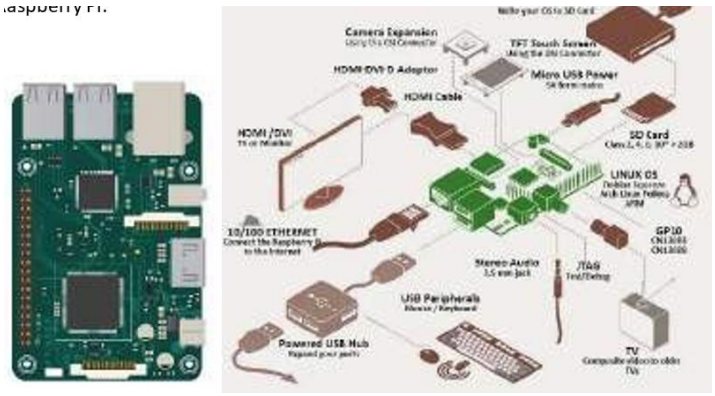


Fig. 1.1.15: Raspberry Pi

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

Notes

UNIT 1.2: Functioning of Sensors and Actuators

Unit Objectives

By the end of this unit, the participants 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:

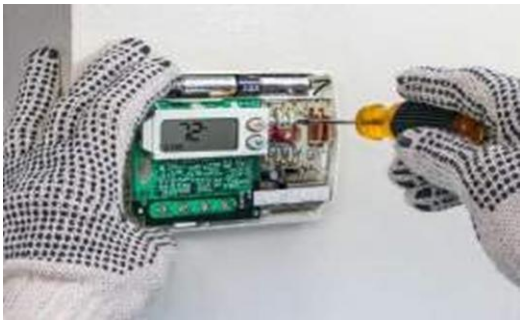


Fig. 1.2.1: Temperature sensor in a heating and cooling thermostat

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:

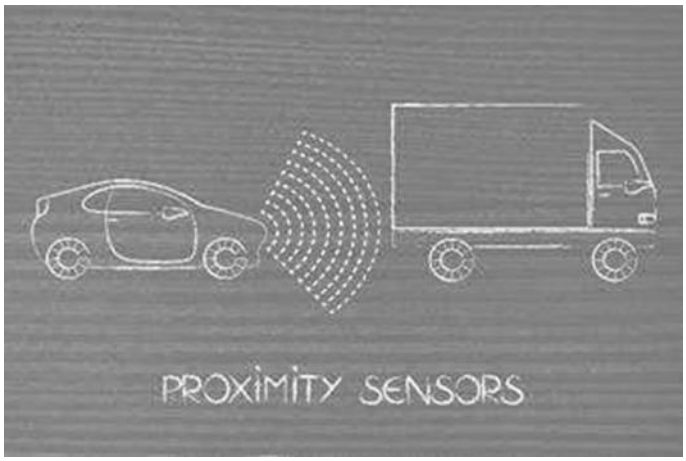


Fig. 1.2.2: Proximity sensor in a car

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:

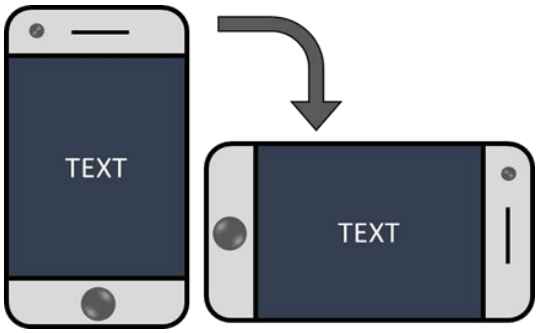


Fig. 1.2.4: Changing the display orientation of a smartphone

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:

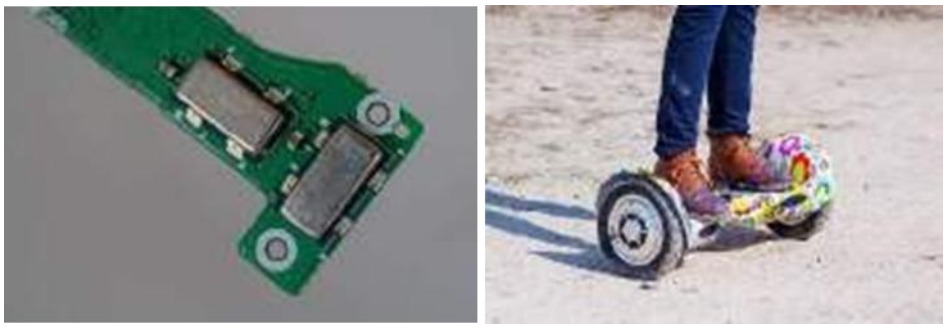


Fig. 1.2.5: Gyroscope sensor and a self-balancing scooter

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 ahumidity 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:

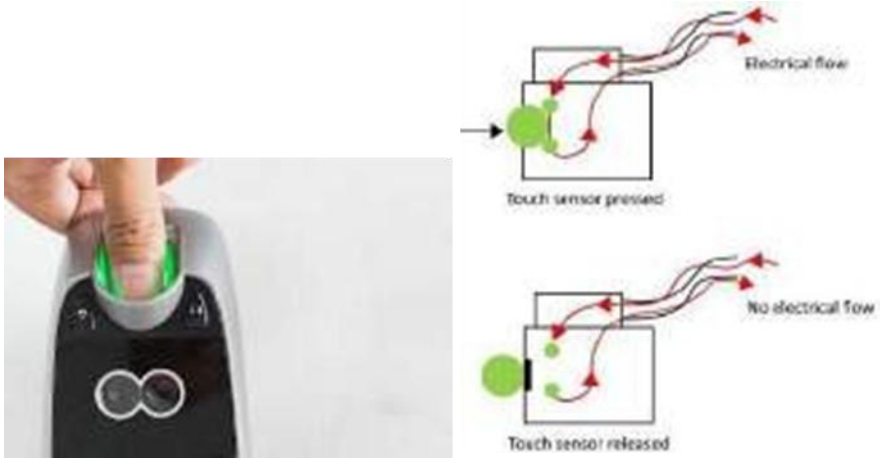


Fig. 1.2.7: Touch sensor in a door lock and its working

- **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:.

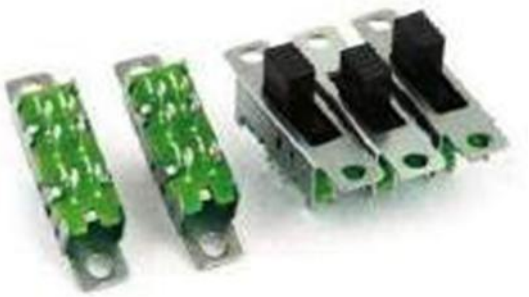


Fig. 1.2.8: PCB integrated sliding switch actuator

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:

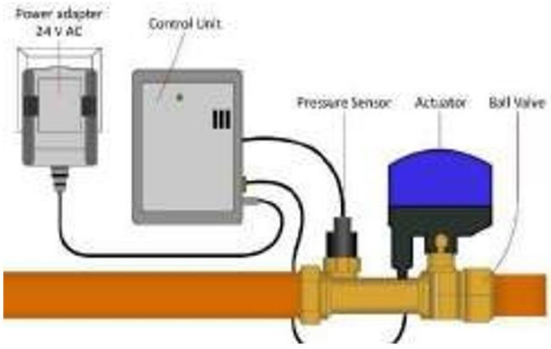


Fig. 1.2.9: A water flow system

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:

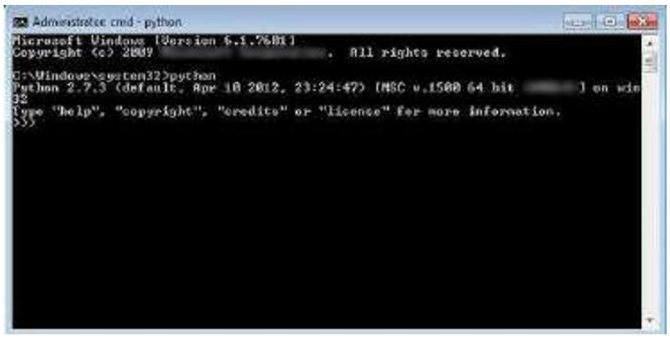


Fig. 1.2.10: Python interpreter

- 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.

Notes

UNIT 1.3: Application of Communication Protocol in Internet of Things

Unit Objectives

By the end of this unit, the participants 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
4. Describe the communication technologies used in IoT, including 5G, NB-IoT, LoRaWAN, Wi-Fi, Bluetooth, and Zigbee.

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:

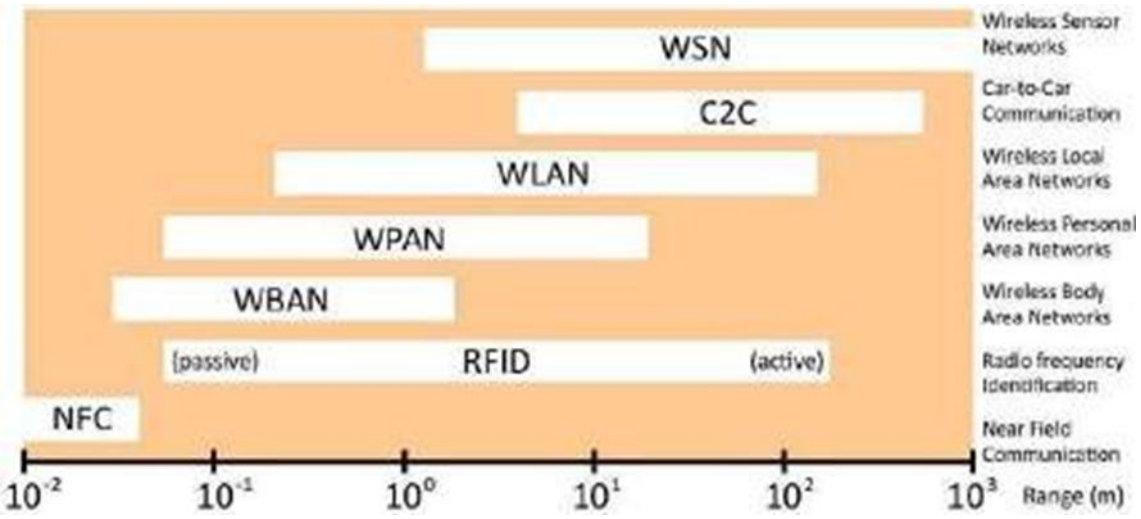


Fig. 1.3.1: Short-range communications technologies and their typical operating ranges

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:

- Point-to-point
- Star
- 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:

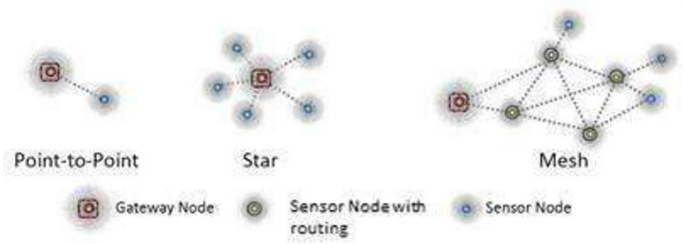


Fig. 1.3.3: Types of short-range communication architecture

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

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.

Notes

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

Unit Objectives

By the end of this unit, the participants 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:

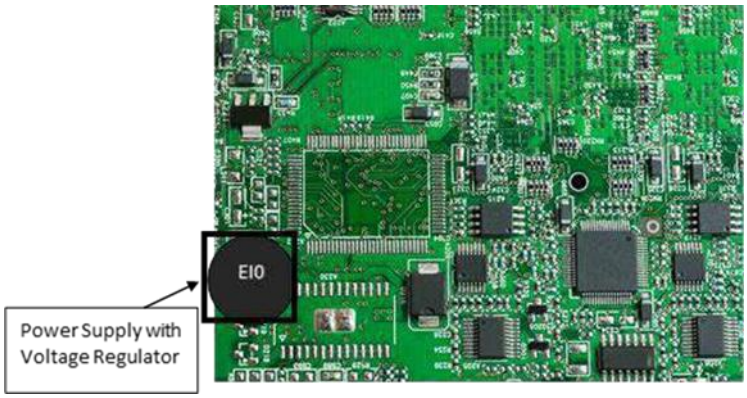


Fig. 1.4.3: Voltage regulator

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

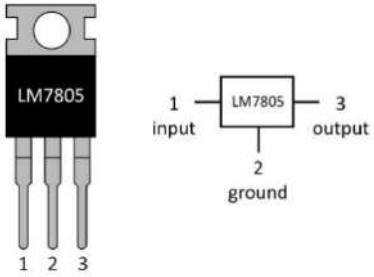


Fig 1.4.4: 7805 Voltage regulator IC pin configuration

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

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
- 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:

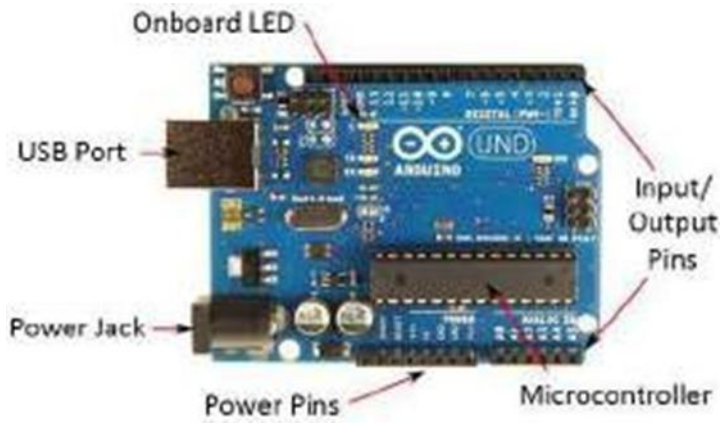


Fig. 1.4.6: Arduino pins

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:

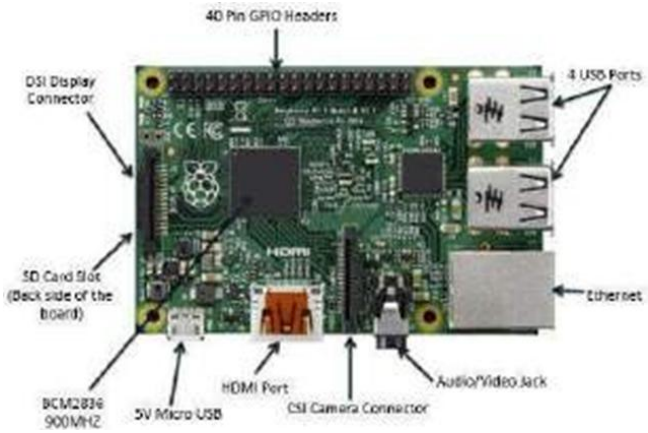


Fig. 1.4.8: Raspberry Pi

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:

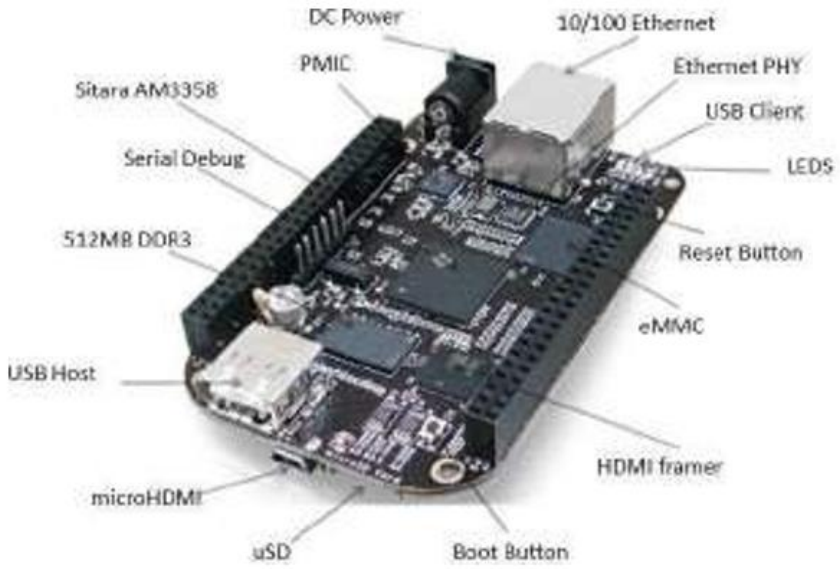


Fig. 1.4.9: BeagleBone Black development board

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 headerpin.	5V from USB mini B connector, 2.1mm jack, or headerpin.	3.3V power regulator with 150mA output capability	5V from USB micro B connector, or headerpin.
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

Notes

UNIT 1.5: Understanding Edge Devices

Unit Objectives

By the end of this unit, the participants 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:

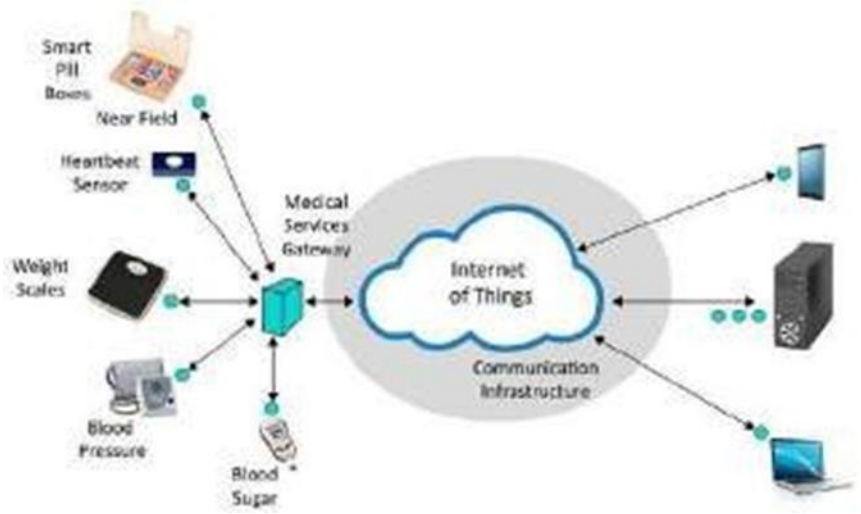


Fig. 1.5.1: IoT edge device

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:

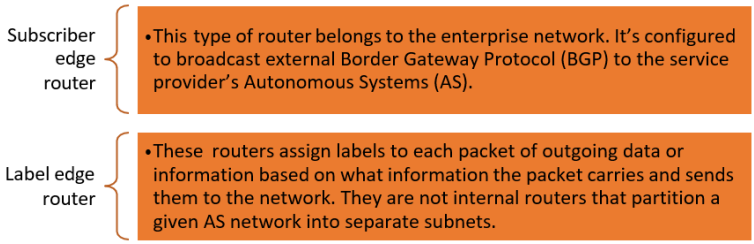


Fig. 1.5.2: Types of edge routers

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:

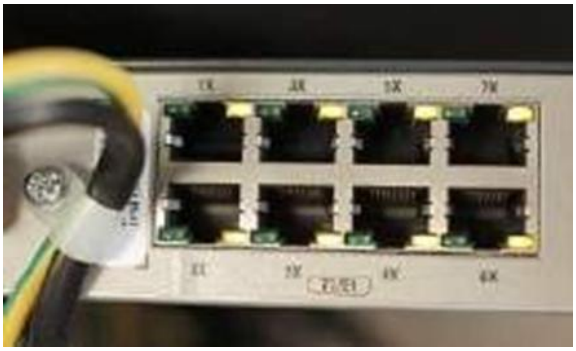


Fig. 1.5.3: Multiplexer

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

Notes

UNIT 1.6: Nodes and Gateways

Unit Objectives

By the end of this unit, the participants 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:

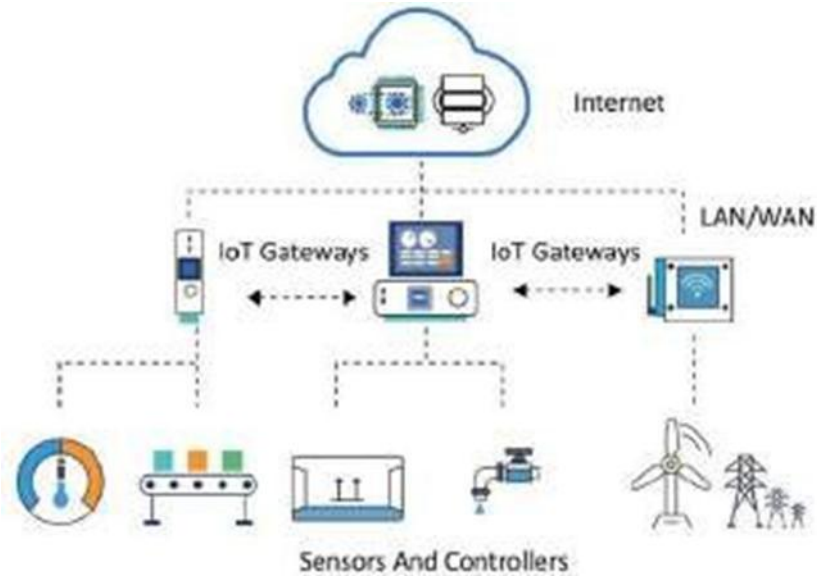


Fig. 1.6.1: IoT gateway architecture

In the current scenario, IoTgateways 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:

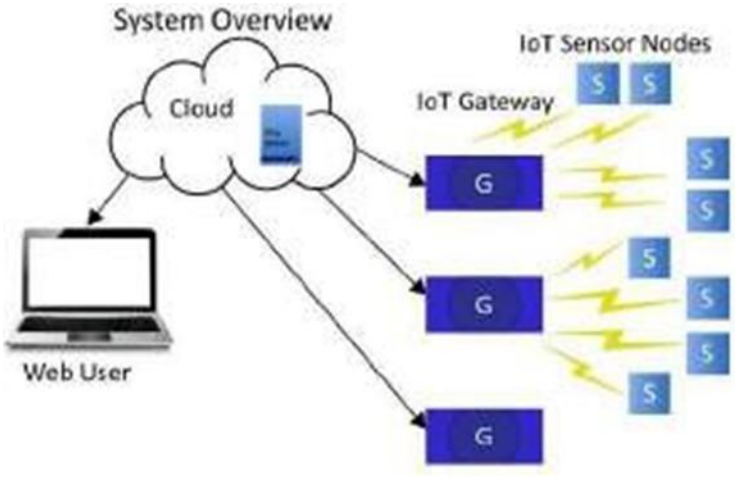


Fig. 1.6.2: IoT gateway and nodes

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.

Notes

UNIT 1.7: Cloud Computing

Unit Objectives

By the end of this unit, the participants 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:

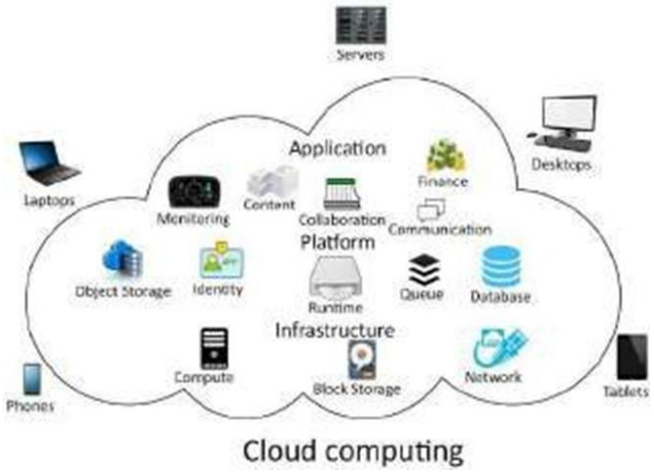


Fig. 1.7.1: Concept of cloud computing

Characteristics of Cloud Computing

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

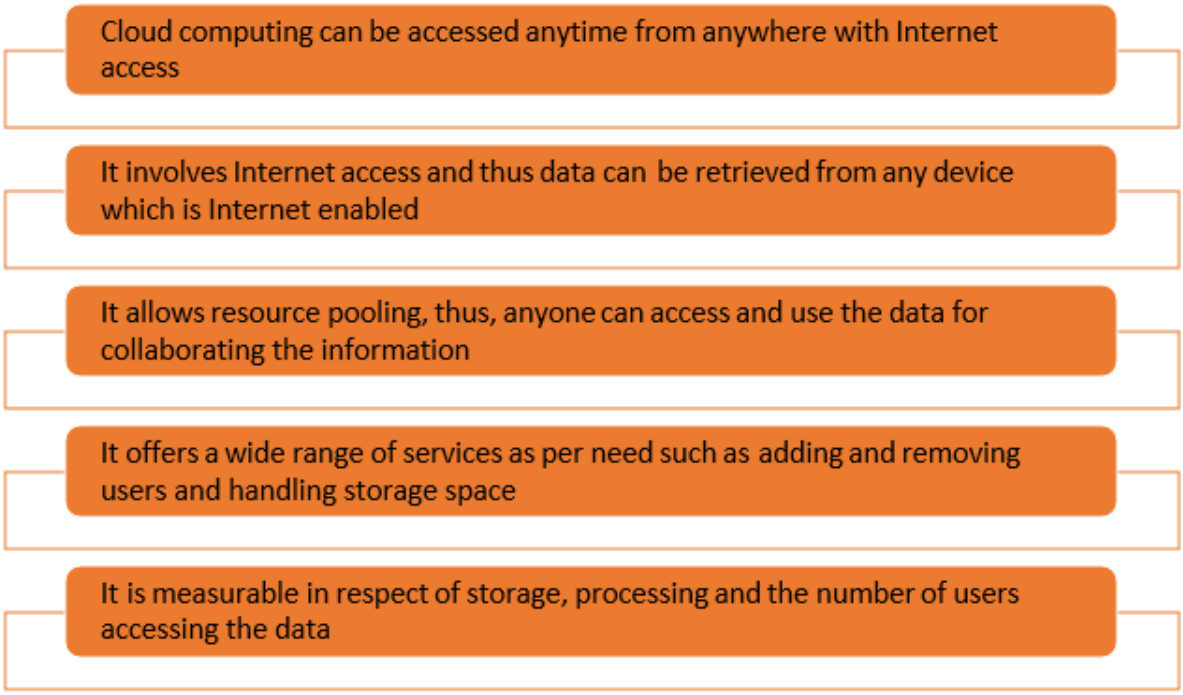


Fig. 1.7.2: Characteristics of cloud computing

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:

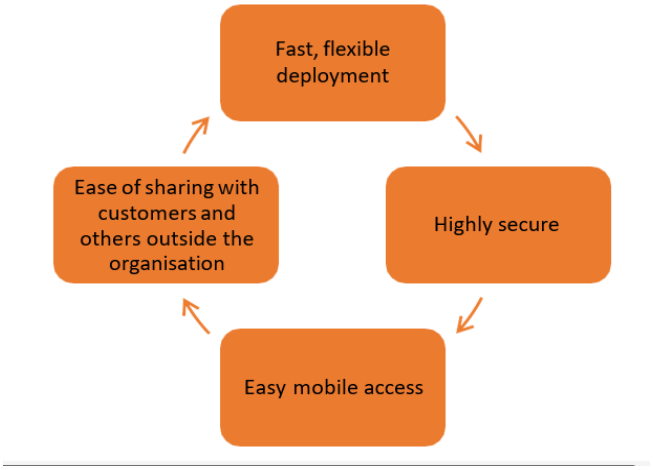


Fig. 1.7.3: Characteristics of cloud

- **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.

- **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. 1.7.3: Characteristics of cloud

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.

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

Short Questions:

1. Explain the role of the telecom sector in supporting the manufacturing and assembly of IoT devices and systems.
2. Describe the key technical skills required for a Telecom Technician working with IoT systems.
3. Discuss the main challenges encountered during the assembly and testing of IoT devices in the telecom industry.
4. Explain the importance of precision and quality control in the production of IoT-enabled telecom devices.
5. Describe the responsibilities of a Telecom Technician in maintaining production efficiency and product reliability.

Multiple Choice Questions (MCQs):

1. Which of the following best defines an IoT device?
   a. A standalone electronic gadget
   b. A device connected to the internet for data exchange and remote control
   c. A communication tower used for signal transmission
   d. A non-networked sensor system
2. A Telecom Technician working with IoT devices should have expertise in:
   a. Data entry and record keeping
   b. Sensor integration, circuit testing, and device configuration
   c. Civil structure maintenance
   d. Cable painting and marking
3. The biggest challenge in assembling IoT systems is ensuring:
   a. Color coding of parts
   b. Reliable connectivity, compatibility, and precision
   c. Fast shipment of equipment
   d. Reduction in workforce requirements
4. Quality control in IoT device manufacturing ensures:
   a. Increased production without testing
   b. Compliance with standards and device reliability
   c. Elimination of assembly processes
   d. Decrease in equipment lifespan

5. The primary responsibility of a Telecom Technician in IoT manufacturing is to:
   a. Supervise office documentation
   b. Assemble, test, and verify the performance of connected devices
   c. Handle customer complaints
   d. Plan marketing campaigns

Fill in the Blanks

1. The _____ sector provides the communication backbone for IoT devices to operate efficiently.
2. A Telecom Technician must possess strong skills in _____, testing, and troubleshooting IoT systems.
3. Ensuring _____ during assembly helps in achieving consistent performance and reliability in IoT devices.
4. Common challenges in IoT system manufacturing include device _____ and signal integrity.
5. Maintaining detailed _____ of assembly and testing processes is essential for quality assurance in telecom IoT systems.

Notes

2. Lay Install and Configure IoT Devices at Customer Premises

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

By the end of this module, the participants will be able to:

1. Explain the principles of IoT architecture, including the roles of microcontrollers, sensors, actuators, gateways, and cloud platforms.
2. Discuss the applications of IoT in smart cities, healthcare, Industry 4.0, and agriculture.
3. Describe the communication technologies used in IoT, including 5G, NB-IoT, LoRaWAN, Wi-Fi, Bluetooth, and Zigbee.
4. Explain IoT data transfer protocols and their role in machine-to-machine communication.
5. Elucidate the workings of Ethernet, TCP/IP, and VPN in IoT installations.
6. Explain the cellular IoT technologies, including LTE-M and 5G variants.
7. Describe wireless IoT technologies such as Wi-Fi 6, Zigbee, and LoRaWAN.
8. Explain the process of installing and configuring smart meters, connected cameras, and industrial IoT devices.
9. Discuss the impact of signal interference, data packet loss, and power failures on IoT performance.
10. Explain proper handling, grounding, and safety measures during IoT device installations.

UNIT 2.1: Establishing Framework for Internet of Things

Unit Objectives

By the end of this unit, the participants 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. Explain the principles of IoT architecture, including the roles of microcontrollers, sensors, actuators, gateways, and cloud platforms.
5. Explain IoT data transfer protocols and their role in machine-to-machine communication.
6. Discuss the integration of edge computing and AI in IoT installations and real-time data processing.
7. Describe the use of fog computing to reduce latency in telecom applications

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:

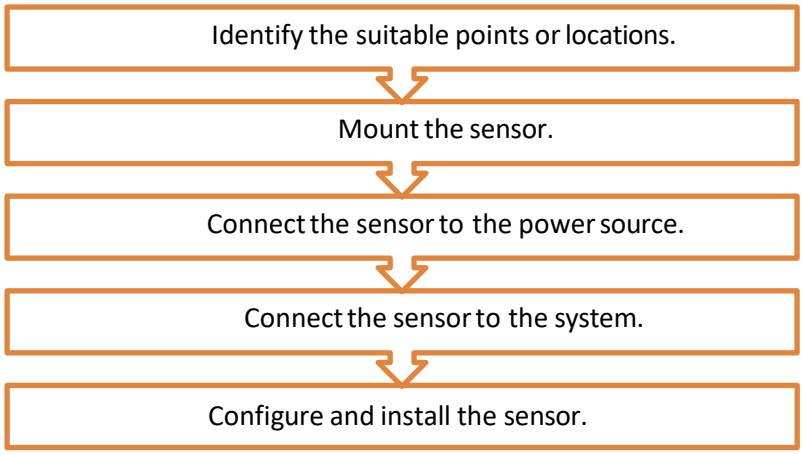


Fig. 2.1.2: Steps for installing a motion sensor

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:

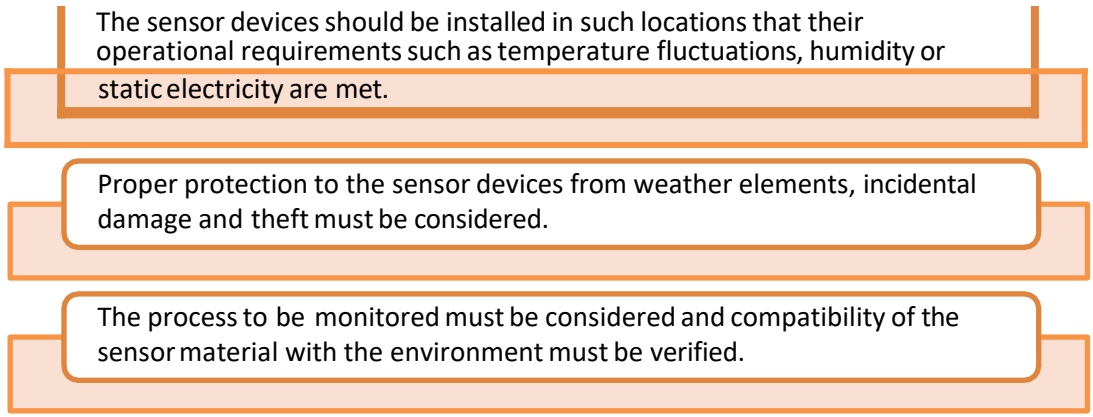


Fig. 2.1.3: Criteria for securing IoT devices

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:

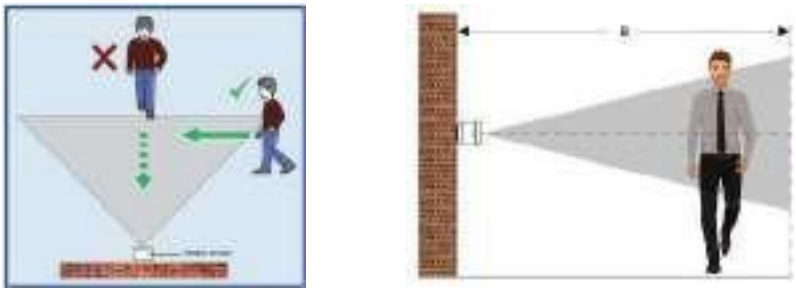


Fig. 2.1.5: Scope of a motion sensor

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:

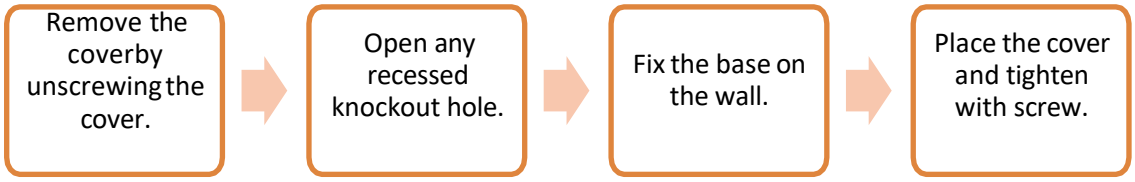


Fig. 2.1.6: Steps for mounting a sensor

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:

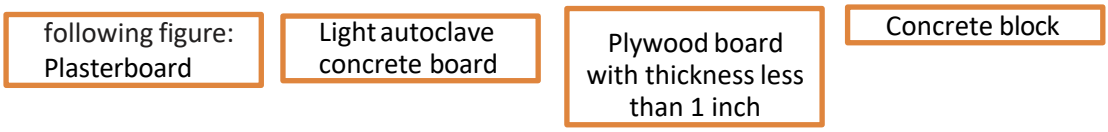


Fig. 2.1.7: Surfaces to be avoided for mounting

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

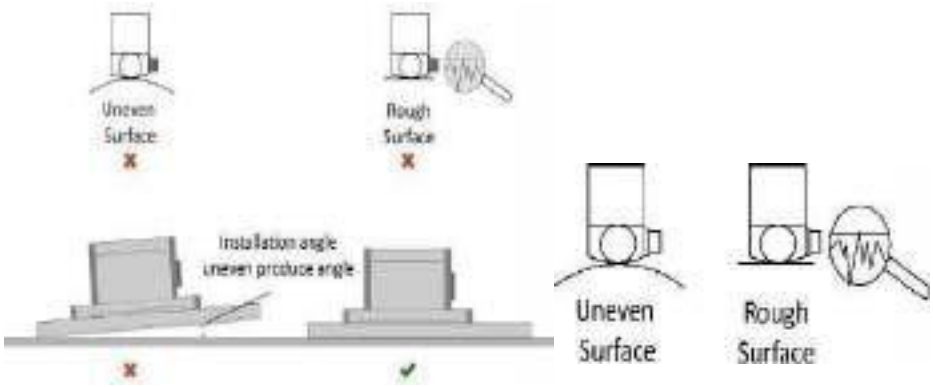


Fig. 2.1.8: Suitable and unsuitable surfaces for mounting

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:

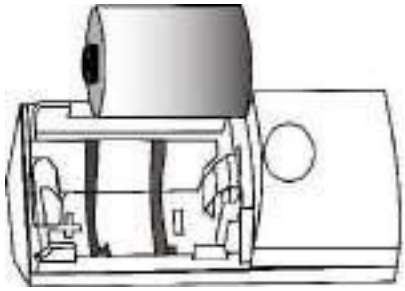


Fig. 2.1.10: Installing the battery

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:

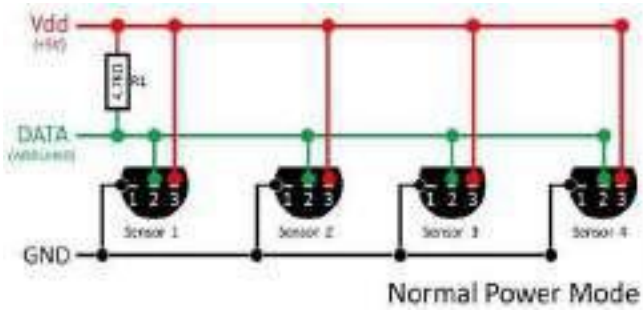


Fig. 2.1.11: Schematic diagram of sensor connectivity to the power supply

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:

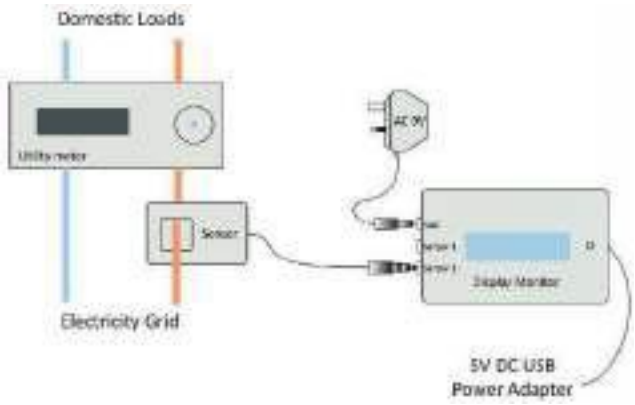


Fig. 2.1.12: Schematic diagram for connecting a sensor to a display monitor

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:

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:

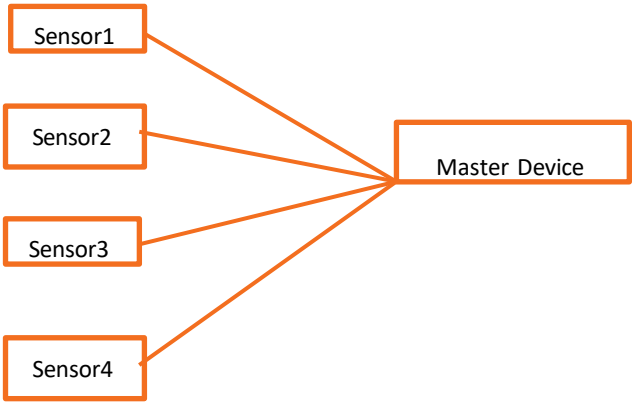


Fig. 2.1.16: Collating installation points

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

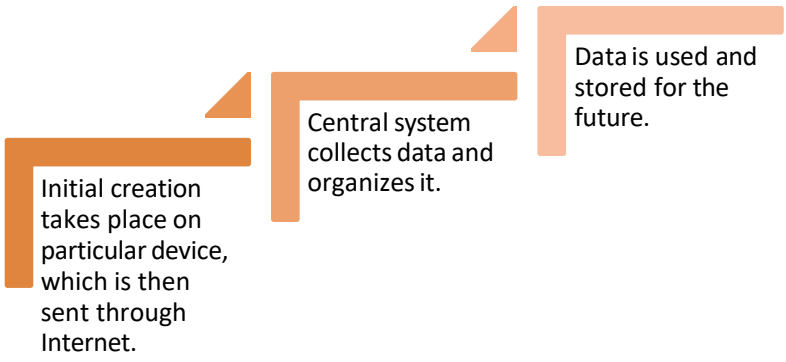


Fig. 2.1.17: Data creation stages

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:

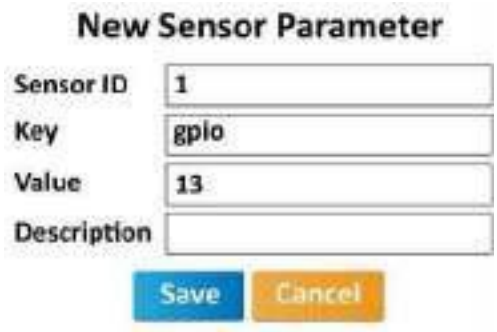


Fig. 2.1.18: Input parameters of sensors

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.

2.1.5 Principles of IoT Architecture

The core principles of IoT architecture focus on creating systems that are effective, reliable, and secure across a multi-layered structure. These principles guide the design, deployment, and management of connected devices, data flow, and applications.

Core Design Principles

Key principles for successful IoT architecture and design include:

- **Scalability:** The architecture must support the addition of a growing number of devices, users, and applications without performance degradation. Cloud-based and distributed solutions often facilitate this.
- **Interoperability:** Given the wide variety of vendors and communication protocols, the system should use open standards (e.g., MQTT, CoAP, Zigbee) to allow different devices and platforms to communicate and work together seamlessly.
- **Security and Privacy:** Security must be a foundational "security by design" principle, implemented from the initial stages of development. Measures include strong encryption, authentication, access controls, and transparent data handling to protect sensitive information.
- **Reliability and Fault Tolerance:** Systems should continue to operate effectively even if individual components or network connections fail. This often involves redundancy and failover mechanisms to ensure continuous operation, especially in critical applications.
- **Energy Efficiency:** Many IoT devices are battery-powered or in remote locations, requiring energy-efficient designs, low-power communication protocols, and sleep modes to extend operational life.
- **Modularity and Flexibility:** A modular design allows for components to be updated, replaced, or extended without disrupting the entire system, enabling faster innovation and adaptation to new technologies.

- **Data Management and Analytics:** The architecture needs a robust system for handling the vast amounts of generated data efficiently, from collection and filtering to processing and analysis, to derive actionable insights.
- **Real-Time Capability (Low Latency):** For many applications (like autonomous vehicles or industrial automation), data must be processed and acted upon with minimal delay. Edge computing, which processes data closer to the source, is often used to minimize latency.
- **User-Centricity/Experience:** The end-user experience (UX) is crucial. Interfaces should be intuitive, provide meaningful information, and allow users to control devices seamlessly through apps, dashboards, or voice.

Architectural Layers

- These principles are applied across a layered architecture, commonly described in a four-layer or five-layer model:
- Perception (Sensing) Layer: The physical layer consisting of sensors, actuators, and devices that collect data from the environment and interact with the physical world.
- Network Layer: Responsible for connectivity and data transmission between devices and cloud systems using various technologies like Wi-Fi, Bluetooth, cellular networks, etc..
- Processing (Middleware/Edge) Layer: This layer handles data aggregation, pre-processing, and initial analysis, often at the edge to reduce latency and bandwidth usage.
- Application Layer: Provides the services and user interfaces, such as mobile apps and web dashboards, through which users monitor and control the system.
- Business Layer: Focuses on managing the overall system, integrating insights into business operations, strategies, and optimization for business value.

2.1.6 IoT Data Transfer Protocols

IoT data transfer protocols are the "language" that machines use to communicate autonomously without human intervention, which is the core of machine-to-machine (M2M) communication. Their role is to provide the rules and standards for efficient, reliable, and secure data exchange tailored to the specific needs of resource-constrained IoT devices.

Role in Machine-to-Machine (M2M) Communication

In M2M communication, these protocols enable devices to exchange data and perform actions independently, often in closed, point-to-point networks. They ensure:

- **Automation and Efficiency:** By enabling autonomous data transfer (e.g., a smart meter sending usage data to a utility provider), they automate processes and reduce the need for manual labor.
- **Interoperability:** Protocols ensure that diverse devices, potentially from different manufacturers, can understand and work with each other seamlessly within an ecosystem.

- **Optimization for Constraints:** Unlike traditional internet protocols (like HTTP, which is "heavy" for simple sensors), M2M protocols are designed to be lightweight, using minimal bandwidth, memory, and power, which is critical for battery-operated devices in remote locations.
- **Scalability:** They facilitate the addition or removal of thousands of devices from a network without disruption, allowing for large-scale deployments like smart cities or industrial automation.
- **Reliability and Security:** Protocols incorporate mechanisms for error detection, data integrity, and encryption (like TLS/DTLS) to ensure data is delivered securely and reliably, even in unstable networks.

Common IoT Data Transfer Protocols

The choice of protocol depends on the specific application's requirements, such as range, power consumption, and data rate.

- **MQTT (Message Queuing Telemetry Transport):** A lightweight, publish/subscribe messaging protocol operating over TCP/IP. It is highly efficient for remote monitoring and real-time data updates, ideal for devices with limited bandwidth and power (e.g., smart home sensors, industrial monitoring).
- **CoAP (Constrained Application Protocol):** A web transfer protocol designed for resource-constrained devices and networks that uses a request/response model similar to HTTP but operates over UDP for lower overhead. It is suitable for smart city and building automation applications.
- **AMQP (Advanced Message Queuing Protocol):** An open standard for reliable and secure message queuing and routing. It provides robust delivery guarantees, making it suitable for enterprise-level and financial applications where data integrity is critical.
- **HTTP/HTTPS (Hypertext Transfer Protocol Secure):** The standard protocol of the internet, often used for data transfer to cloud platforms and web-based applications. HTTPS adds a layer of security (SSL/TLS) for encrypted communication. While robust, it can be resource-intensive for simple IoT devices.
- **DDS (Data Distribution Service):** A high-performance, real-time, publish/subscribe protocol primarily used in demanding, mission-critical M2M applications like autonomous vehicles, robotics, and industrial control systems.
- **Zigbee and Z-Wave:** Low-power, short-range wireless protocols used predominantly in home automation and sensor networks. They form mesh networks, allowing devices to relay data to extend coverage and reliability.
- **Bluetooth Low Energy (BLE):** A short-range wireless communication protocol optimized for very low power consumption, commonly used in wearable devices and health monitors that connect to smartphones.
- **LoRaWAN (Long Range Wide Area Network):** A protocol for low-power, wide-area networks, enabling communication over several kilometers with minimal power use. It is widely used for applications like smart agriculture, asset tracking, and environmental monitoring.

2.1.7 Integration of Edge Computing and AI in Iot Installations and Real-Time Data Processing

The integration of edge computing and Artificial Intelligence (AI) in IoT installations enables real-time data processing, transforming reactive systems into autonomous, efficient, and highly responsive environments. This synergy involves deploying AI models directly on local devices or nearby edge servers, allowing for immediate analysis and decision-making at the source of data generation.

The Role of Edge Computing

Edge computing shifts data processing away from centralized cloud data centers, bringing computational resources physically closer to IoT devices. This fundamental architectural change provides several benefits essential for real-time operations:

- **Ultra-Low Latency:** Processing data locally eliminates the time delay (latency) associated with sending data to the cloud and waiting for a response. This is critical for time-sensitive applications like autonomous vehicles, where split-second decisions can be life-saving.
- **Bandwidth Optimization:** Instead of transmitting vast amounts of raw data (e.g., continuous video feeds) to the cloud, edge computing pre-processes and filters data locally. Only essential insights or summaries are sent to the cloud for long-term storage or deeper analytics, significantly reducing network traffic and associated costs.
- **Enhanced Reliability:** Edge devices can operate and make decisions independently, even with intermittent or lost cloud connectivity. This ensures the continuous operation of mission-critical systems in remote or unstable network environments.

The Role of AI in Edge Installations

- AI provides the "intelligence" at the edge, enabling devices to analyze data, learn patterns, and make intelligent decisions autonomously.
- **Real-Time Analytics and Decision-Making:** AI models running on edge devices can perform complex tasks like image recognition, anomaly detection, and predictive modeling instantly. For example, AI-powered cameras can detect security threats in real-time on-site, triggering immediate alerts without cloud reliance.
- **Predictive Maintenance:** In industrial IoT (IIoT), AI algorithms analyze sensor data from machinery to predict equipment failures before they occur. This allows for proactive maintenance scheduling, minimizing costly unplanned downtime.
- Adaptive Learning: Through techniques like federated learning, AI models can be continuously updated and improved collaboratively across multiple edge devices without the need to send sensitive raw data to a central server, ensuring the system remains relevant and accurate over time.

Synergistic Applications

- The combined power of edge computing and AI is driving innovation across various industries:
- Autonomous Vehicles: Onboard AI systems process data from cameras, LiDAR, and sensors in real-time to navigate and react instantly to road conditions, ensuring safety and efficiency.
- Smart Cities: Edge AI optimizes traffic flow by analyzing data from interconnected cameras and sensors to adjust signal timings dynamically, reducing congestion and improving emergency response times.

- Healthcare: Wearable monitors use edge AI to track vital signs and detect abnormalities instantly, alerting medical professionals to critical issues faster than cloud-based systems.
- Smart Manufacturing: AI vision systems on the factory floor detect product defects in real-time, allowing immediate correction and ensuring high quality control without operational delays.

In essence, the integration of edge computing and AI transforms IoT from simple data collection to a decentralized, intelligent ecosystem capable of immediate, impactful action.

Notes

UNIT 2.2: Installing Gateway as per the Power Supply Requirements

Unit Objectives

By the end of this unit, the participants 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. Demonstrate how to differentiate between IoT nodes and gateways, assessing their roles in data transmission and network management.
4. Explain the importance of robust battery backups and energy-efficient IoT deployments.
5. Demonstrate how to determine optimal installation points considering environmental factors, power supply availability, and network signal strength.
6. Demonstrate how to connect and secure power supply sources while ensuring proper grounding and compliance with safety standards.

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:

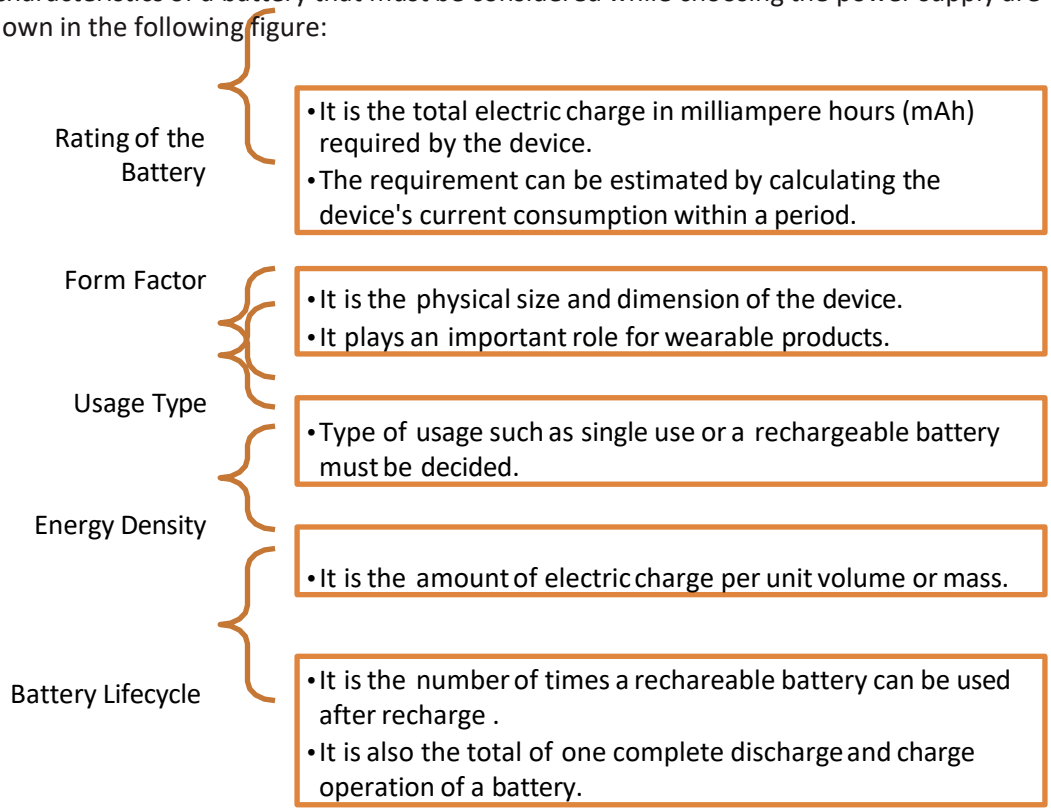


Fig. 2.2.1: Characteristics of a battery

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:

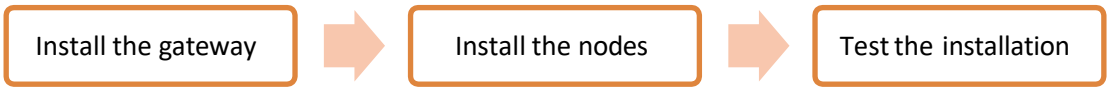


Fig. 2.2.2: Steps for connecting power supply with gateway and nodes setup

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:

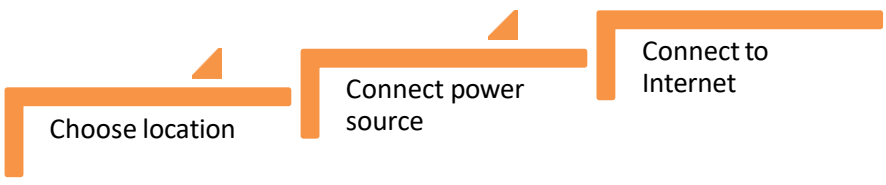


Fig. 2.2.3: Installation steps of IoT gateway

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:

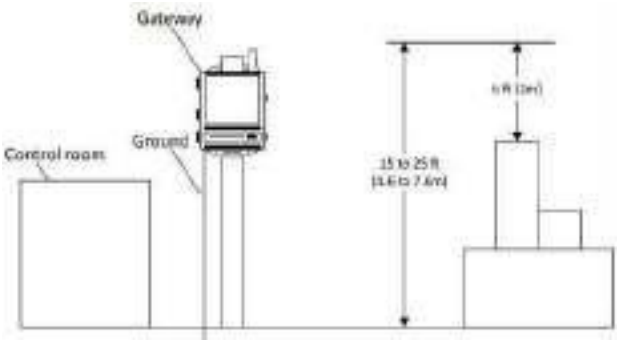


Fig. 2.2.4: Position of IoT gateway

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:

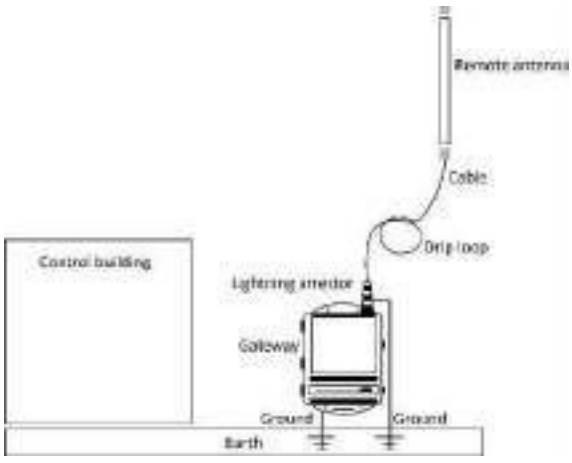


Fig. 2.2.7: A gateway connected to a power outlet

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:

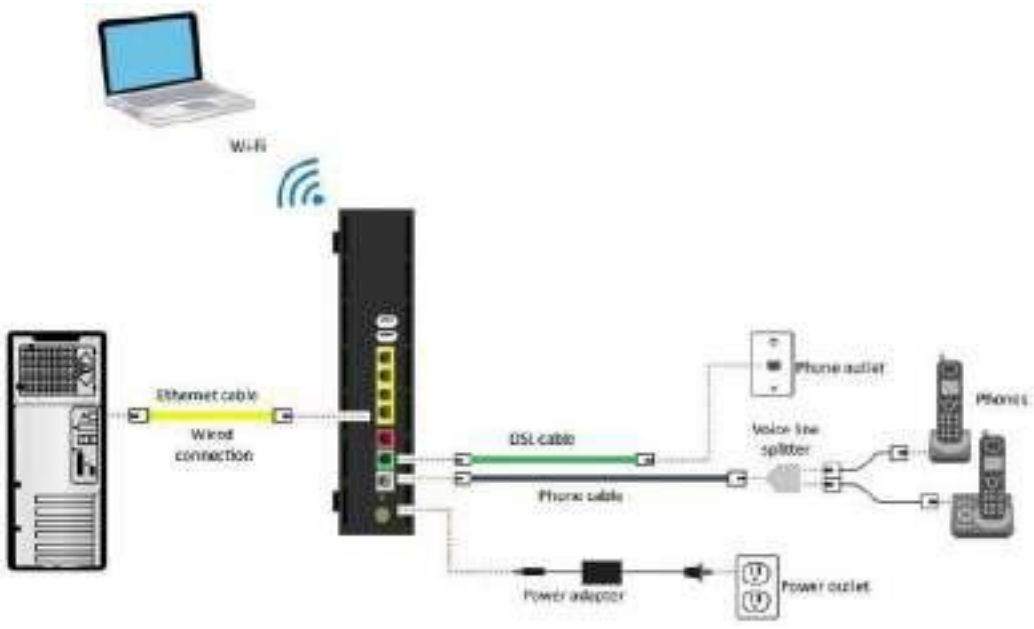


Fig. 2.2.8: Overview of cabling a gateway

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:

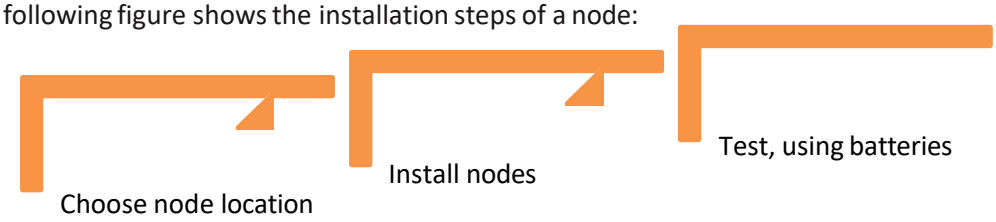


Fig. 2.2.10: Installation steps of IoT nodes

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:

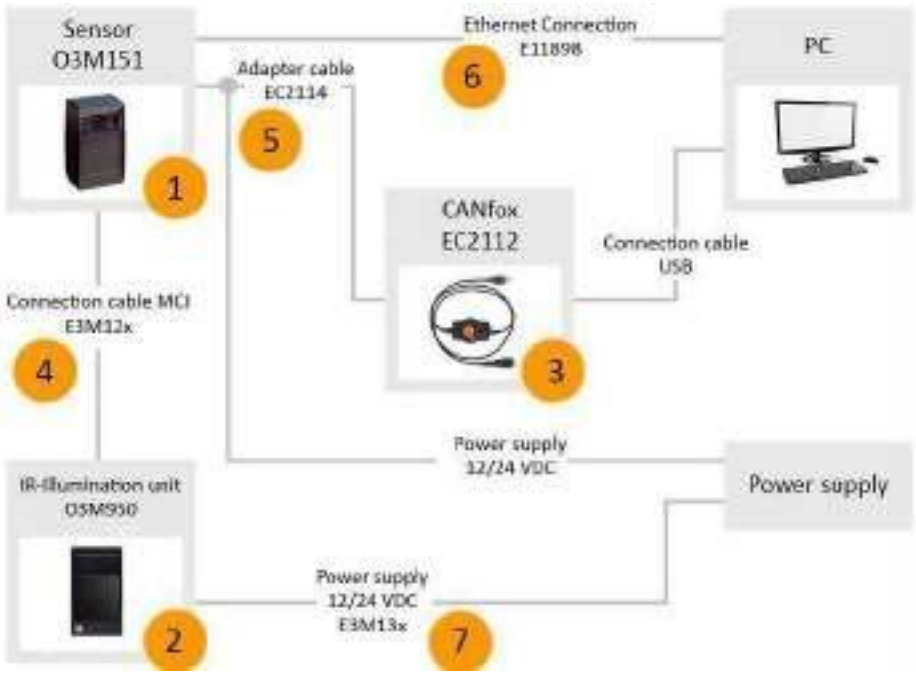


Fig. 2.2.12: Connection of IoT nodes

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:

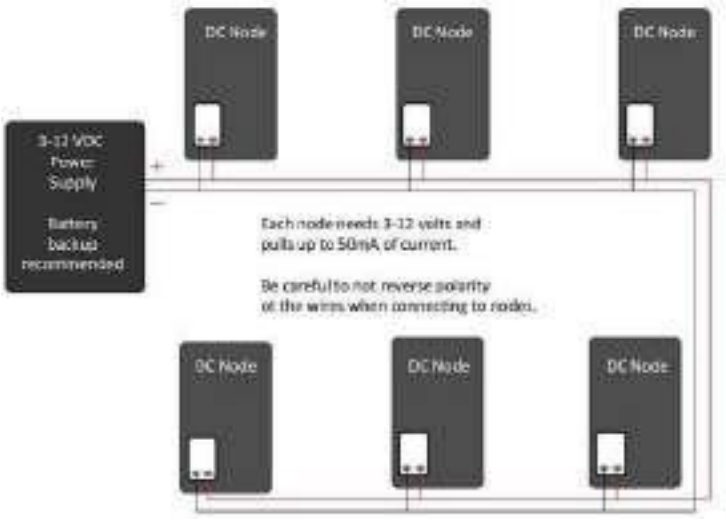


Fig. 2.2.14: Connection of DC nodes

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:

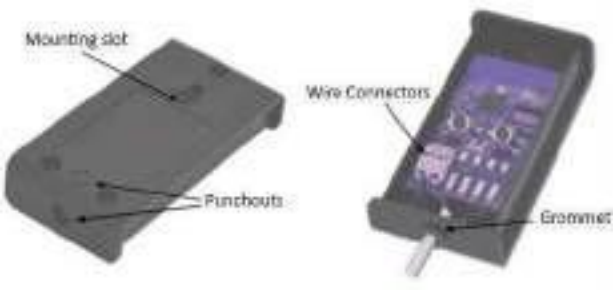


Fig. 2.2.15: Parts of a node or hub

- 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:

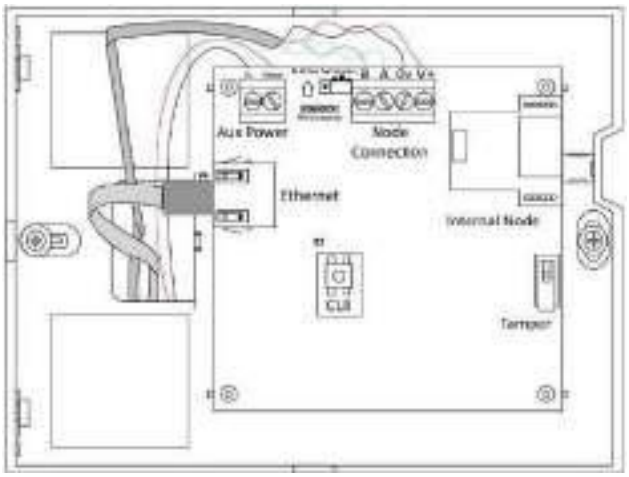


Fig. 2.2.17: Connection diagram of the gateway

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:

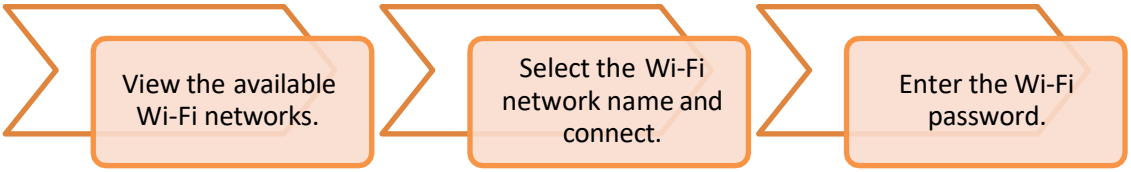


Fig. 2.2.18: Connecting a Wi-Fi device

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.

2.2.3 Importance of Robust Battery Backups and Energy-Efficient Iot Deployments

Robust battery backups and energy-efficient designs are paramount in IoT deployments to ensure operational reliability, reduce costs, and promote environmental sustainability. These factors directly influence the long-term viability and success of IoT solutions, particularly those in remote, critical, or hard-to-reach locations.

Importance of Robust Battery Backups

Robust battery backup systems (often Uninterruptible Power Supplies or UPS) are crucial for maintaining the continuity and integrity of IoT operations during main power outages.

- **Operational Continuity:** For critical applications like medical devices (e.g., pacemakers, monitors), industrial control systems, or smart city infrastructure (e.g., traffic management, emergency systems), uninterrupted power is essential to prevent potentially catastrophic failures or service disruptions.
- **Data Integrity and Security:** Sudden power losses can corrupt data, disrupt ongoing system updates, or compromise the security of data in transit. Backups ensure safe shutdowns or continuous operation, protecting valuable data and maintaining system security.
- **Enhanced Reliability and Trust:** Dependable backup power increases the overall reliability of the IoT system, which builds customer trust and ensures the solution performs as intended, even in challenging environments.
- **Remote Management:** Many IoT gateways and devices are in remote or inaccessible locations. Battery backups ensure that these devices remain online, allowing for continuous remote monitoring, diagnostics, and management without requiring costly on-site visits.

Importance of Energy-Efficient Deployments

Energy efficiency in IoT goes beyond merely saving power; it is a core design principle that impacts the entire system lifecycle.

- **Extended Device Lifespan:** By optimizing power consumption, devices can run for years, or even a decade, on a single battery, reducing the frequency and cost of maintenance and replacements.
- **Reduced Total Cost of Ownership (TCO):** While hardware is an initial cost, operational and maintenance costs quickly become dominant. Energy efficiency significantly lowers operational expenses (OpEx) related to electricity consumption and labor costs for battery servicing, contributing to a lower overall TCO.
- **Scalability:** For large-scale deployments, such as smart agriculture or massive sensor networks, managing billions of power-hungry devices is logistically and financially unfeasible. Energy-efficient designs make such vast networks viable and manageable.
- **Environmental Sustainability:** The widespread deployment of billions of IoT devices raises significant environmental concerns regarding energy consumption and electronic waste. Energy-efficient designs, the use of low-power components, and integration with energy harvesting technologies (solar, kinetic, thermal) reduce the carbon footprint and promote sustainable practices.

- **Optimized Performance:** Energy-efficient practices, such as putting devices into "deep sleep" modes (e.g., Power Saving Mode, PSM) or using low-power communication protocols (e.g., LoRaWAN, BLE), balance power savings with connectivity needs, optimizing performance for specific application requirements.

Notes

UNIT 2.3: Establishing Communication between Nodes, Gateway and Servers

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to establish communication line connectivity using suitable nodes, gateways, and networks.
2. Show how to establish effective connectivity between IoT gateways and backend cloud platforms or local networks.

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.

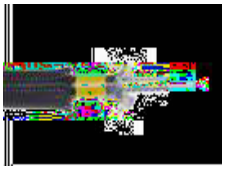
Coaxial/Helix cable		This has a thin conducting wire inside a tubular conducting shield, which is protected by a tubular insulating jacket. It is used to connect video equipment and carry television signals.
Optical fibre cable		This contains one or more optical fibres for carrying light. The optical 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:

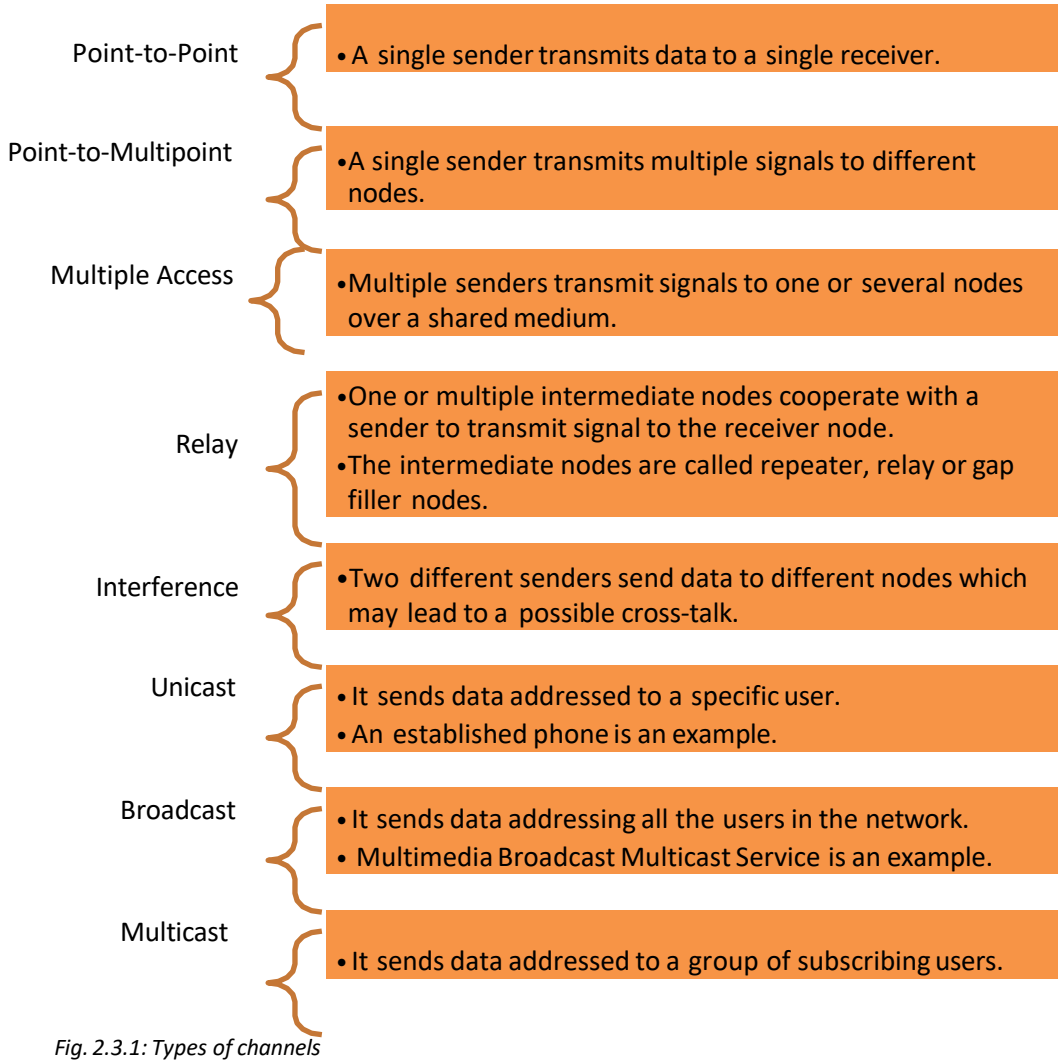


Fig. 2.3.1: Types of channels

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 appli cations 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:

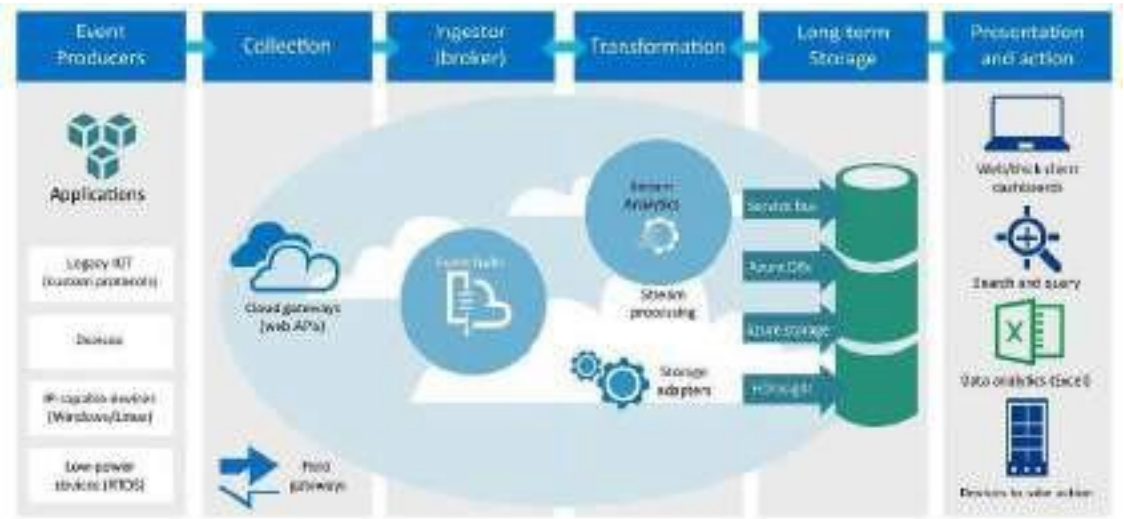


Fig. 2.3.2: Azure framework

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:

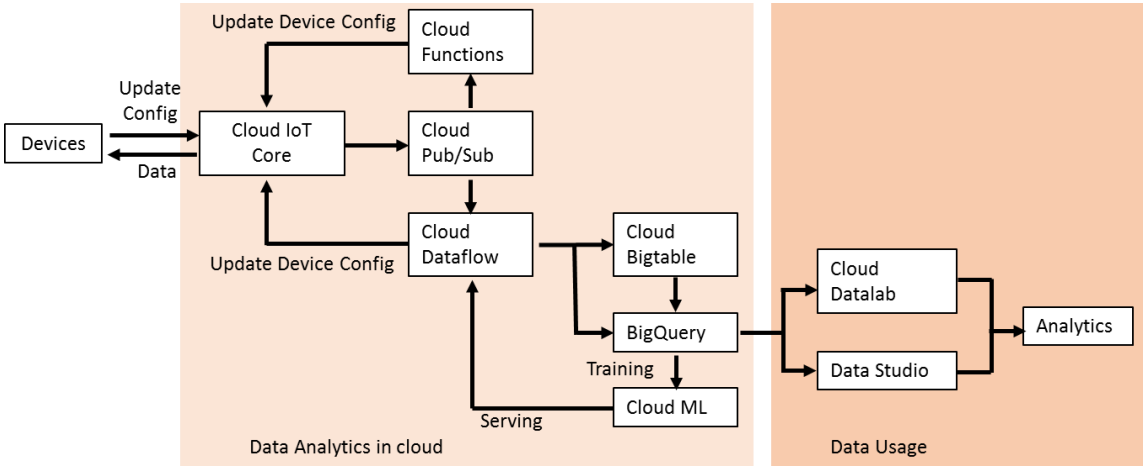


Fig. 2.3.3: IoT data management in cloud platform

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:

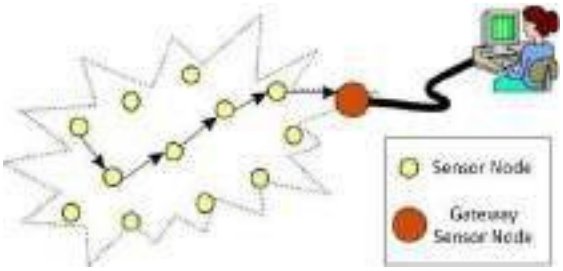


Fig. 2.3.4: WSN

The following figure shows the structure of a sensor node:

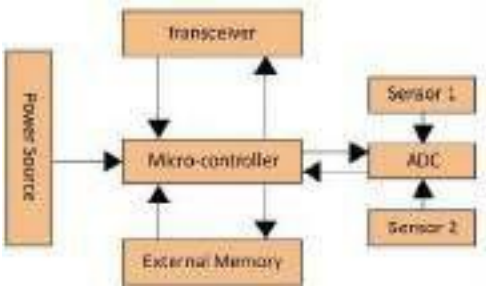


Fig. 2.3.5: Structure of a sensor node

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:

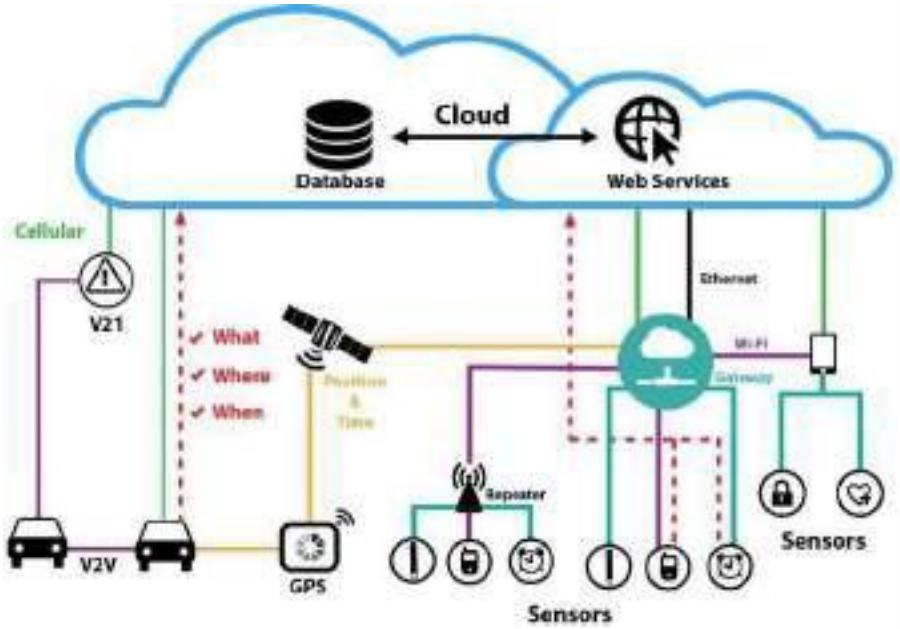


Fig. 2.3.6: Sensor connectivity model

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

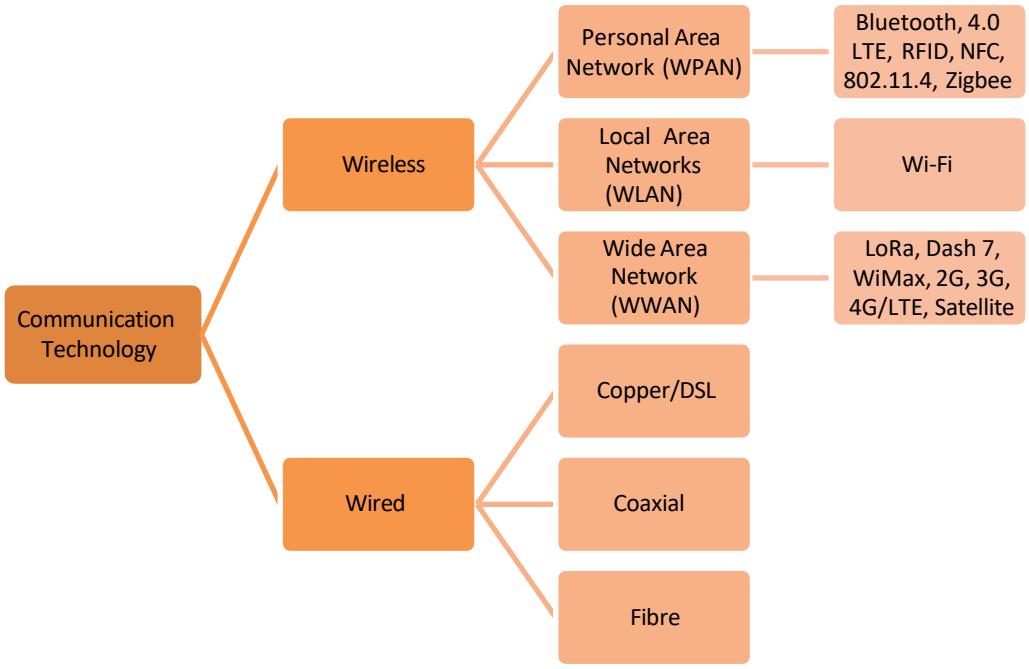


Fig. 2.3.7: Communication technologies

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
		Short	Intermediate	Short

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

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:

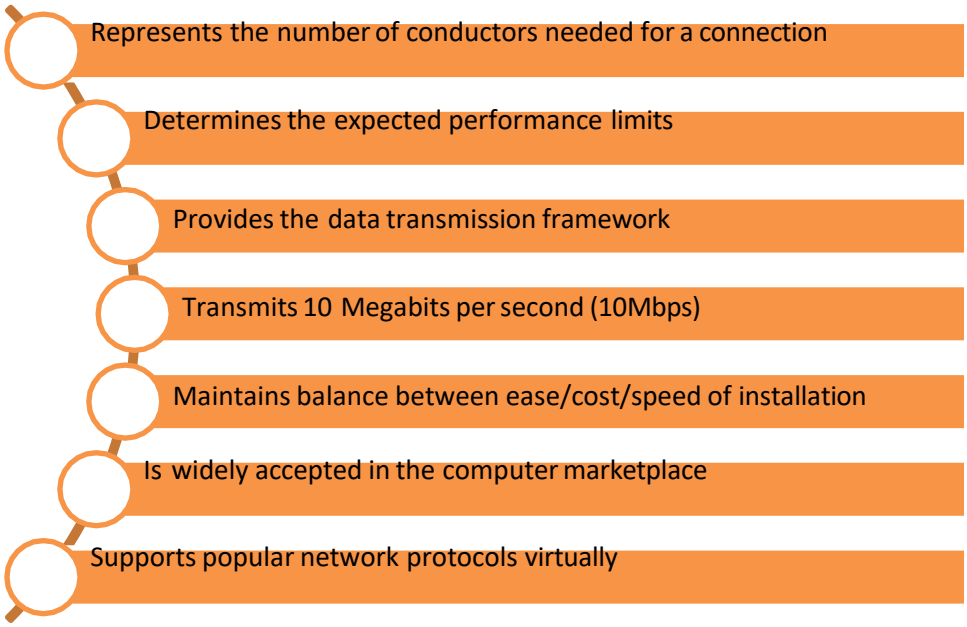


Fig. 2.3.9: Characteristics of Ethernet

The following figure lists the types of Ethernet:

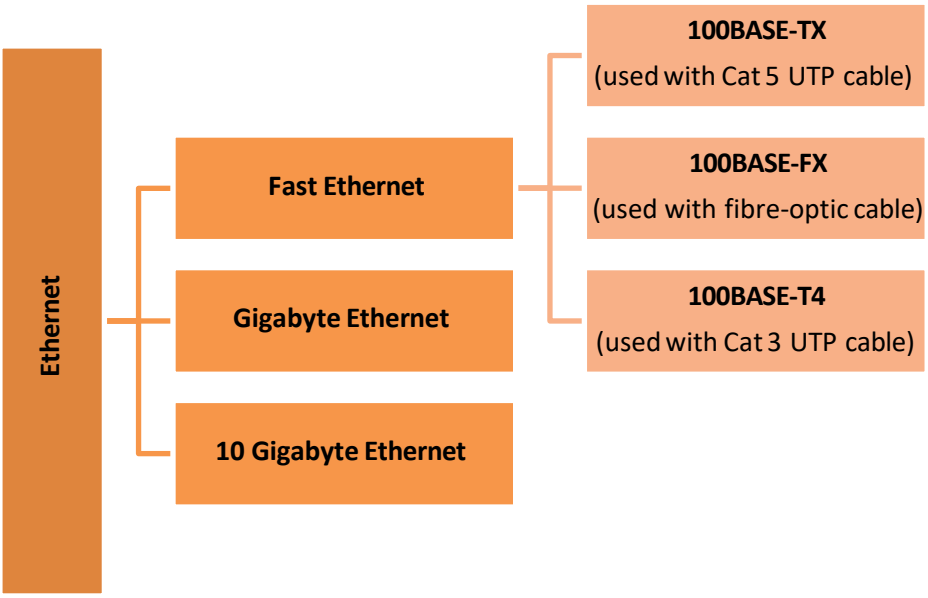


Fig. 2.3.10: Types of Ethernet

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:

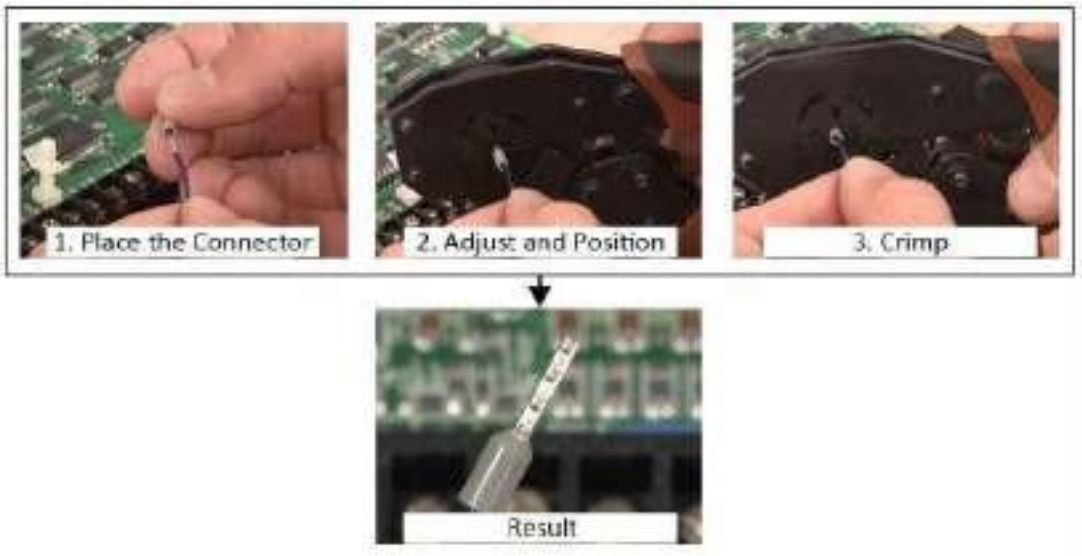


Fig. 2.3.12: Crimping

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:

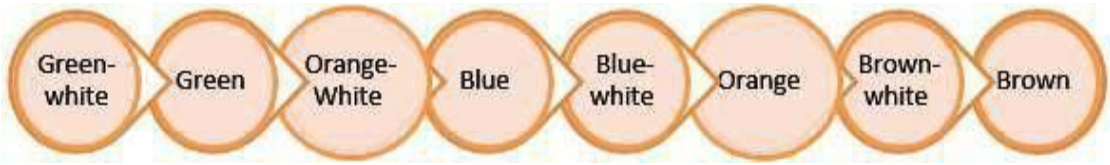


Fig. 2.3.5: Colour code for crimping RJ45 crossover cable

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:

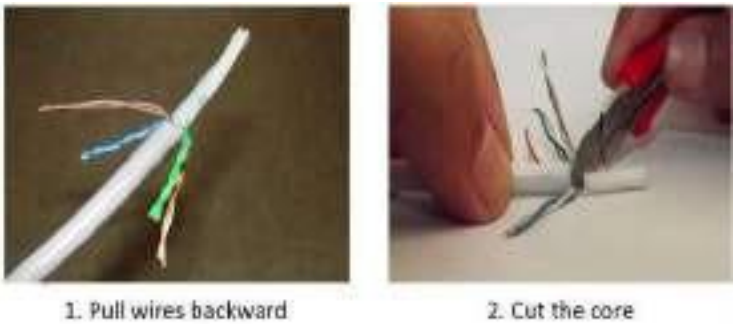


Fig. 2.3.15: Cutting the core

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

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:

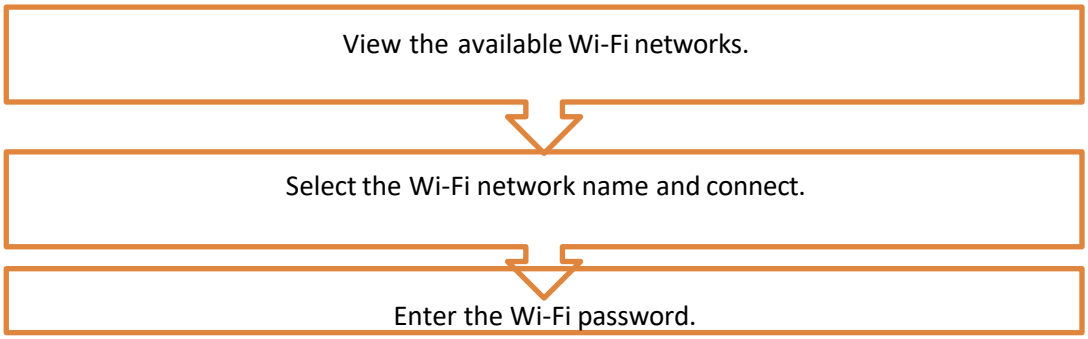
- Connect one end of the Ethernet cable to the Ethernet port as shown in the following image:

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:

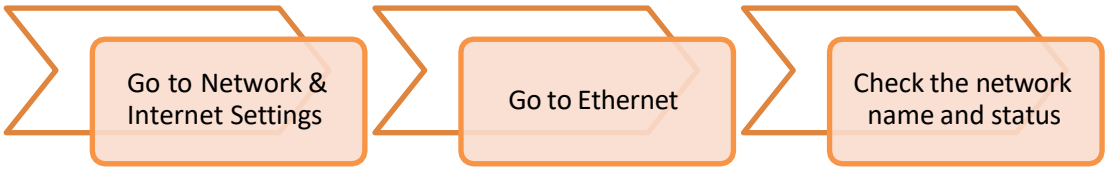


Fig. 2.3.21: Steps to check the network connectivity

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:

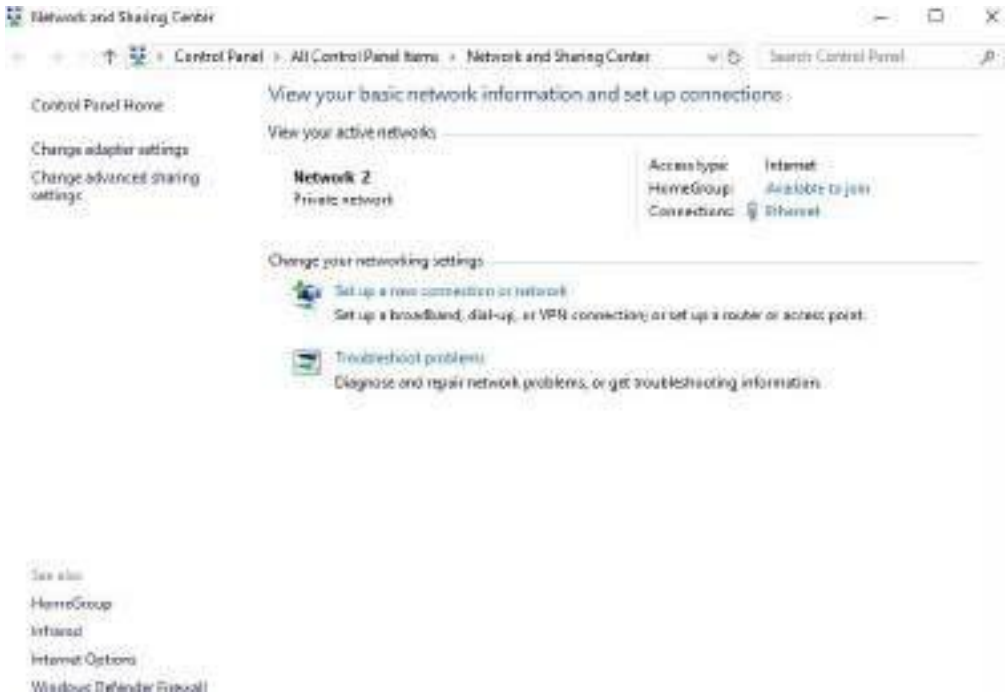


Fig. 2.3.24: Network and Sharing Centre window

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

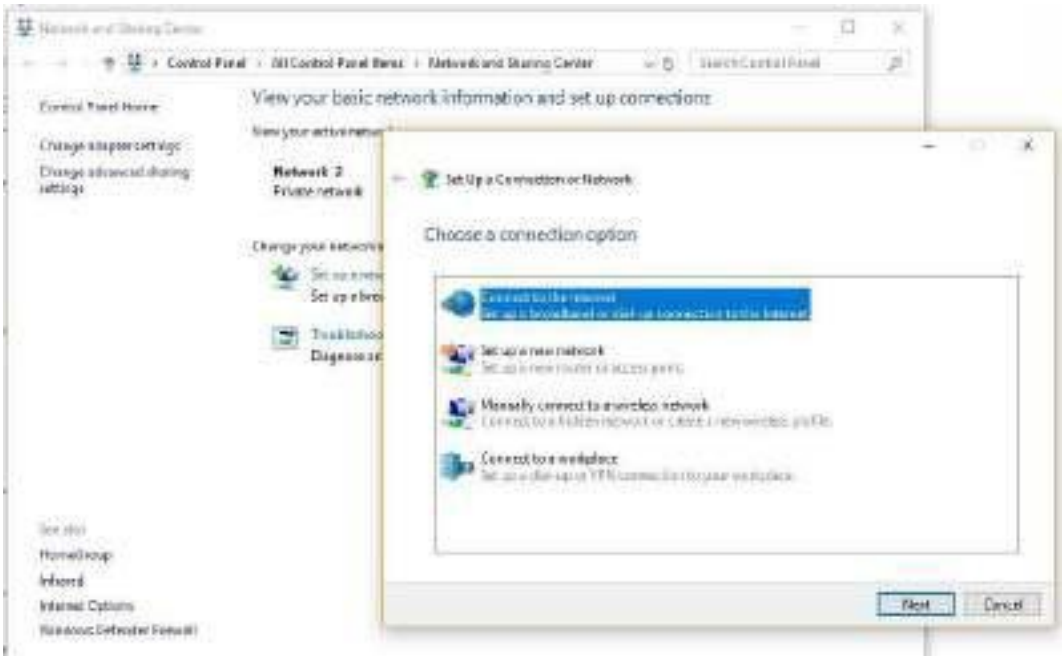


Fig. 2.3.25: Set up a connection window

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

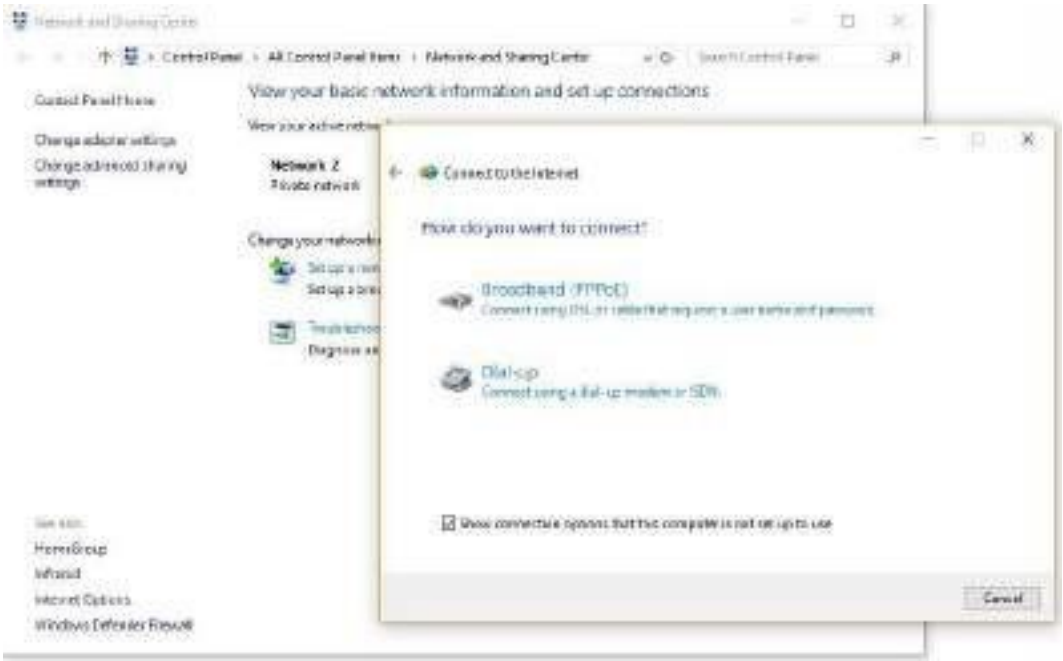


Fig. 2.3.26 Internet connection options

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

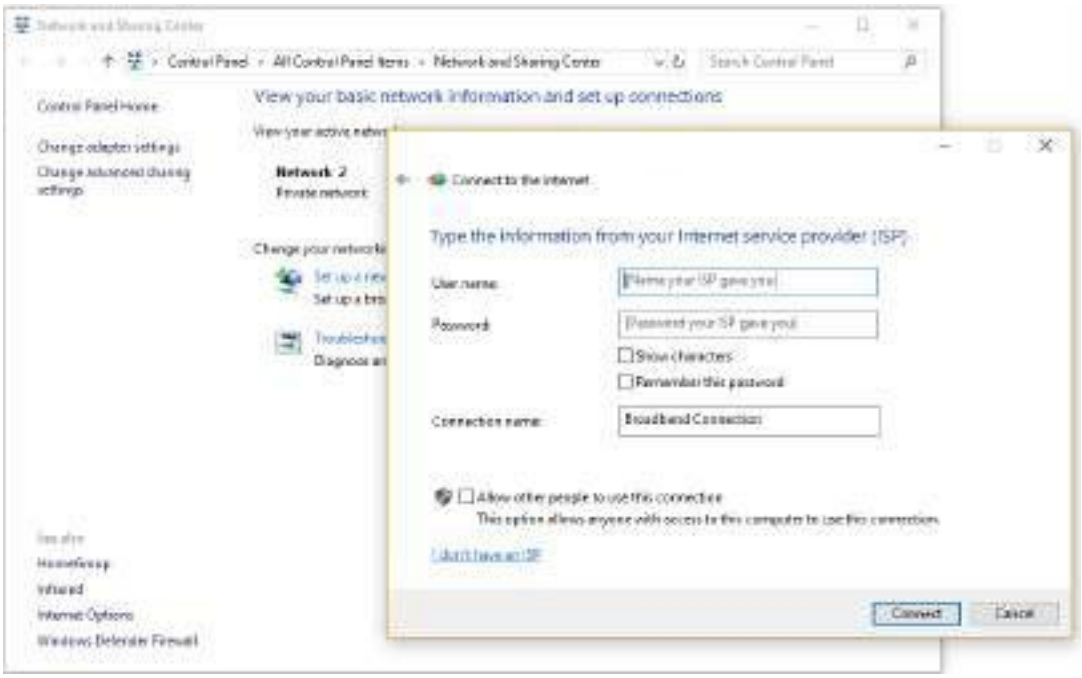


Fig. 2.3.27: Entering connection information

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

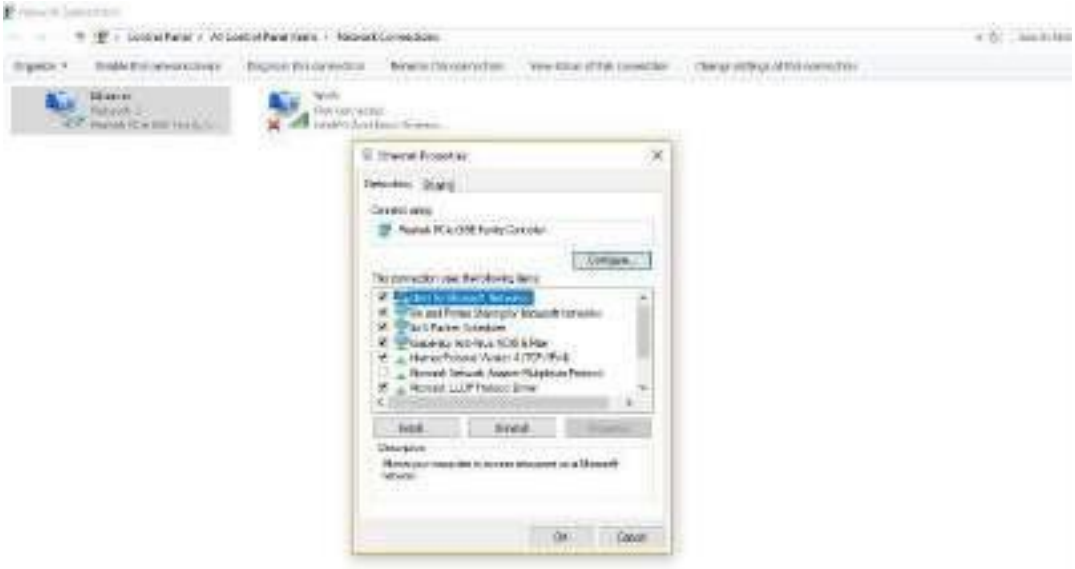


Fig. 2.3.28: Ethernet Properties window

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

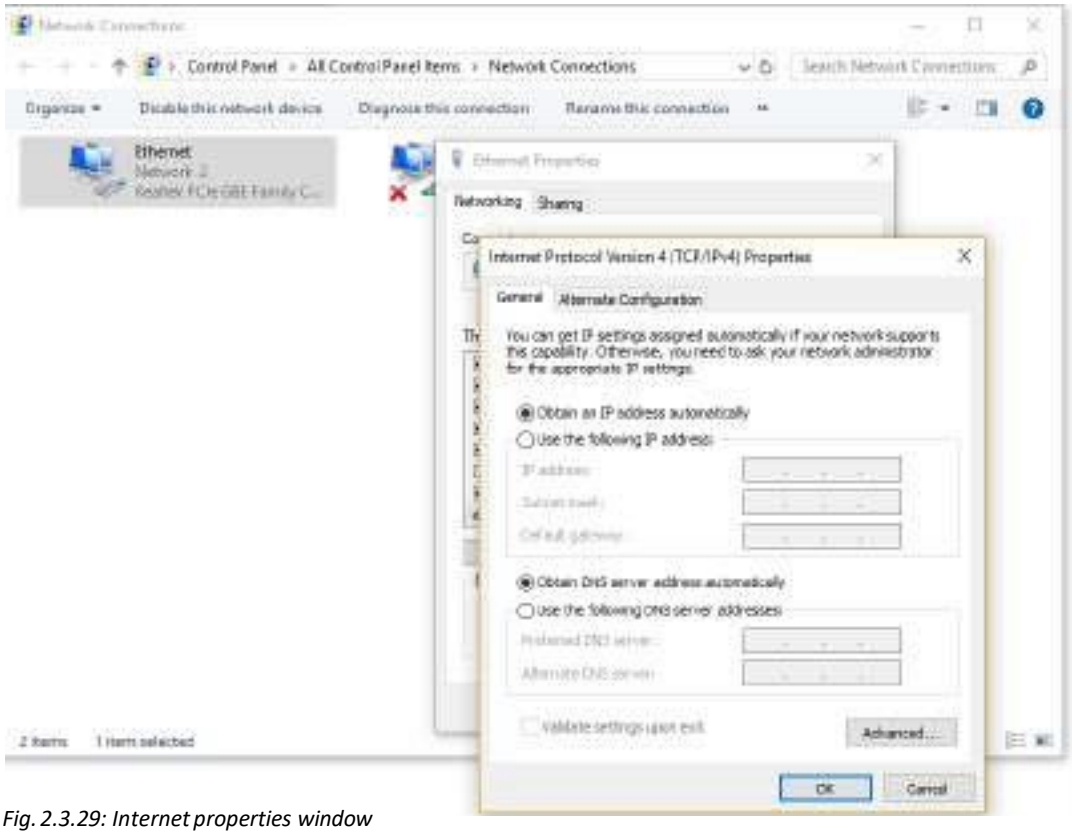


Fig. 2.3.29: Internet properties window

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.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=D7J37mbEj0M

IoT Cloud Framework

UNIT 2.4: Establishing Ethernet Connectivity

Unit Objectives

By the end of this unit, the participants 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
7. Elucidate the workings of Ethernet, TCP/IP, and VPN in IoT installations.

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:

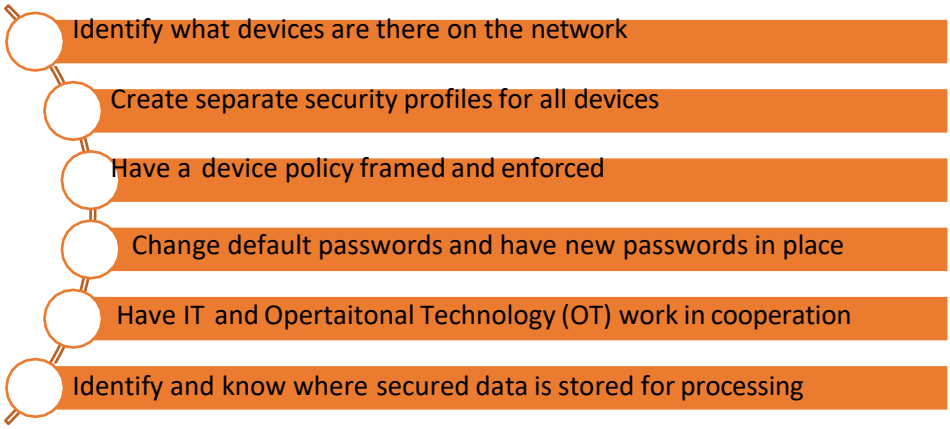


Fig. 2.4.2: Security check list for edge devices

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:

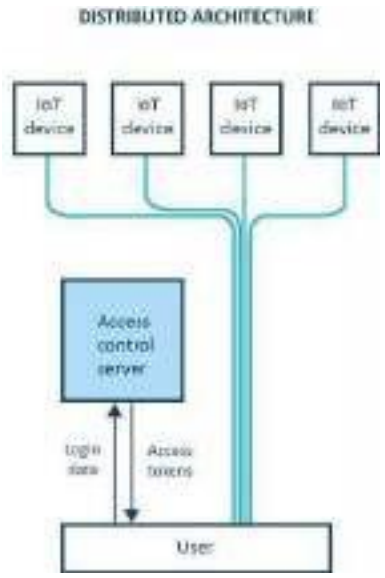


Fig. 2.4.6: Distributed architecture

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:

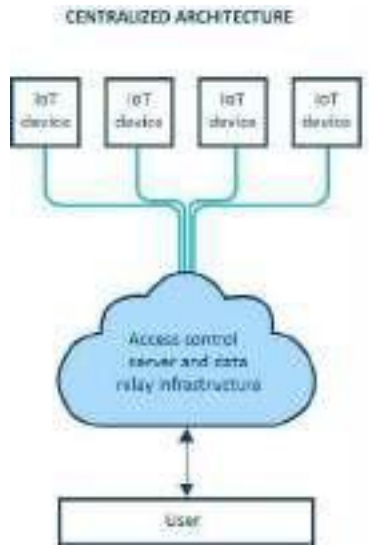


Fig. 2.4.7: Centralized architecture

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:

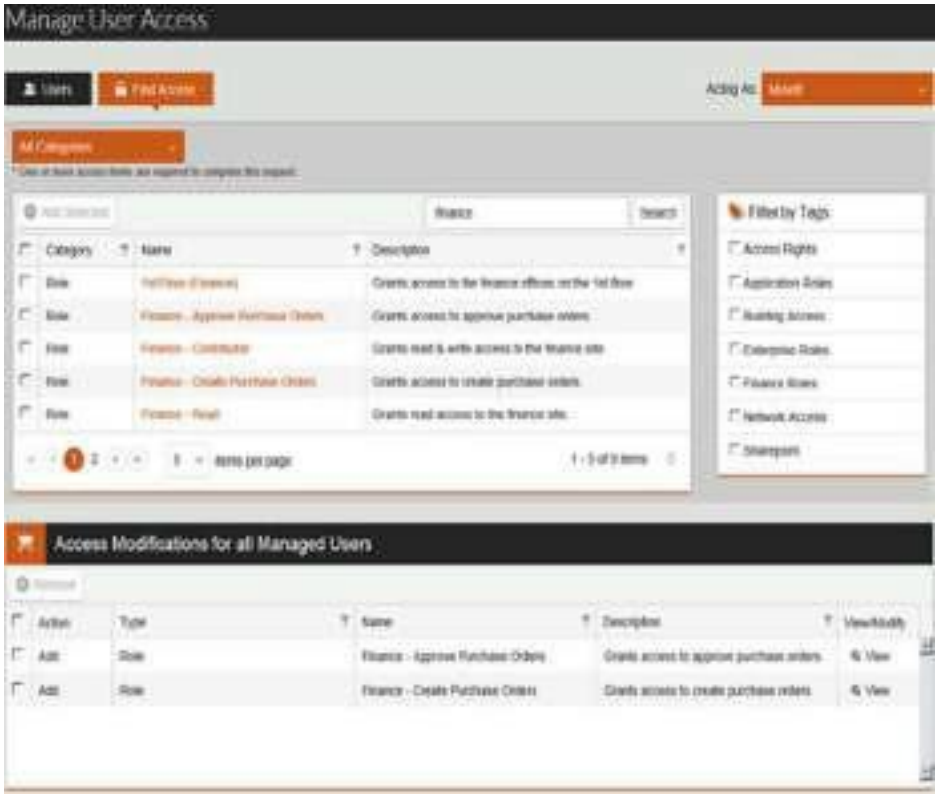


Fig. 2.4.8: Access modification window

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:

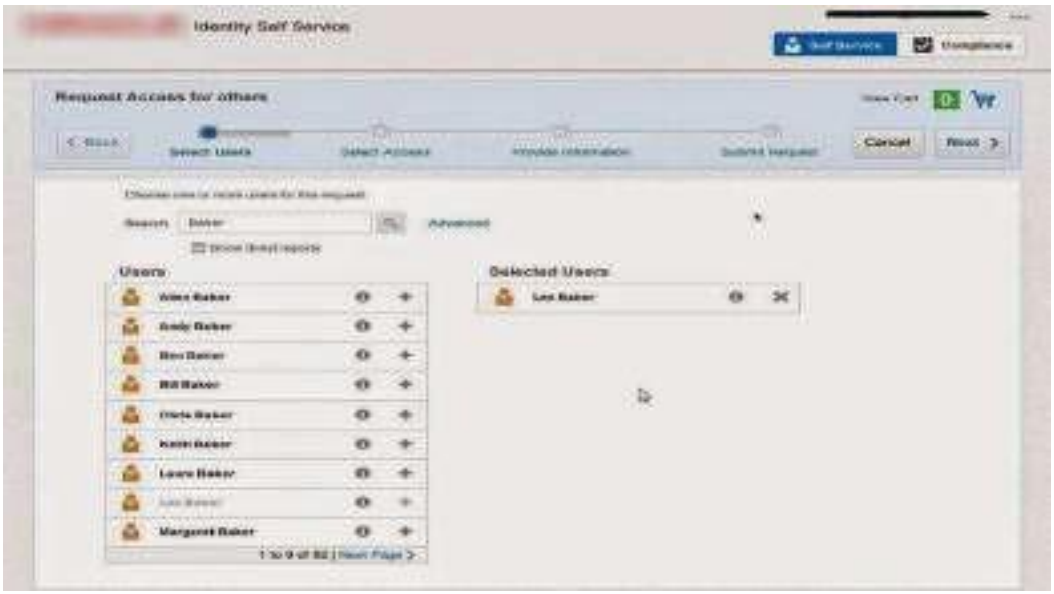


Fig. 2.4.9: Oracle Identity Self Service window

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

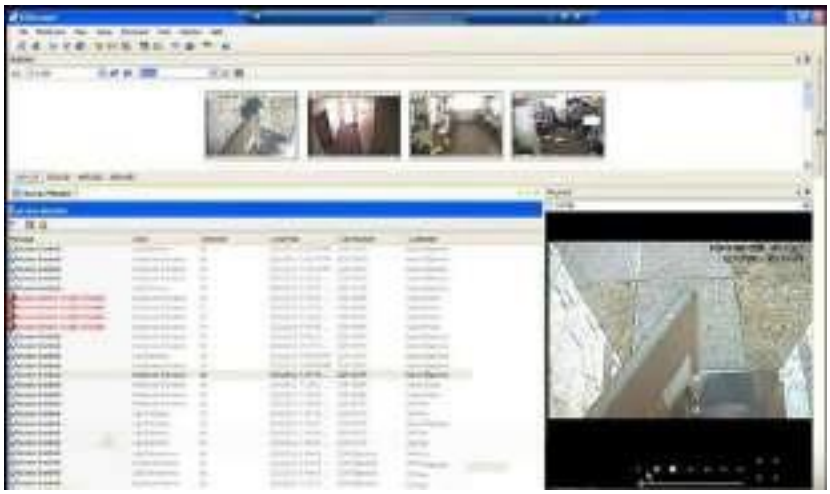


Fig. 2.4.12(b): Access denied

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 timezone settings as per requirement. The following screenshot shows the time settings window:

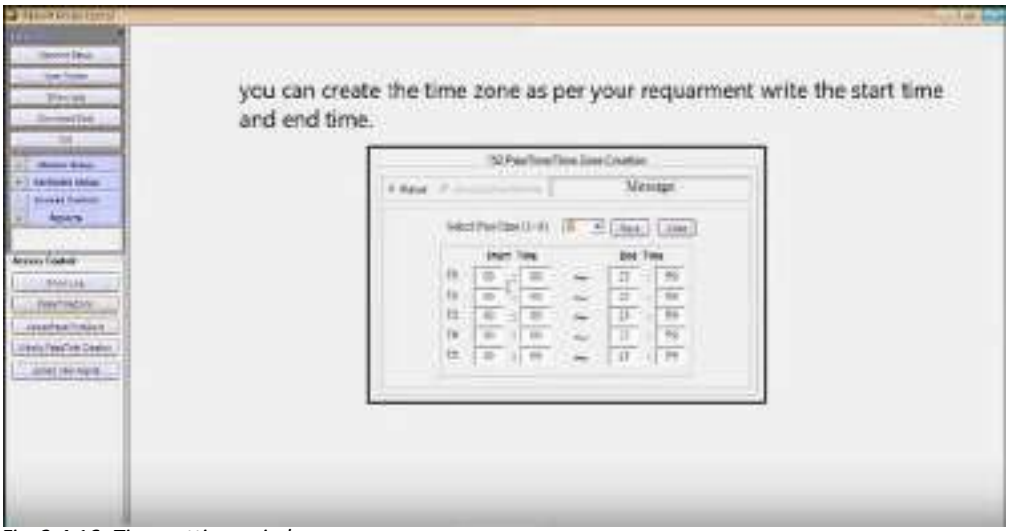


Fig. 2.4.16: Time settings window

- **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 employeedetails. 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:

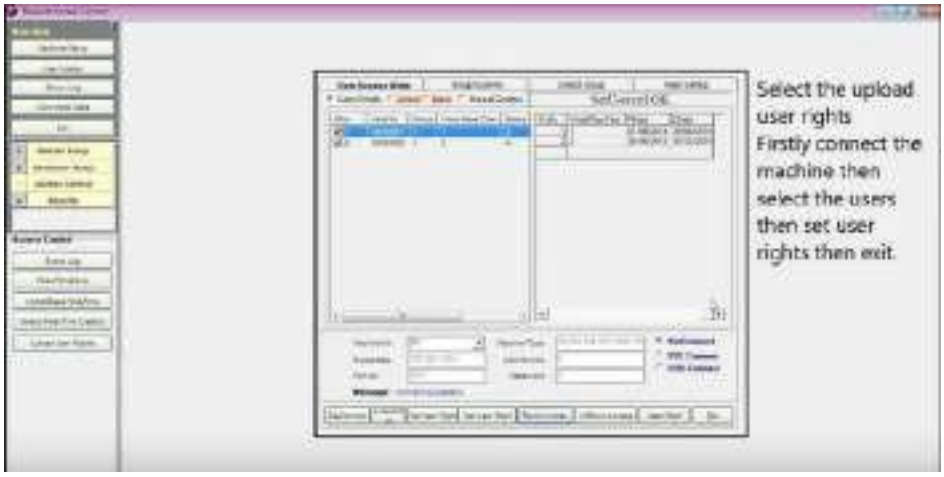


Fig. 2.4.20: Uploading user rights to the device

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

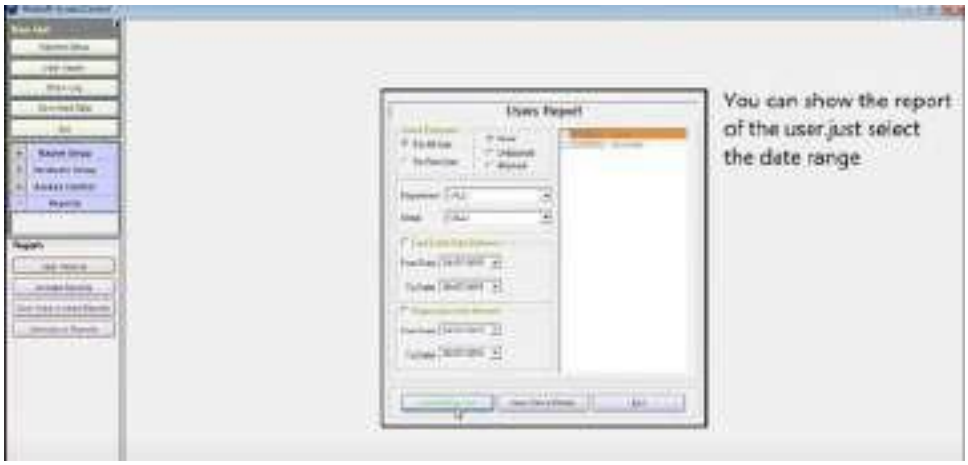


Fig. 2.4.21: Generating report

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:

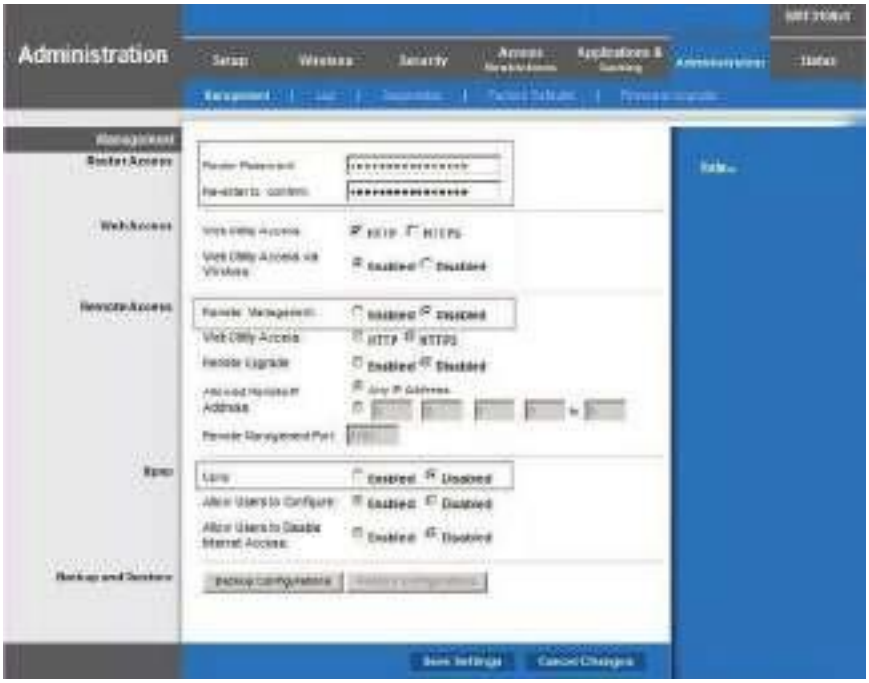


Fig. 2.4.22: Changing the router default settings

- 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:

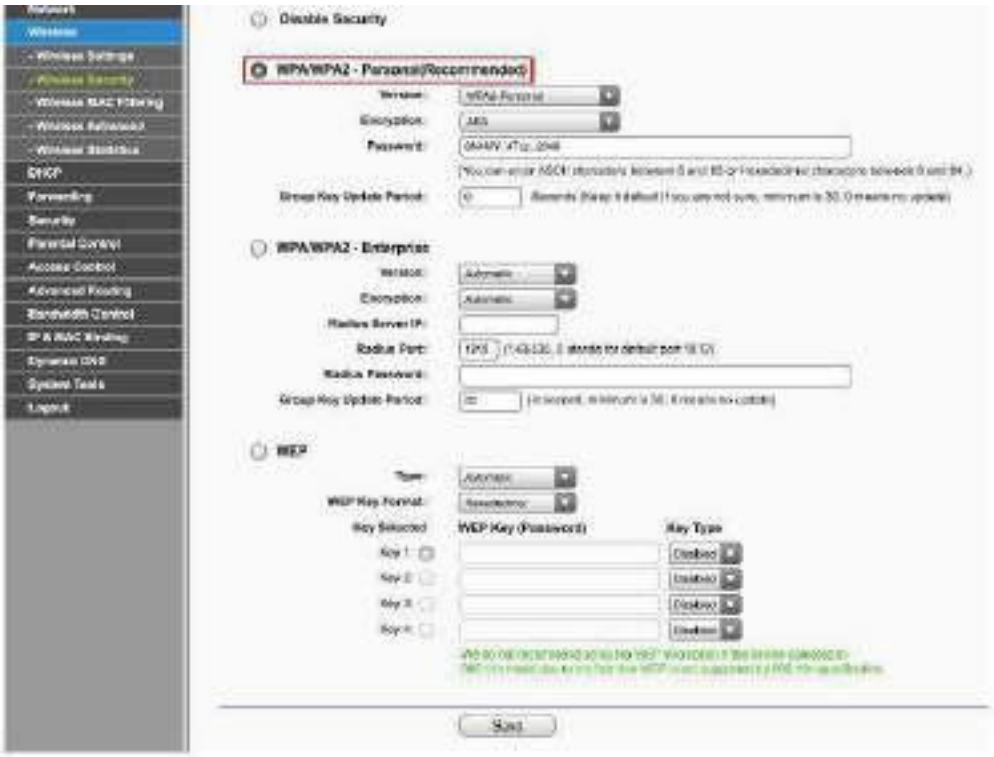


Fig. 2.4.24: WAP2 selected as encryption method

- 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:

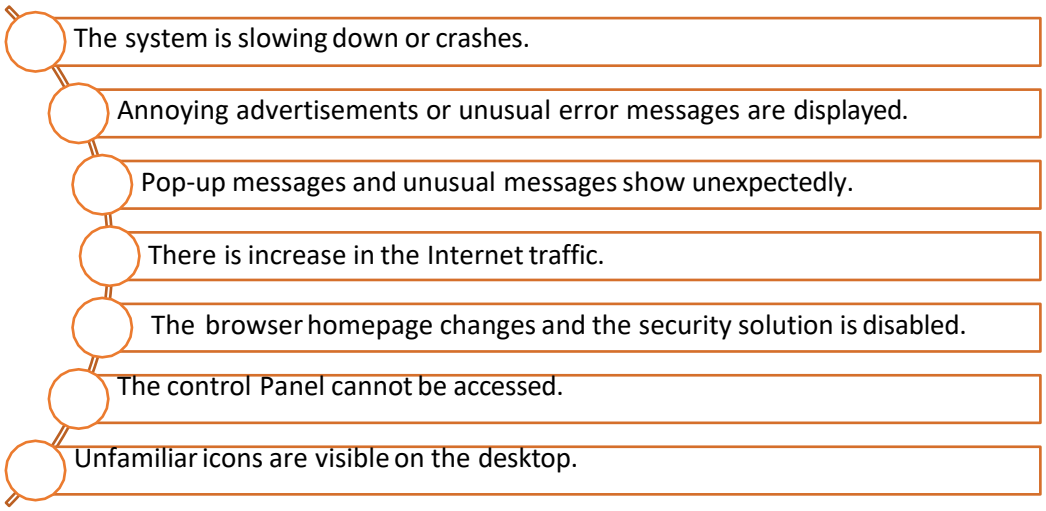


Fig. 2.4.26: Symptoms of malware affecting a device

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

2.4.9 Workings of Ethernet, TCP/IP, and VPN in IoT Installations

Ethernet, TCP/IP, and Virtual Private Networks (VPNs) are fundamental networking technologies in IoT installations, each operating at different levels of the communication stack to ensure physical connectivity, data exchange, and security.

Ethernet

Ethernet is a set of standards that defines the physical and data link layers of a Local Area Network (LAN).

- **Function in IoT:** It provides a reliable, high-speed wired connection for stationary IoT devices in environments like smart factories, commercial buildings, or data centers where stability and security are prioritized over mobility.
- **Working Mechanism:** Data is organized into frames, which include the source and destination Media Access Control (MAC) addresses. These frames are transmitted as electrical signals over physical media (typically Ethernet cables) to a network switch. The switch reads the MAC addresses and forwards the frames only to the intended recipient device on the local network, ensuring efficient and direct communication within the local environment.

- **Benefits:** Key advantages include high reliability, low latency, and robust security within the local network perimeter, which are essential for time-sensitive or critical applications. Power over Ethernet (PoE) functionality also allows a single cable to provide both power and data, simplifying installations.

TCP/IP (Transmission Control Protocol/Internet Protocol)

The TCP/IP suite is the foundational framework for communication across different networks, including the global internet. It is layered on top of the physical network infrastructure (like Ethernet).

- **Function in IoT:** It governs how data is broken down, addressed, transmitted, and reassembled, enabling devices to communicate across diverse networks regardless of their underlying hardware or operating systems.

Working Mechanism:

- **TCP:** Operates at the transport layer and provides reliable, connection-oriented communication. It breaks data into smaller segments, assigns sequence numbers to each, and ensures all segments arrive at the destination in the correct order, requesting retransmission for any lost or corrupted packets. This is ideal for applications where data integrity is crucial, such as firmware updates or data transfers to cloud platforms.
- **IP:** Operates at the internet layer and handles addressing and routing. It assigns each device a unique IP address (e.g., IPv4 or IPv6) and adds a header to each data packet containing the source and destination IP addresses. Routers use this information to determine the most efficient path to forward packets across different networks until they reach their destination.

VPN (Virtual Private Network)

- A VPN is a security solution that extends a private network across a public network (like the internet), allowing devices to send and receive data securely as if they were directly connected to the private network.
- Function in IoT: VPNs provide a crucial layer of security for IoT installations, which often transmit sensitive data over public or cellular networks. They safeguard communication from threats like interception, unauthorized access, and tampering.

Working Mechanism:

- **Secure Tunneling:** The VPN establishes a secure "tunnel" between the IoT device (or gateway) and the network server or cloud platform.
- **Encryption:** All data traveling through this tunnel is encrypted, making it unreadable to anyone who might intercept it. This protects the confidentiality and integrity of the data.
- **Authentication and Access Control:** VPNs authenticate devices to ensure only verified entities can access the private network resources, helping to prevent unauthorized access or spoofing.
- **Remote Access:** They allow developers and administrators to securely monitor, manage, and troubleshoot remote IoT devices from anywhere without exposing the devices to the open internet, which enhances privacy and control.

Notes

UNIT 2.5: Authentication and Access Control Mechanism

Unit Objectives

By the end of this unit, the participants will be able to:

1. Describe the common IoT cybersecurity threats and preventive measures.
2. Discuss the security standards and compliance requirements, including ISO 27001, GDPR, and NIST.

2.5.1 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:

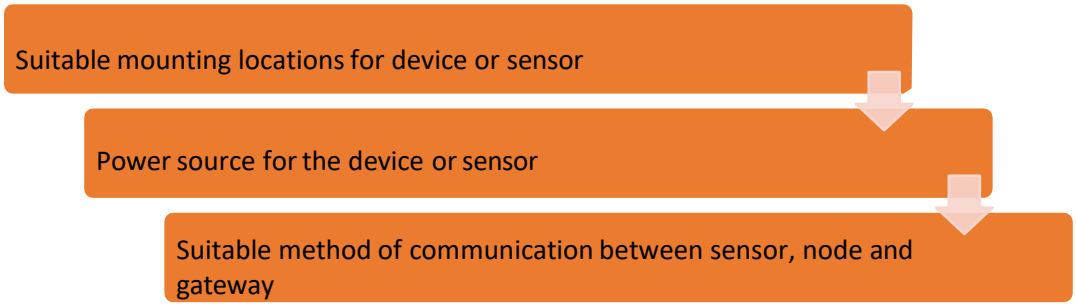


Fig.2.5.2: Site analysis

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:

Location for mounting device:

Building material type:

Power source:

Special site requirement:

Tools and equipment's needed

Equipment required:

Tools 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.

2.5.2 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

2.5.3 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:

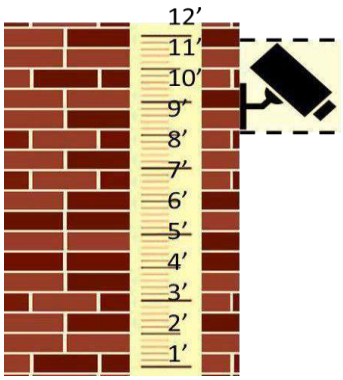


Fig. 2.5.16: Camera installed at an optimum height

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

2.5.4 Common IoT Cybersecurity Threats and Preventive Measures

IoT cybersecurity involves protecting interconnected devices, the networks they use, and the data they generate from theft, damage, or unauthorized access. The expanding attack surface created by billions of IoT devices makes robust security essential.

Common IoT Cybersecurity Threats

IoT devices are susceptible to various threats, primarily due to resource constraints (limited processing power and memory for advanced security features), insecure defaults, and difficulty in patching.

- **Weak Authentication and Default Passwords:** Many devices ship with hardcoded, default credentials ("admin"/"password") that users often fail to change. Attackers can easily exploit these to gain unauthorized access and control devices.
- **Botnets and Malware:** Compromised IoT devices are often recruited into large networks of hijacked devices called botnets. These botnets are then used to launch massive-scale cyberattacks, such as Distributed Denial of Service (DDoS) attacks, which overwhelm target servers with traffic.
- **Eavesdropping and Data Interception:** Data transmitted over insecure or unencrypted networks can be intercepted and read by unauthorized parties. This risk is high in applications involving sensitive information like health data, financial details, or confidential industrial processes.
- **Physical Tampering and Device Hijacking:** Inaccessible or physically unsecured devices can be tampered with. Attackers might physically access ports, extract data, or inject malicious code directly into the device hardware.
- **Insecure Web Interfaces and Cloud Vulnerabilities:** Many IoT devices are managed through web portals or mobile apps which may have software vulnerabilities (e.g., SQL injection, cross-site scripting). Exploiting these allows attackers to compromise the entire system through the management interface.
- **Lack of Patch Management:** Many manufacturers do not provide regular security updates (patches) for their devices, leaving known vulnerabilities unaddressed and exploitable for extended periods.

Preventive Measures and Best Practices

Securing IoT installations requires a multi-layered approach, combining security by design principles with ongoing management and monitoring.

- **Implement "Security by Design":** Security measures should be integrated from the initial planning and design phases, not added as an afterthought. This includes using secure coding practices and choosing hardware with built-in security features.
- **Strong Authentication and Access Control:** Enforce complex, unique passwords, multi-factor authentication (MFA), and the principle of least privilege (granting only necessary permissions). Default passwords should be changed immediately upon installation.
- **Data Encryption (In Transit and At Rest):** All data should be encrypted while being transmitted across networks (using protocols like TLS/SSL) and when stored on the device or in the cloud.
- **Network Segmentation:** Isolate IoT devices from critical corporate networks using VLANs or separate firewall rules. If a device is compromised, segmentation limits the attacker's ability to move laterally across the broader network.

- **Regular Software Updates and Patch Management:** Manufacturers must provide a mechanism for regular, secure firmware updates. Users should promptly install these patches to fix known security vulnerabilities.
- **Continuous Monitoring and Threat Detection:** Use intrusion detection systems and security analytics to monitor network traffic for suspicious activity. Timely detection of anomalies allows for quick incident response.
- **Physical Security:** Where applicable, ensure IoT devices are physically secure to prevent unauthorized access or tampering.
- **Security Audits and Risk Assessments:** Regularly conduct security audits and vulnerability assessments to identify potential weaknesses in the system and address them proactively.

2.5.5 Iot Security Standards and Compliance Requirements

IoT security standards and compliance requirements provide essential frameworks for organizations to manage risks, protect data, and meet legal obligations. Adhering to standards like ISO 27001, GDPR, and NIST guidelines helps organizations establish robust security postures and build trust with customers and regulators.

ISO 27001

ISO/IEC 27001, an internationally recognized standard, outlines the requirements for establishing, implementing, maintaining, and continuously improving an Information Security Management System (ISMS).

- **Focus:** It takes a risk-management approach to security, requiring organizations to identify potential threats and vulnerabilities and implement controls to mitigate them. It covers all aspects of an organization's information security, not just the technical elements.
- **Role in IoT:** For IoT installations, ISO 27001 helps structure the management of security across the entire ecosystem, from device design and deployment to data transmission and storage. It ensures security risks related to devices, networks, and cloud platforms are systematically addressed.

Key Requirements:

- Risk Assessment: Mandates a thorough assessment of information security risks relevant to the IoT environment.
- Controls Implementation: Requires the implementation of appropriate security controls (from a list of suggestions within the standard) to manage identified risks.
- Continuous Improvement: Promotes a Plan-Do-Check-Act (PDCA) cycle to ensure the ISMS evolves with new threats and changes in technology.

GDPR (General Data Protection Regulation)

- The General Data Protection Regulation (GDPR) is a stringent data privacy and security law that governs how organizations handle the personal data of individuals within the European Union (EU) and the European Economic Area (EEA).

- Focus: It protects individuals' fundamental right to data privacy and grants them control over their personal information.
- Role in IoT: IoT systems often collect vast amounts of personal data (location, health metrics, behavioral patterns). GDPR mandates strict accountability for how this data is collected, processed, and stored.

Key Requirements:

- Lawfulness, Fairness, and Transparency: Data processing must be lawful, fair to the individual, and transparent.
- Data Minimization and "Privacy by Design": Organizations must collect only necessary data and integrate privacy considerations into the design of their IoT systems from the outset.
- Individual Rights: Grants individuals rights to access, correct, erase, and transfer their data.
- Data Breach Notification: Mandates reporting certain data breaches to authorities and affected individuals within 72 hours. Non-compliance can result in substantial fines.

NIST (National Institute of Standards and Technology) Frameworks

NIST provides a range of cybersecurity guidelines and frameworks that are widely adopted voluntarily, particularly in the United States. They offer practical, actionable guidance for managing cybersecurity risks.

- **Focus:** NIST frameworks are designed to improve an organization's ability to prevent, detect, and respond to cyber attacks.
- **Role in IoT:** NIST has developed specific guidelines for IoT security, such as the NIST Cybersecurity Framework (CSF) and the Core Cybersecurity Capabilities for Managed Service Providers (NIST SP 800-161 Rev. 1). These provide a structured approach to securing diverse IoT ecosystems.
- **Key Requirements/Functions (from the CSF):** The framework is structured around five core functions that help prioritize and manage security activities:
- **Identify:** Understand the assets, data, and risks within the IoT system.
- **Protect:** Implement safeguards to ensure the delivery of critical services (e.g., access control, training).
- **Detect:** Implement mechanisms to identify the occurrence of a cybersecurity event (e.g., monitoring, anomaly detection).
- **Respond:** Develop plans and capabilities to act when a security incident is detected.
- **Recover:** Implement plans for resilience and restoring services impaired during a security incident.

Notes

UNIT 2.6: Mounting the Devices at Desired Locations

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to mount IoT devices securely using industry-approved techniques and tools.
2. Demonstrate how to identify various types of microprocessor boards and microcontrollers used in IoT installations.
3. Show how to check the components, pin configurations, and interconnectivity provisions of microcontroller boards.
4. Explain the process of installing and configuring smart meters, connected cameras, and industrial IoT devices.

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:

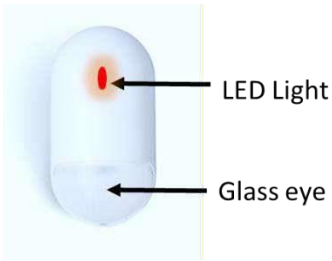
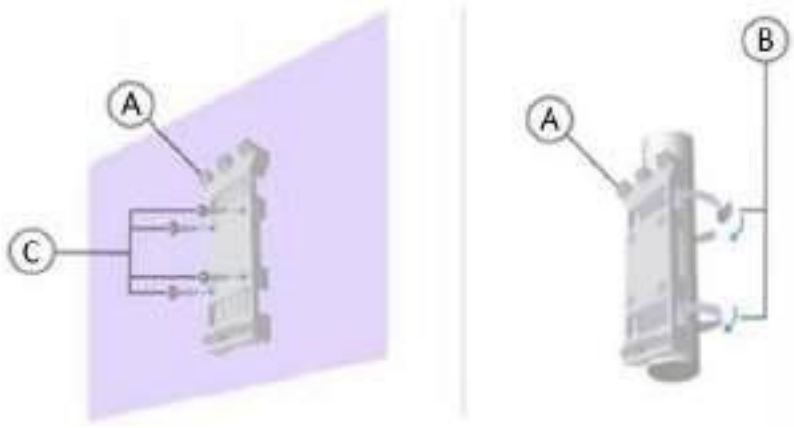


Fig. 2.6.5: Placing of motion detector sensor

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:

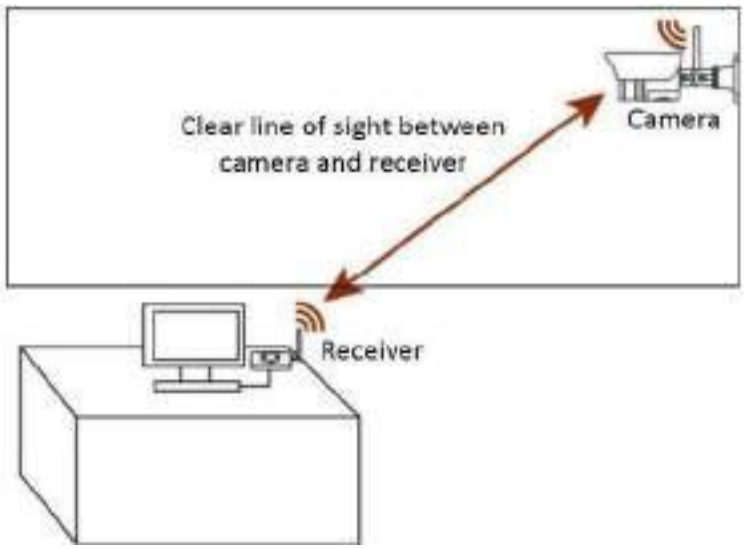


Fig. 2.6.8: Line of sight communication inside a room

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

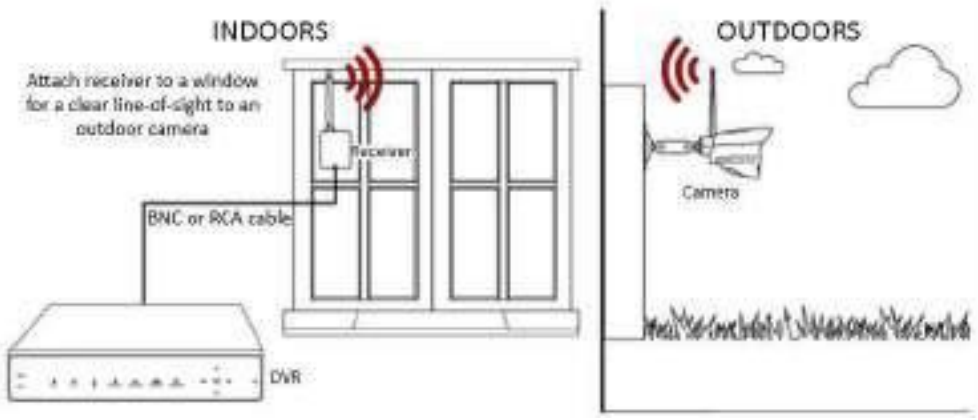


Fig. 2.6.9: Line of sight between outdoor and indoor areas

- **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:

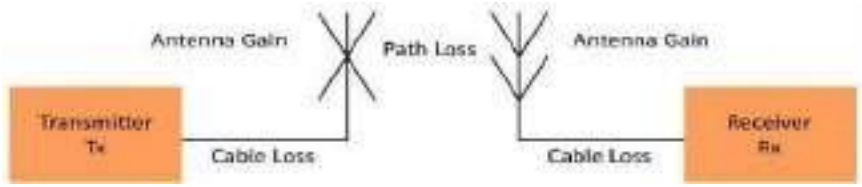


Fig. 2.6.10: Drop in signal strength

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:

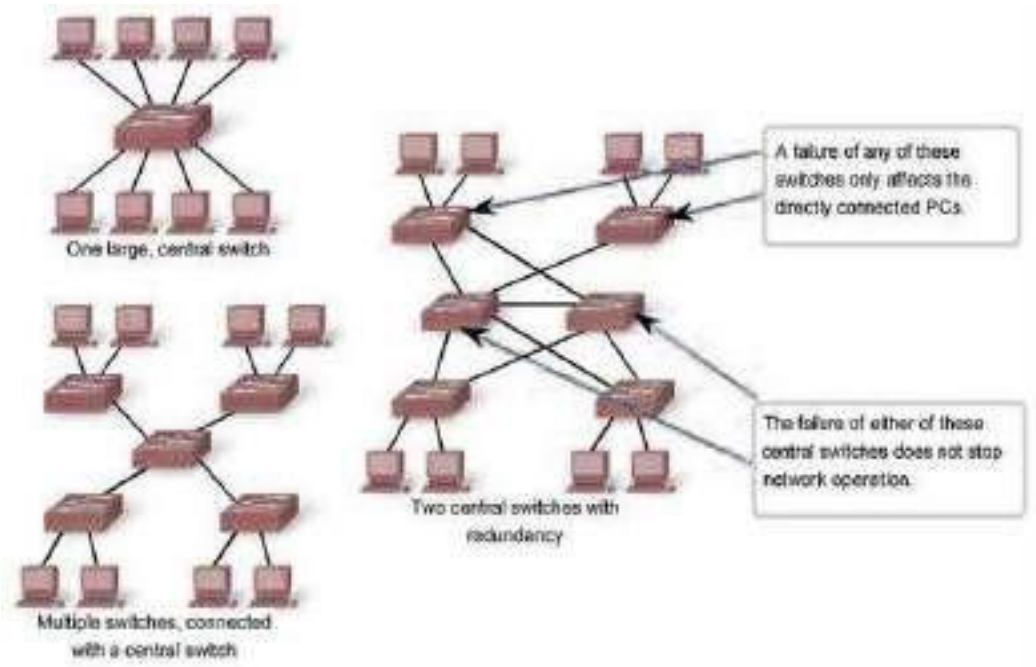


Fig. 2.6.11: Switch selection for a LAN network

- **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:

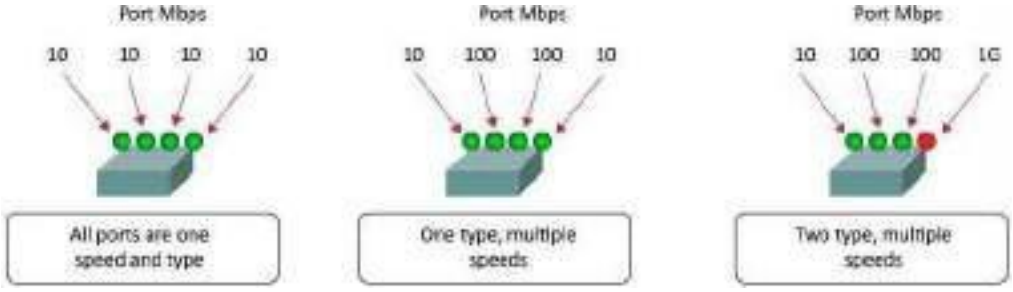


Fig. 2.6.12: Speed factor for selecting switch for LAN network

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:

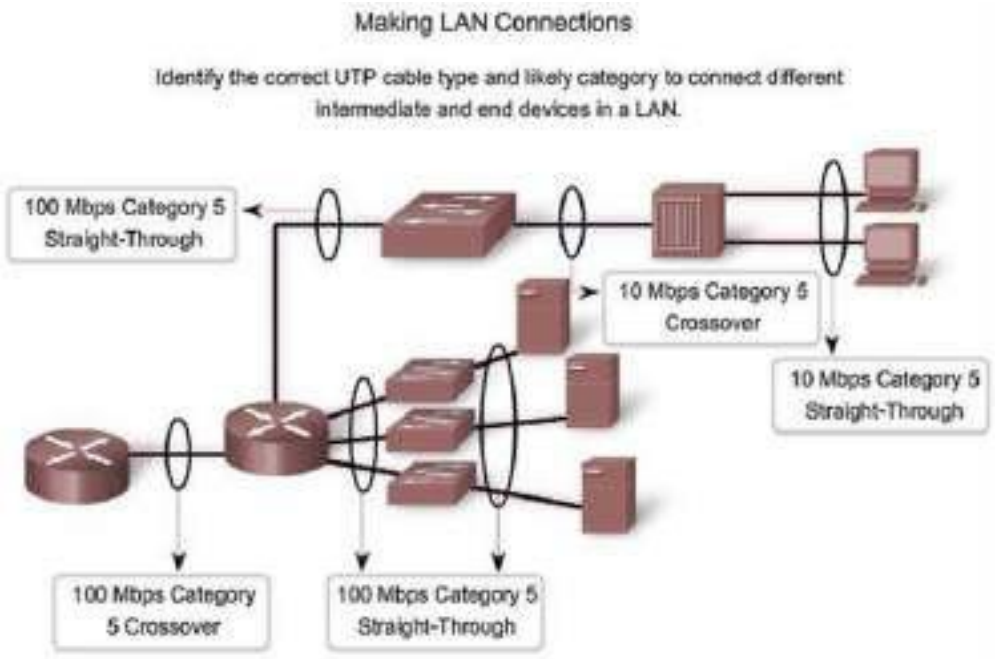


Fig. 2.6.13: Cabling set up for a LAN network

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:

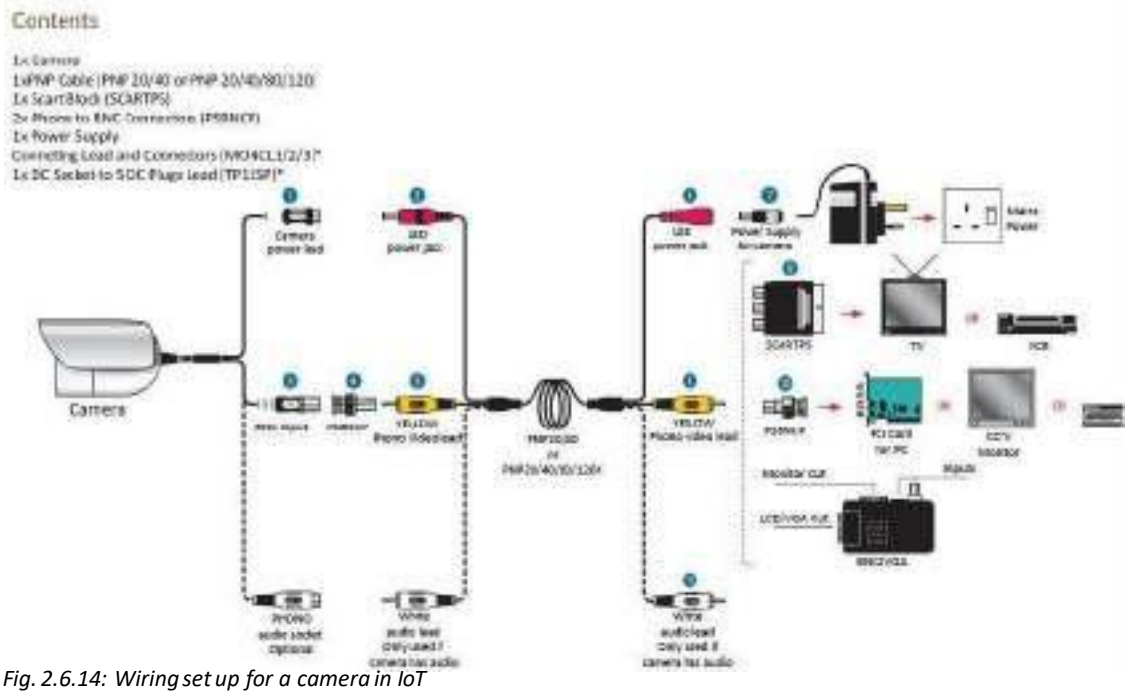


Fig. 2.6.14: Wiring set up for a camera in IoT

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

Notes

UNIT 2.7: Performing Checks and Connections

Unit Objectives

By the end of this unit, the participants will be able to:

1. Discuss the impact of signal interference, data packet loss, and power failures on IoT performance.
2. Elucidate the tools and techniques for RF signal strength measurement and spectrum analysis.
3. Explain the hazards of RF radiation exposure and the appropriate safety procedures.
4. Demonstrate how to perform signal strength testing and RF spectrum analysis to optimize IoT device placement.
5. Explain proper handling, grounding, and safety measures during IoT device installations.

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:

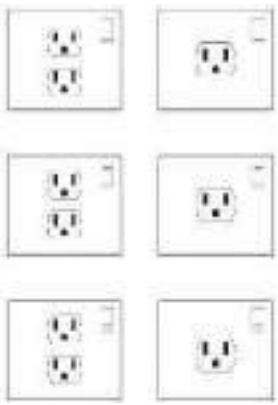


Fig. 2.7.3: Plug point with grounding pin

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:

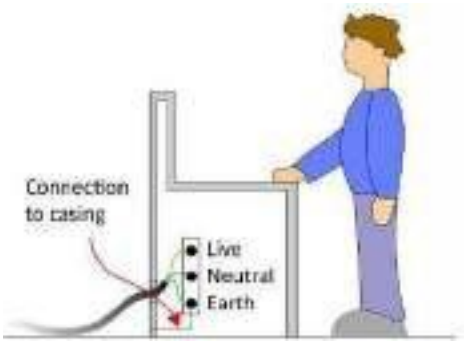


Fig. 2.7.4: Grounding of an electrical connection

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:

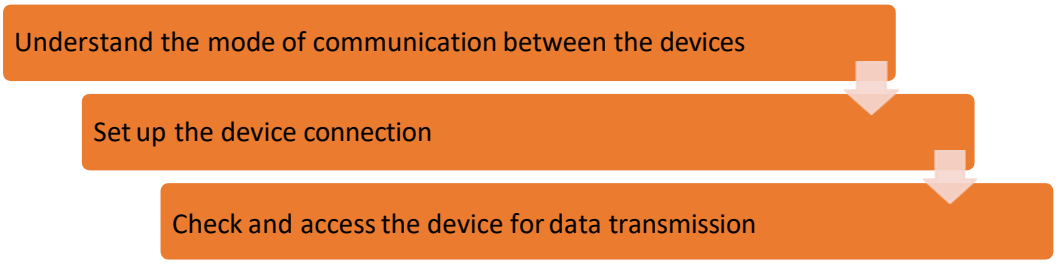


Fig. 2.7.5: Steps in IoT data transmission set up

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:

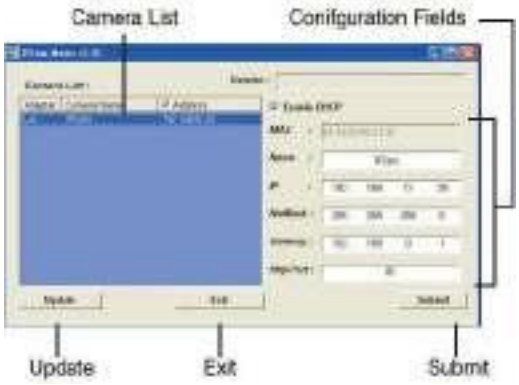


Fig. 2.7.6: Configuration of device through PC

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.

2.7.5 RF Signal Strength Measurement and Spectrum Analysis

RF signal strength measurement and spectrum analysis are critical for the design, deployment, and maintenance of robust IoT wireless networks. These processes use specialized tools and techniques to identify signal quality, pinpoint sources of interference, and ensure reliable connectivity.

Tools for RF Measurement and Analysis

- Spectrum Analyzers: The primary tool for RF analysis, spectrum analyzers measure and display the magnitude (power/amplitude) of signals across a defined range of frequencies. They are essential for visualizing the spectral environment and detecting unwanted signals or noise.
    - o Swept-Tuned Analyzers: The traditional type, well-suited for stable, continuous signals. They sweep through a range of frequencies to measure amplitude at each point.
    - o Real-Time Spectrum Analyzers (RTSAs): These instruments can capture and analyze transient, dynamic, or intermittent signals by processing data in real-time without "blind spots". They are ideal for troubleshooting modern, complex wireless systems where signals may burst intermittently.
    - o Vector Signal Analyzers (VSAs): These go beyond amplitude to measure both the magnitude and phase of a signal, enabling the analysis of complex digital modulations (e.g., Wi-Fi, LTE).

  - Handheld/Portable Analyzers: Compact, battery-powered versions of the above, used for field work, site surveys, and interference hunting outside of a lab environment.
- RF Power Meters/Sensors: Simpler tools that provide a direct numerical measurement of signal power (typically in dBm or Watts), often with high accuracy for stable signals, but without the detailed frequency spectrum display of a spectrum analyzer.
- Network Analyzers (VNAs): Primarily used in the lab to characterize RF components (like antennas, filters, and cables) by measuring how they pass or reflect RF energy, including parameters like gain, return loss, and S-parameters.
- RF Signal Generators: Used to create controlled test signals with specific power, frequency, and modulation parameters to test the performance of IoT receivers or other components.

Techniques for RF Measurement and Analysis

- Received Signal Strength Indication (RSSI): A simple metric available in most wireless devices that indicates the power level of a received radio signal. While useful for basic coverage mapping (e.g., in-building Wi-Fi signal strength is good between -50 dBm and -67 dBm), it lacks the precision and detail of dedicated test equipment.
- Spectrum Monitoring and Interference Hunting: Using a spectrum analyzer to scan a specific frequency band to identify sources of interference (unwanted signals that disrupt desired communications). This involves observing amplitude versus frequency plots to spot abnormal peaks or spectral components.
- Occupied Bandwidth (OBW) and Channel Power Measurement: Techniques used to ensure that a transmitted signal stays within its assigned frequency channel and does not "leak" into adjacent channels, which is essential for regulatory compliance.
- Over-the-Air (OTA) Testing: For modern devices without a direct RF connector, testing is often done over the air within a shielded chamber to measure total radiated power (TRP) and total isotropic sensitivity (TIS) under real-world conditions.
- Kriging and Spatial Mapping: Geostatistical techniques used to interpolate RF signal strength levels at unsampled locations to create detailed, high-resolution coverage maps of an area, which accounts for physical obstructions like walls and furniture.
- Signal-to-Noise Ratio (SNR) Analysis: A measurement technique to quantify the ratio of desired signal power to background noise power. A high SNR is crucial for reliable communication and accurate data transfer in IoT applications.

2.7.6 Radio Frequency (RF) Radiation Hazards

Radio Frequency (RF) radiation hazards primarily stem from the thermal effects of exposure to very high levels of RF energy, which can heat biological tissue and cause burns or other tissue damage. Appropriate safety procedures focus on minimizing exposure through engineering controls, administrative measures, and personal protective equipment.

Hazards of RF Radiation Exposure

RF energy is a type of non-ionizing radiation, meaning it does not have enough energy to damage DNA directly. The established health effects are associated with high-intensity, short-term exposure, typically encountered in occupational settings near powerful transmitters, rather than the low levels found in everyday public environments from sources like mobile phones or Wi-Fi routers.

- Thermal Injuries: The main hazard is the rapid heating of biological tissue, similar to how a microwave oven heats food. The body can dissipate small amounts of heat, but excessive heat absorption can cause burns or heat stress (headache, dizziness, nausea).
- Vulnerable Tissues: Tissues with limited blood flow, such as the eyes (cornea) and testes, are particularly vulnerable to thermal damage because they cannot dissipate excess heat effectively. High-level exposure could potentially cause cataracts or sterility.
- Electromagnetic Interference (EMI): High levels of RF radiation can interfere with electronic equipment, including sensitive medical devices like cardiac pacemakers, implantable defibrillators, or hearing aids, leading to potential malfunction or failure.
- Electrical Shocks and Fires: RF energy can induce currents in conductive materials (e.g., metal tools, wiring). Contact with these objects can cause electrical shocks or create sparks, which pose a fire and explosion risk in flammable environments.

Appropriate Safety Procedures

Safety procedures aim to keep exposure levels below established Maximum Permissible Exposure (MPE) limits set by regulatory bodies such as the FCC (Federal Communications Commission) and the ICNIRP (International Commission on Non-Ionizing Radiation Protection).

- Distance and Time Management: Exposure levels decrease dramatically with distance from the source.
  - Maximize Distance: Maintain a safe distance from active antennas and high-power RF sources. Follow any posted signs or barriers.
  - Limit Exposure Time: Minimize the duration of time spent in areas with high RF fields.
- Administrative and Engineering Controls:
  - Power Down Equipment: If work is required in an area with high RF fields, contact the site owner to request the transmitter be turned off or switched to a low-power auxiliary transmitter. Use proper lockout/tagout procedures.
  - Warning Signs and Training: Post clear, standardized warning signs in hazardous areas. Ensure all workers in proximity to RF sources receive proper safety training and understand the associated risks and procedures.
  - Shielding: Use shielding materials (e.g., proper cabinetry, protective screens) around high-exposure areas to contain radiation leakage.
- Personal Monitoring and Protective Equipment (PPE):
  - Personal RF Monitors: Workers who regularly work near RF sources should be equipped with personal RF meters that alert them when exposure levels approach or exceed safe limits.
  - Protective Clothing: Full RF protective suits (hood, overshoes, socks, gloves) should only be used as a last resort when engineering and administrative controls are not feasible. Monitors should be worn outside the protective clothing to verify its effectiveness.
- Device Management:
  - Medical Device Interference: Individuals with implanted medical devices should consult their physician and device manufacturer for precautions and avoid placing RF devices (like mobile phones) in pockets close to the implant site.
  - Proper Maintenance: Ensure all RF-emitting equipment is well-maintained and free from damage, especially door seals on devices like microwave ovens, to prevent accidental leakage.

  - Handheld/Portable Analyzers: Compact, battery-powered versions of the above, used for field work, site surveys, and interference hunting outside of a lab environment.
- RF Power Meters/Sensors: Simpler tools that provide a direct numerical measurement of signal power (typically in dBm or Watts), often with high accuracy for stable signals, but without the detailed frequency spectrum display of a spectrum analyzer.
- Network Analyzers (VNAs): Primarily used in the lab to characterize RF components (like antennas, filters, and cables) by measuring how they pass or reflect RF energy, including parameters like gain, return loss, and S-parameters.
- RF Signal Generators: Used to create controlled test signals with specific power, frequency, and modulation parameters to test the performance of IoT receivers or other components.

Techniques for RF Measurement and Analysis

- Received Signal Strength Indication (RSSI): A simple metric available in most wireless devices that indicates the power level of a received radio signal. While useful for basic coverage mapping (e.g., in-building Wi-Fi signal strength is good between -50 dBm and -67 dBm), it lacks the precision and detail of dedicated test equipment.
- Spectrum Monitoring and Interference Hunting: Using a spectrum analyzer to scan a specific frequency band to identify sources of interference (unwanted signals that disrupt desired communications). This involves observing amplitude versus frequency plots to spot abnormal peaks or spectral components.
- Occupied Bandwidth (OBW) and Channel Power Measurement: Techniques used to ensure that a transmitted signal stays within its assigned frequency channel and does not "leak" into adjacent channels, which is essential for regulatory compliance.
- Over-the-Air (OTA) Testing: For modern devices without a direct RF connector, testing is often done over the air within a shielded chamber to measure total radiated power (TRP) and total isotropic sensitivity (TIS) under real-world conditions.
- Kriging and Spatial Mapping: Geostatistical techniques used to interpolate RF signal strength levels at unsampled locations to create detailed, high-resolution coverage maps of an area, which accounts for physical obstructions like walls and furniture.
- Signal-to-Noise Ratio (SNR) Analysis: A measurement technique to quantify the ratio of desired signal power to background noise power. A high SNR is crucial for reliable communication and accurate data transfer in IoT applications.

Notes

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

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to set up appropriate connectivity options on microcontroller boards for seamless data transfer.
2. Show how to use compatible cable connectors and microcontrollers to link IoT devices with data transfer interfaces.
3. Demonstrate how to select appropriate short-range and long-range communication protocols for IoT applications.
4. Show how to determine the functions, characteristics, and applicability of different IoT sensors and actuators.
5. Demonstrate how to validate data transfer between devices using system logs, LED indicators, or real-time dashboards.

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:**

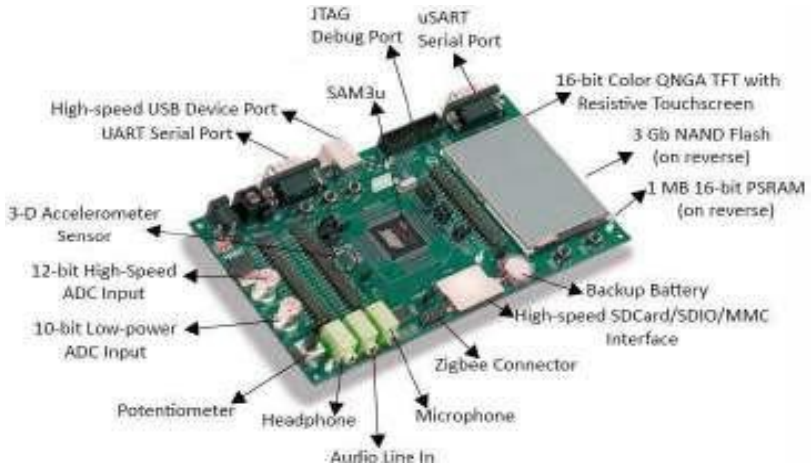


Fig. 2.8.1: A microcontroller board with different connectivity ports

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:

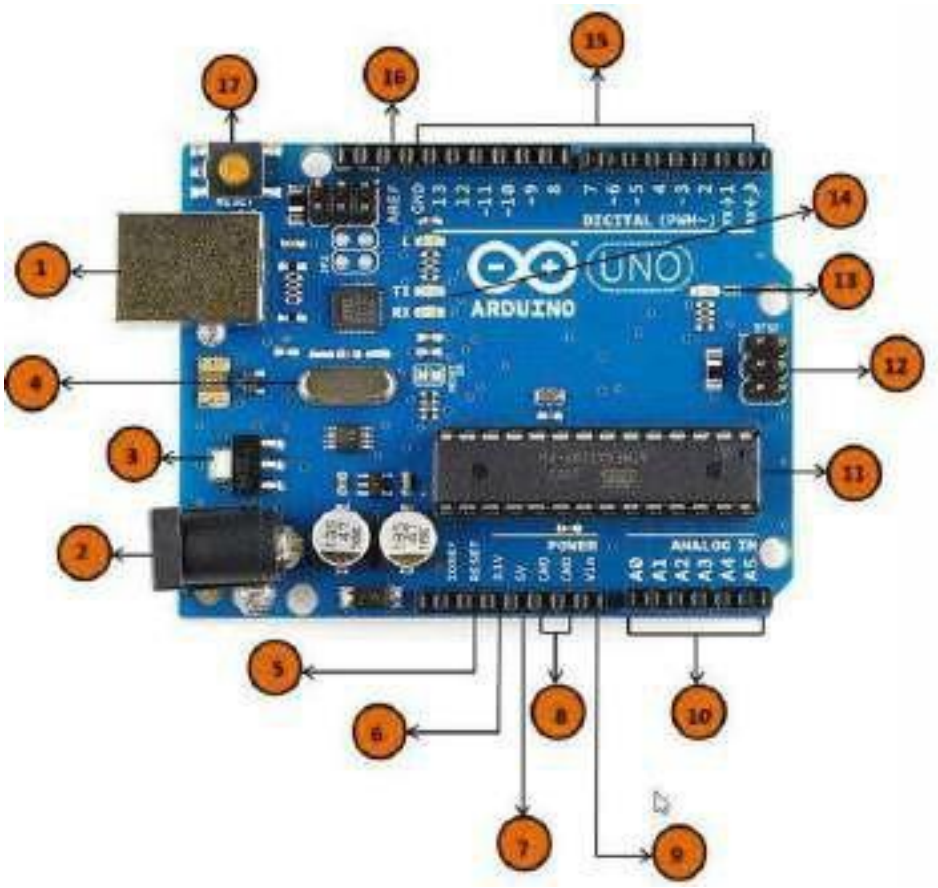


Fig. 2.8.2: Pin configuration of an Arduino board

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:

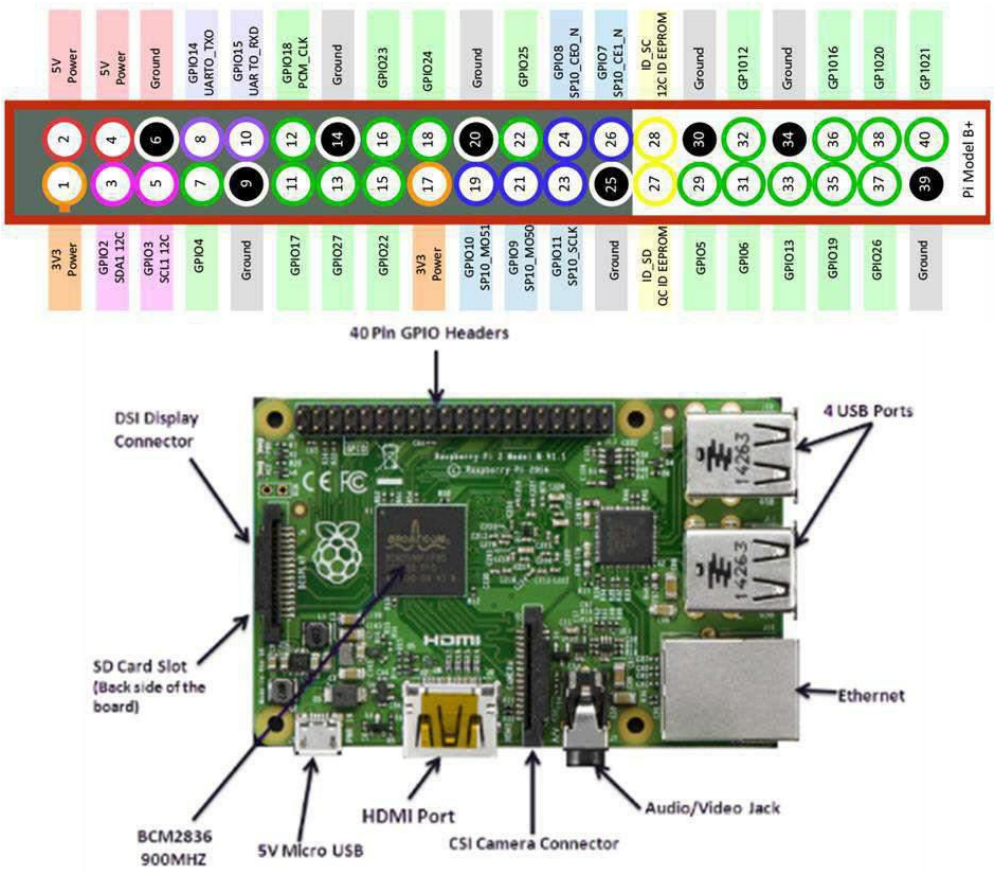


Fig. 2.8.3: Pin configuration of a Raspberry Pi board

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.

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

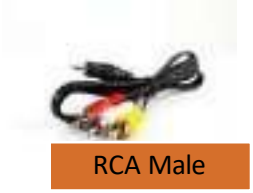
CAT 6A Ethernet RJ 45 Connector

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

Notes

UNIT 2.9: Installing Suitable Framework

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to install and configure firmware/software frameworks for IoT device communication with cloud platforms.
2. Explain the configuration and troubleshooting process of cloud-based IoT management platforms.

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:

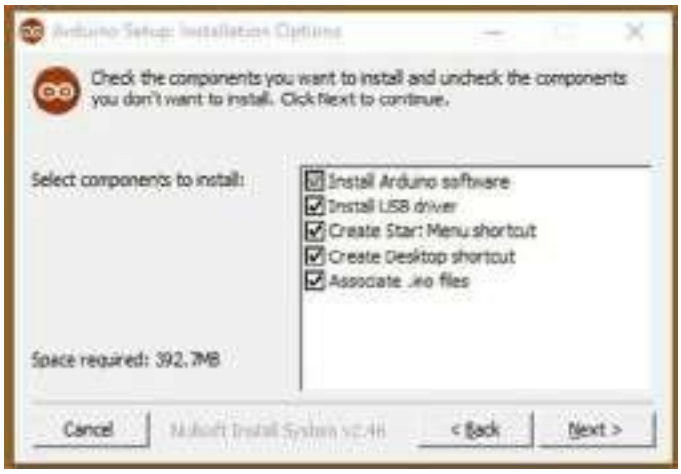


Fig. 2.9.3: Arduino installation window

- 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:

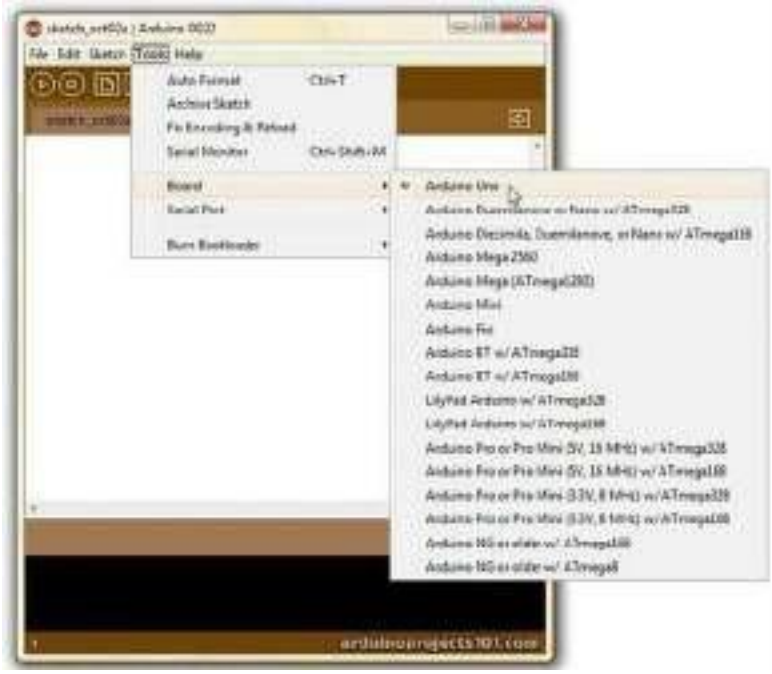


Fig. 2.9.6: Identifying the board

- 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:

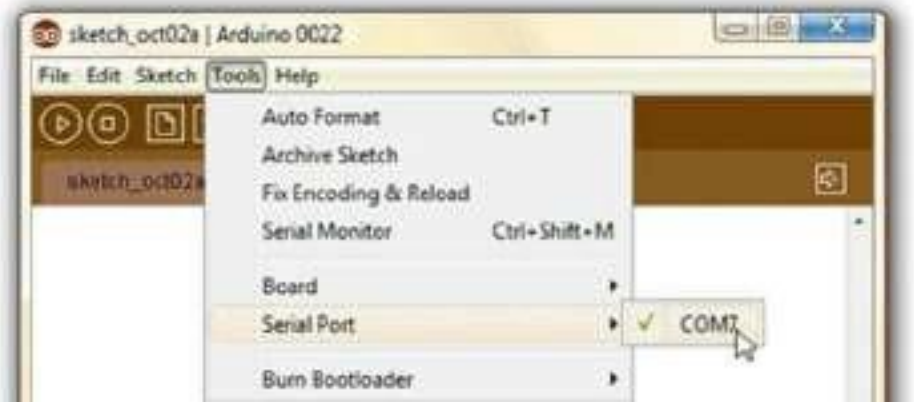


Fig. 2.9.7: Selecting the serial port

- 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:

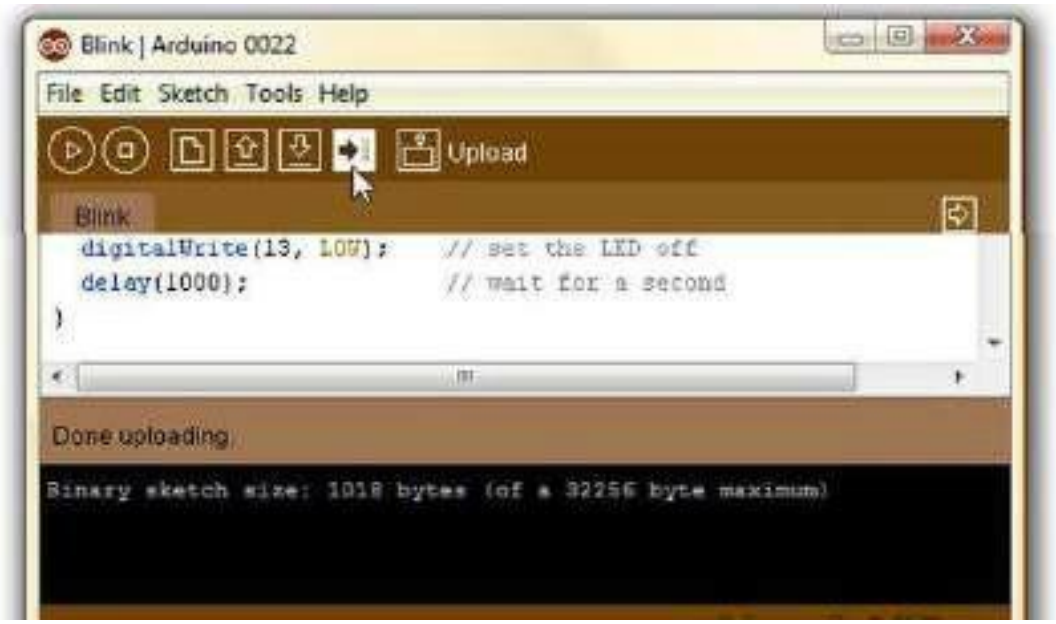


Fig. 2.9.10: Uploading a code

- 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:

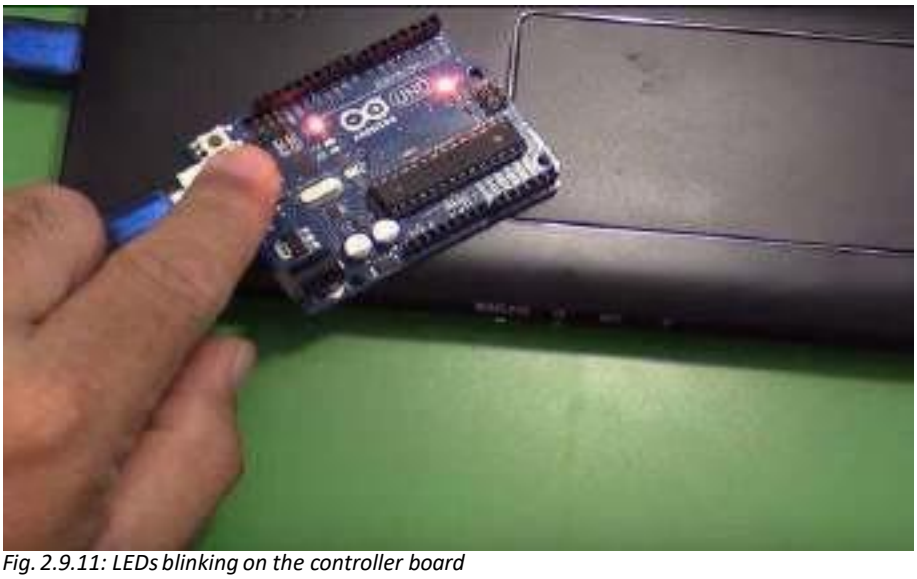


Fig. 2.9.11: LEDs blinking on the controller board

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:

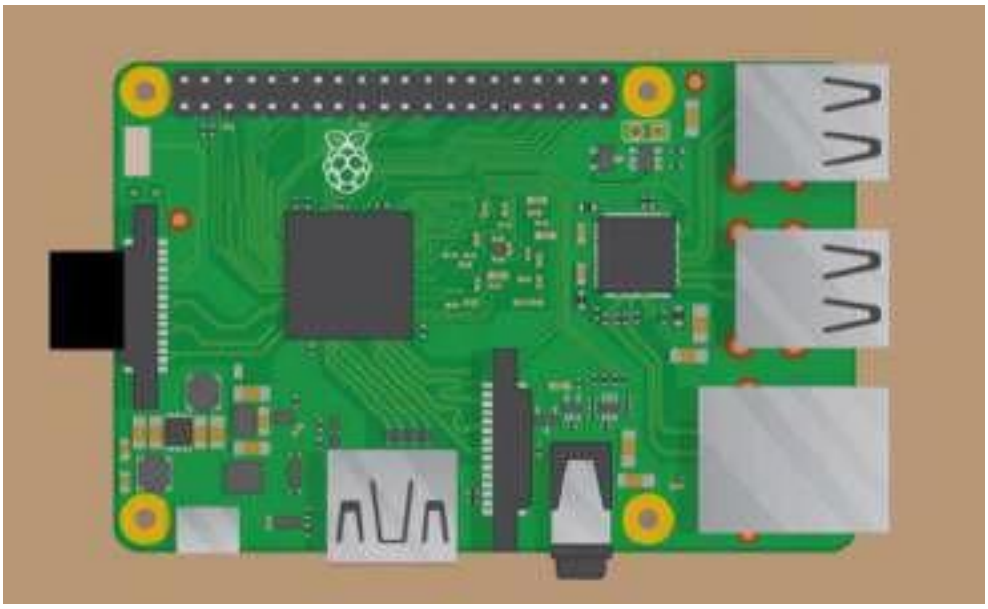


Fig. 2.9.12: Placing the SD card

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

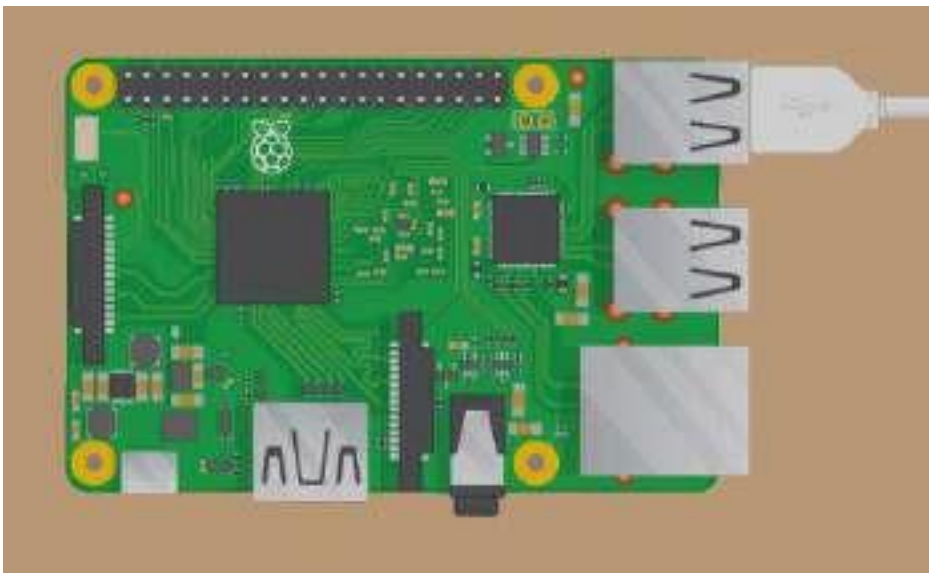


Fig. 2.9.13: Plugging cables to the USB ports

- 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:

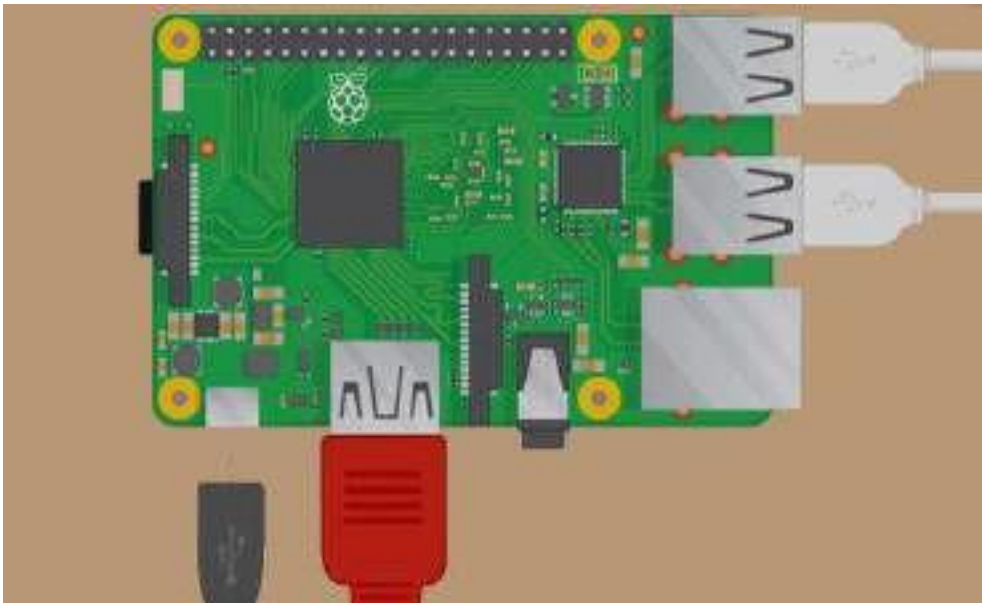


Fig. 2.9.14: Plugging HDMI cables to the board

- 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.

Notes

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

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to compile and upload software code to microcontrollers while ensuring compatibility with communication protocols.
2. Elucidate best practices for writing and debugging software code for IoT microcontrollers.

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:

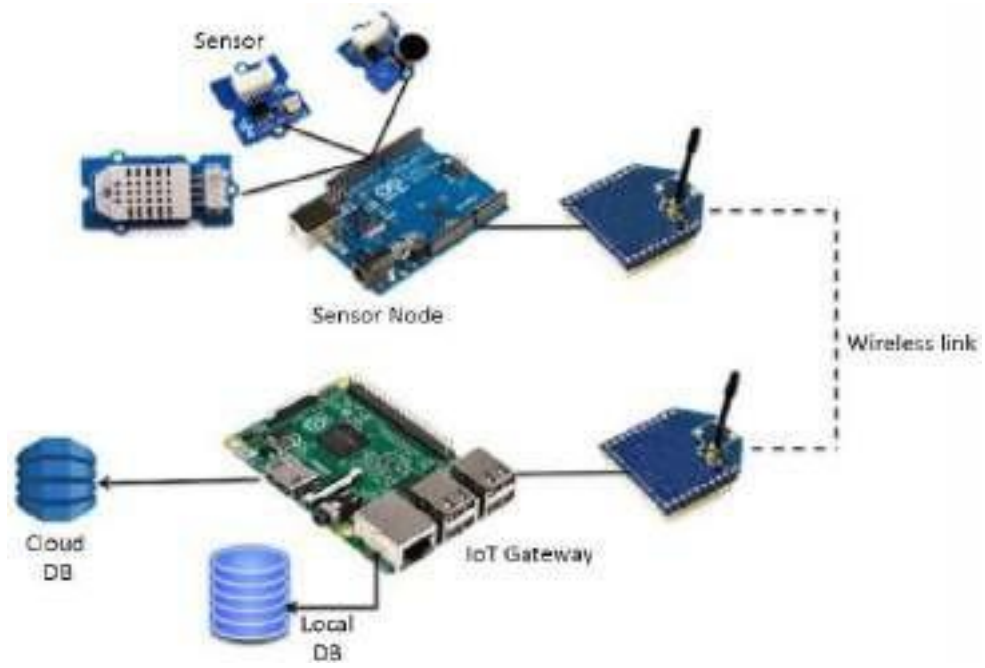


Fig. 2.10.1: Nodes and gateway

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:

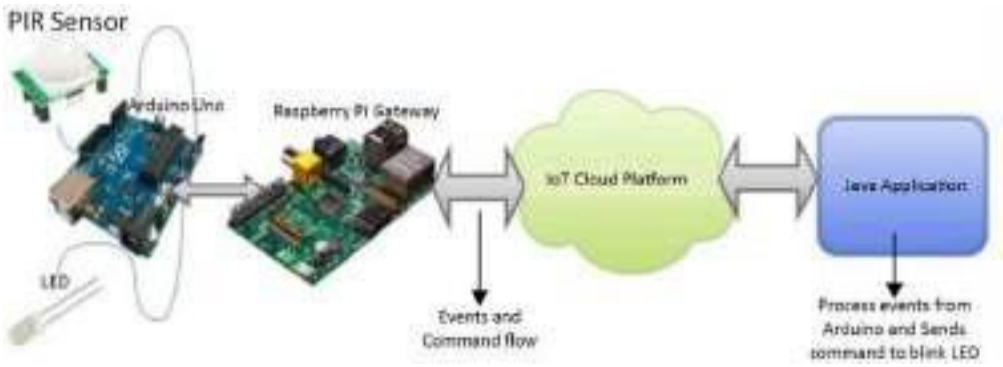


Fig. 2.10.2: An IoT network

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

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:

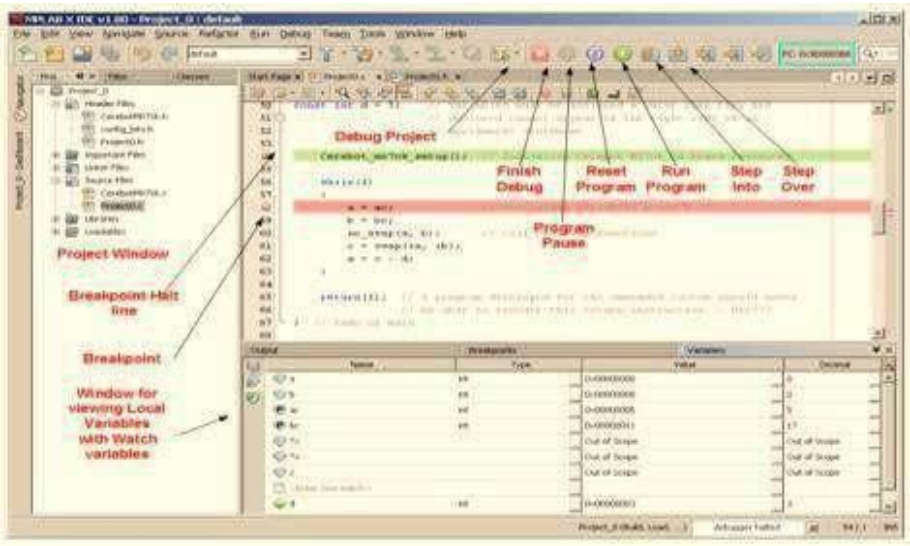


Fig. 2.10.9: MPLAB XC 32 C pic microcontroller compiler

- 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:

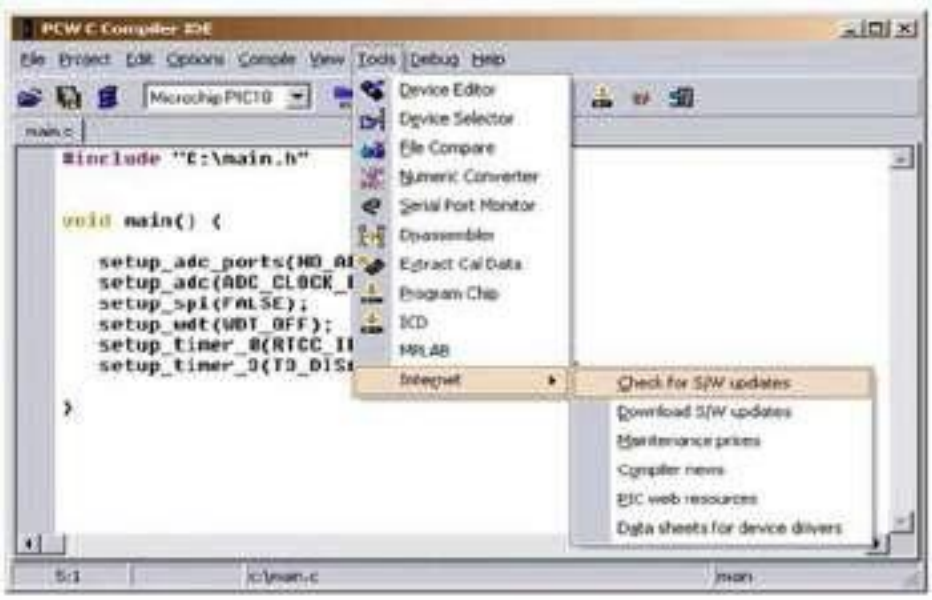


Fig. 2.10.10: PIC CSS pic microcontroller compiler

Notes

UNIT 2.11: Understanding Error Codes and Debug Software

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to debug software errors and optimize system performance using emulators and network testing tools.
2. Describe remote diagnostics, monitoring tools, and predictive maintenance methodologies.

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:

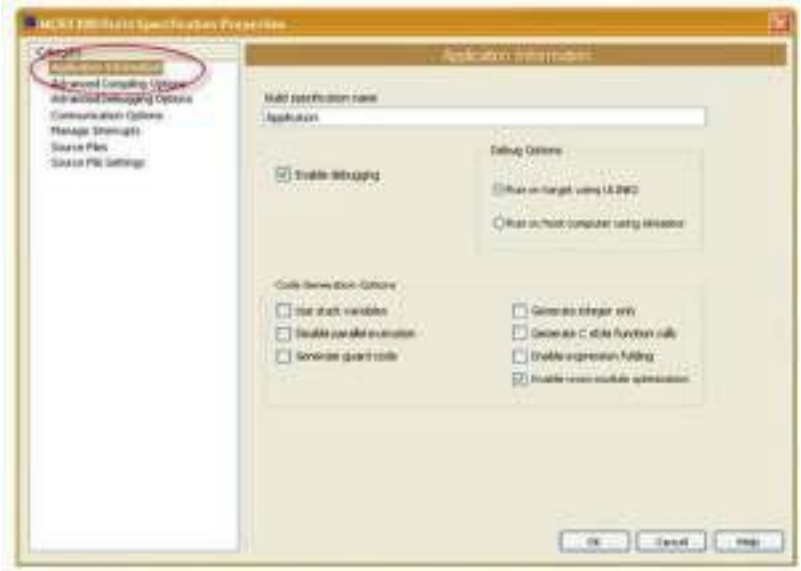


Fig. 2.11.3: Setting build specifications properties

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:

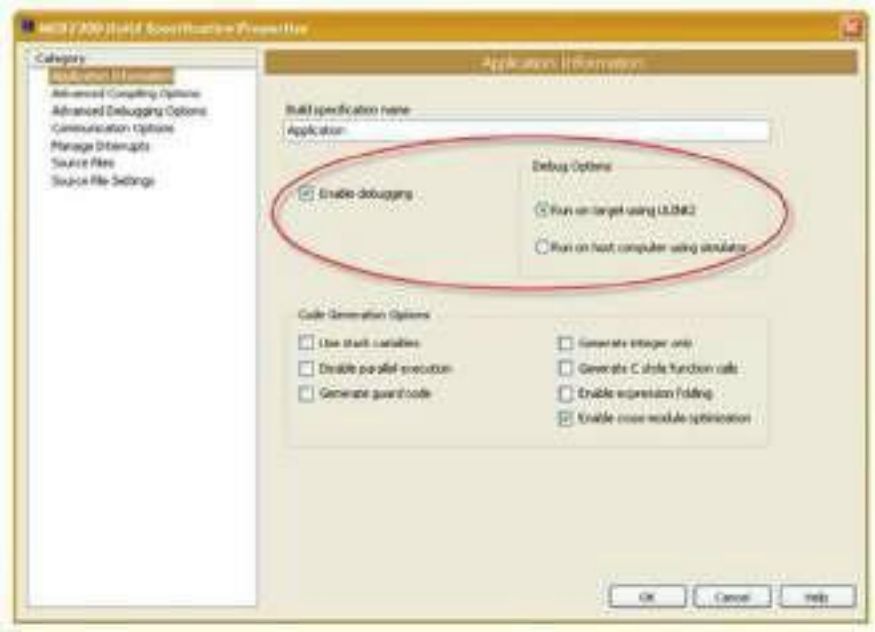


Fig. 2.11.4: Setting debug options

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:

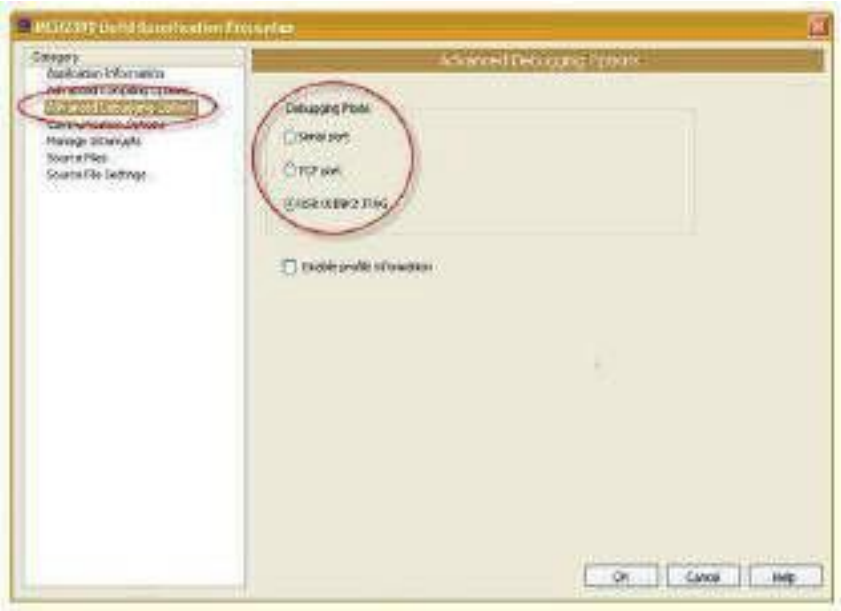


Fig. 2.11.5: Setting communication options

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:

```
/*--- Blink an LED ---//
//Associate LEDs with an Arduino Digital pin.
//The Arduino already has a built-in LED that we can use on D
int ledPin = 23;  \\We're using Digital Pin 23 on the Arduino

void setup();
{
   pinMode(ledPin OUTPUT);   //Set up Arduino pin for output
}

loop()
{
   /The HIGH and LOW values set voltage to 5 volts when HIGH
   digitalWrite(ledPin, High); //Setting a digital pin HIGH t
   delay(1000);  //Get the microcontroller to wait for one se
   digitalWrite(ledPin, LOW);  //Setting the pin to LOW turns
   Delay(1000);  //Wait another second with the LED turned of
   }
}
```

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

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=LlhmzVL5bm8

Understanding Edge Devices

UNIT 2.12: Functioning of Micro-Controller and Attached Devices

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to verify the proper execution of installed software by setting up nodes and gateways correctly.
2. Demonstrate how to confirm data reception at the backend server and escalate unresolved connectivity issues.

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 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.

Fig. 2.12.1: Home security system

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:

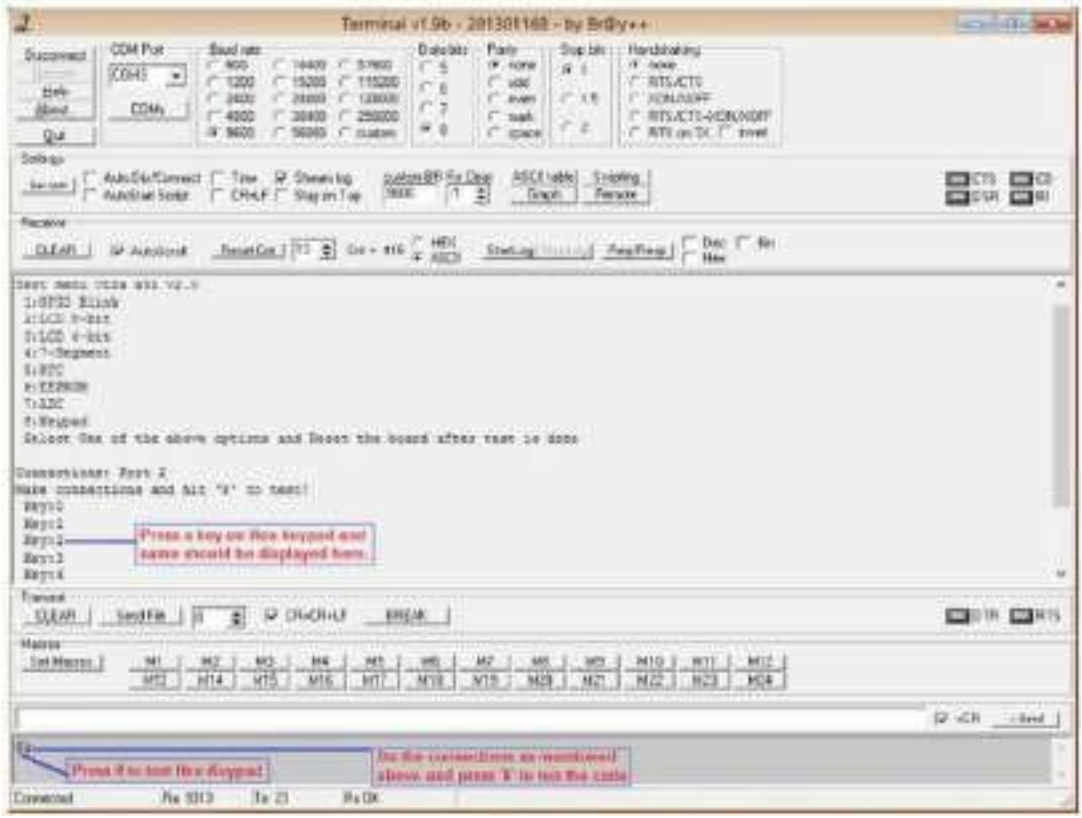


Fig. 2.12.9: Keypad test output

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:

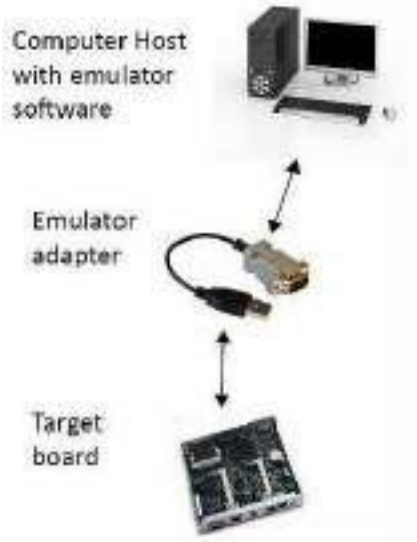


Fig. 2.12.10: Connection of emulator

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:

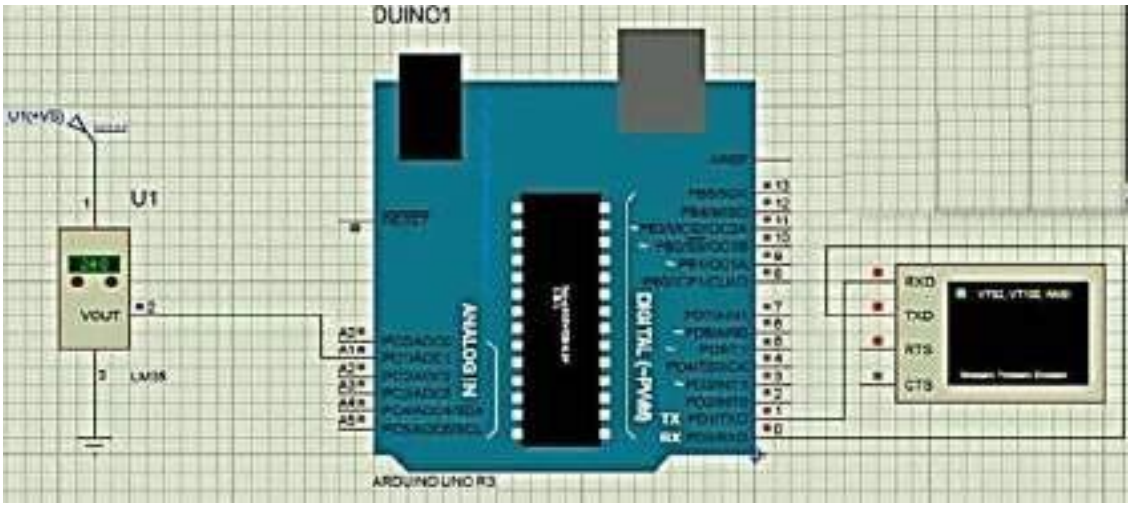


Fig. 2.12.12: Designing the circuit

Step 2: Save the design and open the code in the application for the Arduino coding as shown in the following screenshot:

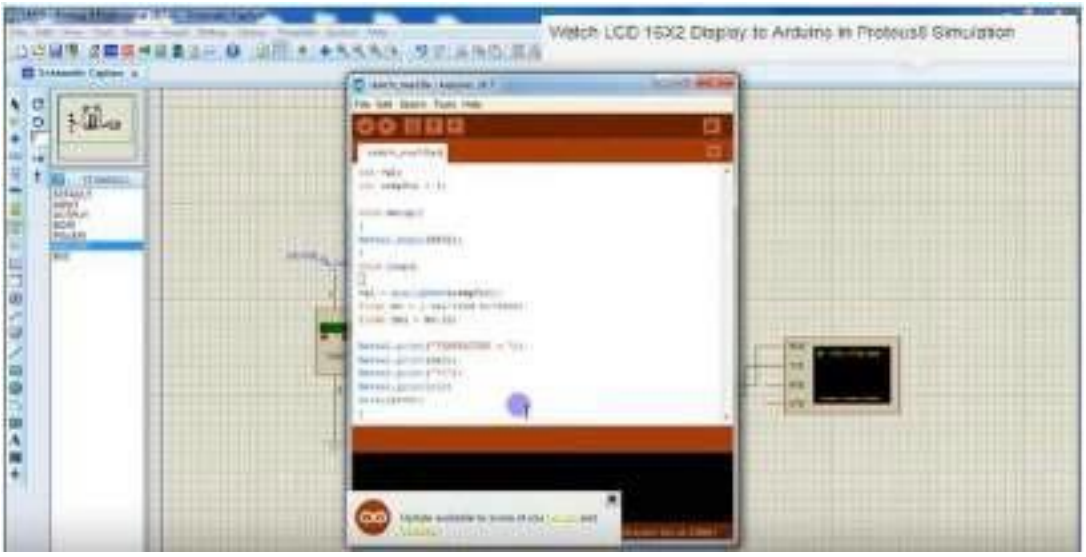


Fig. 2.12.13: Arduino code

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:

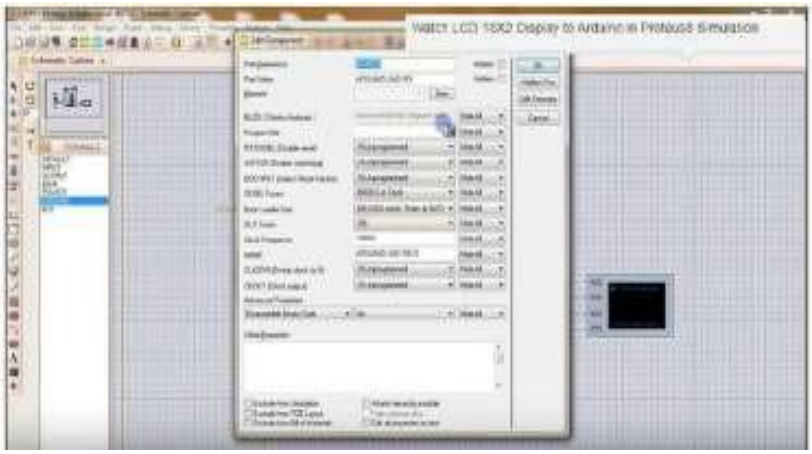


Fig. 2.12.15: Edit component window

Step 5: Browse the Arduino code and run. A virtualterminal with output will appear, as shown in the following screenshot:

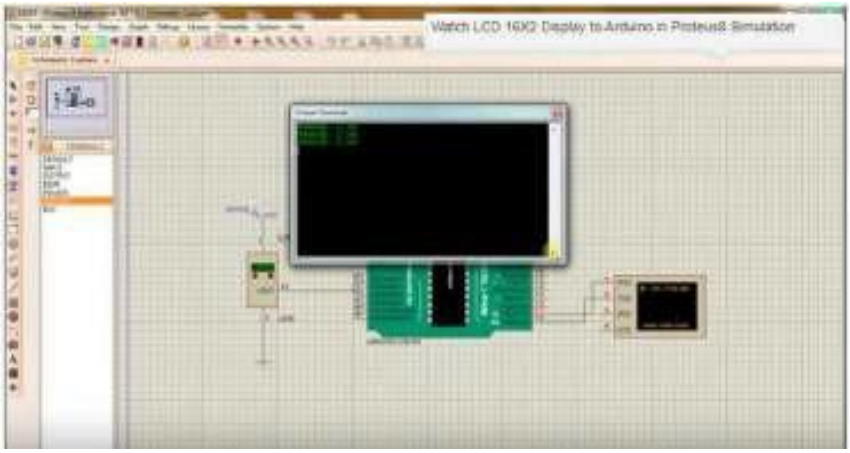


Fig. 2.12.16: Virtual terminal window with output

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.

Notes

UNIT 2.13: Initializing Nodes and Gateways

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to establish initial configurations for nodes and gateways for operational readiness.
2. Discuss how to validate communication flow from devices to gateways during initialization.

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:

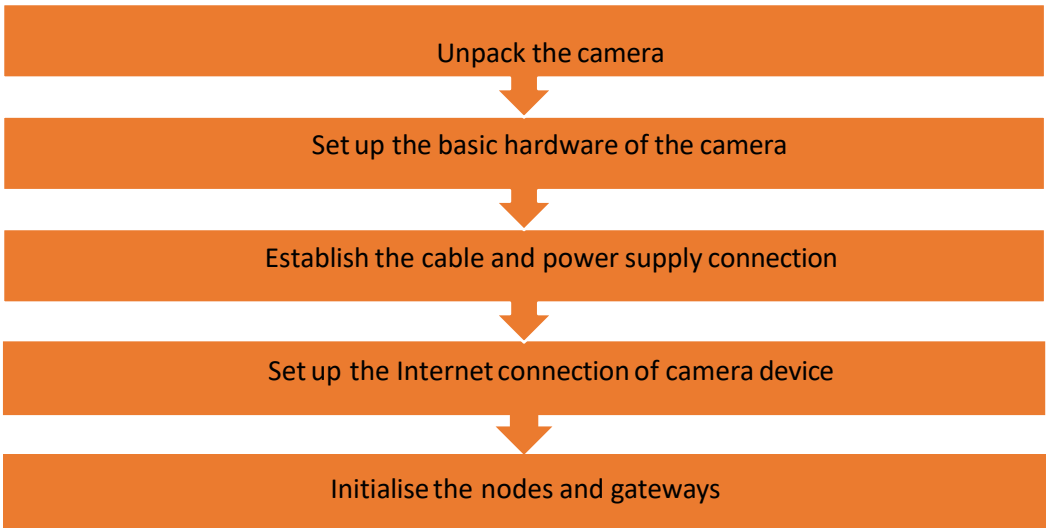


Fig. 2.13.1: Prerequisite steps for an IoT camera device installation

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:

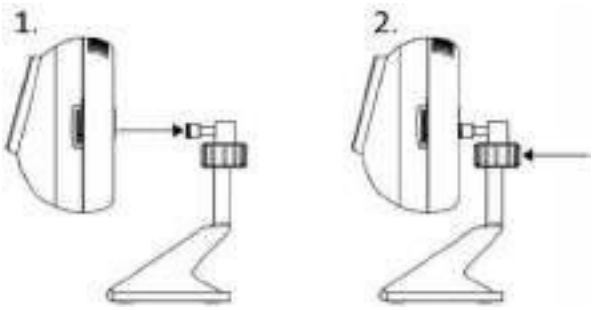


Fig. 2.13.2: Camera hardware set up

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:

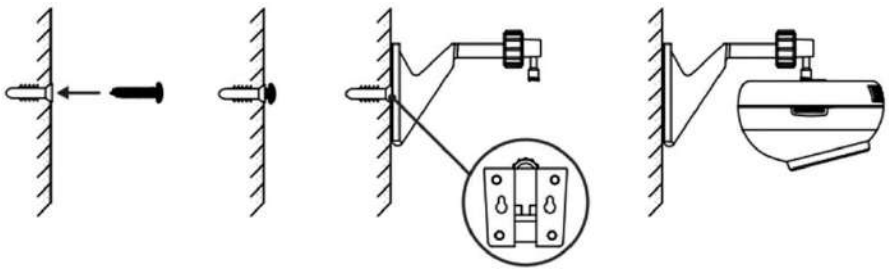


Fig. 2.13.3: Mounting of camera on a wall

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:

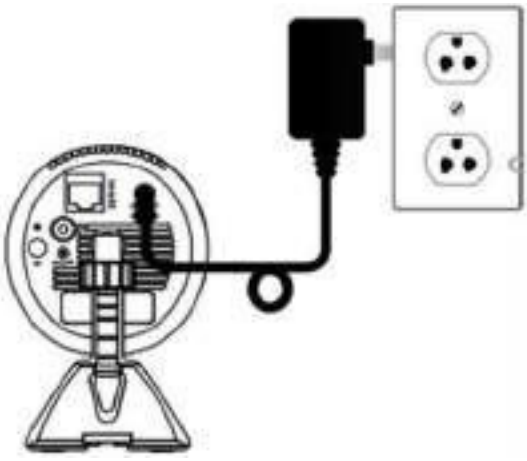


Fig. 2.13.5: Power adaptor connection

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:

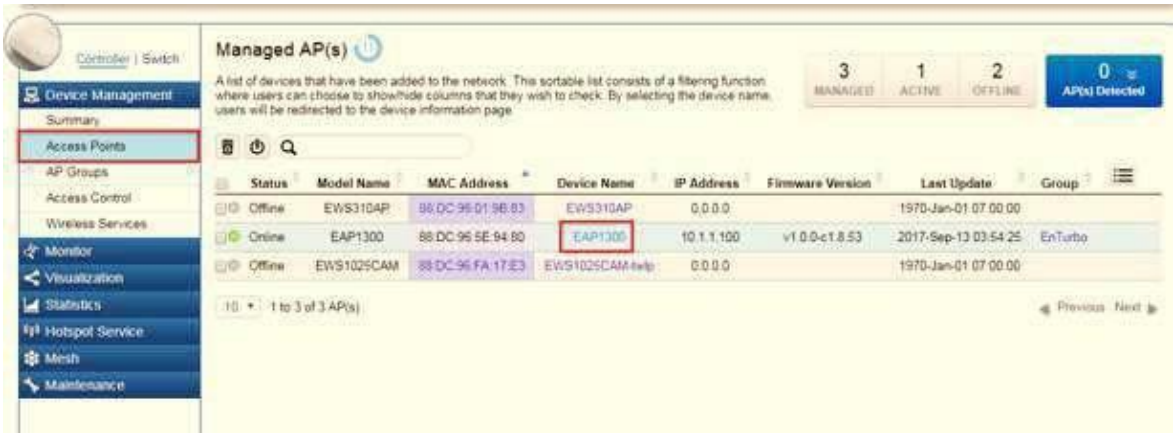


Fig. 2.13.7: Screenshot showing the camera listed in the utility tool

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:

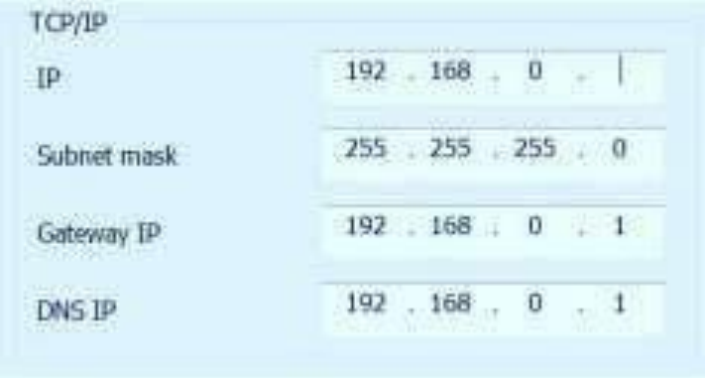


Fig. 2.13.10: Screenshot showing the manual network setup wizard

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:

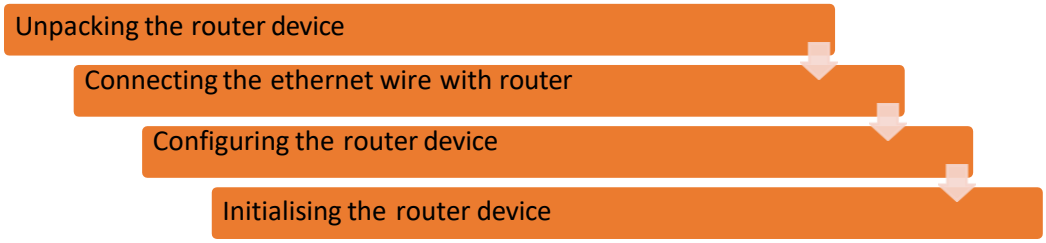


Fig. 2.13.12: Router installation steps

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:

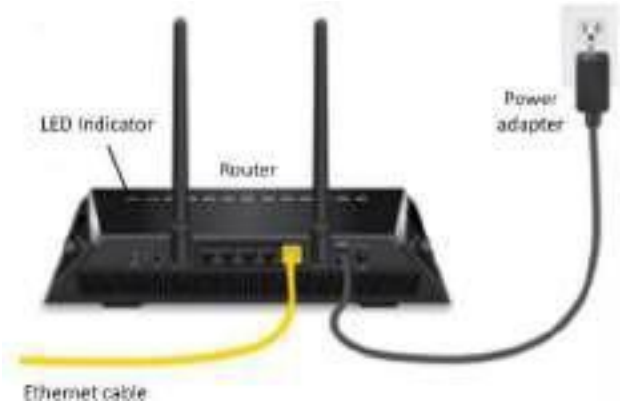


Fig. 2.13.14: Power and Ethernet cable connection with router

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:

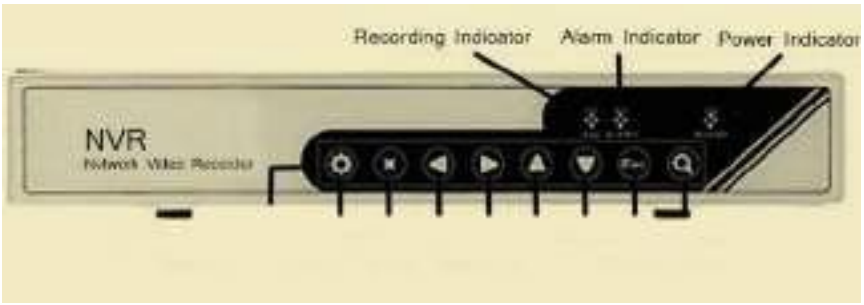


Fig. 2.13.19: NVR device indicators

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:

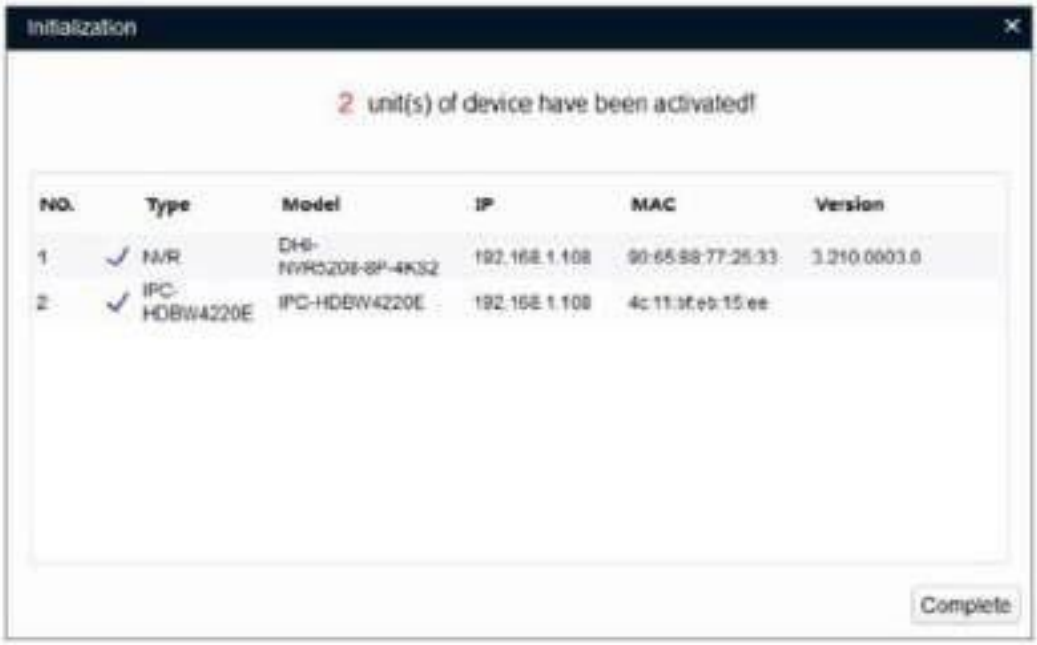


Fig. 2.13.24: Detected devices after initialization

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:

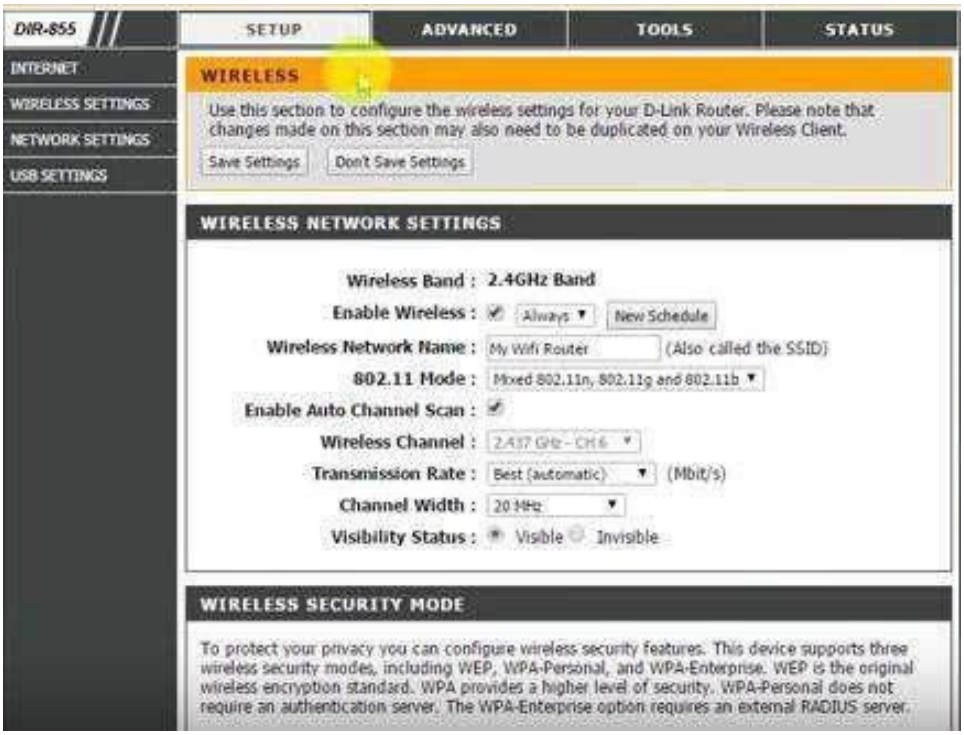


Fig. 2.13.27(b): Screenshot of router settings

Fig. 2.13.27(c): Screenshot of router settings

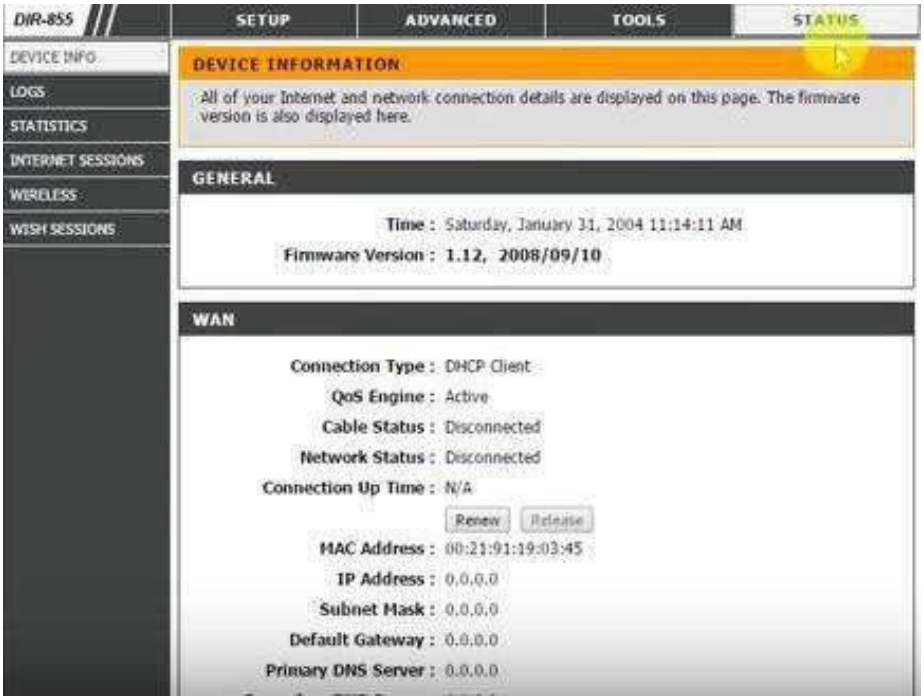


Fig. 2.13.27(d): Screenshot of router settings

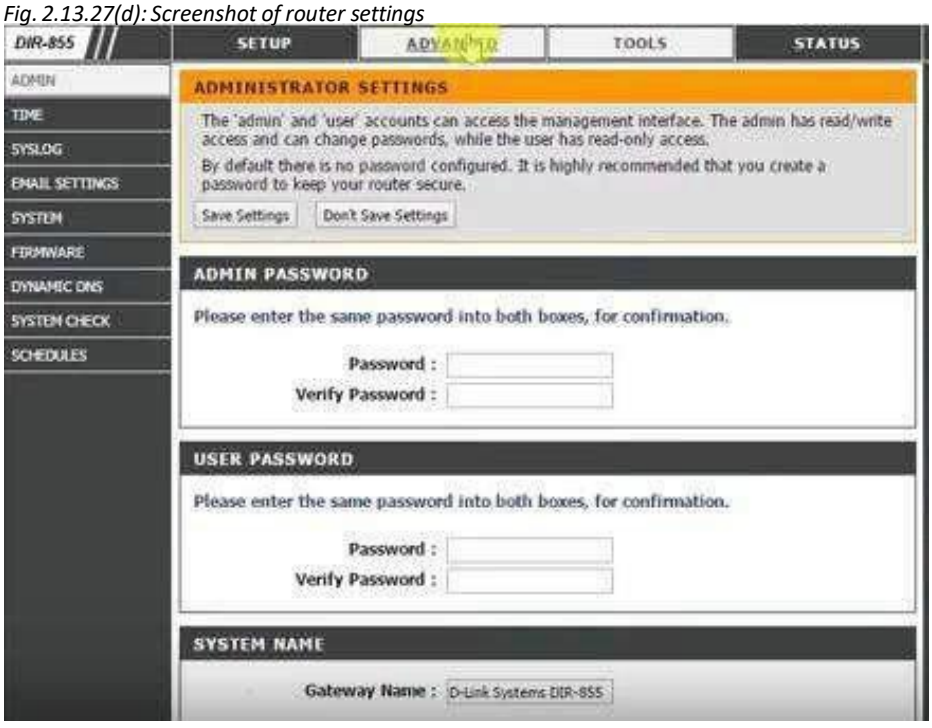


Fig. 2.13.27(e): Screenshot of router settings

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

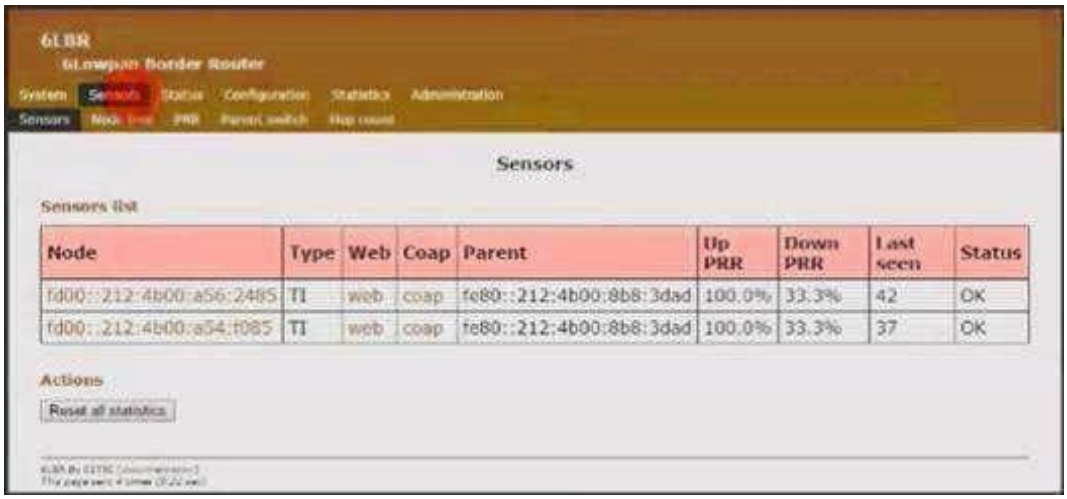


Fig. 2.13.28(b): Screenshot of list of sensors connected

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:

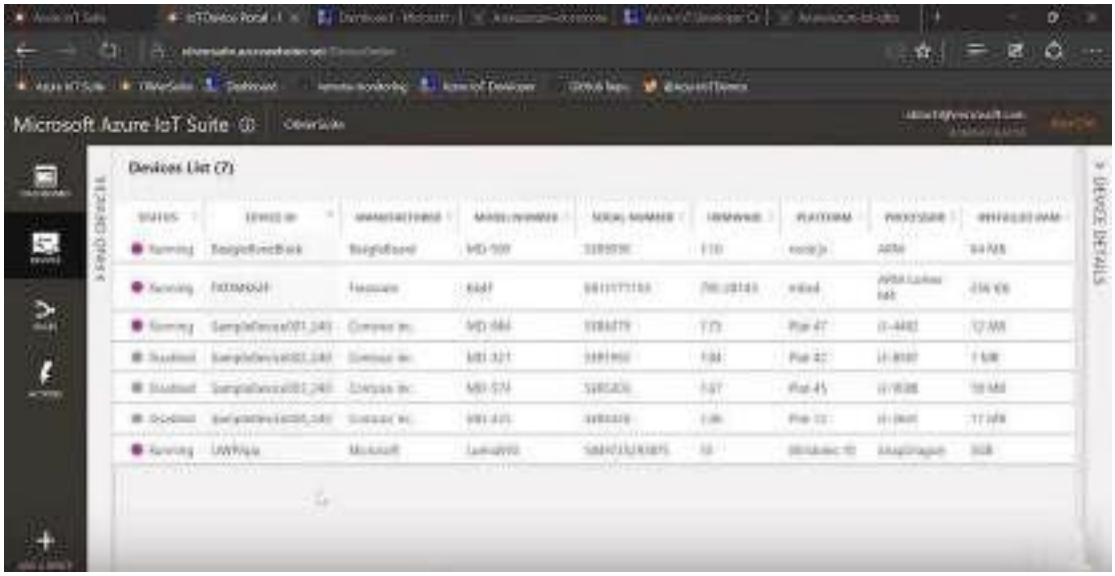


Fig. 2.13.29: Screenshot of Microsoft Azure window

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:

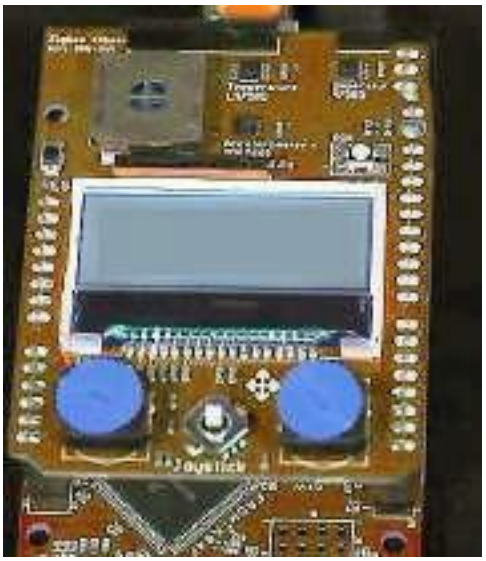


Fig. 2.13.34: Checking whether the device is functioning according to the command

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:

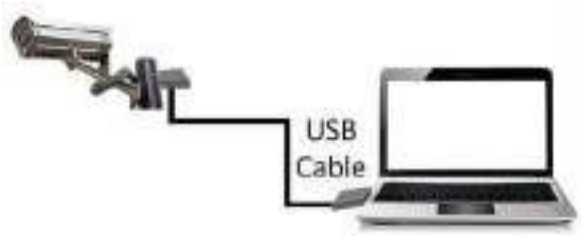


Fig. 2.13.35: Connection between camera and laptop with a USB cable

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:

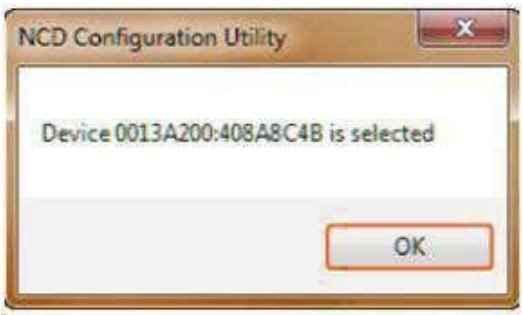


Fig. 2.13.38: NCD configuration window

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:

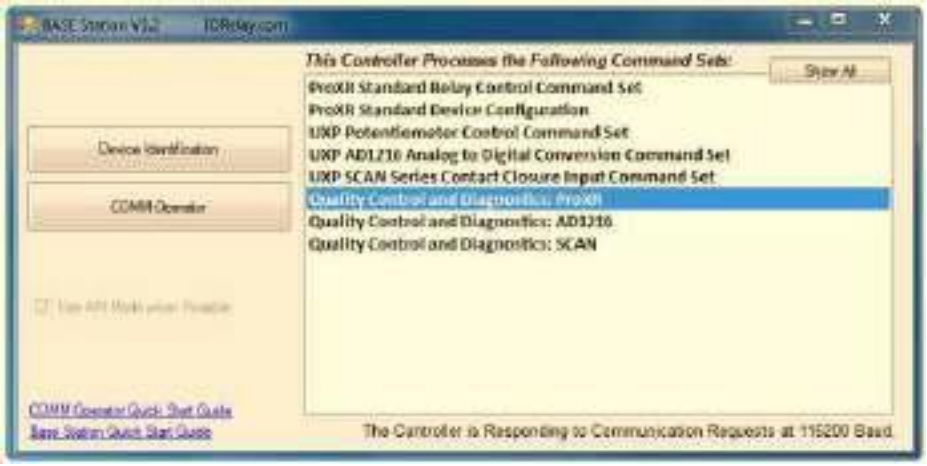


Fig. 2.13.39: Command option window

Notes

UNIT 2.14: Launching the Software on Nodes and Gateways

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to configure and activate IoT software modules on nodes and gateways.
2. Demonstrate steps to ensure proper boot-up, registration, and network joining of IoT devices.

2.14.1 Launching the Software on Nodes and Gateways

The prerequisites for the software to function on the devices and the gateway are as shown in the following figure:

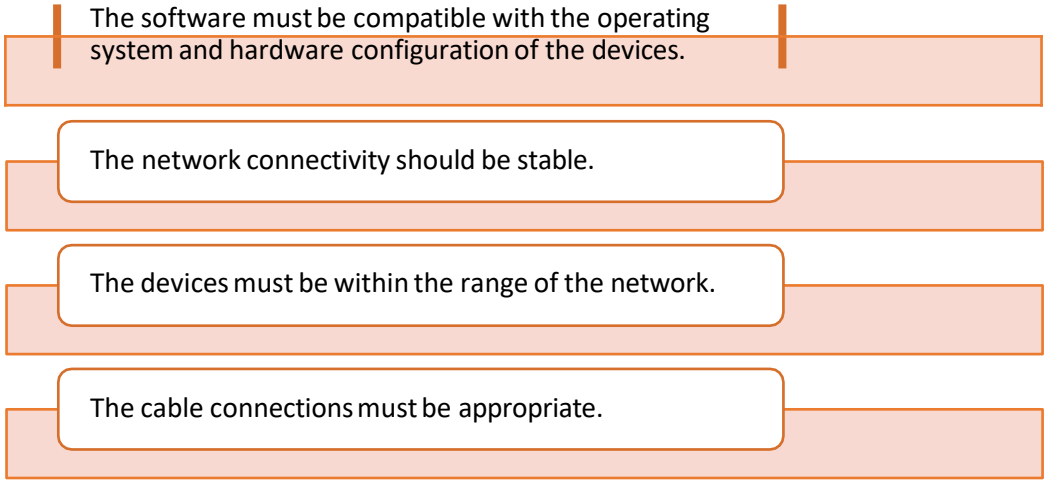


Fig. 2.14.1: Launching prerequisites

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.

Notes

UNIT 2.15: Confirming Communication and Establishing Connectivity

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to perform network performance testing to detect latency, packet loss, or interference issues.
2. Show how to confirm data reception at the backend server.

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

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:

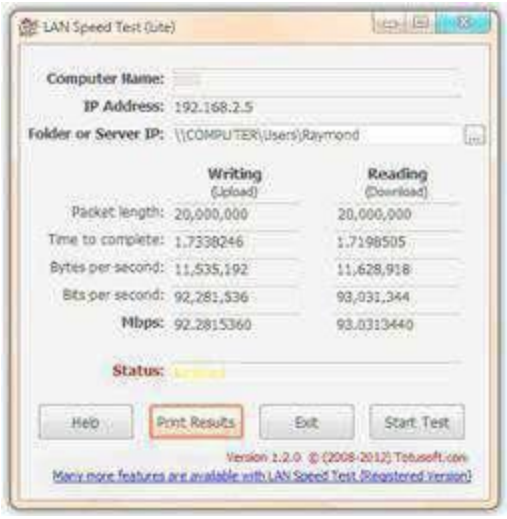


Fig. 2.15.2: Lite window

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:

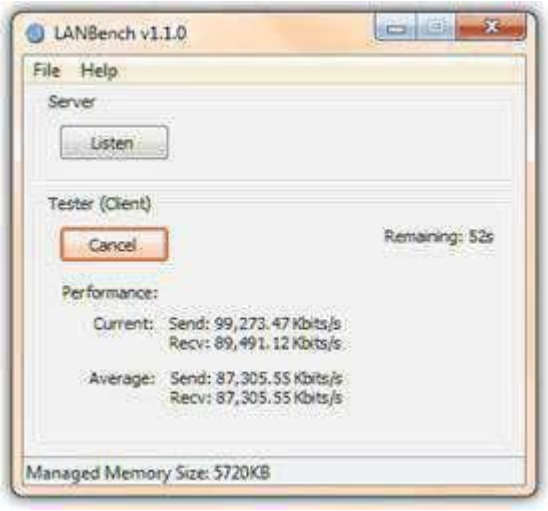


Fig. 2.15.3: LANBench window

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 switches hubs should be replaced with Gigabit
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

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:

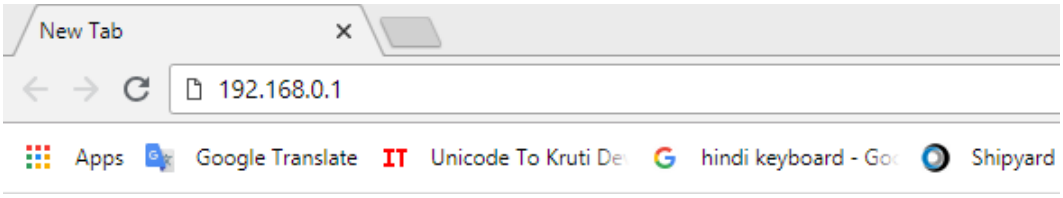


Fig. 5.4.1: IP address at address bar

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:

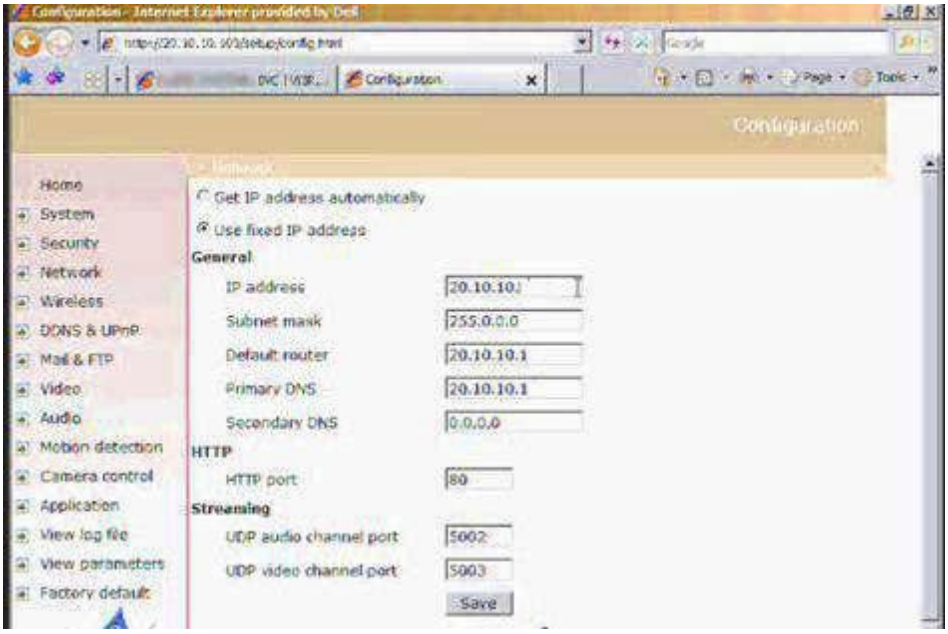


Fig. 2.15.9: Accessing the camera remotely

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:

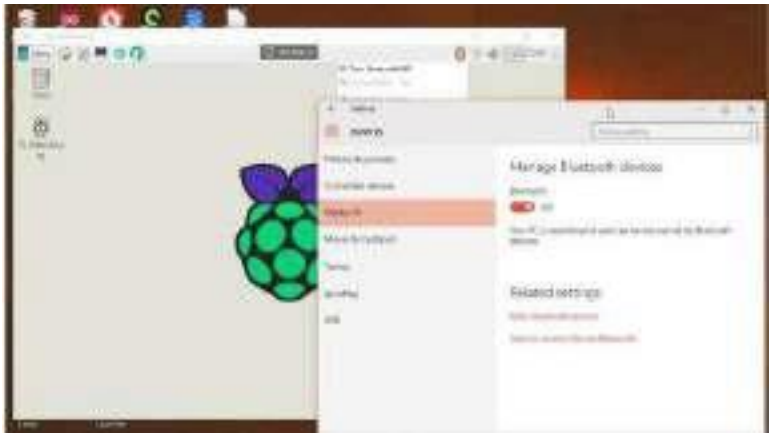


Fig. 2.15.12: Searching for Bluetooth devices

Step 4: Check for the Raspberry Pi and pair the devices as shown in the following screenshot:

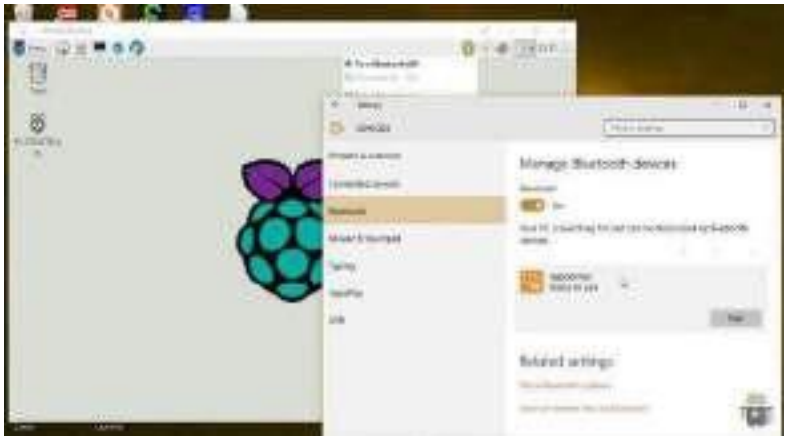


Fig. 2.15.13: Pairing the Bluetooth devices

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:

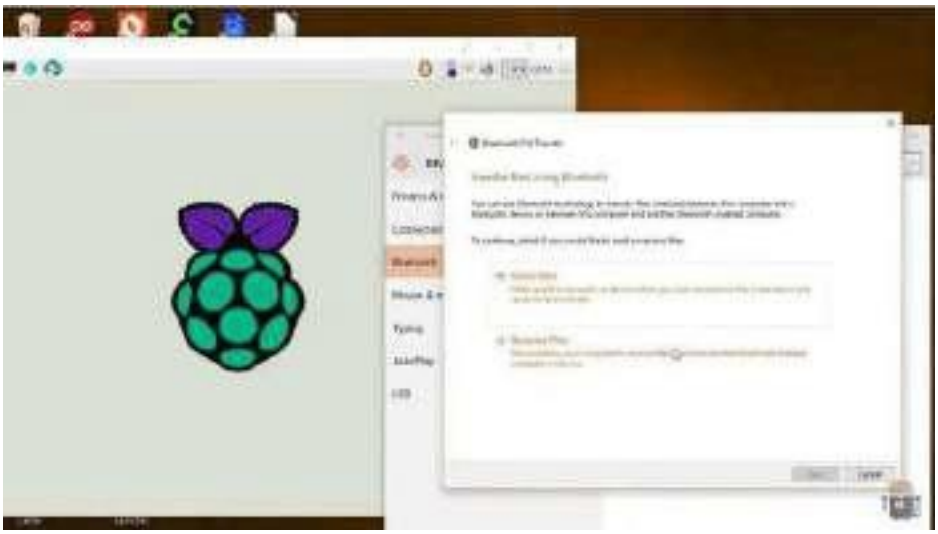


Fig. 2.15.15: Sharing the files

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:

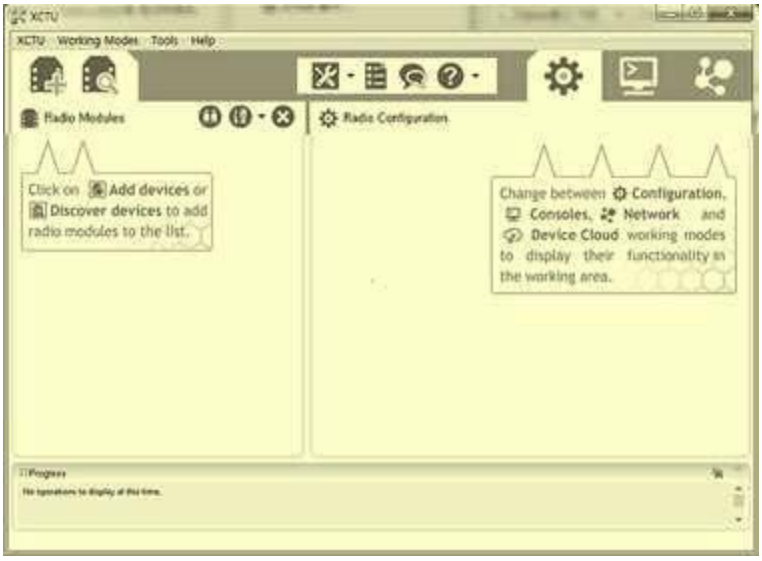


Fig. 2.15.16: XCTU interface window

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:

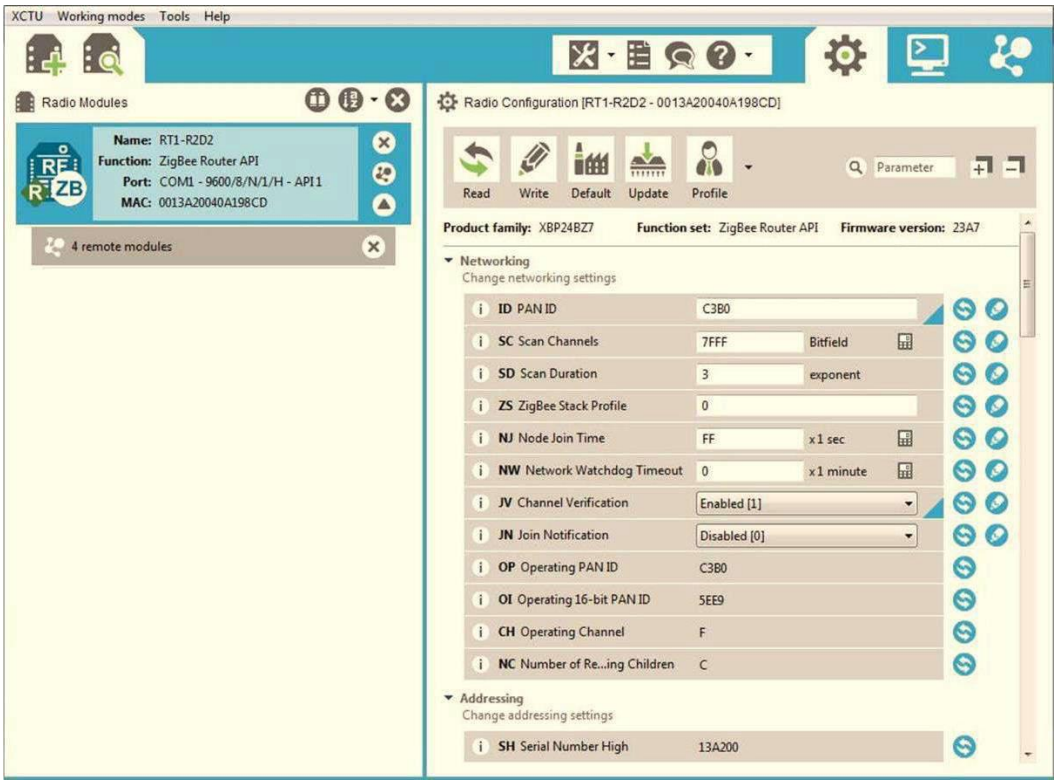


Fig. 2.15.20: Configuring the radio module

Notes

UNIT 2.16: Controlling Edge Appliances and Hubs and Checking for Data Transfer and Confirming from the Server End

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to monitor data flow across nodes, gateways, and edge appliances.
2. Show how to verify seamless end-to-end data transfer and system responsiveness.
3. Demonstrate procedures to check communication status using dashboards, logs, and performance indicators.

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:

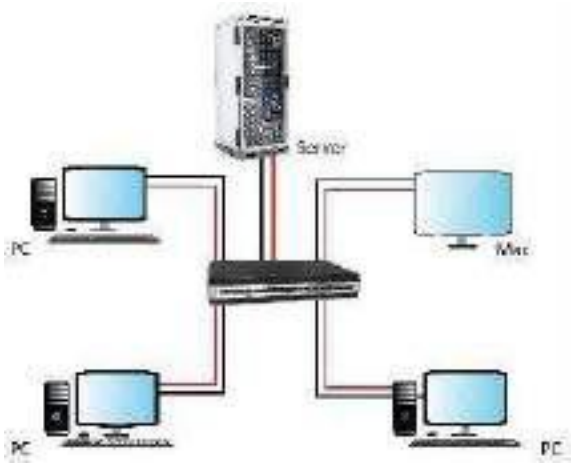


Fig. 2.16.3: Multiple devices connected to a hub

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.

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.

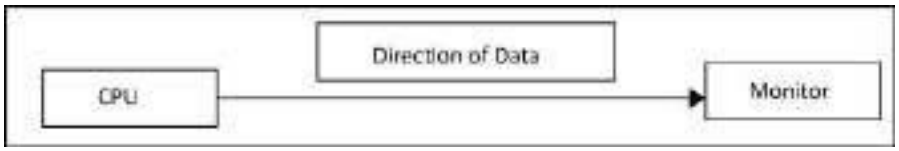


Fig. 2.16.6: Simplex mode

- **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.

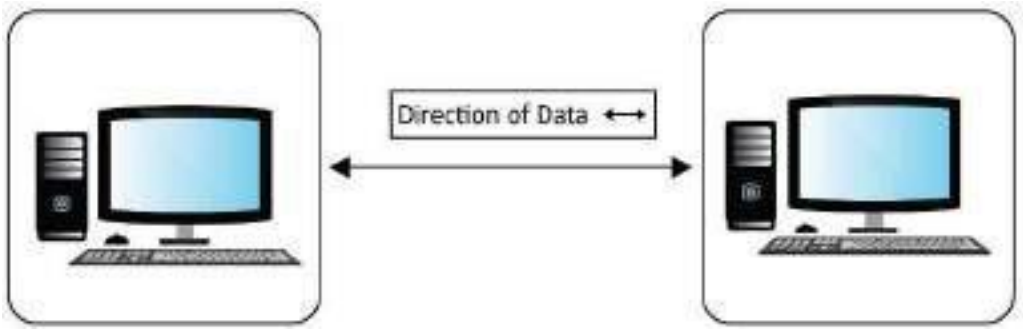


Fig. 2.16.8: Duplex

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:

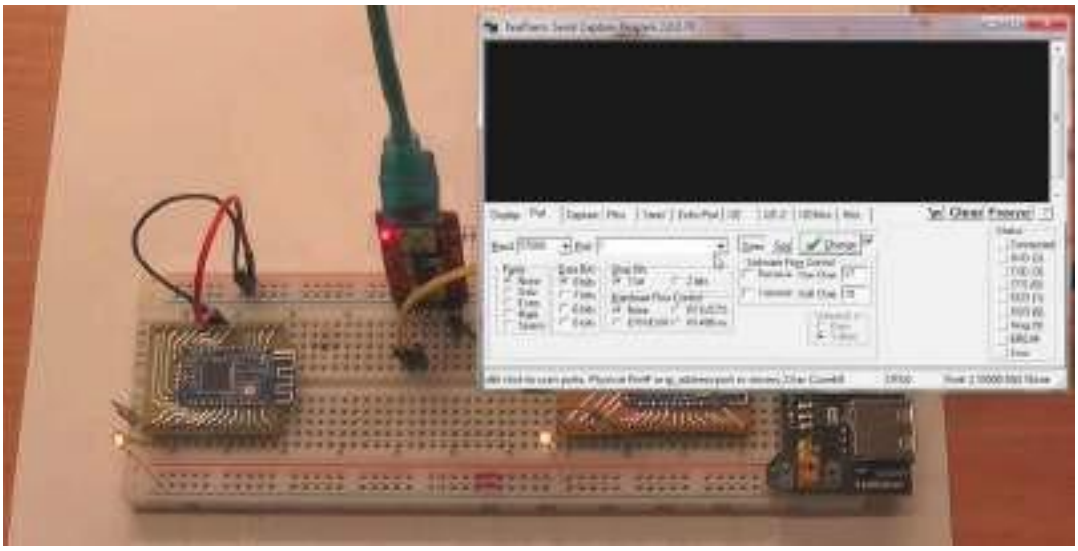


Fig. 2.16.9: Baud rate of a set up

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:

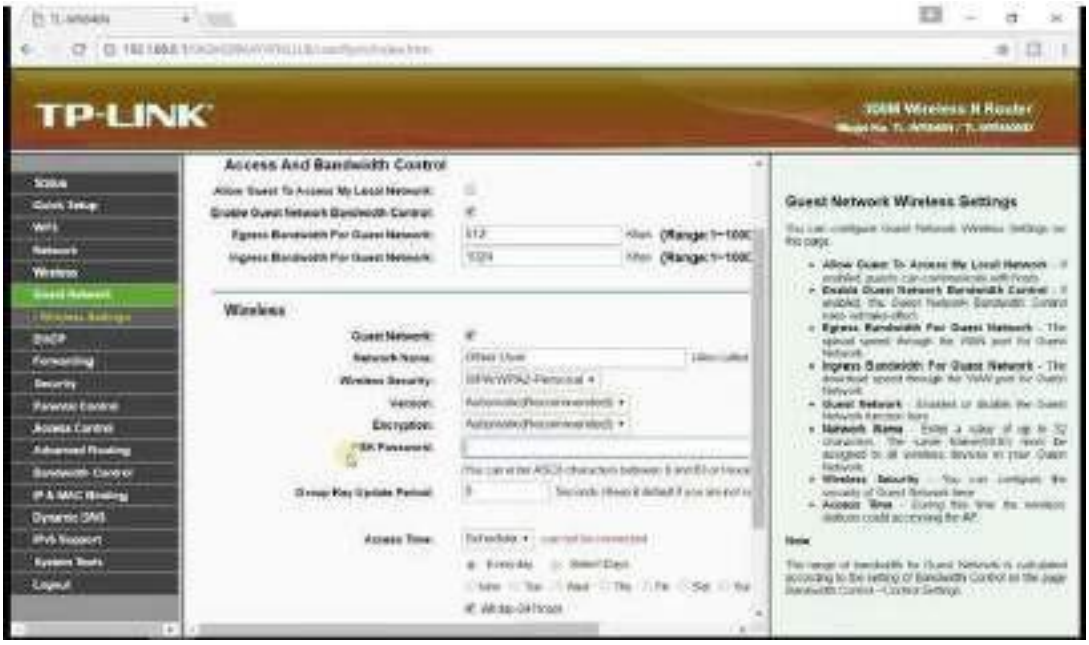


Fig. 2.16.10: Wireless settings for TP-Link

Exercise

A. Short Answer Questions:

1. Explain the role of gateways in managing communication between IoT nodes and backend servers.
2. What are the key differences between short-range and long-range IoT communication protocols?
3. Why is RF signal strength measurement important during IoT device installation?
4. How does edge computing improve the performance of IoT systems?
5. Describe two common cybersecurity threats in IoT and how they can be prevented.

B. Multiple Choice Questions (MCQs):

1. Which component acts as the central controller in most IoT devices?
    a. Actuator
    b. Microcontroller
    c. Gateway
    d. Sensor
2. LoRaWAN is primarily used for:
    a. Short-range high-speed communication
    b. Long-range low-power communication
    c. Video streaming
    d. High-bandwidth LAN use
3. Which of the following is a cloud-based IoT management function?
    a. Mechanical alignment of devices
    b. Firmware flashing
    c. Remote diagnostics and monitoring
    d. Device grounding
4. ISO 27001 is a standard related to:
    a. Hardware manufacturing
    b. Power supply optimization
    c. Information security management
    d. RF testing
5. Which tool helps detect packet loss and latency issues in IoT networks?
    a. Multimeter
    b. Spectrum analyzer
    c. Network testing tools
    d. Screw gauge

C. Fill in the Blanks:

1. _____ computing helps reduce latency by processing data closer to the device.
2. A device that collects data from sensors and transfers it to gateways or cloud platforms is called a _____.
3. _____ is a long-range, low-power wireless technology widely used in IoT applications.
4. _____ and _____ are common indicators used to validate data transfer during IoT testing.
5. The process of uploading firmware or code to a microcontroller is known as _____.

Notes

3. Configuring Equipment and Establishing Wireless Network Connectivity

Telecom Sector Skill Council

TEL/N6234

Key Learning Outcomes

By the end of this module, the paricipants will be able to:

1. Explain CPE configuration steps, network security, and integration with broadband and smart home systems.
2. Demonstrate establishing and troubleshooting connectivity between CPE, service provider networks, and end-user devices.
3. Explain the process of connecting CPE to the service provider gateway and end-user devices.
4. Demonstrate network diagnostics, troubleshooting, and performance optimization.

UNIT 3.1: Network Topologies

Unit Objectives

By the end of this unit, the participants will be able to:

1. Describe wired and wireless CPE configurations, including VLAN, NAT, and QoS settings.
2. Explain the basics of VPNs and Internet Lease Lines (ILL) and their role in secure network communications.
3. Describe IPv6 addressing, subnetting, NAT configurations, and the impact of QoS on broadband services.
4. Explain connectivity options for CPE and end-user devices, including advanced Wi-Fi security settings.
5. Describe how to integrate smart home systems (Amazon Alexa, Google Home, Apple HomeKit) with broadband networks.
6. Explain cybersecurity fundamentals, including securing home networks, firewall configurations, and threat mitigation strategies.
7. Explain the escalation matrix for troubleshooting major network failures and handling emergencies.

3.1.1 App-Based and Automated Training Platforms

Schematic description of the planning of a network is referred to as topology when discussing communication networks.

Network geometry is defined in following two ways:

1. Physical topology

2. Logical (or signal) topology

- Bus network topology: This topology has each workstation connected through the main cable called bus. Or simply put, all devices are connected sequentially to every other in the network.
- Star network topology: has the central device, the server, connected to all other computers in a network. In this type, each computer is indirectly connected to each other through the server.

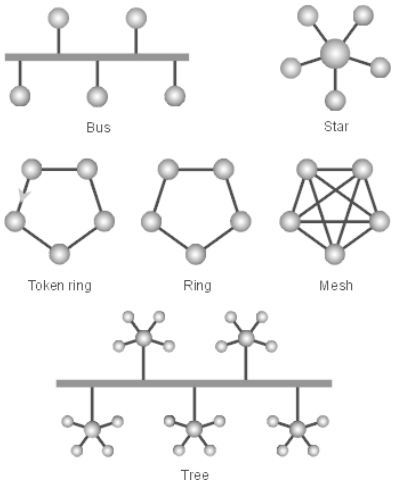


Fig 3.1.1 Types of topologies

- **Ring topology:** has all computers connected in a closed loop configuration.
  - Signal travels in a singular direction if a Token Ring protocol is used either on star or on ring topology.
  - The mesh network topology consists of two types: full mesh and partial mesh. When each system is interconnected directly it's called as full mesh topology. In case where some systems are connected to each other while the others are only connected to those, which exchange data in abidance, is referred to as partial mesh topology.
  - When two or more-star networks are connected together it's referred to as tree network topology.
  - Logical (or signal) topology: is the path used by signals to follow from node to node. In most of the cases logical topology and physical topology is the same.
- **Ring topology:** has all computers connected in a closed loop configuration.
  - Signal travels in a singular direction if a Token Ring protocol is used either on star or on ring topology.
  - The mesh network topology consists of two types: full mesh and partial mesh. When each system is interconnected directly it's called as full mesh topology. In case where some systems are connected to each other while the others are only connected to those, which exchange data in abidance, is referred to as partial mesh topology.
  - When two or more-star networks are connected together it's referred to as tree network topology.
- **Logical (or signal) topology:** is the path used by signals to follow from node to node. In most of the cases logical topology and physical topology is the same.

3.1.2 Broadband Network Element

Network Gateway

The network point which is like an entrance to another network is called as gateway.

Host nodes are referred to as either of the ones which a specific user uses and also the computer that serves pages to users. The computers that are responsible for controlling traffic, whether it's within the company or at service provider end are denoted as gateway nodes.

IP address

Internet Protocol is the full form of IP addresses. Any computer is identified by an IP address on TCP/IP network.

Any IP address is 32 numeric numbers, which are written as set of four numbers and are separated by periods. The range of these numbers varies from zero to 255. For example, 1.150.12.240 can be an IP address.

Unique and random IP addresses can be assigned on an isolated network. In case of a private network, one is required to use only registered IP addressees, which ensures there is no duplicity.

An IP address can be static or dynamic. In case of static IP address, the address never changes unlike in case of a dynamic IP address which is a temporary address that gets assigned to a system every time it's connected to Internet. There are two standards for IP addresses. They are IPv4 and IPv6, where "v" stands for version.

Most of the systems are configured on IPv4 address system. Many of them are now moving to new IPv6 address system. The differences between the two versions are as follows:

5. IPv4 uses 32 binary bits. This type of address is written in a format which is separated by dots and is set of four numbers. For example: 216.27.61.137. Each number is the decimal representation for an eight-digit binary number, also called an octet. The decimal representation is called base-10 and the eight-digit binary representation is called base- 2.
6. IPv6 uses 128 binary bits. The address is represented by eight groups of hexadecimal numbers separated by colons. For example2001: cdba:0000:0000:0000:0000:3257:9652. The hexadecimal representation is also called base-16. Groups of numbers with all zeros, are mostly removed in order to save space, leaving a colon separating the groups, to mark the gap. For example, the previous example is written as 2001: cdba::3257:9652.

Subnet Mask

Helps in routing traffic within a subnet through a series of numbers. On an arrival of any packet at any organization's gateway, it routes it to its desired destination subnet number. A router identifies these number series to understand the routing. For an instance, in a binary mask,

- a "1" over a number denotes "Look at the number underneath;"
- a "0" denotes "Don't look."

Using such a mask prevents the router from handling the whole32 bit address. The router looks only at the bits selected by the mask.

Using the previous example, the combination of the network number and subnet number acquires 24 bits or three of the quads. The appropriate subnet mask for the packet would be: 255.255.255.0. It may also be represented as a string of all 1's for the first three quads and 0's for the host number. Subnet masking allows the routers to transfer the packets more quickly.

Ethernet Address

In computers or printers, a number which is assigned by a manufacturer to its hardware is referred to as an Ethernet or wireless address. To ensure the uniqueness of Ethernet and Wireless number all the manufactures work together under a code.

An Ethernet address, also known as wireless hardware address, is a 6-byte hexadecimal number. For example, 080007A9B2FC. Each byte is represented as two hexadecimal digits that makes the address of twelve hexadecimal digits, where each of these digits have a number between 0 to9 and a letter from A to F (can be either upper / lowercase).

Sometimes a '0x' is written before the value to indicate that the value should be interpreted as a hexadecimal one. But, the '0x' should not be taken as part of the value.

It is commonly seen that these are separated by six pairs of hexadecimal digits with colons or dashes. The letters A-F, are considered as hexadecimal digits. For example like: 08:00:07: A9:B2:FC or 00-00-94-ba-0e-cc. Leading zeros can be dropped; and the address is represented as 8:0:7:A9:B2:FC or 0:0:94:ba:e:cc.

Note: One should not confuse an Ethernet addresses with an IPv4 address.

MAC Address

It doesn't matter if one works in a wired network or wireless environment because it anyways takes software and hardware together for data transfer. For the right data to reach a specific system requires the addresses. It is important for the hardware to have its own address because of NIC; interface card. NIC is a circuit card through your computer gets connected to a network.

NIC converts date into electrical signals.

Every NIC has a hardware address called MAC; Media Access Control, which is related to hardware, as IP addresses are linked to TCP/IP.

Network adapter gets its unique MAC address during the time of manufacturing, and the IP address gets translated to MAC address by ARP (Address Resolution Protocol).

MAC address at times is also stated as the burned-in address (BIA). For example, 00:0a:95:9d:68:16 is a MAC address for an Ethernet NIC.

Dell, Belkin, Nortel and Cisco are some common manufacturers of NIC. These manufacturers put a unique number sequence, known as Organizationally Unique Identifier (OUI), in front of the MAC address identifying them as the manufacturer.

Example are as follows:

Dell: 00-14-22

Nortel: 00-04-DCO

Cisco: 00-40-96

Belkin: 00-30-BD

Larger manufacturers may have more than one set of OUIs.

Networks and MAC addresses

While diagnosing network issue MAC addresses are considered to be reliable because of their fixed addressed.

Wireless Routers and MAC Filtering

MAC filtering is a measure of security implemented on wireless networks to prevent unauthorized access by intruders or hackers. In such set up router are configured in a manner that they only accept traffic from specified addresses. This way, only approved MAC addresses computers communicate through the network.

3.1.3 Wired and Wireless CPE Configurations, Including VLAN, NAT, and QOS Settings

Customer Premises Equipment (CPE) refers to devices such as routers, switches, and access points installed at the customer's location to connect to broadband services. Proper configuration ensures optimal performance, security, and network segmentation.

a. Wired CPE Configuration

LAN Ports Setup: Configure static or dynamic IP addresses for devices connected via Ethernet.

VLAN (Virtual Local Area Network):

- Segments traffic logically within the same physical network.
- Used for separating different types of traffic, such as guest Wi-Fi, IoT devices, and internal systems.
- Example: VLAN 10 for office systems, VLAN 20 for guest access.

NAT (Network Address Translation):

- Allows multiple devices in a private network to share a single public IP address.
- Translates internal IP addresses to external ones, enhancing security and conserving IP resources.

QoS (Quality of Service):

- Prioritizes traffic based on type or application.
- Ensures critical applications like video conferencing or voice calls get higher bandwidth.

b. Wireless CPE Configuration

- **SSID Setup:** Configure multiple wireless networks with different access rules.
- **Security Protocols:** Use WPA3 or WPA2 encryption for protection.
- **Channel Selection:** Avoid interference by selecting optimal channels.
- **VLAN and QoS Integration:** Wireless traffic can also be segmented and prioritized using VLAN tags and QoS rules.

3.1.4 Basics of VPNs and Internet Lease Lines (ILL) and their Role in Secure Network Communications

a. VPN (Virtual Private Network)

- Creates a secure, encrypted tunnel between two networks over the internet.
- Used to connect remote workers, branch offices, or external devices safely.
- VPN types include:
  - Site-to-Site VPN: Connects two office networks.
  - Remote Access VPN: Allows individual users to securely access the network.

Benefits:

- Protects data from interception.
- Ensures authentication and privacy.
- Bypasses geo-restrictions.

b. Internet Lease Line (ILL)

- A dedicated, symmetrical, and high-speed connection between the customer and ISP.
- Provides consistent bandwidth, low latency, and guaranteed uptime.
- Ideal for businesses requiring secure, high-performance internet access.

Benefits:

- No shared bandwidth fluctuations.
- Better SLA (Service Level Agreements).
- Enhanced security and reliability.

3.1.5 IPv6 Addressing, Subnetting, NAT Configurations, and the Impact of QoS on Broadband Services

a. IPv6 Addressing

- A newer version of IP addressing that expands available address space from IPv4's 32

bits to 128 bits.

- Example: 2001:0db8:85a3:0000:0000:8a2e:0370:7334.
- Supports automatic address assignment and improved routing.

b. Subnetting

- Divides large networks into smaller, manageable segments.
- In IPv6, subnetting is used for organization and traffic management.
- Allows assigning subnets to different departments or device groups.

c. NAT in IPv6

- NAT is less common in IPv6 because of its vast address space.
- Direct addressability improves peer-to-peer connections but requires robust firewall configurations.

d. Impact of QoS

- QoS ensures that bandwidth is allocated according to priority.
- Reduces packet loss and jitter for latency-sensitive applications like VoIP and streaming.
- Helps manage bandwidth for smart devices, ensuring network stability.

3.1.6 Connectivity Options for CPE and End-User Devices, Including Advanced Wi-Fi Security Settings

Connectivity Options

Ethernet (Wired): Stable, high-speed connection with minimal interference.

Wi-Fi (Wireless): Convenient but susceptible to environmental interference.

Powerline Communication: Uses electrical wiring for network connectivity.

Fiber to the Premises (FTTP): High-speed connection via optical fiber.

Advanced Wi-Fi Security Settings

- **WPA3 Encryption:** Provides robust protection against brute-force attacks.
- **MAC Address Filtering:** Allows only authorized devices to connect.
- **Hidden SSID:** Prevents casual scanning by attackers.
- **Guest Network Segmentation:** Isolates guest traffic from internal devices.
- **Firmware Updates:** Regular updates patch known vulnerabilities.

3.1.7 Integrating Smart Home Systems with Broadband Networks

Smart home devices like Amazon Alexa, Google Home, and Apple HomeKit rely on broadband networks to function.

Integration Steps

1. Connect CPE to the Internet: Ensure stable connectivity with adequate bandwidth.
2. Assign Static or Reserved IP Addresses: For devices like hubs or smart controllers.
3. Enable Device Discovery: Allow automatic pairing protocols like mDNS.
4. Secure the Network:
    - Use strong passwords and encryption.
    - Isolate smart devices from critical data systems using VLANs.
5. Cloud Account Setup:
    - Link devices to vendor platforms for remote access and automation.
6. QoS Management:
    - Prioritize smart home traffic to ensure responsiveness.

3.1.8 Cybersecurity Fundamentals for Broadband Networks

a. Securing Home Networks

- Use complex passwords and avoid default credentials.
- Enable automatic firmware updates.
- Segment networks using VLANs or guest networks.

b. Firewall Configurations

- Block unauthorized inbound traffic.
- Allow specific outbound services only when necessary.
- Set rules for logging suspicious activity.

c. Threat Mitigation Strategies

- Use anti-malware tools.
- Regularly audit connected devices.
- Educate users on phishing, suspicious downloads, and unsafe practices.
- Implement intrusion detection systems (IDS).

3.1.9 Escalation Matrix for Troubleshooting Major Network Failures and Handling Emergencies

Escalation Process

1. First Level – Technician Response

- Perform basic diagnostics (restart, test cables, verify configurations).
- Resolve common issues such as device resets or loose connections.

2. **Second Level – Support Engineer**
    - Analyze system logs, run deeper tests (ping, traceroute).
    - Coordinate with upstream network teams.
3. **Third Level – Network Administrator**
    - Review security configurations, address routing failures, and manage service restoration.
4. **Fourth Level – Emergency Response**
    - In case of hardware failure or security breach, escalate to senior management.
    - Notify affected users, initiate backup services, and deploy incident response teams.

Emergency Handling

- Follow predefined contact protocols.
- Document the issue, response steps, and downtime.
- Post-incident review to prevent recurrence.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=uSKdjjw5zow

Network Topology

UNIT 3.2: Establishing Connectivity

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to ping the service provider gateway and analyze response time for troubleshooting.
2. Show how to analyze connectivity test results, including latency, throughput, and packet loss.
3. Demonstrate how to configure LAN/Wi-Fi connectivity, including SSID and security settings.

3.2.1 Basic Commands

IPCONFIG Command ipconfig

It is used to check the current IP and TCP setting. This even allows you to check the default gateway along with finding the subnet mask.

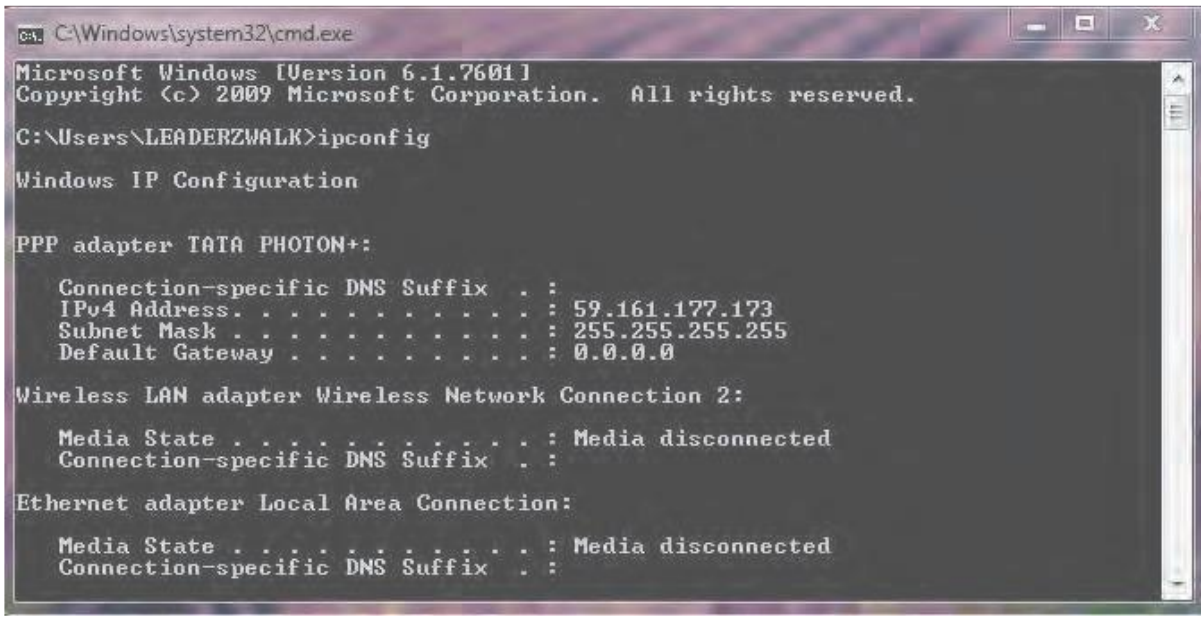


Fig 3.2.1 Ipconfig Command

ipconfig /all

This command lets a user check all information related to IP, DNS server and MAC Address.

One can even find the IP address of the gateway with this command.

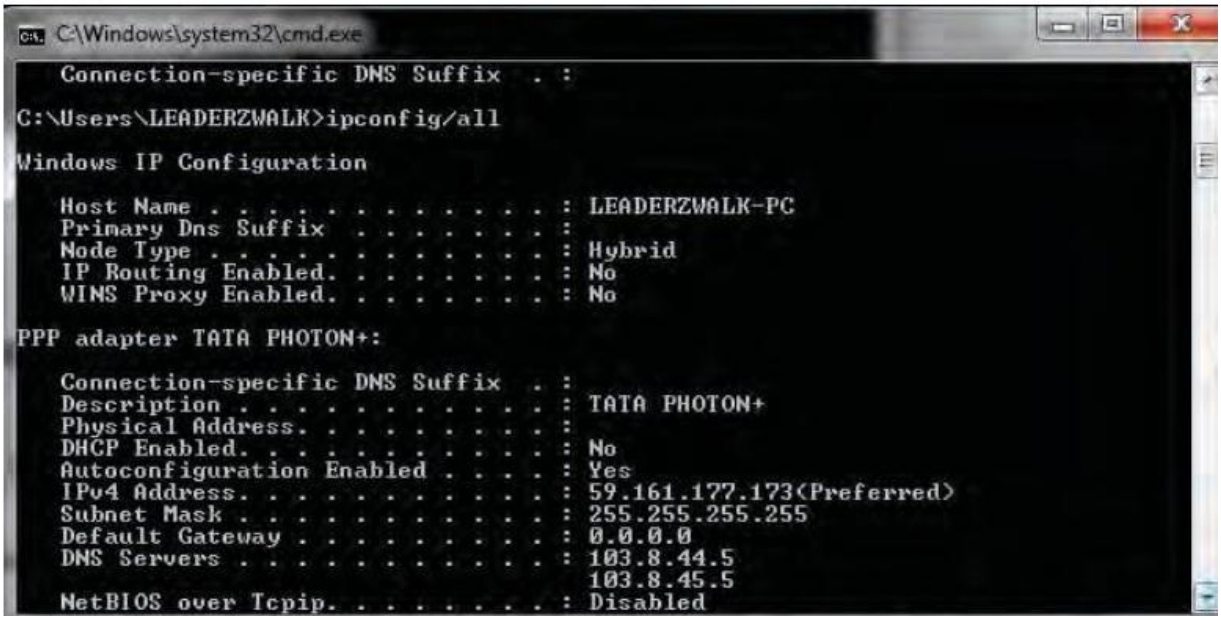


Fig 3.2.2 Finding IP address of gateway through ipconfig command

3.2.2 PING Command List

Ping

This is a primary TCP/IP command and is used to troubleshoot connectivity, name resolution and reachability. It verifies IP-level connectivity of a computer with another TCP/IP computer by sending Internet Control Message Protocol (ICMP) Echo request messages.

PING Command

In all of these examples **"xxx.xxx.xxx.xxx"** is an example of a Domain Name or an IP Address.

Ping **xxx.xxx.xxx.xxx**

To Ping an IP Address, type Ping followed by the IP address in the command prompt. “xxx.xxx.xxx.xxx” is representing the address here.

Ping <<site>>.com (web address)

To ping a website, the domain name of the website is to be typed following Ping. In case one is aware of websites IP Address, he/she may ping that too.

Ping Command Switches

The switches may be used together.

Continuous Ping (Ping xxx.xxx.xx.xx –t)

This will continue to run the ping process till Ctrl + C is used to stop. This is useful while troubleshooting intermittent connections.

Number of Pings (Ping xxx.xxx.xx.xx -n 10)

The switch "n" is used to set the number of pings. By default, the ping command transmits 4 packets of 32 bytes each.

Size of Packet (Ping xxx.xxx.xx.xx -l 1500)

By default, 32 bytes is used for sending packets. One can set the size up to the maximum of 65500 bytes. This comes handy while running a stress test on any local network.

Time Out (Ping xxx.xxx.xx.xx -w 5000)

The time given, is in milliseconds. Default timeout is 4,000 milliseconds, amounting to 4 seconds.

Resolving Host name Address (Ping -a xxx.xxx.xx.xx)

This is used for finding the model number of a router. Host of an IP address can be resolved by using this command.

Notes

UNIT 3.3: Connectivity of CPE and End User Devices

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to connect a laptop/PC, smart/IP TV, IoT devices, and other customer devices to the CPE and establish connectivity.
2. Show how to configure the CPE with base settings, including IP, gateway, mask, NAT, QoS, and enable IPv6 support.
3. Demonstrate setting up a VPN or Internet Lease Line (ILL) based on customer requirements.
4. Show how to apply basic cybersecurity settings such as strong password policies, firewalls, and MAC filtering.
5. Show how to verify all cables and connectors are properly plugged in and functional.
6. Demonstrate how to configure LAN/Wi-Fi connectivity, including SSID and security settings.
7. Show how to integrate broadband with smart home systems like Amazon Alexa, Google Home, or Apple HomeKit.

3.3.1 Broadband Connectivity

A telecommunications hardware that is positioned at customer's home or at the business of a customer is referred to as CPE device. Some examples of such equipment are set-top boxes which are used for cable, digital subscriber line or broadband routers, VoIP base stations, telephone handsets, etc.

In most cases, such devices need to support Wi-Fi 6 or 10G connections to mobile phones, laptops, tablets, game consoles, and smart home devices. Internet of Things (IoT) devices are challenging as they can't connect to main CPE.

Following illustrations explains the broadband connectivity from the main infrastructure to end users' devices. Which can be a computer, telephone, television sets, and digital cameras. Packet-based infrastructure is allowed by the gateway equipment.

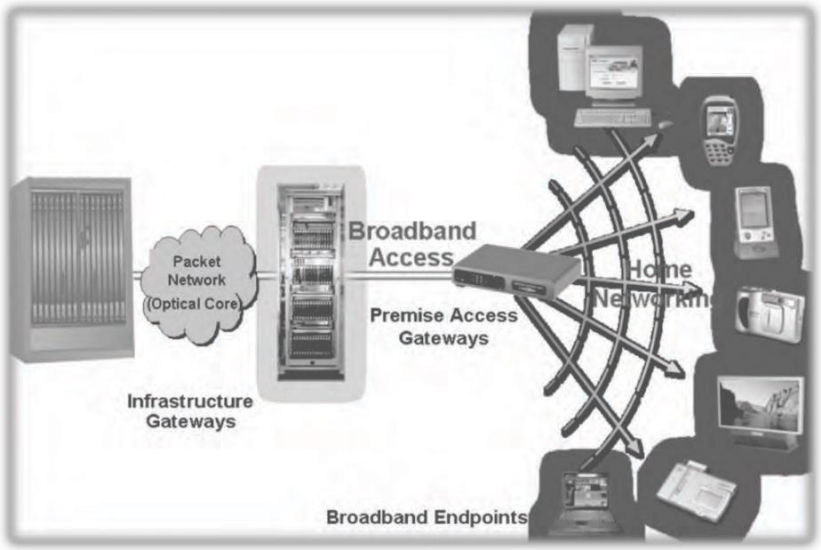


Fig 3.3.1: Broadband Connectivity

3.3.2 Connectivity

Once the installation of CPE is completed one can connect either a computer or other devices to the Internet.

Fig 3.3.2: Steps for Internet browsing

If the desired website opens, it means the Internet is connected. If not, recheck the Website address. If the problem persists, it's advised to check the cable connection and re configure the modem/router.

3.3.3 Configurating TCP/ IP for Windows 11

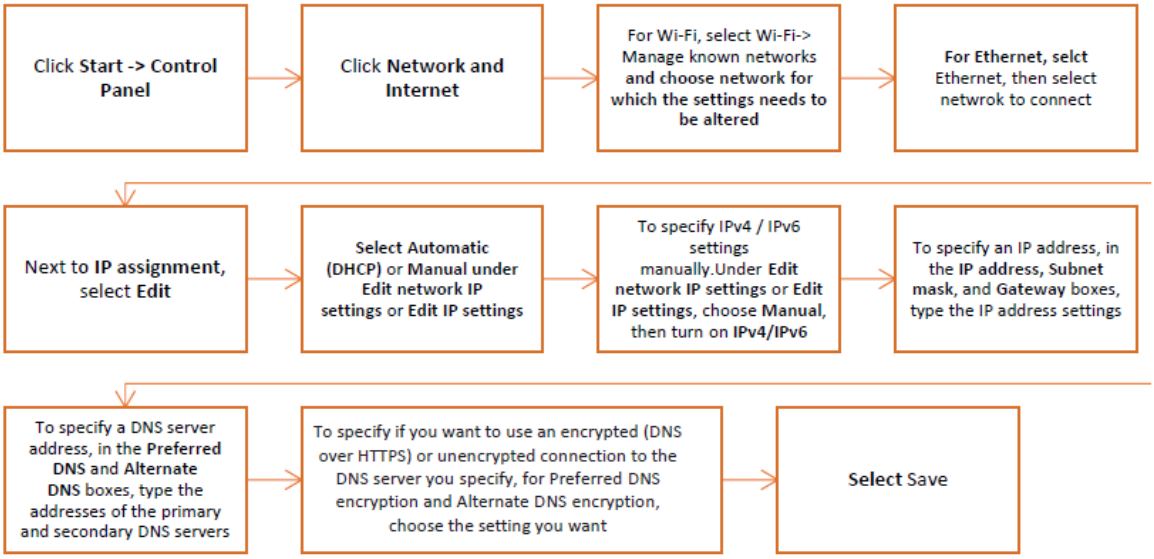


Fig 3.3.3 Steps to configure TCP/IP

3.3.4 Connecting Customer Devices to the CPE and Establishing Connectivity

The Customer Premises Equipment (CPE), such as a router or gateway, serves as the central point where all devices connect to access broadband services. Different devices—laptops, PCs, smart TVs, IoT devices, and others—can be connected either via wired (Ethernet) or wireless (Wi-Fi) interfaces. Below is a structured guide showing how to connect these devices and ensure proper network access.

1. Connecting a Laptop/PC to the CPE

A. Wired Connection (Using Ethernet Cable)

1. Locate the LAN ports on the CPE (usually labeled LAN1, LAN2, etc.).
2. Plug one end of the Ethernet cable into the laptop/PC's network port.
3. Insert the other end into an available LAN port on the CPE.
4. Verify connection:
   - The network icon should show connectivity.
   - The laptop/PC should automatically obtain an IP address if DHCP is enabled.
5. Test connectivity by opening a web browser and visiting a website.

B. Wireless Connection (Wi-Fi)

1. On the laptop/PC, open the Wi-Fi settings.
2. Search for the SSID broadcasted by the CPE.
3. Select the correct network and enter the password.
4. Once connected, ensure internet access by browsing websites or checking network settings.

2. Connecting a Smart/IP TV to the CPE

A. Wired Connection

1. Insert one end of the Ethernet cable into the TV's Ethernet port.
2. Connect the other end to the CPE's LAN port.
3. Access the TV's network settings and ensure DHCP is enabled or assign a static IP if required.
4. Test the connection by streaming content or checking for software updates.

B. Wireless Connection

1. Access the TV's network settings.
2. Select the appropriate Wi-Fi network name.
3. Enter the password provided by the customer.
4. Confirm connection and test internet access via streaming apps or live channels.

3. Connecting IoT Devices (Smart Lights, Cameras, Thermostats, etc.)

A. Wireless Connection

1. Ensure the IoT device supports Wi-Fi and is powered on.
2. Open the manufacturer's mobile app or control interface.
3. Follow setup instructions to connect the device to the customer's Wi-Fi network.
4. Confirm successful pairing by observing the device's status indicator or app confirmation.

B. Wired Connection (For Devices That Support Ethernet)

- Connect the device's Ethernet port to the CPE's LAN port using a cable.
- Verify connectivity through the app or user interface.

C. Security Considerations

- Place IoT devices on a separate VLAN or guest network if supported.
- Use strong, unique passwords for device accounts.
- Enable firmware updates automatically where possible.

4. Connecting Other Customer Devices (Printers, Game Consoles, Media Players, etc.)

A. Wired

- Plug the device's Ethernet cable into the CPE's LAN port.
- Configure the device's network settings as needed.
- Test by performing a network operation like printing or downloading updates.

B. Wireless

- Access the device's network menu.
- Scan for available Wi-Fi networks.
- Choose the correct SSID and input the network password.
- Verify connection by running a test function.

5. Verifying Network Connectivity

After connecting any device:

- Check the device's network status.
- Confirm that it has obtained an IP address from the CPE.
- Test internet access by browsing or streaming content.
- Check for stable connectivity without frequent drops or errors.

Issue	Possible Cause	Solution
No internet access	Incorrect Wi-Fi password	Re-enter the password carefully
Wired connection not detected	Faulty Ethernet cable	Replace or reconnect the cable
Device not appearing in network	DHCP disabled or IP conflict	Restart CPE, check settings, or assign static IP
Slow speeds	Interference or weak Wi-Fi	Change Wi-Fi channel or move closer to CPE

3.3.5 Setup of a VPN or Internet Lease Line (ILL) Based on Customer Requirements

Setting up a Virtual Private Network (VPN) or Internet Lease Line (ILL) requires understanding the customer's needs, configuring the devices appropriately, and ensuring secure and reliable connectivity. Below is a structured, textbook-style guide showing how to set up both VPN and ILL for customer networks.

1. Understanding Customer Requirements

Before setting up VPN or ILL, it is important to gather the following information:

- **For VPN:**
  - Type of VPN required (site-to-site, remote access).
  - Number of users or locations to connect.
  - Required encryption protocols (IPSec, SSL/TLS).
  - Devices or servers that need access.
- **For ILL:**
  - Required bandwidth (symmetric or asymmetric).
  - Service level agreements (uptime, latency).
  - Type of connection (fiber, copper, etc.).
  - Backup or failover requirements.

Discuss these details with the customer, review security policies, and ensure compatibility with existing infrastructure.

Setting Up a VPN

A. Hardware/Software Requirements

- CPE router with VPN capability.
- VPN client software (for remote users).
- Authentication keys or credentials.

B. Steps to Set Up Site-to-Site VPN

1. Access the CPE Configuration Interface
   - Login via web portal using admin credentials.

2. Enable VPN Service

- Navigate to VPN settings.
- Choose the VPN type (e.g., IPSec).

3. Configure Tunnel Parameters

- Enter the remote network's IP address or hostname.
- Set the encryption algorithm (AES-256).
- Configure the authentication method (pre-shared key or certificates).

4. Define Local and Remote Subnets

- Local subnet example: 192.168.1.0/24.
- Remote subnet example: 10.0.0.0/24.

5. Set Routing Rules

- Allow traffic to flow between the local and remote networks.
- Ensure policies are in place for permitted traffic types.

6. Test the VPN Tunnel

- Ping devices across the VPN.
- Confirm that files and services are accessible.

C. Setting Up Remote Access VPN

1. Enable VPN Server Functionality

- Allow users to connect individually.

2. Create User Accounts

- Assign usernames, passwords, and access permissions.

3. Configure Firewall Rules

- Permit VPN traffic through secure ports.

4. Distribute VPN Client Software

- Provide configuration files and instructions.

5. Test User Access

- Validate connection from external devices.

Setting Up an Internet Lease Line (ILL)

A. Requirements

- Dedicated circuit from ISP.
- Compatible router or gateway at the customer site.
- Authentication credentials or static IP addresses.

B. Steps to Configure ILL

1. Connect the Physical Line

Fiber or copper line connected to the CPE's WAN port.

2. Enter ISP Credentials

- Configure static IP, gateway, and DNS addresses provided by the ISP.

3. Set Routing Preferences

- Define default routes pointing to the leased line.
- Configure backup routes if required.

4. Enable Monitoring Tools

- Set alerts for uptime, packet loss, and latency.

5. Perform Speed and Stability Tests

- Validate connection using tools like ping, traceroute, or throughput tests.

6. Document Configuration

- Save IP assignments, credentials, and contact details for support.

4. Security Measures During Setup

- Change default admin passwords.
- Enable encryption protocols where possible.
- Restrict access to authorized devices and users.
- Set firewall rules to prevent unauthorized entry.
- Regularly monitor VPN or ILL for anomalies.

5. Testing and Customer Verification

A. Verify End-to-End Connectivity

- Perform tests from local and remote devices.

b. Check Performance Metrics

- Ensure bandwidth, latency, and jitter meet expectations.

c. Walk Customers Through Access

- Show how to use the VPN client or monitor the leased line.

d. Provide Documentation

- Share configuration details, troubleshooting steps, and contact information.

e. Obtain Customer Sign-Off

- Confirm that the network is functioning as per their requirements.

3.3.6 Integrating Broadband with Smart Home Systems (Amazon Alexa, Google Home, Apple HomeKit)

Integrating broadband with smart home systems enables customers to control devices such as lights, thermostats, cameras, and appliances remotely or through voice commands. A properly configured broadband network ensures seamless communication between devices and cloud services, providing convenience, automation, and enhanced security.

1. Importance of Integration

- Enables centralized control of devices.
- Supports automation scenarios like scheduling, voice control, or remote management.
- Ensures stable and secure communication between devices.
- Enhances user experience by providing faster response times and reliable connectivity.

2. Pre-Integration Requirements

Before beginning the integration process, ensure the following:

A. Stable Broadband Connection

- Adequate bandwidth to support multiple devices.
- Reliable router or CPE with strong Wi-Fi signals or Ethernet ports.

2. Compatible Devices

- Smart speakers, displays, hubs, or accessories supporting Alexa, Google Home, or HomeKit.
- Devices should be powered on, reset if needed, and ready for pairing.

3. User Accounts

- Amazon, Google, or Apple accounts set up.
- Authentication and permissions configured for secure access.

4. Updated Firmware

- Ensure the router/CPE and smart devices are updated to the latest versions to avoid compatibility issues.

3. Integration with Amazon Alexa

Steps

1. Connect the Smart Device to Broadband

- Via Wi-Fi: Join the device to the customer's Wi-Fi network using the mobile app.
- Via Ethernet: Connect the hub to the router's LAN port if applicable.

2. Open the Alexa App

- Download and install the Amazon Alexa app.
- Sign in with the customer's Amazon account.

3. Add Device

- Tap "Devices" → "Add Device."
- Select the correct category (light, camera, thermostat, etc.).
- Follow prompts to connect the device to the broadband network.

4. Enable Skills

- In the Alexa app, go to "Skills & Games."
- Search for the device's brand and enable the skill.
- Authenticate with third-party credentials if required.

5. Test Voice Commands

- Ask Alexa to control the device, e.g., "Alexa, turn on the living room lights."

4. Integration with Google Home

Steps

1. Ensure Device Connectivity

- Connect via Wi-Fi or Ethernet, depending on the device type.

2. Open Google Home App

- Download the app from the App Store or Google Play Store.
- Sign in with the Google account.

3. Set Up Device

- Tap "Add" → "Set up device."
- Choose "Works with Google" to link third-party devices.
- Follow the manufacturer's instructions for authentication.

4. Configure Rooms and Routines

- Assign devices to rooms.
- Create automation routines such as "Good Morning" or "Away Mode."

5. Test Functionality

- Use commands like "Hey Google, set the thermostat to 72°F."

5. Integration with Apple HomeKit

Steps:

- **Connect the Device**
  - ✓ Join the device to the customer's Wi-Fi network.
- **Open the Apple Home App**
  - ✓ Use an iPhone or iPad running the latest iOS version.
  - ✓ Sign in with the Apple ID linked to iCloud.
- **Add Accessory**
  - ✓ Tap "+" → "Add Accessory."
  - ✓ Scan the HomeKit setup code on the device or its manual.
- **Configure Settings**
  - ✓ Assign devices to rooms and create scenes (e.g., "Movie Night").
- **Test Control**
  - ✓ Use Siri commands like "Hey Siri, turn off the bedroom lights."

6. Network Configuration Tips for Smart Home Integration

- **Assign Static IPs**
  - ✓ Reserve IP addresses for hubs and critical devices to ensure stable communication.
- **Use Separate Wi-Fi Networks**
  - ✓ Create guest or IoT networks to isolate smart devices from sensitive systems.
- **Enable Firewall Rules**
  - ✓ Allow communication between smart hubs and cloud servers while blocking unauthorized access.
- **Optimize Wi-Fi Coverage**
  - ✓ Place routers in central locations and reduce interference for seamless operation.

7. Security Best Practices

- Use strong, unique passwords for the broadband router and cloud accounts.
- Enable two-factor authentication wherever available.
- Regularly update device firmware and apps to patch vulnerabilities.
- Educate users on avoiding phishing and unauthorized access attempts.

8. Testing and Verification

1. **Check Device Connectivity**
   - Ensure devices are connected to the network and visible in the app.
2. **Perform Functional Tests**
   - Trigger actions such as turning lights on/off or adjusting settings.
3. **Monitor Response Time**
   - Ensure commands are executed without noticeable delays.
4. **Check Remote Access**
   - Verify that devices can be controlled from outside the home network.

3.3.7 Verifying All Cables and Connectors Are Properly Plugged In and Functional

Ensuring that all cables and connectors are securely connected and functioning properly is critical during broadband installation or troubleshooting. Faulty connections can lead to poor performance, intermittent connectivity, or total service failure. Below is a structured, textbook-style explanation demonstrating how to verify cables and connectors.

1. Importance of Verifying Cables and Connectors

Prevents service interruptions caused by loose or damaged cables.

- Ensures optimal signal strength and transmission quality.
- Avoids time-consuming troubleshooting later.
- Enhances safety by ensuring proper grounding and shielding.
- Supports stable performance for wired and wireless devices.

2. Visual Inspection of Cables and Connectors

Steps

1. **Turn off all devices temporarily to avoid accidental short circuits during inspection.**
2. **Check physical connections:**
   - Ensure connectors are fully inserted into ports (Ethernet, coaxial, power cables).
   - Look for bent or broken pins in RJ45 connectors or USB ports.
   - Verify that fiber connectors are clean and dust-free.
3. **Inspect cable integrity**:
   - Look for cuts, abrasions, or sharp bends.
   - Ensure cables are not stretched tightly or crushed under furniture.
4. **Check labeling:**
   - Confirm that each cable is correctly labeled according to its purpose (WAN, LAN1, etc.).

3. Using Tools to Verify Functionality

A. LAN Tester / Cable Tester

1. Plug both ends of the Ethernet cable into the tester ports.
2. Turn the tester on and observe the LEDs:
   - A sequence of lights confirms proper continuity.
   - Missing or flickering lights indicate a fault or loose connection.
3. Repeat the process for each cable in use.

B. PoE Tester (for Power over Ethernet)

1. Insert the cable ends into the tester.
2. Check if power is being delivered to devices requiring PoE.
3. Identify issues like under-voltage, reversed pairs, or no power delivery.

C. Multimeter (for Advanced Testing)

- Measure continuity between connector pins.
- Check for proper grounding.
- Verify that power supplies are delivering the correct voltage.

4. Functional Testing After Plugging In

A. Ethernet / Wired Connections

- Check if the device is obtaining an IP address from the router.
- Perform a "ping" test to confirm communication between devices.
- Use a speed test tool to ensure performance meets expectations.

B. Power Connections

- Verify that the device powers on without flickering or overheating.
- Check LED indicators to confirm status (power, activity, link).
- Confirm that backup power (UPS or PoE) is working.

C. Fiber Connections

- Use an Optical Time Domain Reflectometer (OTDR) to test fiber continuity and loss.
- Inspect connectors with a microscope or lens to ensure cleanliness.

5. Troubleshooting Common Issues

Symptom	Possible Cause	Verification Action
No connectivity	Loose connector or unplugged cable	Re-seat the connection and test continuity
Slow speeds	Damaged or long cable run	Replace cable or test attenuation
Intermittent signals	Faulty connector or interference	Check shielding and connector pins
No power delivery	PoE not configured or faulty cable	Use PoE tester to confirm

6. Safety Precautions During Verification

- Always power off devices when handling connectors.
- Avoid touching exposed wires or metal parts.
- Use tools certified for electrical testing.
- Wear personal protective equipment (PPE) if working near power supplies or outdoor installations.
- Ensure cables are not tangled or under tension.

7. Documenting Results

- Maintain a checklist for each cable and port connection.
- Record test results, including date, technician name, and any corrective actions.
- Take photos of properly installed cables for reference and audits.

Notes

UNIT 3.4: Configuration Testing

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to ping the service provider gateway and analyze response time for troubleshooting.
2. Show how to analyze connectivity test results, including latency, throughput, and packet loss.
3. Show how to ping the CPE from an end-user device, analyze the response, and optimize network settings for stability.
4. Demonstrate how to enable Quality of Service (QoS) settings to prioritize network traffic based on user needs.
5. Demonstrate how to record CPE configuration settings, including network security configurations and VPN/ILL setups.
6. Show how to document end-user device configurations, including IP allocation and firewall settings.
7. Demonstrate how to record the pinging procedure and expected result parameters for troubleshooting reference.

3.4.1 Verifying IP address in Windows 11 for Wi-Fi

Once TCP/IP configuration is complete in windows 11, go for verifying the IP Address

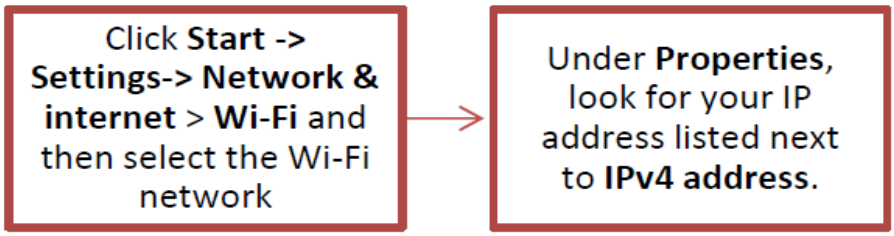
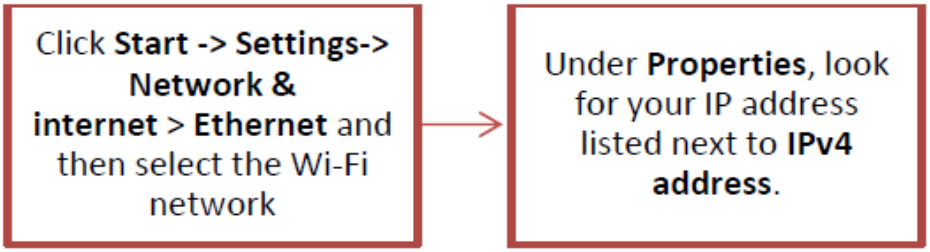


Fig 3.4.1: Steps to test TCP/IP configuration Windows 11

3.4.2 Verifying IP address in Windows 11 for Ethernet

Once TCP/IP configuration is complete in windows 11, go for verifying the IP Address



3.4.3 Ping the Service Provider Gateway and Analyze Response Time

The ping command is a fundamental network diagnostic tool used by broadband technicians to check connectivity between a customer's device and the service provider's gateway (the first hop outside the local network). By analyzing the response time and packet statistics, technicians can determine whether connectivity issues originate from the local network, the customer premises equipment (CPE), or the service provider's network.

1. Purpose of Ping Test

- Verify that the customer's device can reach the ISP gateway.
- Measure latency (response time) between the device and gateway.
- Detect packet loss, which can indicate cable faults, interference, or misconfigured equipment.
- Confirm that the CPE (modem/router) is functioning properly.
- Narrow down troubleshooting areas before escalating issues.

2. Steps to Perform a Ping Test

Step 1: Identify the Service Provider Gateway

- Log in to the CPE/router (using 192.168.0.1 or 192.168.1.1 typically).
- Navigate to WAN/Status page to find the ISP-assigned default gateway IP.
- This IP is the first external hop, usually within the ISP's network.

Step 2: Open the Command Interface

- On Windows: Press Win + R, type cmd, and press Enter.
- On Linux/macOS: Open Terminal.

Step 3: Execute Ping Command

- Type:
- ping <gateway_IP>

Example:

ping 100.72.1.1

Press Enter. The system will send ICMP echo requests and receive replies from the gateway.

3. Analyzing the Ping Results

A standard ping result displays:

Reply from 100.72.1.1: bytes=32 time=12ms TTL=60

Key Metrics

1. Bytes – Size of the packet sent.

2. Time (ms) – Response time / latency between device and gateway.

- <20 ms = Excellent (local network working fine).
- 20–100 ms = Acceptable (normal ISP latency).
- 100 ms = Potential congestion or line issue.

3. TTL (Time To Live) – Number of hops allowed; helps confirm routing.

Packet Statistics

After the test ends, results show:

- Packets Sent, Received, Lost
  - ✓ 0% loss = Good connection.
  - ✓ 0% loss = Possible cable fault, wireless interference, or service issue.
- Round-Trip Times (Minimum, Maximum, Average)
  - ✓ Helps check for jitter (variation in latency).
  - ✓ Large variation indicates unstable connection.

4. Troubleshooting Based on Ping Results

Symptom	Possible Cause	Technician Action
High latency (>100 ms)	Network congestion, routing issues	Check local traffic, escalate to ISP if external
Packet loss (10–100%)	Loose cable, wireless interference, damaged connector	Inspect and replace cables, relocate router
Request timed out	Gateway unreachable, CPE misconfigured	Verify router WAN settings, reboot equipment
Stable ping locally, unstable to ISP gateway	External ISP issue	Escalate to ISP NOC team

3.4.4 Ping the CPE from an End-User Device, Analyze the Response, and Optimize Network Settings for Stability

Pinging the Customer Premises Equipment (CPE) from an end-user device (such as a laptop, smartphone, or tablet) is one of the first diagnostic steps to check whether the local network is functioning properly. By analyzing the results, technicians and users can identify issues like packet loss, high latency, or unstable connections and take corrective actions by optimizing network settings

1. Purpose of Pinging the CPE

- Verify that the end-user device is connected to the local network.
- Check for proper communication between the device and router/modem.
- Analyze latency, jitter, or packet loss that may cause unstable connectivity.
- Identify whether problems are within the local setup or external to it.
- Assist in troubleshooting and optimizing network performance.

.

2. Steps to Ping the CPE from an End-User Device

Step 1: Identify the CPE's IP Address

1. Windows:

- Open Command Prompt and type ipconfig.
- Look for Default Gateway (e.g., 192.168.1.1).

2. macOS/Linux:

- Open Terminal and type ifconfig or ip route.
- Identify the gateway IP (e.g., 192.168.1.1).

3. Smartphones/Tablets:

- Access Wi-Fi settings → Tap on the connected network → Find gateway address.

Step 2: Run the Ping Command

1. On Windows:
2. ping 192.168.1.1
3. On macOS/Linux:
4. ping -c 10 192.168.1.1
5. On Android/iOS (using network utilities app):

- Open the app → Enter the gateway IP → Tap "Ping".

Step 3: Observe and Analyze the Response

Example output:

Reply from 192.168.1.1: bytes=32 time=4ms TTL=64

Key Metrics

Time (ms):

- <10 ms → Excellent connection.
- 10–50 ms → Acceptable but may need monitoring.
- 50 ms → Potential interference or congestion.

Packet Loss:

- 0% → Ideal.
- 1–5% → Possible network instability.
- 5% → Problematic; may require troubleshooting.

Jitter:

If response times vary widely, connection instability is present.

3. Optimizing Network Settings for Stability

A. Adjust Router Placement

- Place the CPE centrally to ensure equal Wi-Fi coverage.
- Avoid interference from walls, electronic devices, or metal objects.

B. Check Wireless Channel

- Use tools or router settings to find the least congested channel.
- Switch to a higher frequency (5 GHz or 6 GHz where available) for faster, interference-free communication.

C. Secure Network Access

- Use strong passwords and encryption (WPA3/WPA2).
- Restrict unknown devices from accessing the network.

D. Update Firmware

- Keep the router's firmware up to date to fix bugs and enhance performance.

E. Limit Background Applications

- Ensure devices running large downloads or video streams aren't hogging bandwidth unnecessarily.

F. Enable QoS (Quality of Service)

- Prioritize essential traffic like video calls or work-related applications.
- Reduce latency spikes and jitter during peak usage.

G. Configure IP Settings

- Assign static IPs to devices prone to disconnection.
- Avoid IP conflicts by ensuring DHCP settings are configured correctly.

4. Advanced Diagnostics

- Traceroute: Shows the path taken to the gateway and helps identify hops causing delays.
- Speed Test: Confirms throughput to ensure it matches the plan subscribed.
- Network Monitoring: Apps or built-in tools that monitor latency over time to spot patterns of degradation.

5. Troubleshooting Based on Ping Results

Observation	Possible Cause	Recommended Action
High latency (>50 ms)	Distance from router, interference	Move closer or adjust router settings
Packet loss (>5%)	Weak signal, faulty cable, overheating device	Inspect cables, reboot devices, reduce interference
Inconsistent times (jitter)	Network congestion or interference	Enable QoS, limit background apps
No response	IP mismatch, device disconnected	Verify IP, reconnect, restart router

3.4.5 Analyze Connectivity Test Results – Latency, Throughput, and Packet Loss

After performing connectivity tests, such as ping, speed test, or network analyzer checks, it is essential to interpret the results to identify issues affecting network performance. The three most important metrics are:

- **Latency –** The time taken for data to travel between devices.
- **Throughput –** The actual speed at which data is transferred.
- **Packet Loss –** The percentage of data packets lost during transmission.

Understanding these results helps technicians troubleshoot problems, optimize settings, and ensure reliable broadband service.

1. Analyzing Latency (Response Time)

Latency is the delay, measured in milliseconds (ms), between sending a request and receiving a response from the destination device (CPE or service provider gateway).

Typical Causes of High Latency

- Long cable runs or poor-quality cables.
- Wireless interference from other devices.
- Network congestion.
- Routing issues in the ISP's network.

Interpreting Latency Values

Latency Range	Interpretation	Actions
<20 ms	Excellent	No action needed
20–50 ms	Acceptable	Monitor usage patterns
50–100 ms	Warning sign	Check interference or congestion
>100 ms	Poor	Investigate cables, router settings, or ISP connection

How to Use Latency Results

- If ping times are consistent and low → stable connection.
- If times fluctuate widely → jitter may affect performance.
- If times are consistently high → check router placement, firmware, or cable quality.

2. Analyzing Throughput (Speed Test Results)

Throughput refers to the amount of data successfully transmitted over the network in a given time, measured in Mbps (megabits per second).

Factors Affecting Throughput

- ISP bandwidth limits.
- Hardware capacity (router, cables).
- Number of devices sharing the network.
- Background applications consuming bandwidth.

Interpreting Throughput Results

Measured Speed	Expected Outcome	Actions
≥80% of subscribed speed	Good connection	Monitor periodically
50–80%	Moderate performance	Check for network congestion or interference
<50%	Poor	Inspect cables, firmware, or ISP issues

Using Throughput Results

- Compare results from wired and wireless tests.
- Identify whether throughput drops during peak usage.
- Test multiple devices to confirm network-wide issues.

3. Analyzing Packet Loss

Packet loss occurs when data packets fail to reach their destination. It is expressed as a percentage (%) of total packets sent.

Causes of Packet Loss

- Damaged cables or connectors.
- Interference in wireless networks.
- Router buffer overflows.
- Faulty network equipment or overheating.

Interpreting Packet Loss Results

Packet Loss (%)	Interpretation	Actions
0%	Ideal, stable connection	No action needed
<1%	Normal fluctuations	Monitor network activity
1–5%	Noticeable	Inspect cables and interference
>5%	Severe issue	Replace hardware or escalate to ISP

3.4.6 Quality of Service (QoS) Settings

Quality of Service (QoS) is a network feature that helps prioritize certain types of traffic, ensuring that critical applications like video calls, gaming, or remote work receive the necessary bandwidth even when the network is congested. By enabling and configuring QoS settings on the CPE (router/modem), technicians can improve user experience and ensure smooth performance for high-priority applications.

1. When to Use QoS

- During peak usage hours when multiple devices share the connection
- For business-critical applications like video conferencing or VoIP
- For households with streaming services, online gaming, or remote learning
- When troubleshooting latency or jitter issues
- To allocate bandwidth fairly among users

2. Pre-Configuration Requirements

- Access to the router/CPE's administration panel via browser or app
- Administrative login credentials
- Knowledge of devices or applications that require prioritization
- Understanding of available QoS options supported by the device

3. Step-by-Step Guide to Enable QoS

Step 1 – Log into the Router/CPE

- Open a browser and enter the router's IP address (usually 192.168.1.1 or 192.168.0.1).
- Enter the username and password provided by the ISP or set during installation.
- **Step 2 – Locate QoS Settings**
- Navigate to sections like:
- Advanced Settings → QoS
- Traffic Control → Priority Settings
- Some routers have a dedicated QoS Setup Wizard.

Step 3 – Enable QoS

- Toggle the option to Enable QoS or Traffic Prioritization**.**

Step 4 – Choose a QoS Type

Common options include:

- **By Application**
  Prioritize traffic based on services like video streaming, VoIP, gaming, or browsing.
- **By Device**
  Prioritize traffic for specific devices (laptops, smart TVs, or IP phones).
- **By Ethernet Port**
  Assign priority based on which port the device is connected to.
- **Bay Bandwidth Allocation**
  Set maximum or minimum bandwidth limits for devices or services.

Step 5 – Define Rules

Example:

- Set Video Calls (Zoom, Teams) → High Priority
- Set Streaming services (Netflix, YouTube) → Medium Priority
- Set Browsing, Downloads → Low Priority

For device-based rules:

- Assign Laptop (Work-from-home) → High Priority
- Assign Gaming Console → Medium Priority
- Assign Smartphone → Normal Priority

Step 6 – Save and Apply

- After selecting priorities, click Save, Apply, or Activate.
- The router may reboot to apply settings.

Step 7 – Test QoS Functionality

- Run latency-sensitive tasks like video calls.
- 2Start streaming or downloading on another device.
- Verify that the prioritized device or application remains responsive and unaffected by network load.

Notes

UNIT 3.5: Comprehension and Interpretation of Technical Data

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to brief customers on basic troubleshooting steps/self-help techniques, including cybersecurity best practices.
2. Demonstrate how to guide customers in monitoring network activity and updating firmware for security and performance improvements.

3.5.1 Interpretation of Technical Data

It is very important for a broadband technician to know how to interpret the technical data. He should be aware of technical data and its interpretation.

Let's learn to read and understand IP Configuration and network problems.

Configuration of Internet protocol is the backbone of Internet service and networking. Various settings on the system can be checked with IP Config utilities. In such a case, one should start from finding a network issue.

To start with, open command prompt and type "ipconfig /all". Only type the command itself into a command window. Start - Run - "ipconfig /all..." should not be typed.

Export the data to text file for easy access, type the following commands one by one:

- "ipconfig /all >c:\ipconfig.txt" (less the "")
- "notepad c:\ipconfig.txt" (less the ""), for immediate examination.
- Or, copy file to another computer by typing "c: \ipconfig.txt", for comparative examination.

The following image shows an example of IPConfig ("ipconfig /all") from a pair of computers on a LAN:

```
Windows IP Configuration
Host Name . . . . . . . . . . . . : Search1
Primary Dns Suffix . . . . . . . :Node
Type . . . . . . . . . . . . . . : Broadcast IP
Routing Enabled. . . . . . . . . : No
WINS Proxy Enabled. . . . . . . . : No
DNS Suffix Search List. . . . . . : search.net

Ethernet adapter Local Area
connection:
Connection-specific DNS Suffix. :
```

```
Description . . . . . . . . . . . : 3Com Ether Link XL 10/100 PCI For
Complete PC Management NIC (3C905C-TX)
Physical Address. . . . . . . . . : 00-04-76-D7-C5-6A
Dhcp Enabled. . . . . . . . . . . : Yes
Auto configuration Enabled . . . . : Yes
IP Address . . . . . . . . . . . . : 92.168.1.50
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.11
192.168.1.33
Lease Obtained . . . . . . . . . . : Wednesday, April 16, 20 15 11:19:12
Lease Expires . . . . . . . . . . : Wednesday, April 23, 20 15 11:19:12
```

```
Windows IP Configuration
Host Name . . . . . . . . . . . . : PChuck2
Primary Dns Suffix . . . . . . . :
Node Type . . . . . . . . . . . . : Hybrid IP
Routing Enabled. . . . . . . . . : No
WINS Proxy Enabled. . . . . . . . : No
DNS Suffix Search List. . . . . . : search.net
```

```
Ethernet adapter Local Area
connection:
Connection-specific DNS Suffix:
Description . . . . . . . . . . . : 3Com Ether Link XL 10/100 PCI For
Complete PC Management NIC (3C905C-TX)
Physical Address. . . . . . . . . : 00-04-76-D7-76-BC
Dhcp Enabled. . . . . . . . . . . : Yes
Auto configuration Enabled . . . . : Yes
IP Address . . . . . . . . . . . . : 92.168.1.51
Subnet Mask . . . . . . . . . . . : 255.255.255.0
Default Gateway . . . . . . . . . : 192.168.1.1
DHCP Server . . . . . . . . . . . : 192.168.1.1
DNS Servers . . . . . . . . . . . : 192.168.1.11
192.168.1.33
Primary WINS Server . . . . . . . : 192.168.1.1
Lease Obtained . . . . . . . . . . : Wednesday, April 16, 2015 11:53:45
Lease Expires . . . . . . . . . . : Wednesday, April 23, 2015 11:53:45
```

1. What does this tell us?
2. Host Name . . . . . : Search1
3. This is the name of the computer, as seen by Internet Protocol.PrimaryDns..
4. DNS Suffix Search List. . . . . : search.net

3.5.2 Monitoring Network Activity and Updating Firmware for Security and Performance Improvements

Helping customers monitor their network activity and update firmware is essential for maintaining optimal broadband performance, ensuring security, and preventing disruptions. As a broadband technician, guiding customers through these processes empowers them to take control of their network while minimizing risks like hacking, malware, or service outages.

1. Why Monitoring Network Activity and Updating Firmware is Important

- Detect unauthorized devices or suspicious activity
- Prevent bandwidth overuse and network slowdowns
- Identify potential security threats like malware or hacking attempts
- Ensure performance improvements through firmware updates
- Fix bugs and vulnerabilities that could compromise network safety

2. Guiding Customers to Monitor Network Activity

Step 1 – Access the Router's Dashboard

1. Ask the customer to open a web browser.
2. Enter the router's IP address (typically 192.168.1.1 or 192.168.0.1).
3. Log in using the admin username and password.

Step 2 – Show the Network Status Page

- Navigate to Connected Devices, Network Map, or Device List.
- Review all active devices on the network.
- Look for:
  - ✓ Unknown devices.
  - ✓ Devices consuming high bandwidth.
  - ✓ Repeated connection attempts.

Step 3 – Analyze Bandwidth Usage

- Go to Traffic Monitor, Data Usage, or Bandwidth Statistics.
- Show how customers can see:
  - ✓ Which devices use the most data.
  - ✓ Which applications or services are consuming bandwidth.
- Educate them on identifying unusual spikes that may signal malware or unauthorized usage.

Step 4 – Enable Alerts or Logging (Optional)

- Show how to turn on notifications when new devices connect.
- Teach customers to periodically review the logs for suspicious activity.

3. Guiding Customers to Update Firmware

Step 1 – Check for Firmware Updates

- Navigate to System, Administration, or Firmware Update section.
- Check the current version installed.
- Click Check for Updates.

Step 2 – Backup Settings (Optional but Recommended)

- Teach customers how to export or save current settings before updating to prevent data loss if reset is needed.

Step 3 – Perform the Firmware Update

- If an update is available, click Download or Install Update.
- Confirm the action and wait for the process to complete.
- The router will restart automatically.

Step 4 – Verify the Update

- Log back into the router dashboard.
- Confirm that the new firmware version is installed.
- Check that all settings are intact and devices are reconnecting properly.

Customers often face common broadband issues such as slow speeds, intermittent connectivity, or device setup problems. By providing them with clear guidance on basic troubleshooting and self-help techniques, technicians can help customers resolve minor issues themselves while improving network security and reducing unnecessary service calls.

4. Key Objectives When Briefing Customers

- Help customers identify and resolve simple problems independently
- Increase their confidence in managing their home network
- Encourage safe and secure internet practices
- Reduce service downtime and technical dependency
- Educate customers on cybersecurity threats and preventive measures

5. Basic Troubleshooting Steps to Share with Customers

Step 1 – Check Physical Connections

- Ensure all cables (power, Ethernet, coaxial) are properly plugged in.
- Confirm that no cables are damaged or bent.
- Verify that the router and modem are switched on and the power light is stable.

Step 2 – Restart the Router/Modem

- Turn off the device, wait for 30 seconds, and turn it back on.
- Explain that rebooting clears memory and refreshes the connection.

Step 3 – Check Device Connections

- Confirm the device is connected to the correct Wi-Fi network.
- Turn Wi-Fi off and on again to reconnect.
- For wired connections, check that Ethernet cables are securely attached.

Step 4 – Run Speed and Connectivity Tests

- Open a browser and use tools like Fast.com or Ookla's Speedtest to check internet speed.
- If speeds are lower than expected, limit background apps and retry.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=Hm6Urf8ng3M

Interpreting Technical Data

UNIT 3.6: Executing Speed Test and Analyze

Unit Objectives

By the end of this unit, the participants will be able to:

1. Perform a speed test, record throughput data, and demonstrate network performance as per the subscribed plan.

3.6.1 Speed Test Measures

To measure Internet connection's ultimate speed, like, speed of uploading and downloading information by accessing nearby test servers, speed tests are required.

The test impersonates online activity of a user in a controlled setting by downloading sample files and recording speeds. These tests are helpful for isolating ISP's performance as a variable in the quality of the connection. Speed tests won't project absolute Internet speed, but they will give a nearby estimate. Results may vary depending on location and the time of day.

Speed test results match what's stated in ISP plan given to the user.

Certain terminologies

- Download speed – how fast data can be fetched from the server to user's location, measured in megabits per second (Mbps)
- Upload speed – how fast data is sent to others, measured in megabits per second (Mbps)
- Megabits per second (Mbps) – a unit of measure for bandwidth
- Latency – the time data took to travel to its destination and returned back to user
- Ping – a tool to measure latency between user's system and remote destination

How to run a speed test

Switch off any slow applications (Photoshop, Spotify, etc.) before running speed test as it will interfere with measurement. Search Google for "Internet speed tests," there are number of options available. Speedtest.net by Ookla is effective.

By clicking on "Begin" option at home page, system will attempt to download a file from the server. As the download completes, download speed will be measured. Once the download process completes, system will attempt to upload a file to the test server, therefore calculating the upload speed. Download speed here is expressed in Mbps (Megabits per second. 1 Mbps is the equivalent of 1,000 Kbps (Kil

Interpret the Results

Both upload and download speed should have a score almost close to ISP's service plan. In most of the cases, connections are planned to download faster than they upload. The majority of online activity—like loading web pages or streaming music—consists of downloads. Upload speed is necessary when there is a need to send big files via email or for video conferencing.

In a gigabit connection, hardware like an ethernet cable, solid-state drive, and CPU needs to be checked to analyze the challenges for an effective Internet speed. Most of the services, display "ping" results, which are measured in milliseconds, accompanied by download/upload speed. This refers to the latency of the connection.

Troubleshoot a faulty speed test

- Check for the devices connected to network which may interfere
- Ensure healthy condition of hardware equipment like computer, router, modem, and cables
- In case of cable, check each end of the coaxial connection for any looseness or damage
- Disconnect attached equipment for 30 seconds
- If Wi-Fi is used, switch it off and put your system on modem directly

3.6.2 Communication with Client

Interpret the Results Both upload and download speed should have a score almost close to ISP's service plan. In most of the cases, connections are planned to download faster than they upload. The majority of online activity—like loading web pages or streaming music—consists of downloads. Upload speed is necessary when there is a need to send big files via email or for video conferencing. In a gigabit connection, hardware like an ethernet cable, solid-state drive, and CPU needs to be checked to analyze the challenges for an effective Internet speed. Most of the services, display "ping" results, which are measured in milliseconds, accompanied by download/upload speed. This refers to the latency of the connection.

Troubleshoot a faulty speed test:

- Check for the devices connected to network which may interfere
- Ensure healthy condition of hardware equipment like computer, router, modem, and cables
- In case of cable, check each end of the coaxial connection for any looseness or damage
- Disconnect attached equipment for 30 seconds
- If Wi-Fi is used, switch it off and put your system on modem directly
- It is very critical to communicate the speed results and analysis with the client. However, prior to that, it is equally important to listen to the problem of the client by giving utmost attention while client is speaking or asking questions. This will help to understand their thought process and expectations.
- Treat the client with respect. Client can be aggravated owing to the challenges of connection, staying calm and composed in that situation will resolve half of the matter. Words like "Sorry" and "Thanks for your patience" are considered to do magic, so try them often.
- Circulate all important correspondence, updates, and action plans via email to client to keep them updated. Keeping them informed will assure client that the action is happening and wins their confidence.
- Make yourself available over the phone and always respond to emails within the specific timelines and keep a close watch on timely closures. Following such practices will improve your reputation and you will be respected by everyone.
- Keep client updated on the reasons for lower speed and what could be the possible scenarios of it. Educate client by sharing some useful tips on maintaining the connection effectively.

Exercise

Short Answer Questions:

1. Explain how you can access the CPE settings using command-line or browser interface, and why it is important to update default credentials.
2. What are VLAN and NAT configurations, and how do they affect network traffic management?
3. How does enabling IPv6 support improve network connectivity and future-proof the broadband service?
4. Describe how Quality of Service (QoS) settings can enhance user experience in a home broadband setup.
5. What steps would you take to perform Level 1 and Level 2 diagnostics for troubleshooting connectivity issues?

Multiple-Choice Questions (MCQs):

1. Which of the following is a secure method to protect a Wi-Fi network from unauthorized access?
   a) Using default passwords
   b) Enabling MAC filtering and firewalls
   c) Broadcasting the SSID openly
   d) Disabling encryption settings

2. What is the primary purpose of using a VPN or Internet Lease Line (ILL) in home networks?
   a) Increase Wi-Fi range
   b) Provide secure communication over the internet
   c) Reduce the number of connected devices
   d) Automatically detect nearby networks

3. Which command is commonly used to test the connectivity between a device and the service provider gateway?
   a) tracert
   b) ping
   c) nslookup
   d) Ipconfig

4. When integrating smart home devices with a broadband network, which of the following should be prioritized?
   a) Weak passwords to allow easy access
   b) High throughput without considering security
   c) Compatibility and secure network access settings
   d) Disabling firewalls to increase connection speed

5. What does jitter in a network performance test indicate?
   a) Stable connection with no fluctuation
   b) Variations in packet delay affecting real-time applications
   c) High download speed
   d) Secure encryption settings

Fill in the Blanks :

1. The command used to check the response time from the service provider's gateway is _____.
2. To prevent unauthorized access, it is recommended to change the CPE's default _____ immediately after the first login.
3. The technology that allows multiple virtual networks to coexist on the same physical network infrastructure is called _____.
4. The broadband network performance test that measures packet delay and variability is known as _____.
5. Smart home systems like Amazon Alexa or Google Home can be integrated with broadband networks by configuring _____ and ensuring secure connectivity.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=ad4tTK43VKc&ab_channel=Maxis

How to perform speed test

4. Troubleshoot and Rectify Faults

Telecom Sector Skill Council

Key Learning Outcomes

By the end of this module, the paricipants will be able to:

1. Determine the methods used to diagnose and rectify wiring faults in wireless networks.
2. Explain the process of troubleshooting and repairing Wi-Fi backhaul equipment operating at 5 GHz.
3. Describe the procedures for troubleshooting and restoring Wi-Fi access points operating at 2.4 GHz.
4. Discuss the steps involved in carrying out documentation and restoring the worksite after wireless network fault rectification.

UNIT 4.1: Escalation Matrix

Unit Objectives

By the end of this unit, the participants will be able to:

1. Explain escalation procedures and risk factors for unresolved broadband issues.
2. Explain the importance of documentation in broadband troubleshooting and service maintenance.
3. Explain best practices for customer communication and remote troubleshooting assistance.

4.1.1 Escalation Matrix

Escalation matrix is a process of set protocols and procedures which defines the steps while handling any potential dispute and/or problem. These are proved beneficial while dealing with issues and delays. This matrix usually takes care of the following types of problems and can be modified to include more fields as needed:

- Operational (scheduling, service cancellations, etc.)
- Logistical (delivery, in transit missing products, etc.)
- Technical (error messages, etc.)

Let us take Escalation Matrix Guideline of the company "Vistara" for example.

The Escalation Matrix allows you to specify more than one user to be contacted or notified in case of critical issues. This contact information is presented to the service delivery NOC when the service ticket is created or updated. This helps you notify the right people at the right time about critical errors. These alerts need to be informed about irrespective of the business hours. The point to note is that, the escalation matrix is time zone specific and is usually available 24 by 7. The key features of escalation matrix are as follows:

- The escalation levels are based on schedules.
- The service is available 24X7 and schedules are allocated accordingly.
- The schedules are time zone specific.
- You can now define multiple matrices for a given customer orpartner.
- A matrix can be defined at more than one levels ranging from partner and customer level to a combination of sites, device groups and devices.

This implies that you can now have exclusive user group's notified of issues depending on device roles or locations or issue types.

To view the escalations list, go to Navigation:

- Log on to Vistara.
- Go to Setup option.
- Select Escalation Matrix (New).

In the Escalations List page, a new column Applicable For is added to get a sneak peek into the customers, sites, device groups and devices associated with the escalation matrix.

4.1.2 Escalation Matrix Format

Let us take the sample escalation matrix format to understand it

Problem Escalation Matrix

How to Use This Form

The left side of the columns reflects the time you spend waiting to reach someone before trying to contact someone else to help you solve your problem or resolve your issue. The right side of the columns reflect the time you spend not getting a resolution before you have to escalate to the next level.

Type of Escalation	1st Escalation Level		2nd Escalation Level		3rd Escalation Level		4th Escalation Level		5th Escalation Level		6th Escalation Level	
Operational	**Project Team Contact**		**Project Manager**		**Account Manager**		**Sales Manager**		**Project Sponsor**		**Executive Level**	
	¼ hr.	2 hrs.	¼ hr.	2 hrs.	¼ hr.	2 hrs.	¼ hr.	2 hrs.	½ hr.	2 hrs.	½ hr.	2 hrs.
Scheduling												
Obtaining Instructions												
Customer Information												
Service Information												
Obtaining Materials												
Performance Issues												
Service Cancellations												
Logistical	**Project Team Contact**		**Project Manager**		**Account Manager**		**Sales Manager**		**Project Sponsor**		**Executive Level**	
	¼ hr.	2 hrs.	¼ hr.	2 hrs.	¼ hr.	2 hrs.	¼ hr.	2 hrs.	½ hr.	2 hrs.	½ hr.	2 hrs.
Product Delivery												
DOA Product												
Missing Product												
Order Cancellations												
Order Verification												
Order Status												
Other												

Fig 4.1.1: Sample of an escalation matrix form

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=opB5oOvB3cI

What Is An Escalation Matrix?

UNIT 4.2: Problem Solving

Unit Objectives

By the end of this unit, the participants will be able to:

1. Describe common network faults like No Service, degraded service, and intermittent connectivity, and their root causes.
2. Describe the common causes of broadband service disruptions (signal loss, attenuation, interference).
3. Identify various network troubleshooting techniques, including speed tests, ping tests, and trace routes.
4. Explain the use of AI-based predictive maintenance and remote diagnostic tools in broadband troubleshooting.

4.2.1 Reporting the Problem

Typically, customers want that their problems should be easy to report, quickly acknowledged and timely acted upon with compassion and fairness.

Some ideas to achieve the key principles that can help a technician act on the reported problem and thus help in developing good complaints management systems are as follows.

Report the Problem

You should ensure that your contact details are readily available to the customers – e.g., in the appropriate section of the telephone book.

When the problem is reported

- Appreciate the customer for bringing the issues forward Handle the customer in an empathic and courteous manner
- Talk to the customer to understand the concern in detail, rather than purely relying on the written documents and previous records
- Be attentive and patient while customer is sharing the concern Probe to make sure you have clearly understood the problem
- Don’t become judgmental, defensive, or put the blame on customer Acknowledge by narrating the summary of the problem to the customer
- Be responsive and share the action plan along with time frame to the customer

4.1.2 Solving the Problem

- Take ownership and explain your intentions to the customer
- Learn and understand the complete situation by referring to old records, if any Involve the customer to be a part of the solution, keep him posted about your steps
- Take verbal consent from the customer that he agrees with the solution which you propose
- Don’t over-promise and stay within the limits of policies of the company. If the customer is over demanding and is asking for something which is not doable, explain the policies or take him/her to the company website. If he/she is still adamant, you may refer him/her to the Citizens Advice Bureau to check his/her legal rights

- In situations that have no legal obligations, one can offer a resolution that works best in customer favour. For example, if the customer is entitled for a repair, by law, one can offer him a replacement, keeping customer satisfaction in mind.
- Always give tentative timelines to the customer, rather than promising exact time frames. However, in case of delay, always make sure to keep the customer updated about the new timelines.
- Share the measure your company will take to ensure such situation(s) never arise in future.

4.2.3 Following up after the Problem

- Maintain a record of conversation including the important points along with the offered resolution.
- Make sure customer agrees to your method of solution to his problem. Records all the issues and complaints.
- These records will help in analysing the measures used for handling complaints and identifying products or services which are prone to more issues complaints.
- One will be able to identify the turnaround time for handling grievances.

Use the Information to Decide

- Do I have right resources to handle each issue?
- Is each team member aware of the protocols which need to be followed to resolve any situation/problem?
- Do I need to a refresher to update myself on the product? Should this brand be stocked?

Making Repairs

- Using the right kind of machinery for repairs ensures the work is done with the set quality
- standards and time limits. This is important for restoring customers' faith.

4.2.4 Checklist

The following checklist will come in handy in various type of trades and situations, when carry out repairs:

- Exhibit your understanding of the problem and respect urgency
- Explain briefly in a layman's term the cause and action plan for the customer's problem
- Share the time frame with the customer and take his/her verbal agreement on the same
- Inform about the cost involved in fi xing the customer's issue in case he/she is not covered under warranty. It is advised to always give a quote in writing to avoid conflicts at the time of payment
- Be patient and informative while explaining the cause of the problem to the customer and never argue if he retaliates
- Thoroughly investigate the cause before fixing the problem and give precautionary advice, if necessary
- Do everything possible under your power to keep your promise
- Inform the customer in case there is any change in plan from the one decided at the beginning:
  - Always note contact details of the customer
  - Notify the customer once the issue is fixed

- Give the customer record of the work performed
- As an additional measure, ensure the customer has the manual. In some cases, you may also educate the customer about the steps performed to resolve the current issue and how to present it from reoccurring.
- Share your contact details and encourage the customer to update you in case the same issue arises.

Notes

UNIT 4.3: Identifying and Repairing Faulty Cables and Connectors

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to replace faulty connectors and damaged cables.
2. Show how to take readings at splitter points and terminated cable ends.
3. Demonstrate how to rectify signal leakage, cable faults, and interference in a broadband network.

4.3.1 Identify Faulty Cables/Connectors

Cables/connectors are under a relentless rotation of heating and cooling, expansion and contraction. Whenever a switch is used or appliances are plugged in, usual result is that wire connections loosen over time.

Electrical system has a lot of precautions against bad cabling or connections hazards, such as grounding system, circuit breakers, and other standard protection. Yet, we can encounter sparking every time there is a loose wire connection in system.

Here are some common cabling / connector issues with recommended solutions:

1. Loose cable connections at Switches and Outlets

Screw terminal connections at wall switches and outlets become loose. These areas get maximum electric traffic, these are the first to be looked at. Loose wire connections at a switch, outlet, or light fixture are often signaled by a buzzing or crackling sound or by a light fixture that flickers.

To address this situation, first turn off the power to the suspected wall switch, light fixture, or outlet. Now remove the cover plate and use a flashlight to examine the screw terminals inside where the cables are connected. If there are any loose cables, tighten the screw terminals.

If device is made with the push-in fittings, remove them and reconnect the cables to the screw terminals on the device. If there are pass-through wire connections inside the box that are made with connector, check these to ensure the cables are tightly joined together.

2. Wire Connections Made with Electrical Tape

When wires are joined together with electrical tape rather than a wire nut or other sanctioned connector, there is a danger of a possible hazard. To address this situation, turn off the power to the circuit and remove electrical tape from cables and clean them. After getting sure of amount of exposed wire (about 3/4 inch), join the wires together with an approved connector.

If ends look damaged, remove the ends of wires and undress about 3/4 inch of insulation to make a Proper Connection.

3. Two or More Wires Under One Screw Terminal

There could be a situation when two or more wires are held under a single screw terminal on a switch or outlet. This can lead to distinct fire hazards. It is acceptable to have a single wire under each of the two screw terminals on the side of an outlet or switch, but it is a code violation to have two wires wedged under a single screw.

Immediately switch off the power. Remove two offending wires from their screw terminal. Cut a 6-inch wire of the identical color. Strip 3/4 inch of insulation from each end of the pigtail, then join one end to the two wires you just disconnected, using a wire connector. Attach the free end of the wire to the screw terminal that once held the two wires.
This creates a bridge connecting wires to the desired screw terminal on the outlet or switch.

4. Loose Connections on Circuit Breaker Terminals

When the hot wires on circuit breakers in the key service panel are not strongly connected to the breaker. In this case, lights flicker, or problems on fixtures all along the circuit are faced. After making connections to circuit breakers, ensure to strip the proper amount of wire insulation from the wire and make sure that only the bare wire is placed under the terminal slot before tightening.
To address this problem, turn off the breaker and then unclip it from the hot bus bar in the main service panel. She/he will check the hot wire connected to the breaker to validate that the screw is tight and that there is no insulation under the terminal and no exposure of excess bare copper wire. After the repair, put breaker back into place on the hot bus bar and turn the breaker back on.

5. Faulty Neutral Wire Connections at Circuit Breaker Panels

When the white circuit wire is not correctly mounted to the neutral bus bar in the main service panel, hazards are prone to occur.
To address the problem, the electrician will check to validate the neutral wire is sufficiently exposed and correctly attached to the neutral bus bar.

4.3.2 Cable Testing Using OTDR / Signal Level Meters OTDR

OTDR stands for Optical Time-Domain Reflectometer. It is an optoelectronic instrument for understanding the character of an optical fiber. For testing, continuous light pulses are injected into the optical fiber, and light is mined from the same end of the optical fiber. This light is either scattered or reflected along with the fiber. The scattered or reflected light demarcates the depiction of optical fiber.

Testing a Fiber Optic Cable

This test will acquire a trace of a single-mode or multimode fiber optic cable plant, including the loss of all fiber, splices, and connectors.

Equipment required to execute this test

- OTDR of fiber to be tested
- Use same fiber type and size as cable plant for launch and reference and need connectors compatible with the reference cables.

Test Procedure

- Step 1: Start the OTDR and allow it to warm up.
- Step 2: Carefully clean connectors and adapters.
- Step 3: Connect launch cable to OTDR. Connect receiving cable to the far end of the cable.
- Step 4: Configure the test parameters on the OTDR.
- Step 5: Connect wire to test to end of launch cable. Connect receiving cable to the far end of the cable
- Step 6: Get a trace.

Signal Level Meters

The signal level meter is also known as Field Strength Meter (FSM). It is used for installation of new equipment in a network as well as for finding faults and for timely maintenance

It also ensures that signal levels are delivered as required.

Types of Signal Level Meters

Commonly, Signal Level Meters are categorized in three groups:

1. CCTV Signal Level Meters: Today CCTV testers come with equipped functions to program the cameras and evaluate wide range of variables; thus, one device is enough. It is able to test and also program the cameras from a location with a particular device, thereby saving money and time.
2. Satellite & CATV Signal Level Meters: They are used to test and measure the quality of TV and satellite signals, ensuring that the signal levels are delivered as essential. Signal levels are measured over a definite frequency assortment, usually articulated in decibel- milliwatts, dBm.

Guidelines to use a sound level meter:

- Position sound level meter at a sufficient distance from obstacles or reflectors
- Position microphone of sound level meter about 1.3 – 1.5 m above the ground
- Position microphone of the sound level meter in the direction of the sound sour

4.3.3 Connecting a Cable to an RJ-45 Connector

Following tools are used to build cables with RJ45 connectors.

Tools

- Cat 3 cable or Cat 5 cable
- RJ45 connectors
- Wire stripping and crimping tool

Step 1: Cut the outer jacket of the wire by about 1 -1.5 inches by using a wire stripper.

Caution: Be careful while cutting the outer jacket, the wires inside the jacket should not get damaged.

Step 2: Before installing the wire, arrange them in the order in which they are supposed to go in the RJ45 connector.

Note: Arrangement of the wires order depends on the connection which you are making. The connection may be crossover, rollover or straight -through.

Step 3: After the wires are arranged in the specified order, cut them at least ½ inch from the point, which will be used for installation.

Step 4: Push the cables into the connector, for ensuring that the wires are below the gold crimping pins, towards the end of the cable and. One should confirm that each wire has gone into the right place.

Step 5: Specific tool should be used for crimping the cable. To check the connection, tug the cable slightly. Accordingly crimp again, if required.

Note: With the use of crimping tool, the wires are pressed into the plastic wedge and to the cable jacket. This keeps the cable in its place. The crimping pins are then pushed into the wires to respective connector channels.

The following figure shows installing cable in an RJ45 connector:

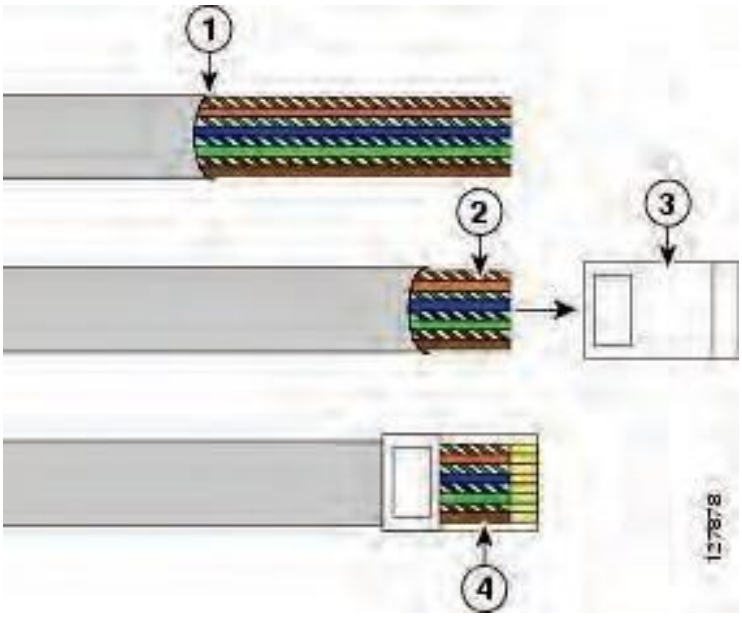


Fig 4.3.5: Illustration of installing a cable in RJ45 connector

1. Cut the outer jacket of the wire
2. Cut the wire into 1 and 1/2 inch in length
3. RJ45 connector
4. Cable installed in RJ45 connector

4.3.3 Replace Faulty Connectors and Damaged Cables

Faulty connectors and damaged cables are common causes of poor broadband performance, including intermittent connectivity, low speeds, or complete network outages. Replacing these components promptly is crucial for maintaining reliable service. Broadband technicians must follow proper procedures to ensure safety, network integrity, and optimal power delivery for PoE devices.

Tools and Materials Required

- Cable cutters/strippers
- Crimping tools (for RJ45, RJ11, or coaxial connectors)
- Replacement connectors (RJ45, RJ11, F-type, etc.)
- Cable testers or continuity testers
- Screwdrivers, pliers, and electrical tape
- PPE (gloves, safety glasses)
- Labeling materials (optional)

Safety Precautions

- Turn off all connected equipment before working on cables.
- Disconnect power sources to avoid electric shock.
- Wear PPE when handling sharp tools or working in outdoor/industrial environments.
- Avoid bending cables sharply; maintain manufacturer-specified bend radius.
- Follow grounding practices when replacing cables carrying PoE.

Identifying Faulty Cables and Connectors

A. Visual Inspection

- Check for visible cuts, abrasions, or kinks in the cable.
- Inspect connectors for bent or broken pins, corrosion, or loose connections.

B. Testing

- Use a cable tester or multimeter to verify continuity.
- For PoE cables, check voltage levels to ensure power delivery is within limits.
- Mark cables that fail testing for replacement.

Step-by-Step Procedure for Replacing Connectors

Step 1 – Prepare the Cable

- Cut off the faulty connector using cable cutters.
- Strip the outer insulation of the cable (typically 1–2 cm) without damaging internal wires.
- Untwist and arrange the individual wires according to the connector type and standard (e.g., T568A or T568B for Ethernet).

Step 2 – Insert Wires into Connector

- Carefully insert each wire into the corresponding slot of the connector.
- Ensure wires reach the end of the connector and maintain correct order.

Step 3 – Crimp the Connector

- Place the connector into a crimping tool.
- Apply firm pressure to secure the wires and create a solid electrical connection.

Step 4 – Test the New Connector

- Use a cable tester to check continuity and verify proper pin configuration.
- Ensure there is no short circuit between wires.

Step-by-Step Procedure for Replacing Damaged Cables

Step 1 – Disconnect the Cable

- Remove the damaged cable from both ends (CPE, switch, or device).

Step 2 – Measure and Cut a Replacement Cable

- Use a new cable of the same type and length.
- Ensure the replacement cable meets the required specifications (Cat5e, Cat6, coaxial, etc.) for bandwidth and PoE support.

Step 3 – Terminate Both Ends

- Attach connectors at both ends following the correct wiring standard.
- Crimp connectors and test using a cable tester for continuity and proper function.

Step 4 – Reconnect and Test

- Connect the new cable to devices.
- Verify network performance using ping tests, speed tests, or PoE voltage verification.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=sDLci29nl-g

Explaining Optical Time Domain Reflectometry (OTDR) Testing Method

UNIT 4.4: Electro Magnetic Interference (EMI) and Electro Magnetic Compatibility (EMC)

Unit Objectives

By the end of this unit, the participants will be able to:

1. Explain broadband communication systems and signal transmission principles.
2. Describe signal loss, attenuation, and interference factors affecting network performance.

4.4.1 Need of EMI & EMC

The most significant elements in electronic products and system integration are;

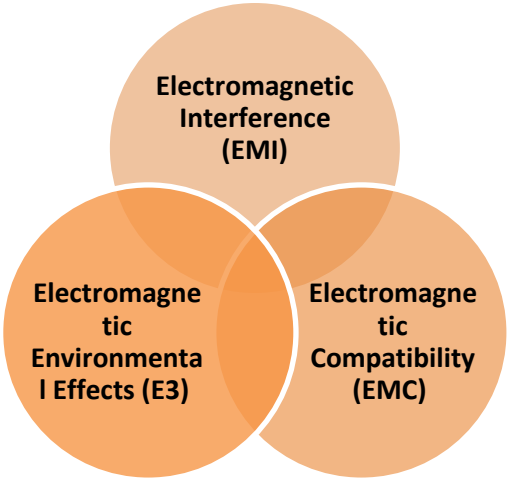


Fig. 4.4.1: Elements in electronic products and system integration

By law, any product, before entering the market must comply with international EMC standards. These standards are put into place to control and regulate the radiations which are emitted from every electronic product.

All electronic products should be immune to electromagnetic intrusion some of which are Electrical Fast Transients (EFT) and Electrostatic Discharge (ESD). The need for such is because these systems at times may get exposed to extreme electromagnetic environments (lightning strikes or (EMP) electromagnetic pulses) and they should be able to withstand the situation.

Both EMI and EMC are vital for product development companies across the world. Accurate guidelines must be adhered to by manufacturers while designing the product, which will ensure clearance of the product after EMI/EMC testing. Using EMI/EMC compliant components in the design have proven to be beneficial for many manufacturers.

All the details should be taken into consideration right from the initial stage; else one will be waiting time to meet such needs. The basic different between EMI/EMC are discussed as following. The products under developments should always maintain specific military or industrial standards.

As mentioned, for all manufactured devices, EMI and EMC levels should always be verified by regular testing.

4.4.2 Electromagnetic Interference (EMI)

Electromagnetic Interference (EMI)

EM waves are radiated from mostly every device which can affect the working of the nearby wireless or FR systems. This phenomenon is referred to as EMI. Thus, EMI levels should be maintained within the limits to ensure the adjoining systems perform appropriately.

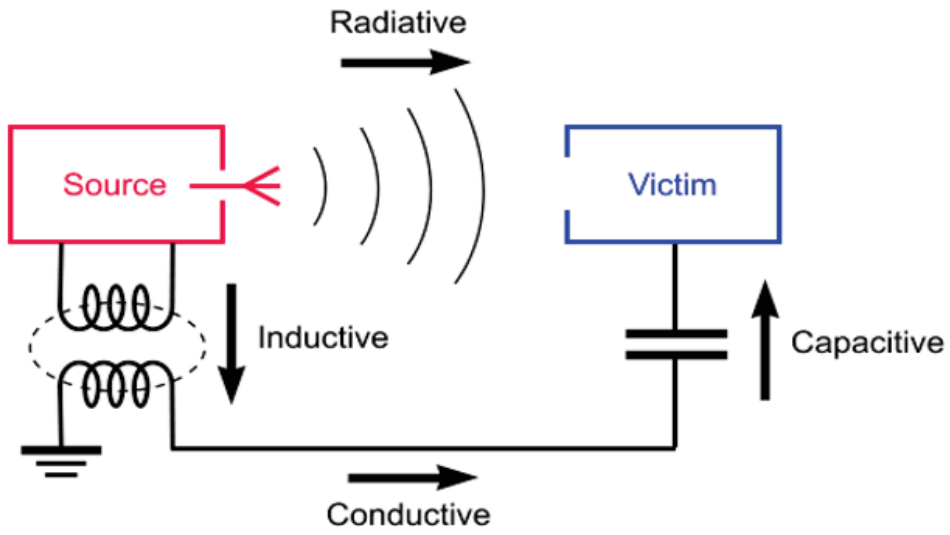


Fig 4.4.2: Electromagnetic interference

4.4.3 Electromagnetic Compatibility (EMC)

The electric noise produced by every device passes through cables, which can affect the working of adjoining devices connected to the same electric system. This is termed as EMC levels, and these should also be maintained within certain limits, for accurate functioning of the other systems.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=I88Qzdahn_o

EMI - Electromagnetic Interference and EMC - Electromagnetic Compatibility Explained

UNIT 4.5: Crimping and Soldering

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate the process of re-connectorization or crimping of cable pairs.
2. Show how to perform crimping and soldering techniques ensuring proper connectivity.

4.5.1 Crimping vs. Soldering

These days a defective coaxial connection is attributed for reducing performance of digital systems like Ethernet, Wi-Fi, and WLANs and also in high-end videos like DTV, SDTV and HDTV. In earlier days, an improperly installed CCTV connector caused a 1dB or less loss on a CCTV system. But, in recent days, the same bad connection can cause a 10dB loss on a 1GHz system.

Some essential factors which should be considered while establishing a coaxial connections and cable assemblies will be discussed in this topic.

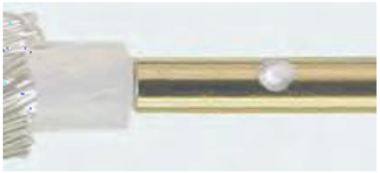
Right tools and skills are the most crucial aspects whether someone is using soldering or crimping method for soldering.

Solder or crimp methods have proved to be more sustainable when it comes solid mechanical and electrical connections such as installing contact between the connector's centre to the centre conductor of the cable or assemblies which needs to preform over 1 GHz.

4.5.2 Soldering

This fabrication method is often considered the most labour intensive as it is a preferred method while performing heavy duty tasks and is reliable in making connections and can be applied on cable with solid or stranded center conductors.

Advantages for connectorization by solder method are as follows:



Preferred

1. Solder is shiny and smooth around joint
2. Outside joint there is no visible evidence of solder flow
3. The hole created by solder filled with pin surface

Fig 4.5.1: Soldering

The prime tools in use is a solder iron with low-wattage and with variety of IPS. To hold the work in right place, installation is done by using a decent vise. Apart from this, only materials that are used are flux and solder.

Preferred

1. Solder is shiny and smooth around joint
2. Outside joint there is no visible evidence of solder flow

Fig 4.5.2: Joint after soldering

For non-optimum technique soldering is tolerant.

Disadvantages of solder method:

- While terminating soldering takes more time.
- In case of cold soldering there can be occurrence of solder not holding the joint properly.
- Solder fatigue and small cracks are evident in case of exposure to excessive vibration.
- In case of mechanical or temperature stresses soldering can become inconsistent.
- One should take precaution and control the heat while soldering as this can garble the cable.

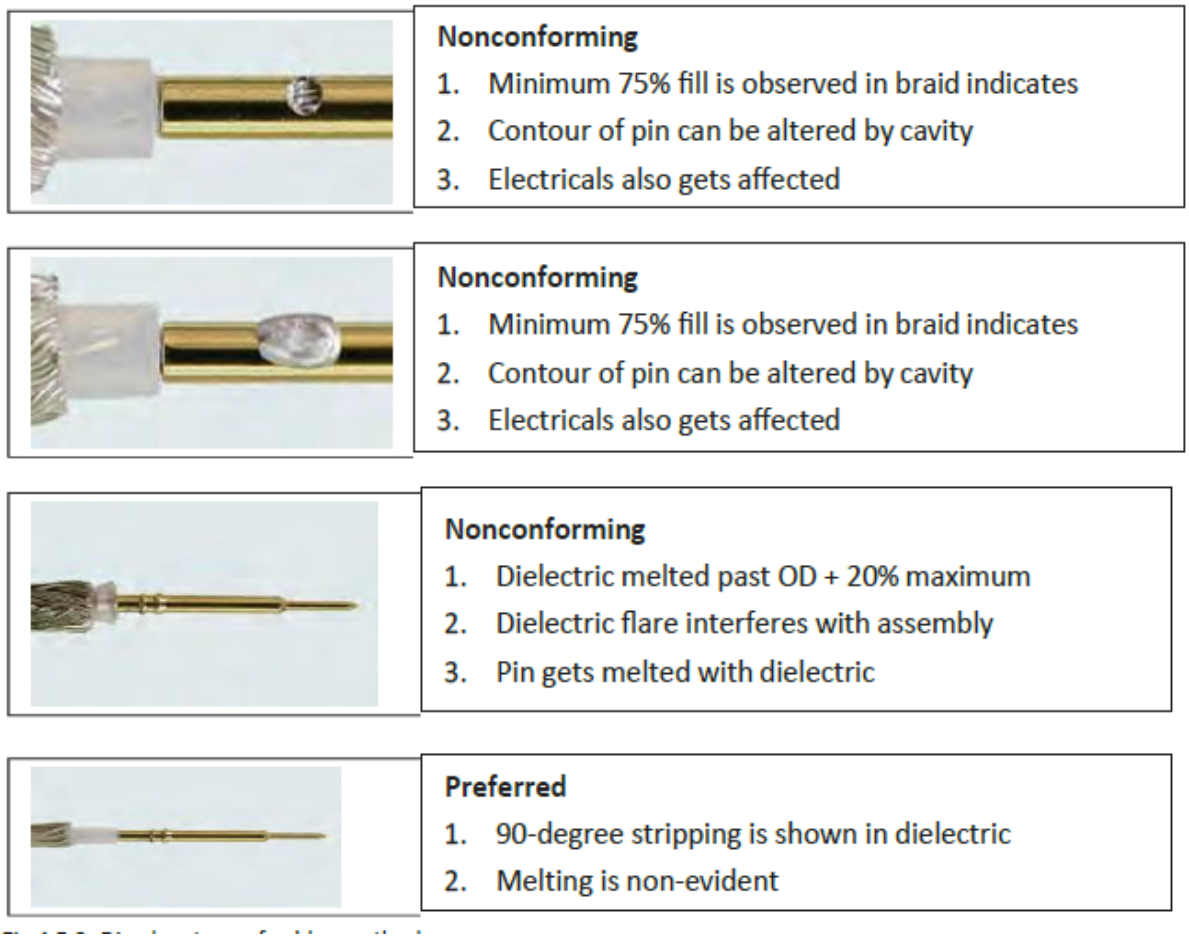


Fig 4.5.3: Disadvantage of solder methods

4.5.3 Crimping

One of the most preferred methods to terminate connectors on coax cable sometimes also referred to as workhorse of the trade.

Following reasons explain why crimp method is popular:

- Reduction in installation time as soldering is not required.
- An experienced technician will not take more than fifteen seconds for installing a crimp to the crimp connector. Reduction in assembly time is essential because these days lesser number of technicians are required to retain more equipment. Categories like computers, network cables and digital videos are mostly crimped.

- In case of thermal cycling some good connections will keep the metal adequately past the yield point, still allowing enough space for "spring back".
- A crimp connection to be good should be air tight and does not wick: hence at time is also called as "cold weld".
- Can be used on solids and or marooned conductors.

Preferred

1. Equally distribution on the surface of all 6 crimp
2. Crimp die positioned within pin step down

Fig 4.5.4: Crimping

Disadvantages of the crimp method are:

Nonconforming

1. Position of crimp die is outside crimp area
2. Body of pin is no longer concentric
3. Impedance of connector will be affected

Nonconforming

1. Once crimped you cannot bring the pin to its original shape
2. "Dog ear" of excess material is visible at the point of crimp
3. Possible cause can be too much pressure applied

Fig 4.5.5: Crimping disadvantages

In case the crimping is not done by a professional, there are chances that it will not seat accurately and may affect the specifications. This further affects the quality and continuity in the signal.

Once a wire is crimped it is not good for re-installation and also can't be un- crimped, so in case of repair the complete assembly needs to be replaced.

- Solid wires may not be able to hold the crimping, and this may lead to failure.
- Wire can shift and loosen in rare circumstances of frequent flex conditions. This is more evident in clamp connectors rather than crimped ferrule stud connectors.
- Always ensure to use the right type of connector for the coax. Avoid double crimping, particularly at the contact; this is known as "flagging" or "dog ears".

Fig 4.5.6: Visualization of flagging and dog ears

Ferrule Cross Section

- Equal pressure with hexagon shape on all sides.
- Ensure the crimping is done in such a way that "dog ear" is not formed.
- Wrong crimp occurs either because of unequal pressure, inappropriate die or in some cause because of very hard ferrule material used.

It is vital to use right tools when connecting a crimping connector to ferrules. In case of normal duty work use a ratchet crimp tool such as the RFA -4005-20, and in case of heavy-duty tasks apply a piston driven crimp handle, such as the RFA-4009-20. Make sure that the crimp die and connector are of right type.

To relieve stress on the coax a bell mouth crimped connector is used. Savings can be observed in case of cutting the material for large jobs in advance.

Fig 4.5.7: Bell mouth crimper

Notes

UNIT 4.6: Troubleshooting of Cable and Connector

Unit Objectives

By the end of this unit, the participants will be able to:

1. Demonstrate how to check for signal loss, interference, and attenuation using signal level meters.
2. Show how to analyze CPE logs using software tools to detect faults.
3. Show how to diagnose broadband faults using network diagnostic tools (ping, traceroute, OTDR).

4.6.1 Problems during First Startup

Symptom	Problem	Solutions
All LED indicators are not working.	No power to router.	Perform the following tasks sequentially: • Ensure power switch is ON. • Ensure all connections are secure from the power supply. • Ensure there is no power cut. • If all above points are checked, then faulty power supply can be the reason.
Internet indicator not blinking	Issue with cable: • Either the cable is not connected in proper manner. • The cable is damaged.	Perform the following tasks sequentially: • Ensure the device is connected in accurate manner. • Check plugs and connectors • Ensure there is no physical damage to the cable.
No connection to Ethernet devices. (The indicators 1 to 4 are off)	Problem with cable • Either the cable is not connected in proper manner. • The cable is damaged.	Perform the following tasks in order: • Ensure device is connected accurately. • Check plugs and connectors. • Ensure there is no physical damage on cable.
Not able to connect to Internet	• Either the Ethernet switch or modem is not connected or switched on.	• Reconnect the modem or Ethernet switch again and confirm the power supply. • Check the Internet service.
	• Issue with broadband or WAN service. • Router is not configured in right manner.	• Re configure the Router.

Table 4.6.1: Table showing problem during the first startup

4.6.2 Problems in Router

Symptom	Problem	Solutions
Issue with Ethernet connection. (Computer LEDs 1 to 4 are off)	A cable-related issue: • Disconnected cable. • Damaged cable.	Perform the following tasks in order: 1. Check if connections at either end are secure. 2. Check if the cable is not damaged.
Broadband or Ethernet connection is irregular or broken. (The Internet 1 LED on the front panel is off)	A cable-related issue: • Disconnected cable. • Damaged cable.	Perform the following tasks in order: 1. Check if connections at either end are secure. 2. Check if the cable is not damaged. If it is damaged, replace it with the new one.
(The Internet 1 LED is On but front panel LED is off)	Problem with broadband line or WAN service.	Check with the service provider to ensure the service is not interrupted.

Table 4.6.2: Problems faced in router

Notes

UNIT 4.7: Troubleshooting of CPE (Modem, Router, Switch)

Unit Objectives

By the end of this unit, the participants will be able to:

1. Explain the working of diagnostic tools, including signal level meters (SLMs), Optical Time-Domain Reflectometers (OTDRs), and AI-based troubleshooting tools.
2. Show how to access CPE software for diagnostics and troubleshooting.
3. Demonstrate how to perform CPE firmware updates, resets, and reconfigurations to restore connectivity.
4. Show how to assist customers remotely using AI-driven diagnostic tools.

4.7.1 Diagnosing the Cable Modem

On the front side of the modem, the status lights indicate the connection status between the modem network and also the connection between the modem, a computer and the local network.

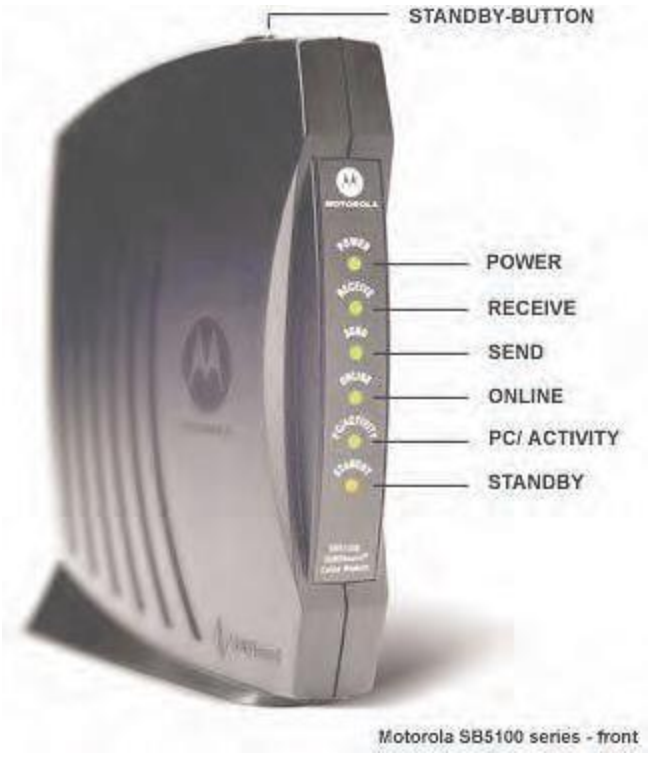


Fig 4.7.1: Front Panel

In normal operation, the status lights provide the information as in the table below:

Light	Flashing	On
Power	Startup diagnostics in progress.	The cable modem is powered on.
Receive	Downstream channel connection scan for receiving.	Connected downstream channel.
Send	Upstream channel scan connection.	Connected upstream channel.
Online	Network connection scan.	Process of startup is complete.
PC/ Activity	Receiving and communicating data.	Network device OR a computer is connected on the panel or either as USB or Ethernet connectors.
Standby	No flashing of lights	Once Standby button is on the Internet gets disconnected. If standby light is on, the rest of the lights will be off.

Table 4.7.1: Status light information the table below

Back/Rear Panel

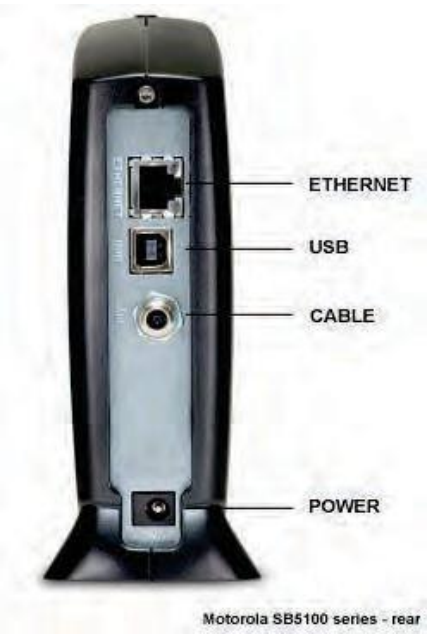


Fig 4.7.2: Rear Panel

Power socket and connectors for cable is found at the back of the panel

Type	Description
Ethernet	For the computers that are Ethernet compatible, an Ethernet port initiates the connection with RJ-45 connector.
USB	USB compatible computers get USB connections through USB ports.
COAX Cable	The CABLE port ensures connection to the coaxial cable also coined as COAX cable.
Power	Modem gets its connection from the power port.

Table 4.7.2: Ports at the back of the panel

The recommended connection type for Cable Broadband is Ethernet.
USB and Ethernet cable can't be used at the same time so never connect them to the same computer.

4.7.2 Troubleshoot a Cable Broadband Connection

Power Cycle Equipment

Occasionally, electrical devices will stop functioning properly, and cause a loss of connectivity. The first step in troubleshooting these issues is restarting the devices involved. This typically means that one needs to switch off the power for all devices such as the cable modem, router, switches, hubs and other systems. Then, after doing this, restart the devices after waiting for a minute, typically starting with the modem.

Once the modem is connected to the network, this will be indicated by four green lights (not blinking but solid) on the cable modem, network devices such as routers/switches can be restarted. Finally, restart the computer system.

Restarting or resetting the cable modem might take up to 5-30 mins.

Network Status

Unplanned network outages can interrupt the cable broadband service.

In the section below, you will find the solution for most common problems while the modem is not connected to the cable modem network.

4.7.3 Troubleshooting using the Cable Modem Indicators

The most frequent and common problems while the modem is not connected to the cable modem network are:

Modem Light	Status	Problem	Solution
Power	OFF	Show no power.	Confirm the supply of power.
	Flashing	Normal operation has been interrupted due to error.	Reset the modem after checking the coax cable.
Receive	Flashing	Searching for cable connection.	Check the cable connection and try resetting the modem.

Table 4.7.3: Indicators on a cable modem

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=39zXmf61McI

Modem, Router, Switch, Hub and Access Point: What's the Difference?

UNIT 4.8: Troubleshooting of Configuration and Connectivity CPE faults

Unit Objectives

By the end of this unit, the participants will be able to:

1. Explain best practices for CPE configuration, firmware updates, and network security.
2. Show how to analyze connectivity test results, including latency, throughput, and packet loss.
3. Demonstrate how to configure LAN/Wi-Fi connectivity, including SSID and security settings.
4. Demonstrate how to enable Quality of Service (QoS) settings to prioritize network traffic based on user needs.

4.8.1 Troubleshoot "No Data Transfer"

In the table below, you will find solution to most common problems while the modem is connected to the cable modem network, indicated by four solid green lights and the PC/ Activity indicator orange solid or flashing. No data transfer means you can't open a website in your browser; the email server can't be found to send or rec eive email, or another program can't connect to a server.

Modem Light	Status	Problem	Solution
Standby	ON	No data transfer.	Push the standby-button at the top.
	OFF	1. No connection between cable modem and computer or router. 2. Local area connection is disabled.	1. Check Ethernet or USB cable. If possible, try another cable. 2. Enable the Local Area Connection as below. Windows 7: Control Panel → Network and Internet → Network Connections Windows Vista: Control Panel → Network and Sharing Centre → Manage network connection Windows XP: Control Panel → Network Connections Windows 2000: Control Panel → Network and Dial-up Connections
	Blinking	An error has occurred during normal operation or can't connect to any server.	1. Check the cables and try resetting the modem. In case the cable is in right manner and the resetting also doesn't work one should call Customer Help. 2. Verify the connection settings and check if the connection is set up with the IP addresses assigned to the connection.

Modem Light	Status	Problem	Solution
PC/ Activity	Blinking	Can't connect to some servers	It is possible that servers on the Internet are down temporarily. Try to open a connection to the server after some time. You can also check connection with a server; it will give you: IP address, a trace route from your system.
	OFF	No coaxial cable connection	Check all connections of the cable and reset the modem.
Send	Flashing	Scanning for the upstream frequency.	Check all connections of the cable and reset the modem.
Online	Flashing	Scanning for the network connection.	Check all connections of the cable and reset the modem.
Activity	Blinking	Transmitting or receiving data	No Problem
Standby	ON	Modem is in standby mode (the other indicators are OFF)	Push the standby-button at the top.
			Computer to the server you can't connect to and the time the trace route has been done.
	ON	No data transfer	Unplug Ethernet or USB cable from computer and reconnect cable. Make sure the PC/ Activity indicator is blinking.

Table 4.8.1: Troubleshooting steps

Notes

UNIT 4.9: Troubleshooting and Repairing of Client's Broadband Service

Unit Objectives

By the end of this unit, the participants will be able to:

1. Show how to identify faults such as No Service, degraded service, and intermittent connectivity.
2. Show how to perform a broadband speed test and interpret the results.
3. Demonstrate how to document troubleshooting steps, test results, and repairs in the system database.

4.9.1 Common Causes of Broken Internet Connection

1. Slow Connection

These are the possible reasons why Internet connection would be ineffective:

- device is located far from router
- bandwidth is spread too thin, specifically if there are multiple devices connected
- Ultimate working hours where good population is connected at once, so congestion (e.g., libraries, hotels, universities, etc.)

2. No Connection at all

Connection is lost due to:

- Problems in router or modem
- Complete service disconnection, due to weather, construction work or power problems

3. Service Fluctuations

Challenges at Internet service providers' (ISPs) end, often result in irregular Internet speed.

4. Equipment Failure

Damaged modem or router results in power blackout damaging the wires. Upgrading of outdated equipment is essential.

5. Operator Error

The most common operator errors that cause faulty Internet include wires plugged into the wrong jack, bad firewall rules set up and duplicating IP addresses.

4.9.2 Diagnosing Internet Connection

1. Check equipment like the modem, the router, the line, and your device or computer.
For instance, network cables may be loose or accidentally unplugged.

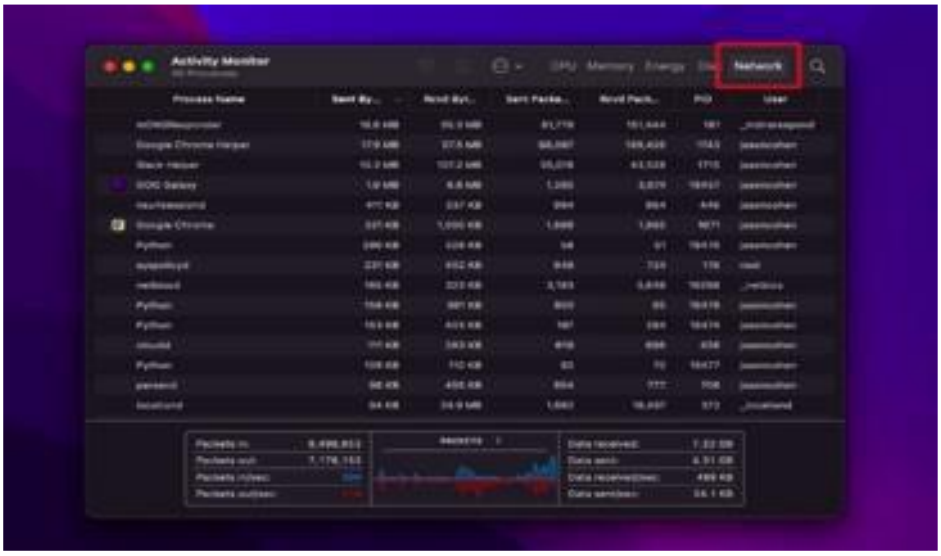


Fig. 4.9.2: Network screen
Pic credit : https://www.pcmag.com/

2. Check for functioning of website
Use the tool Down for Everyone or Just Me to check if the website is working. If it says the site is down just on your end, then proceed to diagnosing the problem.

3. Use Ping command
The Ping command sends a small data from your computer to another, in order to see if there is a connection.
To ping a website on a Windows computer: Search for CMD. On the black box, type “ping <www.website.com>” (e.g. ping www.google.com)
To ping a website from a MAC: Open Applications, then Utilities, then Terminal. On the box, type “ping <www.website.com>” (e.g. ping www.google.com), then press enter.

4. If the box indicates “reply from” followed by numbers, then your Internet is working well. If it, however, indicates anything other than “reply from” (e.g. “request timed out” or “destination host unreachable”), then the problem is on your end.

5. Check for DNS server problems
To check, access a website via its IP address. Google’s IP address, for example, is http://216.58.197.78. If one can access the website via its IP but not through its URL, then DNS has issues.

6. Check Internet package
If Internet is working, but is slower than expected, log on to a site like Speedtest.net and run a speed test. Number in megabits per second denoting the speed of system will be shared.

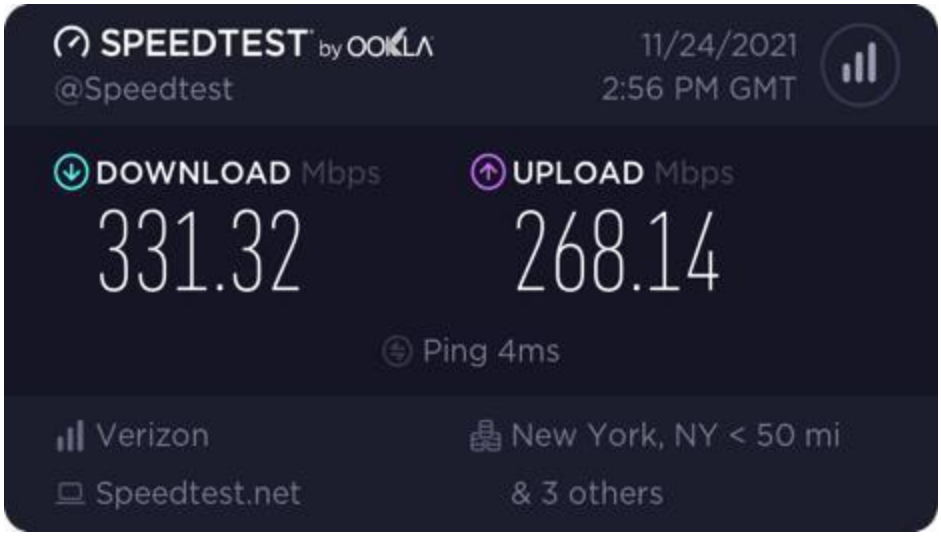


Fig.4.9.2: Speed Test screen

Exercise

Short Answer Questions:

1. Explain the role of OTDR and Signal Level Meters in identifying cable faults in a broadband network.
2. Describe common causes of intermittent connectivity and degraded service in broadband networks.
3. How can AI-based diagnostic tools help in predictive maintenance of broadband infrastructure?
4. What steps would you take to perform a firmware update on a CPE to restore connectivity?
5. Explain why proper documentation of troubleshooting steps and test results is important for broadband service maintenance.

Multiple-Choice Questions (MCQs):

1. Which of the following is a common cause of broadband signal attenuation?
    a) Interference from other devices
    b) Incorrect cable termination
    c) Long cable runs
    d) All of the above
2. What is the primary purpose of a traceroute test?
    a) Measure download speed
    b) Identify the path taken by packets and locate network delays
    c) Update CPE firmware
    d) Monitor Wi-Fi signal strength
3. Which tool would you use to locate a break or fault in a fiber optic cable?
    a) PoE tester
    b) OTDR
    c) Ping command
    d) Multimeter
4. When a broadband connection shows “No Service,” which of the following should be checked first?
    a) Customer billing details
    b) CPE configuration and connectivity
    c) Social media complaints
    d) Router brand
5. What is a key benefit of using AI-driven diagnostic tools in network troubleshooting?
    a) Reduce need for skilled technicians entirely
    b) Automatically resolve all issues without monitoring
    c) Predict potential faults and assist remote troubleshooting
    d) Replace the need for speed tests

Fill in the Blanks :

1. A broadband fault characterized by fluctuating connection quality over time is called _____.
2. The tool that measures optical signal strength and distance to faults in fiber cables is called _____.
3. Performing a _____ test helps determine packet loss, latency, and throughput in a broadband connection.
4. When replacing damaged cables or connectors, the process of properly attaching connectors is called _____.
5. Documenting all readings, troubleshooting steps, and repairs in the system database ensures _____ and traceability.

Notes

5. Follow Sustainable Practices in Telecom Infrastructure Installation

Unit 5.1- Environmental Sustainability and Waste Management in the Telecommunications Industry

TEL/N9105

Key Learning Outcomes

By the end of this module, the paricipants will be able to:

1. Explain sustainable practices in telecom infrastructure installation, including waste management and energy efficiency.
2. Discuss compliance with environmental regulations and the importance of maintaining records of sustainability measures.

UNIT 5.1: Environmental Sustainability and Waste Management in the Telecommunication Industry

Unit Objectives

By the end of this unit, the participants will be able to:

1. Explain national and international environmental laws and regulations governing telecom infrastructure installation.
2. Describe e-waste management and recycling policies applicable to telecom sites.
3. Identify occupational safety and health standards related to environmental practices.
4. List recyclable and refurbishable telecom components and their proper handling techniques.
5. Define methods for reducing electronic waste through responsible procurement and reuse.
6. Explain advancements in eco-friendly telecom infrastructure and the use of renewable energy sources.
7. Elucidate techniques for optimizing energy consumption in telecom operations.
8. Describe proper disposal methods for hazardous and non-hazardous waste.
9. Explain procedures for collaborating with authorized agencies for waste collection and disposal.
10. Identify best practices for reducing the carbon footprint of telecom installations.
11. Show how to identify telecom components suitable for recycling or refurbishment.
12. Demonstrate the process of sorting electronic and non-electronic waste according to disposal protocols.
13. Show the correct labeling and storage of recyclable and refurbishable components.
14. Demonstrate the safe handling and disposal of hazardous and non-hazardous waste.
15. Show the proper coordination process with authorized e-waste recycling units or disposal agencies.
16. Demonstrate the use of energy-efficient tools and equipment during telecom installations.
17. Show how to optimize infrastructure placement to minimize energy consumption.
18. Demonstrate the maintenance of records for waste disposal and sustainability measures.
19. Show how to guide team members on sustainable practices and encourage environmentally responsible habits.

5.1.1 Environmental Sustainability in Telecom Industry

Environmental sustainability is the practice of using resources, designing processes, and conducting operations in a way that meets present needs without compromising the ability of future generations to meet their own needs.

It involves maintaining the health of the planet's ecosystems, reducing waste and pollution, conserving energy and natural resources, and ensuring that human activities do not cause irreversible environmental harm.

Environmental Sustainability in the Telecom Industry

The telecommunications industry, while enabling digital connectivity and economic growth, has an environmental footprint that comes from:

- Energy consumption — Telecom towers, data centers, and network operations consume large amounts of electricity, often generated from fossil fuels.

- **Material usage** — Manufacturing network equipment requires metals, plastics, and rare earth elements.
- **E-waste generaion** — Obsolete telecom devices, batteries, and cables contribute to growing electronic waste streams.
- **Site construcion impacts** — Building telecom towers, laying cables, and installing antennas can disturb local ecosystems.

Environmental sustainability in telecom focuses on minimizing these impacts while still delivering high- quality communication services.

Uses and Importance in the Telecom Industry

- **Reducing Carbon Emissions:** Switching to renewable energy sources (solar, wind) for powering telecom towers and base stations reduces dependence on fossil fuels and cuts greenhouse gas emissions.
- **Efficient Resource Use:** Designing equipment that is modular and upgradable means fewer raw materials are needed over time, reducing mining and manufacturing impacts.
- **E-Waste Management:** Implementing take-back programs and partnering with authorized recyclers ensures that metals, plastics, and hazardous materials from old telecom equipment are recovered and reused safely.
- **Cost Savings:** Energy-efficient equipment and optimized network designs lower electricity bills and operational expenses.
- **Regulatory Compliance:** Following environmental laws like the **E-Waste (Management) Rules** in India or **RoHS** directives globally prevents legal penalties and maintains operator licenses.
- **Reputaion and Corporate Responsibility:** Sustainability initiatives improve a company's public image, attract eco-conscious customers, and strengthen stakeholder trust.
- **Innovaion and Compeiive Advantage:** Telecom companies that integrate sustainability often lead in innovation, for example, by developing low-power 5G technology or green data centers.

5.1.2 Environmental Laws and Regulations in Telecommunications

1. National Environmental Regulations

In India, telecom infrastructure installations are subject to multiple environmental laws designed to control pollution, manage waste, and promote sustainable resource use. These include:

- **The Environment (Protection) Act, 1986:** This umbrella legislation empowers the government to set and enforce environmental quality standards, including emissions from telecom site generators and noise levels from cooling equipment.
- **The E-Waste (Management) Rules, 2022:** These rules impose Extended Producer Responsibility (EPR) on manufacturers, importers, and bulk consumers of electrical and electronic equipment, including telecom operators. Companies must collect and channel e-waste to authorized recyclers, meet annual collection targets, and maintain detailed records of disposal.

- **Hazardous and Other Wastes (Management and Transboundary Movement) Rules, 2016:** These rules classify hazardous substances, such as lead-acid batteries, PCB boards, and certain solvents, and mandate their safe handling, storage, and disposal.
- **The Energy Conservaion Act, 2001**: This legislation encourages telecom operators to adopt energy-efficient practices, such as the use of high-efficiency power systems, renewable energy integration, and load optimization.
- **The Plasic Waste Management Rules, 2022**: These rules regulate the use of plastic in telecom equipment packaging, promoting recyclable and biodegradable alternatives.

2. Internaional Standards and Agreements

Global environmental frameworks also influence the Indian telecom sector, especially for multinational operators and equipment suppliers:

- **Basel Convenion (1989)**: Regulates the cross-border movement of hazardous waste, ensuring that e-waste is not shipped to countries lacking adequate recycling infrastructure.
- **Restricion of Hazardous Substances (RoHS) Direcive**: Limits the use of hazardous substances such as mercury, lead, and cadmium in telecom equipment, protecting both the environment and worker health.
- **ISO 14001: Environmental Management Systems**: Provides a structured approach for companies to integrate environmental management into their operations, covering policy, planning, implementation, monitoring, and continuous improvement.
- **Paris Agreement (2015)**: While not industry-specific, this global climate agreement has prompted many telecom companies to set science-based targets for reducing greenhouse gas emissions.

5.1.3 E-Waste in the Telecom Industry

Understanding E-Waste

E-waste refers to discarded electrical and electronic equipment, which in the telecom sector may include obsolete base transceiver stations (BTS), routers, switches, modems, fiber optic cables, and batteries. Unlike general waste, e-waste often contains hazardous substances such as lead, cadmium, and brominated flame retardants, which can leach into the environment if improperly disposed of.

Fig. 5.1.1 E-Waste in Telecommunicadon Industry

For example, a single telecom tower may have over 500 kilograms of lead-acid batteries, which, if damaged, can contaminate soil and groundwater.

Classificaion of E-Waste

Telecom e-waste is typically categorized into:

- **Recyclable Components** – Metals such as copper and aluminum from cables, and steel from equipment racks.
- **Refurbishable Components** – Functioning or repairable radio units, circuit boards, and power modules.
- **Hazardous Components** – Batteries, mercury switches, and capacitor fluids.

5.1.4 E-Waste Management Process in the Telecom Industry

Telecom networks generate a considerable volume of e-waste during network upgrades, equipment replacements, and periodic maintenance. Unlike domestic e-waste, telecom waste is industrial-scale, often involving heavy equipment, high-capacity batteries, large volumes of cabling, and specialized electronics. The management process follows a structured set of steps to ensure compliance with environmental laws, protect worker safety, and recover maximum material value.

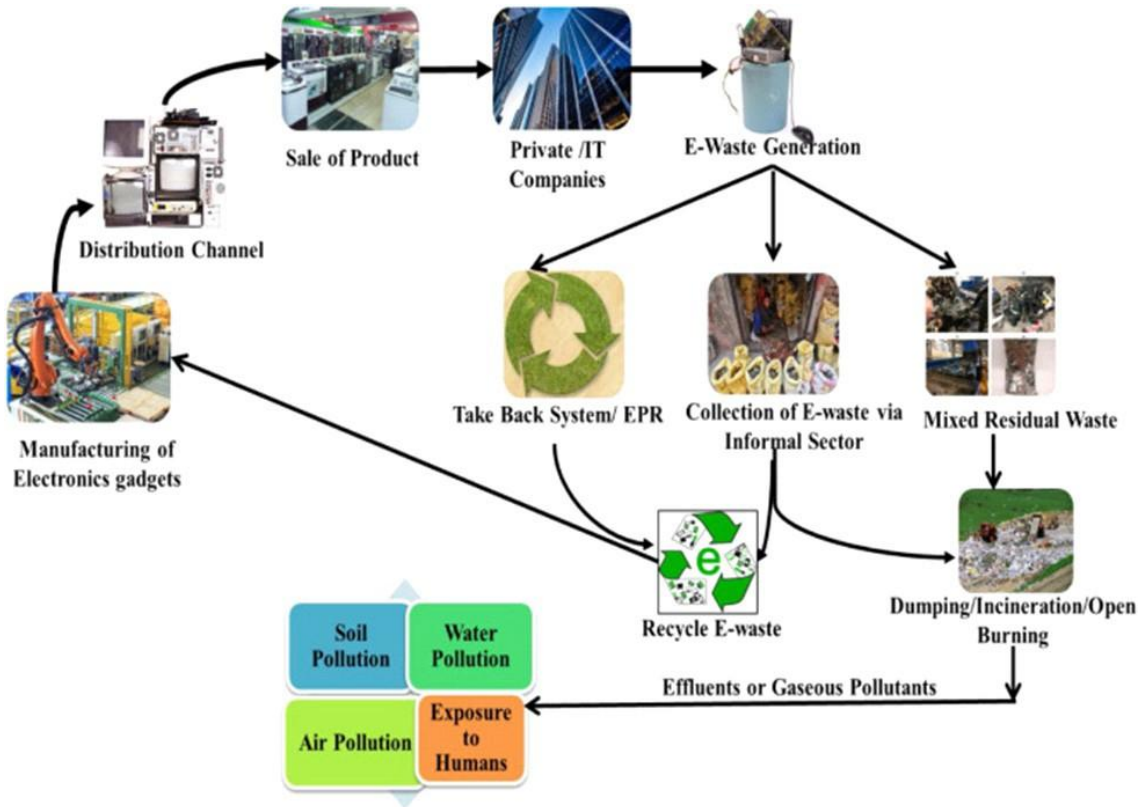


Fig. 5.1.2 E-waste Management

1. Idenificaion and Segregaion

The first and most critical stage of e-waste management is identifying obsolete, damaged, or non-functional equipment during routine inspections, preventive maintenance schedules, or technology upgrades (for example, replacing 3G base transceiver stations with 5G units).

Key Aciviies in Idenificaion:

- **Inventory Audits:** Using asset management systems to record the age, condition, and performance of each component.
- **Funcional Tesing:** Equipment is assessed to determine whether it can be repaired/refurbished or must be decommissioned.
- **Technology Obsolescence Check:** Some components may be fully functional but incompatible with newer protocols — these are classified as "functional obsolete" and evaluated for resale or reuse.

Segregaion Process:

Once identified, materials are segregated into three main categories:

- **Recyclable** – Metals (copper, aluminum, steel) from cables, frames, racks; glass from fiber optic assemblies; plastic housings.
- **Refurbishable** – Circuit boards, radio units, power supply modules, and routers that can be repaired or upgraded.
- **Hazardous** – Lead-acid and lithium-ion batteries, mercury-containing switches, PCB (polychlorinated biphenyl) capacitors.

Best Pracices:

- Apply classification labels such as "R" (Recyclable), "RF" (Refurbishable), "H" (Hazardous) directly on packaging or containers.
- Store segregated waste in designated, weather-protected zones at the site to prevent water ingress, corrosion, or chemical leakage.
- Keep digital records (with serial numbers, date of removal, condition) for each item to facilitate traceability and compliance audits.

Example:

During a telecom tower upgrade, 12 BTS cabinets are removed. Of these, 7 are repairable, 3 are beyond repair and sent for recycling, and 2 contain battery systems classified as hazardous waste requiring special handling.

2. Handling and Storage

Proper handling and storage prevent environmental contamination, protect worker health, and maintain the recyclability of components.

Handling Guidelines:

- **Personal Protecive Equipment (PPE):** Technicians must wear insulated gloves, safety glasses, and — when handling dusty or chemically treated boards — dust masks or respirators.
- **Electrostaic Discharge (ESD) Protecion:** Circuit boards and sensitive electronic modules are handled with anti-static wrist straps and stored in ESD-safe bags to prevent damage if they are intended for reuse.
- **Battery Safety:** Lead-acid batteries are moved with lifting aids to avoid spills; lithium-ion packs are handled with fire-resistant gloves and kept away from high temperatures.

Storage Pracices:

- Batteries: Stored upright in acid-resistant trays; spill containment pallets are used in case of leaks.
- PCBs and Modules: Kept in anti-static containers to prevent physical and electrical damage.
- Cables: Coiled neatly, tied with reusable cable straps (avoiding metal wire ties that can cut into insulation).
- Hazardous vs. Non-Hazardous Separation: Hazardous waste is placed in sealed, labeled containers distinct from general recyclable waste to avoid cross-contamination.

Environmental Protecion Measures:

- Store all e-waste in ventilated, covered storage sheds with impermeable flooring to prevent soil contamination.
- Maintain spill response kits near hazardous waste areas.

3. Authorized Disposal and Recycling

India's **E-Waste (Management) Rules, 2022** mandate that e-waste be disposed of only through **authorized, registered recyclers** to ensure safe processing and recovery of valuable materials.

Procedure for Authorized Disposal:

1. **Selecion of Recycler:** Verify recycler's registration with the Central Pollution Control Board (CPCB) or State Pollution Control Board (SPCB).
2. **Documentaion:**
    - **Waste Manifest Form:** Lists the waste type, quantity, source, and destination.
    - **Transport Authorizaion:** Confirms the transporter is licensed to handle hazardous/e-waste.
    - **Handover Acknowledgement:** Signed receipt from the recycler upon delivery.
3. **Transportaion:** Use closed, labeled transport vehicles to prevent waste loss or spillage en route.
4. **Processing:** The recycler dismantles, segregates, and processes materials for recovery of metals, plastics, and glass; hazardous fractions are treated in compliance with environmental norms.
5. **Cerificaion:** Obtain a Certificate of Recycling or Disposal from the recycler, confirming final processing.

Refurbishment Programs:

Some telecom operators maintain **in-house refurbishment centers** where functional components from decommissioned sites are tested, repaired, and redeployed to other network locations. Example: Power supply modules removed from urban 4G sites are refurbished and reused in rural 2G/3G towers.

Compliance and Reporing:

Annual EPR (Extended Producer Responsibility) compliance reports must be submitted to the CPCB, detailing:

- Quantity of e-waste generated.
- Volume recycled or refurbished.
- Details of authorized recyclers used.

5.1.5 Occupaional Safety in Environmental Pracices for Telecom E-Waste Management

Handling e-waste in the telecom sector presents unique occupational hazards due to the size, complexity, and composition of telecom equipment. In addition to standard workplace safety concerns, technicians face chemical exposure, electrical risks, ergonomic strain, and fire hazards when working with obsolete batteries, high-voltage power units, and delicate electronic components.

To address these risks, telecom companies must integrate ISO 45001 Occupational Health and Safety Management System principles into all e-waste handling, storage, and disposal processes.

1. Risk Categories in Telecom E-Waste Handling

- **Physical Hazards**
  - **Manual handling injuries** from lifting heavy batteries, BTS cabinets, or cable reels.
  - **Sharp edges** on dismantled racks, cut cables, or broken circuit boards.
  - **Trip hazards** from loose cables or stacked materials in work areas.
- **Chemical Hazards**
  - **Lead, mercury, cadmium** in solder, switches, and PCB components.
  - **Sulfuric acid** in lead-acid batteries and potential leaks from lithium-ion cells.
  - **Polybrominated flame retardants** (PBDEs) from plastic casings.
  - **Toxic fumes** released during solder removal or thermal processing.
- **Electrical Hazards**
  - **Residual voltage** in capacitors, even after equipment is powered down.
  - **Staic discharge damage** when handling sensitive boards without proper grounding.
  - **Arc flash risks** during dismantling of live or improperly decommissioned equipment.
- **Ergonomic Hazards**
  - Repetitive motion injuries from unscrewing, cutting, or stripping cables.
  - Strain injuries from awkward postures when working inside tight rack enclosures.

- **Fire and Explosion Hazards**
  - Overheated lithium-ion batteries can ignite if damaged.
  - Accumulated dust in equipment rooms can be combustible in certain conditions.

2. Personal Protecive Equipment (PPE) for Telecom E-Waste Operaions

Telecom safety protocols mandate the use of specialized PPE based on the task and hazard type:

Hazard Type	PPE Requirement	Purpose
Electrical	Insulated gloves, dielectric boots	Prevent electrical shocks during live component handling
Chemical (Batteries, PCB chemicals)	Acid-resistant aprons, face shields, chemical-resistant gloves	Protect against corrosive spills and splashes
Dust and Particulate Matter	Respirators (N95 or higher), safety goggles	Prevent inhalation of harmful particles from boards and insulation
Mechanical / Sharp Objects	Cut-resistant gloves, safety shoes	Prevent cuts and puncture wounds
Fire / Explosion	Flame-resistant coveralls, fire blankets nearby	Minimize burn injuries from battery fires

3. Training Requirements

ISO 45001 emphasizes competence through training, ensuring all telecom site workers are aware of:

- Material Hazards Awareness — Understanding the toxicity of lead, mercury, cadmium, and acids.
- Safe Handling Procedures — Correct lifting techniques, ESD precautions, and lockout/tagout (LOTO) for electrical systems.
- Spill and Leak Response — Immediate containment, neutralization agents (e.g., baking soda for acid), and waste cleanup.
- Fire Safety — Use of Class D extinguishers for metal fires and lithium-ion incidents.
- First Aid — Immediate action for chemical burns, electrical shocks, or inhalation exposure.
- Incident Reporting Protocols — Clear chain-of-command for emergencies.

Training should be conducted annually, with refresher sessions whenever procedures change or new hazards are introduced.

4. Emergency Procedures

Spills and Leaks:

- Evacuate non-essential personnel.
- Wear appropriate PPE before approaching the spill.
- Contain with absorbent pads or neutralizing agents.
- Collect waste into sealed, labeled hazardous waste containers.

Electrical Accidents:

- Disconnect power immediately (LOTO).
- Do not touch the injured person with bare hands—use insulated rescue tools.
- Administer CPR if necessary and call emergency services.

Battery Fires:

- Use sand or Class D extinguishers; do not use water on lithium-ion fires.
- Isolate the area to prevent chain reaction from adjacent batteries.

5. Compliance and Monitoring

Telecom companies should:

- Conduct regular safety audits of e-waste storage and dismantling areas.
- Maintain incident logs for analysis and prevention.
- Ensure PPE inventory and replacement cycles are strictly managed.
- Engage in joint drills with authorized recyclers to coordinate emergency responses

5.1.6 Energy Opimizaion in Telecom Operaions

Telecommunications networks form the backbone of modern connectivity, but their infrastructure—comprising base transceiver stations (BTS), microwave links, switching centers, and data centers—demands continuous power supply, often 24/7.

Globally, the telecom sector consumes 2–3% of total electricity generated, contributing significantly to operational costs and carbon emissions.

Energy optimization strategies aim to reduce power consumption without compromising service quality, simultaneously lowering operating expenses (OPEX) and greenhouse gas (GHG) emissions.

a. Energy-Efficient Infrastructure

Modern telecom site designs focus on **energy efficiency from the ground up**, targeting both active equipment and passive site elements.

1. Advanced BTS (Base Transceiver Staion) Design

- **Semiconductor Innovaion:** New BTS units use high-efficiency power amplifiers with gallium nitride (GaN) and silicon carbide (SiC) transistors, which operate at lower heat and higher electrical efficiency than older silicon-based systems.
- **Dynamic Power Modes:** BTS hardware can switch to low-power or sleep mode during off-peak hours, reducing unnecessary energy draw.
- **Integrated Remote Radio Units (RRUs):** Placing RRUs closer to antennas minimizes feeder cable losses and improves power utilization.

2. Passive Cooling and Thermal Management

- **Free-Air Cooling:** Utilizes outside air instead of air-conditioning for cooling BTS shelters in suitable climates.
- **Heat Exchangers & Venilaion:** Reduce the need for compressor-based cooling systems.
- **High-Reflecivity Coaings:** Roofs and walls painted with reflective material lower internal temperatures, reducing cooling load.

3. Efficient Lighing Systems

- **LED Lighing:** Consumes up to **80% less power** than fluorescent or incandescent lamps, with longer lifespan and lower maintenance.
- **Moion-Sensor Acivaion:** Ensures lighting is only used when staff are present at the site.

b. Renewable Energy Integraion

Renewable energy adoption in telecom is both an environmental responsibility and a practical necessity, especially for **off-grid and rural locaions**.

1. Hybrid Solar-Diesel Systems

- Solar Photovoltaic (PV) Panels supply daytime power, significantly reducing diesel generator runtime.
- Intelligent Energy Controllers manage seamless switching between solar, battery, and diesel inputs.
- Result: Up to 60% reduction in diesel consumption at remote tower sites.

2. Wind Power Soluions

- Small-scale wind turbines complement solar systems in areas with strong, consistent winds.
- Particularly effective in coastal regions and elevated terrains.

3. Energy Storage Advancements

- Lithium-Ion Battery Systems offer higher energy density, faster charging, and longer lifespan compared to lead-acid batteries.
- Hybrid Storage Models combine lithium-ion with supercapacitors for peak load handling.

4. Green Power Purchase Agreements (PPA)

- Urban switching centers and data hubs increasingly use utility-supplied renewable energy through PPAs, ensuring stable power supply with lower carbon footprint.

5.1.7 Reducing the Carbon Footprint in Telecom

The carbon footprint of the telecom industry comes from a combination of direct emissions (Scope 1, e.g., fuel consumption for generators and vehicles) and indirect emissions (Scope 2 & 3, e.g., electricity use in network infrastructure, outsourced logistics, and manufacturing of equipment).

Reducing this footprint requires technological innovation, operational efficiency, and supply chain collaboration.

1. Network Function Virtualization (NFV)

Definition:

Network Function Virtualization replaces dedicated hardware appliances with software-based network functions running on commercial off-the-shelf (COTS) servers.

Benefits in Carbon Reduction:

- Less Physical Equipment: Eliminates the need for multiple proprietary hardware units, reducing manufacturing-related emissions.
- Lower Cooling Load: Virtualized environments run on fewer, more efficient servers, requiring less air-conditioning.
- Scalable Energy Use: Resources can be allocated dynamically, so unused capacity is powered down instead of idling.

Example in Telecom:

Replacing separate hardware firewalls, load balancers, and routers with virtualized equivalents in a Software-Defined Networking (SDN) environment.

2. Equipment Rack Consolidation

Concept:

Consolidating multiple low-utilization racks into fewer, high-utilization ones.

Environmental Benefits:

- Reduced Power Demand: Fewer active devices drawing electricity.
- Cooling Efficiency: Smaller heat output means air-conditioning units can operate less frequently or at lower capacity.
- Optimized Floor Space: Enables more efficient airflow design in data centers.

Implementation Methods:

- Auditing rack utilization rates using Data Center Infrastructure Management (DCIM) tools.
- Deploying high-density blade servers or modular BTS units to replace multiple low-density racks.

3. Green Fleet Initiatives for Maintenance Teams

Telecom field operations, especially tower maintenance, involve significant fuel consumption from service vehicles.

Transitioning to electric vehicles (EVs) or hybrid fleets helps reduce direct Scope 1 emissions.

Strategies:

- EV Charging Hubs: Installed at regional service depots.
- Route Optimization Software: Minimizes travel distances and idle time.
- Driver Training Programs: Encourage eco-driving habits for lower fuel usage.

4. Sustainable Logistics Partnerships

Many telecom companies outsource equipment delivery and retrieval to logistics providers. Partnering with vendors who maintain low-emission or alternative-fuel fleets contributes to carbon reduction.

Examples:

- Contracting suppliers with EURO VI-compliant diesel trucks or CNG-powered vehicles.
- Encouraging backhaul logistics (return trips carrying e-waste or refurbished components) to avoid empty journeys.
- Using smart packaging to reduce material waste and transport volume.

5. Complementary Carbon Reduction Measures

- Renewable Power Purchase Agreements (PPAs): For data centers and switching stations.
- Remote Network Monitoring: Reduces the need for physical site visits.
- Lifecycle Extension of Equipment: Through refurbishment, thus avoiding emissions from manufacturing replacements.

5.1.8. Documentation and Compliance Tracking in Telecom Environmental Management

In the telecom sector, documentation is not just a regulatory requirement—it is the backbone of environmental accountability, performance benchmarking, and continuous improvement. Proper compliance tracking ensures that operators meet both legal obligations and corporate sustainability goals, while also providing auditable evidence for internal and external stakeholders.

Purpose of Documentation in Telecom Environmental Practices

1. Regulatory Compliance:

- National laws (e.g., E-Waste Management Rules, CPCB guidelines in India, EU WEEE Directive, US EPA regulations) require operators to maintain detailed waste movement and recycling records.
- Extended Producer Responsibility (EPR) frameworks mandate proof that a set percentage of products are recovered or recycled annually.

2. Environmental Performance Monitoring:

- Enables tracking of energy efficiency improvements, waste diversion rates, and GHG emission reductions.
- Facilitates identification of recurring inefficiencies (e.g., high diesel usage at specific tower clusters).

3. Risk Management:

- Accurate records reduce the risk of non-compliance penalties and help operators quickly address discrepancies flagged by regulators or auditors.

b. Types of Environmental Documentation in Telecom Operations

1. Waste Disposal Registers

Contents:

- Type of waste (e.g., lead-acid battery, printed circuit board, copper cable).
- Quantity (in kg or units).
- E-waste classification code.
- Date of disposal.
- Name and license number of the authorized recycler.
- Final waste destination (recycling, incineration, landfill).

Format:

Often digital, integrated into Enterprise Resource Planning (ERP) or Environmental Management Information Systems (EMIS).

2. Waste Transfer Manifests

- Legal documents tracking the movement of hazardous or non-hazardous waste from telecom sites to processing facilities.
- Includes chain-of-custody signatures at each transfer stage.

3. Energy Consumption Logs

- Monitors site-level electricity usage, diesel generator runtime, and renewable energy contribution.
- Data collected via IoT-based smart meters and Network Operations Center (NOC) dashboards.

4. Sustainability Performance Reports

Quarterly or annual reports consolidating environmental KPIs:

- Energy savings (kWh/year).
- CO_2 emissions avoided (tons/year).
- EPR compliance percentage.

Often aligned with Global Reporting Initiative (GRI) standards.

5. Audit Records

- Findings from internal and external sustainability audits.
- Action plans for corrective measures.

Sustainability Audits in Telecom

Frequency:

- Typically conducted quarterly for EPR and waste management compliance.
- Annual audits focus on broader environmental goals and certification renewal (e.g., ISO 14001: Environmental Management Systems).

Audit Scope:

- Verification of waste disposal records against recycler receipts.
- Inspection of on-site waste segregation and storage practices.
- Evaluation of energy optimization measures and renewable integration progress.
- Compliance with occupational safety protocols during environmental tasks.

Audit Tools & Methods:

- Digital tracking platforms with QR code–tagged components for real-time waste movement updates.
- Thermal imaging for checking site cooling efficiency.
- Benchmarking reports comparing site performance across regions.

Role of Technology in Compliance Tracking

Modern telecom operators increasingly rely on automated compliance systems:

- RFID & Barcode Tagging for equipment and e-waste items.
- Cloud-Based EPR Portals for submitting disposal data to regulators.
- AI-Driven Energy Analytics to flag abnormal consumption trends.

Benefits of Robust Documentation Practices

- Avoidance of hefty fines and legal disputes.
- Easier CSR reporting and sustainability branding.
- Improved operational efficiency through trend analysis.
- Strengthened stakeholder confidence in environmental stewardship.

Exercise

A. Muliple Choice Quesion:

1. Which of the following is the primary reason for maintaining the minimum bending radius during cable laying?
   a) To reduce installation time
   b) To avoid damage to the cable core
   c) To prevent cable theft
   d) To ensure color coding remains visible
2. In underground cable laying, which method uses pre-installed protective ducts?
   a) Direct burial method
   b) Trenching
   c) Duct laying method
   d) Aerial laying method
3. Which equipment is typically used to pull heavy cables over long distances?
   a) Torque wrench
   b) Cable winch machine
   c) Splicing kit
   d) Heat gun
4. What is the main purpose of using cable rollers during laying?
   a) To measure cable length
   b) To avoid excessive friction and damage
   c) To connect two cables
   d) To mark cable positions
5. In aerial cable installation, what is the recommended method for securing cables to poles?
   a) Using plastic adhesive tape
   b) Using approved cable ties or clamps
   c) Wrapping with fiber cord
   d) Leaving it hanging loosely

B. Descripive Quesions:

1. Explain the step-by-step procedure for laying cables using the direct burial method.
2. Describe the safety precautions that should be followed while laying underground cables.
3. What is the difference between aerial cable laying and underground cable laying in terms of cost, durability, and maintenance?
4. Explain the role and importance of cable jointing and termination in cable laying projects.
5. Discuss the common challenges faced during cable laying in urban areas and the methods to overcome them.

Notes

6. Employability Skills (60 Hours)

Telecom Sector Skill Council

It is recommended that all training include the appropriate. Employability Skills Module. Content for the same can be accessed https://www.skillindiadigital.gov.in/content/list

DGT/VSQ/N0102

7. Annexure

Annexure I - QR Codes –Video Links

Annexure - I

QR Codes –Video Links

Chapter No.	Unit Name	Topic	Page No.	URL Links	QR code (s)
Chapter 2: Lay Cable/System Wiring and Install Equipment at Customer Premises	Unit 2.3 - Establishing Communication between Nodes, Gateway and Servers	IoT Cloud Framework	121	https://www.youtube.com/watch?v=D7J37mbEj0M	
	Unit 2.11 - Understanding Error Codes and Debug Software	Understanding Edge Devices	211	https://www.youtube.com/watch?v=LlhmzVL5bm8	
Chapter 3: Configuring Equipment and Establishing Wireless Network Connectivity	Unit 3.1 - Network Topologies	Network Topology	277	https://www.youtube.com/watch?v=uSKdjjw5zow	
	Unit 3.5 - Comprehension and Interpretation of Technical Data	Interpreting Technical Data	308	https://www.youtube.com/watch?v=Hm6Urf8ng3M	
	Unit 3.6 - Executing Speed Test and Analyze	How to perform speed x test	313	https://www.youtube.com/watch?v=ad4tTK43VKc&ab_channel=Maxis	
Chapter 4: Troubleshoot and Rectify Faults	Unit 4.1 - Escalation Matrix	What Is An Escalation Matrix?	319	https://www.youtube.com/watch?v=opB5oOvB3cI	

Chapter No.	Unit Name	Topic	Page No.	URL Links	QR code (s)
Chapter 4: Troubleshoot and Rectify Faults	Unit 4.3 - Identifying and Repairing Faulty Cables and Connectors	Explaining Optical Time Domain Reflectometry (OTDR) Testing Method	330	https://www.youtube.com/watch?v=sDLci29nl-g	
	Unit 4.4 - Electro Magnetic Interference (EMI) and Electro Magnetic Compatibility (EMC)	EMI - Electromagnetic Interference and EMC - Electromagnetic Compatibility Explained	333	https://www.youtube.com/watch?v=I88Qzdahn_o	
	Unit 4.7 - Troubleshooting of CPE (Modem, Router, Switch)	Modem, Router, Switch, Hub and Access Point: What's the Difference?	346	https://www.youtube.com/watch?v=39zXmf61McI	

NCVET
कौशल गुणवत्ता प्रगति

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
RE IMAGINE FUTURE

Telecom Sector Skill Council

Telecom Sector Skill Council
Estel House,3rd Floor, Plot No: - 126, Sector-44
Gurgaon, Haryana 122003
Phone: 0124-2222222
Email: tssc@tsscindia.com
Website: www.tsscindia.com