



Facilitator Guide



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**



Shri Narendra Modi
Prime Minister of India

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



Acknowledgements

Telecom Sector Skill Council (TSSC) would like to thank all the individuals and institutions who contributed in various ways towards the preparation of this facilitator guide. The facilitator guide could not have been completed without their active contribution. Special gratitude is extended to those who collaborated during the preparation of the different modules in the facilitator guide. Wholehearted appreciation is also extended to all who provided peer review for these modules.

The preparation of this guide would not have been possible without the Telecom Industry's support. Industry feedback has been extremely beneficial since inception to conclusion and it is with their guidance that we have tried to bridge the existing skill gaps in the industry. This facilitator guide is dedicated to the aspiring youth, who desire to achieve special skills which will be a lifelong asset for their future endeavours.

About this Guide

In the last five years, the growth of the Indian telecommunications sector has outpaced the overall economic growth. This sector is poised for strong growth of about 15 percent in short term during 2013–17, driven by growth in organised retail, technological advancements, changing consumer preferences and government support. With over 1000 million subscribers, India is the second largest telecom market in the world.

The sector currently employs over 2.08 million employees and is slated to employ more than 4.16 million employees by 2022. This implies additional creation of ~2.1 million jobs in the nine-year period.

This Facilitator Guide is designed to impart theoretical and practical skill training to students for becoming a Telecom Technician – IoT Devices/Systems. Telecom Technician 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), setup 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 Facilitator Guide 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 Facilitator Guide will provide a sound learning support to our young friends to build an attractive career in the telecom industry.

Symbols Used



Ask



Activity



Do



Demonstrate



Explain



Elaborate



Example



Exercise



Facilitation Notes



Field Visit



Learning Outcomes



Notes



Objectives



Practical



Resources



Team Activity



Summarize




Say

Table of Contents

S.No.	Modules and Units	Page No.
1.	Introduction to the Sector and the Job Role of a Telecom Technician-IoT Devices/Systems (TEL/N6234)	1
	Unit 1.1 - Introduction to Telecom Sector and Role of a Telecom Technician-IoT Devices/Systems	3
	Unit 1.2 - Functioning of Sensors and Actuators	6
	Unit 1.3 - Application of Communication Protocol in Internet of Things	8
	Unit 1.4 - Micro-controller Boards, PIN Configurations and Their Interconnectivity	10
	Unit 1.5 - Understanding Edge Devices	12
	Unit 1.6 - Nodes and Gateways	14
	Unit 1.7 - Cloud Computing	16
2.	Lay Install and Configure IoT Devices at Customer Premises (TEL/N6234)	21
	Unit 2.1 - Establishing Framework for Internet of Things	23
	Unit 2.2 - Installing Gateway as per the Power Supply Requirements	25
	Unit 2.3 - Establishing Communication between Nodes, Gateway and Servers	27
	Unit 2.4 - Establishing Ethernet Connectivity	29
	Unit 2.5 - Authentication and Access Control Mechanism	31
	Unit 2.6 - Mounting the Devices at Desired Locations	33
	Unit 2.7 - Performing Checks and Connections	35
	Unit 2.8 - Connecting Microcontroller Boards for Data Transfer and Connecting the Boards	37
	Unit 2.9 - Installing Suitable Framework	39
	Unit 2.10 - Transferring Software Code to On-board Microprocessor and Compiling Code to On-Board Microprocessor	41
	Unit 2.11 - Understanding Error Codes and Debug Software	43
	Unit 2.12 - Functioning of Micro-controller and Attached Devices	45
	Unit 2.13 - Initializing Nodes and Gateways	47
	Unit 2.14 - Launching the Software on Nodes and Gateways	49
	Unit 2.15 - Confirming Communication and Establishing Connectivity	51
	Unit 2.16 - Controlling Edge Appliances and Hubs and Checking for Data Transfer and Confirming from the Server End	53
3.	Configuring Equipment and Establishing Wireless Network Connectivity (TEL/N4123)	58
	Unit 3.1 - Network Topologies	60
	Unit 3.2 - Establishing Connectivity	62
	Unit 3.3 - Establishing Connectivity	64
	Unit 3.4 - Configuration Testing	66
	Unit 3.5 - Comprehension and Interpretation of Technical Data	68
	Unit 3.6 - Executing Speed Test and Analyze	70



Table of Contents

S.No.	Modules and Units	Page No.
4.	Troubleshoot and Rectify Faults (TEL/N0113)	75
	Unit 4.1 - Escalation Matrix	77
	Unit 4.2 - Problem Solving	79
	Unit 4.3 - Identifying and Repairing Faulty Cables and Connectors	81
	Unit 4.4 - Electro Magnetic Interference (EMI) and Electro Magnetic Compatibility (EMC)	83
	Unit 4.5 - Crimping and Soldering	85
	Unit 4.6 - Troubleshooting of Cable and Connector	87
	Unit 4.7 - Troubleshooting of CPE (Modem, Router, Switch)	89
	Unit 4.8 - Troubleshooting of Configuration and Connectivity CPE faults	91
	Unit 4.9 - Troubleshooting and Repairing of Client's Broadband Service	93
5.	Follow Sustainable Practices in Telecom Infrastructure Installation (TEL/N9105)	98
	Unit 5.1 - Environmental Sustainability and Waste Management in the Telecommunications Industry	100
6.	Employability Skills (60 Hours) – (DGT/VSQ/N0102)	107
	<p>It is recommended that all trainings include the appropriate Employability skills Module. Content for the same is available here: https://www.skillindiadigital.gov.in/content/list</p> 	
7.	Annexure	108
	Annexure I: Training Delivery Plan	109
	Annexure II: Assessment Criteria	115
	Annexure III: List of QR Codes used in PHB	116







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



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

Unit 1.2 - Functioning of Sensors and Actuators

Unit 1.3 - Application of Communication Protocol in Internet of Things

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

Unit 1.5 - Understanding Edge Devices

Unit 1.6 - Nodes and Gateways

Unit 1.7 - Cloud Computing



Key Learning Outcomes



After the completion of this module, the participant 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: Basics of Micro-Processor Boards and Microcontroller Units

Unit Objectives

After the completion of this unit, the participant 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 production of IoT devices and systems.
6. Discuss the applications of IoT in smart cities, healthcare, Industry 4.0, and agriculture.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, sample IoT devices (sensors, routers, smart meters), videos on smart cities and Industry 4.0, notepad, pens.

Note

In this unit, we will understand how the telecom sector plays a critical role in the manufacturing, assembly, testing, and real-world deployment of IoT devices and systems.

Say

Good Morning everyone!

Today's session will introduce you to an exciting and fast-growing area of telecom—the Internet of Things (IoT). From smart homes and cities to modern healthcare and factories, IoT is changing the world. As future broadband and telecom technicians, your role in this transformation is extremely important.

Ask

Ask the participants:

- Have you ever used a smart device like a smart TV, smartwatch, smart light, or smart meter?
- Where do you think these devices send their data?

Write their answers on the whiteboard or flipchart.

Use their responses to transition into the lesson.

Elaborate

In this session, we will discuss the following point:

- Importance of the telecom sector in IoT manufacturing and networking
- Role of communication modules (SIM, routers, gateways) in IoT
- Skills required for a Telecom Technician in IoT assembly and testing
- Challenges in assembling IoT devices such as miniaturization, testing accuracy, and firmware integration
- Importance of precision and quality control in IoT devices
- Technician responsibilities in ensuring high-quality production
- Applications of IoT in:
 - Smart Cities (traffic, street lighting, surveillance)
 - Healthcare (remote monitoring, wearables)
 - Industry 4.0 (automation, robotics, sensors)
 - Agriculture (smart irrigation, soil monitoring)

Say

Let us now do an activity “IoT Application Mapping” to understand how IoT devices work in real life.

Activity

- Duration: 30 minutes
- Resources: Chart paper, markers, projector, images/videos of IoT systems.
- Steps:
 1. Divide the trainees into four groups.
 2. Assign each group one sector:
 - Smart Cities
 - Healthcare
 - Industry 4.0
 - Agriculture
 3. Ask each group to:
 - List at least 5 IoT devices used in that sector
 - Explain how telecom connectivity supports those devices
 4. Each group presents their ideas to the class.

Do

- Write key points from each group on the whiteboard.
- Correct any misunderstandings gently.
- Highlight how broadband, fiber, and wireless networks support IoT.
- Ask one trainee to summarize how IoT is used across different industries.

Notes for Facilitation

- Encourage learners to connect IoT concepts with daily life examples.
- Use simple language while explaining Industry 4.0 and automation.
- Reinforce that IoT is a career growth opportunity in the telecom sector.
- Ask trainees to review IoT applications from their participant manual.
- End the session by motivating them to explore smart technologies actively.

UNIT 1.2: Functioning of Sensors and Actuators

Unit Objectives

After the completion of this unit, the participant 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

Resources to be Used

Participant handbook, whiteboard, markers, laptop, projector, sample sensors (temperature, motion, light), sample actuators (motor, relay, buzzer), microcontroller board (Arduino or similar), USB cable, basic programming software, notepad, pens.

Note

In this unit, we will understand the basic building blocks of IoT systems—sensors, actuators, and how a simple microcontroller is programmed to control them.

Say

Good Morning everyone!

Today's session is where hardware meets intelligence. Sensors collect data, actuators take action, and the microcontroller acts as the brain. By the end of this session, you'll clearly understand how smart devices actually sense and respond to the real world.

Ask

Ask the participants:

- Can you name any device that senses temperature, motion, or light?
- Have you heard of Arduino or any microcontroller board before?

Write their answers on the whiteboard or flipchart.

Use their responses to transition into the lesson.

Elaborate

In this session, we will discuss the following point:

- What is a sensor and why it is used
- Types of sensors
- What is an actuator and its importance
- Difference between a sensor and an actuator
- Role of a microcontroller in IoT systems

Say

Let us now do an activity “Sensor and Actuator Identification” to understand where you will identify real components.

Activity

- Duration: 30 minutes
- Resources: Real sensors and actuators, chart paper, markers, projector.
- Steps:
 1. Divide the trainees into small groups.
 2. Show physical samples or images of sensors and actuators.
 3. Ask each group to:
 - Identify the component
 - State whether it is a sensor or an actuator
 - Explain its real-life application
 4. Each group presents their answers.

Do

- Write the correct answers on the board.
- Clarify mistakes in a positive way.
- Relate each component to real telecom and IoT applications.
- Encourage all trainees to speak.
- Ask one trainee to summarize the types of sensors discussed.

Notes for Facilitation

- Use real-life examples while explaining sensors and actuators.
- Keep programming explanations simple and activity-based.
- Encourage curiosity and hands-on learning.
- Remind trainees that these fundamentals help them grow into IoT and smart system technicians.
- Ask trainees to review the basics from their participant handbook.

UNIT 1.3: Application of Communication Protocol in Internet of Things

Unit Objectives

After the completion of this unit, the participant will be able to:

- List various short-range wireless communications systems
- Identify the protocols used for communication in IoT
- Compare different communication technologies
- Describe the communication technologies used in IoT, including 5G, NB-IoT, LoRaWAN, Wi-Fi, Bluetooth, and Zigbee.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, videos of IoT connectivity, charts showing communication ranges, notepad, pens.

Note

In this unit, we will understand how IoT devices communicate with each other and with networks, and how different wireless technologies are selected based on distance, speed, power, and application.

Say

Good Morning everyone!

Till now, we have learned about sensors, actuators, and controllers. Today, we move to one of the most important parts of IoT—communication. Without communication, even the smartest device is useless. By the end of this session, you will clearly understand how IoT devices send and receive data using different wireless technologies.

Ask

Ask the participants:

- How does your mobile phone connect to the internet—through Wi-Fi or mobile data?
- Have you ever used Bluetooth to connect earphones or transfer data?

Write their answers on the whiteboard or flipchart.

Use their daily-life examples to introduce IoT communication systems.

Elaborate

In this session, we will discuss the following point:

- What is wireless communication in IoT
- Short-range wireless communication systems: Bluetooth, Zigbee, Wi-Fi, RFID, NFC
- Common IoT communication protocols: MQTT, CoAP, HTTP/HTTPS, SAMQP
- Challenges in assembling IoT devices such as miniaturization, testing accuracy, and firmware integration
- Overview of major IoT communication technologies

Say

Let us now take part in an activity “Communication Technology Mapping” to match technologies with real-life applications.

Activity

- Duration: 30 minutes
- Resources: Chart paper, markers, projector, images of smart devices.
- Steps:
 1. Divide the trainees into six groups.
 2. Assign each group one technology:
 - 5G
 - NB-IoT
 - LoRaWAN
 - Wi-Fi
 - Bluetooth
 - Zigbee
 3. Ask each group to:
 - List 5 devices that use their assigned technology
 - Mention range, speed, and power consumption
 - Explain one real IoT application
 4. Each group presents their findings.

Do

- Write the correct answers on the board.
- Highlight how telecom networks support all these technologies.
- Ask one trainee to summarize the differences between Wi-Fi, Bluetooth, and Zigbee.

Notes for Facilitation

- Use real-life examples while explaining wireless technologies.
- Keep programming explanations simple and activity-based.
- Encourage curiosity and hands-on learning.

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

Unit Objectives

After the completion of this unit, the participant will be able to:

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

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, sample microcontroller boards (Arduino UNO, NodeMCU, Raspberry Pi Pico, ESP32), printed board layout diagrams, notepad, pens.

Note

In this unit, we will focus on understanding the internal components and physical layout of microcontroller development boards, which are widely used in IoT and telecom-based applications.

Say

Good Morning everyone!

Today, we will go one step deeper and look inside the microcontroller board itself. By the end of this session, you will be able to confidently identify each part of a development board and understand its purpose.

Ask

Ask the participants:

- Have you seen a microcontroller board before? If yes, which one?
- Looking at a board, what parts can you visually identify?

Write their answers on the whiteboard or flipchart.

Use their responses to transition into the lesson.

Elaborate

In this session, we will discuss the following point:

- Main Components of a Microcontroller Board
- Layout of Different Development Boards
- Importance of Board Layout for Technicians

Say

Let us now take part in an activity “Component Identification on Microcontroller Boards” to visually explore real development boards.

Activity

- Duration: 30 minutes
- Resources: Sample boards, printed diagrams, markers, chart paper.
- Steps:
 1. Divide the class into small groups.
 2. Give each group a real microcontroller board or a printed layout diagram.
 3. Ask each group to:
 - Identify the microcontroller chip
 - Mark the power pins
 - Locate the digital and analog pins
 - Identify the USB connector and reset button
 4. Each group presents their findings to the class.

Do

- Correct the pin identification where needed.
- Explain why certain pins must be handled carefully.
- Highlight common mistakes made during wiring.
- Encourage all trainees to touch, observe, and explore the boards.
- Ask one trainee to summarize the major components of a microcontroller board.

Notes for Facilitation

- Encourage hands-on observation rather than only theory.
- Keep the explanation simple and free from heavy electronics formulas.
- Relate board layout understanding to real-life troubleshooting.
- Reinforce that knowing board components is essential for safe and correct wiring.
- Ask trainees to revise board layouts from their participant manual.

UNIT 1.5: Understanding Edge Devices

Unit Objectives

After the completion of this unit, the participant will be able to:

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

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, sample edge devices (gateway, router, smart camera), videos of edge computing use cases, notepad, pens.

Note

In this unit, we will understand what edge devices are, why they are important in IoT and telecom networks, and the different types of devices used at the network edge.

Say

Good Morning everyone!

Today, we are going to learn about a very powerful part of IoT systems—edge devices. These are the devices that sit between the real world and the cloud, making smart decisions quickly and efficiently.

Ask

Ask the participants:

- Have you ever used a Wi-Fi router or CCTV camera at home?
- Where do you think data from sensors is processed—only in the cloud or somewhere closer?

Write their answers on the whiteboard or flipchart.

Use their responses to transition into the lesson.

Elaborate

In this session, we will discuss the following point:

- What are Edge Devices?
- Functions of Edge Devices
- Types of Edge Devices
- Importance of Edge Devices in Telecom

Say

Now let us take part in an activity “Edge Device Identification Around Us” to identify edge devices used around us.

Activity

- Duration: 30 minutes
- Resources: Chart paper, markers, projector, images of IoT and telecom systems.
- Steps:
 1. Divide the trainees into small groups.
 2. Ask each group to list at least 5 edge devices they see in daily life or telecom systems.
 3. For each device, they must mention:
 - Where it is used
 - What type of data it handles
 - One function it performs
 4. Each group presents their findings to the class.

Do

- Write correct examples on the whiteboard.
- Correct misunderstandings politely.
- Connect each example to a real telecom use case.
- Encourage all trainees to participate.
- Ask one trainee to summarize the key functions of edge devices.

Notes for Facilitation

- Use familiar home and mobile examples while explaining edge devices. Avoid heavy cloud computing theory—focus on practical understanding.
- Reinforce that edge devices make real-time IoT possible.
- Encourage trainees to observe edge devices around them in daily life.
- Ask trainees to revise edge device types from their participant manual.

UNIT 1.6: Nodes and Gateways

Unit Objectives

After the completion of this unit, the participant will be able to:

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

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, sample IoT block diagram charts, notepad, pens.

Note

In this unit, we will understand the core building blocks of an IoT system—nodes, gateways, and the step-by-step process of setting up a complete IoT framework.

Say

Good Morning everyone!

Today, we are going to connect all these pieces together and understand how a complete IoT system is built—from a sensing node to the gateway and finally to the cloud.

Ask

Ask the participants:

- What do you think is the role of a sensor in an IoT system?
- Have you heard the term “gateway” before? Where have you seen it used?

Write their answers on the whiteboard or flipchart.

Use their responses to smoothly introduce nodes and gateways.

Elaborate

In this session, we will discuss the following point:

- What is an IoT Node?
- Types of IoT Nodes
- IoT Gateway Architecture
- Steps in Setting Up an IoT Framework

Say

Now let us participate in an activity “IoT System Building Block Diagram” to clearly understand how a full IoT system is formed.

Activity

- Duration: 30 minutes
- Resources: Chart paper, markers, projector, printed icons (sensor, node, gateway, cloud).
- Steps:
 1. Divide the trainees into small groups.
 2. Ask each group to draw a block diagram of a complete IoT system showing:
 - Sensors
 - IoT node
 - Gateway
 - Cloud
 - User interface (mobile or computer)
 3. Each group must explain the flow of data from sensor to cloud.
 4. Groups present their diagrams to the class.

Do

- Correct block diagram sequencing where needed.
- Emphasize the role of the gateway as a central bridge.
- Appreciate clear explanations given by trainees.
- Encourage quieter students to participate.
- Ask one trainee to summarize the role of a node and a gateway.

Notes for Facilitation

- Keep the explanation application-oriented rather than deeply theoretical.
- Use smart home and smart city examples for clarity.
- Slowly repeat the framework steps to ensure understanding.
- Reinforce that every successful IoT project depends on correct node–gateway–cloud integration.
- Ask trainees to revise block diagrams and setup steps from their participant manual.

UNIT 1.7: Cloud Computing

Unit Objectives

After the completion of this unit, the participant 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

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, internet connection, short videos on cloud services, notepad, pens.

Note

In this unit, we will understand the basic concept of cloud computing, its key characteristics, and how it supports business analytics and modern digital services, especially in telecom and IoT environments.

Say

Good Morning everyone!

Today, we move one level higher—to the cloud. The cloud is where data is stored, analyzed, and turned into useful information for businesses and users.

Ask

Ask the participants:

- Have you ever used Google Drive, Gmail, or online storage?
- Where do you think your photos, emails, and files are actually stored?

Write their answers on the whiteboard or flipchart.

Use their responses to naturally introduce the concept of cloud computing.

Elaborate

In this session, we will discuss the following point:

- Concept of Cloud Computing
- Characteristics of Cloud Computing
- Cloud Computing and Business Analytics
- Advantages of Cloud Utilization

Say

Now let us understand how cloud supports business analytics.

Activity

- Duration: 30 minutes
- Resources: Projector, short video or written case scenario.
- Steps:
 1. Show a small case like:
 - A telecom company analyzing customer data to improve network quality.
 2. Ask trainees to identify:
 - Where the data is stored
 - How it is analyzed
 - How decisions are taken
 3. Facilitate a discussion on how cloud helps businesses grow.

Do

- Emphasize that big data needs big cloud power.
- Relate analytics to telecom customer service and network optimization.
- Encourage logical thinking rather than memorization.
- Ask one trainee to explain cloud and analytics in simple words.

Notes for Facilitation

- Use simple daily-life cloud examples (email, photos, online apps).
- Avoid technical jargon like virtualization at beginner level.
- Reinforce that cloud is the foundation of IoT, analytics, and digital business.
- Encourage trainees to observe cloud usage in real life.
- Ask trainees to revise cloud basics from their participant manual.

Exercise



Answers to exercises for PHB

A. Short Answer Questions:

1. The telecom sector provides connectivity, network infrastructure, and communication protocols required for IoT device manufacturing, integration, and operation.
2. Sensor integration, circuit testing, networking basics, device configuration, and troubleshooting.
3. Ensuring reliable connectivity, device compatibility, accuracy in assembly, and proper testing of sensors and communication modules.
4. It ensures device reliability, safety, performance accuracy, and compliance with industry standards.
5. Ensuring proper assembly, conducting testing, minimizing defects, maintaining equipment, and ensuring consistent product quality.

B. Multiple Choice Questions (MCQs):

1. b) A device connected to the internet for data exchange and remote control
2. b) Sensor integration, circuit testing, and device configuration
3. b) Reliable connectivity, compatibility, and precision
4. b) Compliance with standards and device reliability
5. b) Assemble, test, and verify the performance of connected devices

C. Fill in the Blanks:

1. Telecom
2. Assembly
3. Precision
4. Compatibility
5. Documentation

Notes

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



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



After the completion of this module, the participant 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: Establish an IoT Framework

Unit Objectives

After the completion of this unit, the participant 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

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, IoT architecture charts, sample sensors, microcontroller board, gateway/router, videos of edge and fog computing, notepad, pens.

Note

In this unit, we will learn how a full IoT system is installed step-by-step, how data is collected and transferred, and how modern technologies like edge computing, fog computing, and AI make telecom IoT systems faster and smarter.

Say

Good Morning everyone!

Today, we will connect all those building blocks together into one complete IoT system. By the end of this session, you will clearly understand how an IoT framework is installed, how data flows, and how smart technologies process it in real time.

Ask

Ask the participants:

- If you had to build a smart home system, what would you install first—sensors, internet connection, or software?
- Where do you think the data collected by sensors finally goes?

Write their answers on the whiteboard or flipchart.

Elaborate

In this session, we will discuss the following point:

- Steps of Installation of an IoT Framework
- Data Collection in IoT Systems
- Input Parameters for Sensors
- Principles of IoT Architecture

Say

Now let us take part in an activity to understand the complete IoT system flow in a practical way.

Activity

- Duration: 30 minutes
- Resources: Chart paper, markers, projector.
- Steps:
 1. Divide trainees into small groups.
 2. Ask each group to draw a complete IoT framework flow, starting from:
 - Sensor → Microcontroller → Gateway → Cloud → User
 2. hey must label: Data collection point, Processing point, and Communication method
 3. Each group presents their flow diagram.

Do

- Correct architecture sequence where needed.
- Reinforce the correct role of each component.
- Highlight how gateways and cloud work together.
- Encourage all groups to participate actively.
- Ask one trainee to summarize the IoT architecture in simple words.

Notes for Facilitation

- Use flow diagrams and visual charts for better understanding.
- Avoid deep software coding discussion—focus on system-level understanding.
- Relate every concept to telecom networks and broadband services.
- Reinforce that IoT is a combination of hardware + network + data + intelligence.
- Ask trainees to revise IoT architecture and data flow from their participant manual.

UNIT 2.2: Install Gateway as per the Power Supply Requirements

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, sample IoT node, IoT gateway, different battery types (Li-ion, lead-acid, coin cell), power adapters, solar panel image/sample, grounding wire, multimeter, safety gloves, notepad, pens.

Note

This unit focuses on powering IoT systems safely and efficiently. Learners will understand how to select the right power sources, manage batteries, differentiate between nodes and gateways, and choose safe and reliable installation locations for long-term operation.

Say

Good Morning everyone!

Today, we will learn how IoT nodes and gateways are powered, how batteries work, and how to select safe and optimal installation locations.

Ask

Ask the participants:

- What happens if the battery of a sensor fails?
- Do IoT gateways consume the same power as small sensors?
- Where would you install a gateway in a smart building?

Write their answers on the whiteboard or flipchart.

Elaborate



In this session, we will discuss the following point:

- Characteristics of Power Sources for IoT Nodes and Gateways
- Characteristics of Batteries Used in IoT Framework
- Differentiation Between IoT Nodes and Gateways
- Importance of Robust Battery Backup & Energy-Efficient Deployment
- Selecting Optimal Installation Points
- Connecting and Securing Power Supply with Grounding

Say



Now let us perform hands-on activities to understand how to power and install IoT nodes and gateways safely.

Activity



- Duration: 30 minutes
- Resources: Sample IoT node, gateway, power adapters, batteries.
- Steps:
 1. Show a real IoT node and a gateway.
 2. Ask trainees to identify:
 - Power input rating
 - Power source type
 - Battery or AC supply
 3. Let them record differences in a comparison table.

Do



- Correct incorrect observations.
- Explain why gateways consume more power.
- Reinforce the role of backup power.
- Ask one trainee to summarize differences.

Notes for Facilitation



- Emphasize that power failure is the number one cause of IoT system breakdown.
- Always relate battery backup to telecom uptime and service reliability.
- Avoid deep electrical engineering calculations—keep it technician-oriented.
- Reinforce safety standards and grounding importance repeatedly.
- Encourage eco-friendly and solar-powered deployments wherever possible.

UNIT 2.3: Establishing Communication between Nodes, Gateway and Servers

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, markers, laptop, projector, sample IoT node (sensor), IoT gateway, Ethernet cable, SIM card, Wi-Fi router, power adapters, internet connection, mobile hotspot, cloud dashboard demo (if available), notepad, pens.

Note

This unit focuses on the core working connection of any IoT system—how data actually moves from sensors to the gateway and finally to the cloud or local server. This is one of the most critical real-world job skills for any telecom or IoT technician.

Say

Good Morning everyone!

Today, we move to the most important part—making everything talk to each other. If the communication link fails, the entire IoT system becomes useless. So today, we will learn how to connect nodes, gateways, and cloud platforms in a proper and professional way.

Ask

Ask the participants:

- Have you ever faced a situation where the internet was connected, but data was still not showing on the system?
- What do you think connects a temperature sensor in the field to a mobile app?

Write their answers on the whiteboard or flipchart.

Elaborate

In this session, we will discuss the following point:

- Establishing Communication Line Connectivity Using Nodes, Gateways, and Networks
- Establishing Gateway-to-Cloud or Local Network Connectivity
- Common Connectivity Issues in Field Deployments
- Importance of Reliable Communication in Telecom IoT Systems

Say

Now let us move into hands-on practice, where you will actually perform the connectivity steps just like you would in a real installation site.

Activity

- Duration: 30 minutes
- Resources: IoT node, IoT gateway, power supply, Wi-Fi router, notepad.
- Steps:
 1. Divide trainees into small groups.
 2. Provide each group with one IoT node and gateway.
 3. Ask trainees to identify:
 - Power ON the devices
 - Select the correct protocol
 - Pair the node with the gateway
 4. Ask them to check if dummy data is reaching the gateway.

Do

- Walk around and observe the setup process.
- Correct protocol selection mistakes immediately.
- Help trainees understand LED indicators and status logs.
- Ask one trainee to explain the full connection flow on the board.

Notes for Facilitation

- Emphasize that connectivity issues are the most common field problem in IoT deployments.
- Always reinforce step-by-step logical checking.
- Avoid overloading with networking theories—focus on practical telecom field workflow.
- Encourage trainees to maintain a connectivity checklist during installations.
- Remind them about data security while connecting to the cloud.

UNIT 2.4: Establishing Ethernet Connectivity

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, Wi-Fi router, Ethernet cable, sample IoT gateway, access control software demo screenshots, antivirus software sample screen, notepad, pens.

Note

This unit focuses on cybersecurity and secure communication in IoT systems. Trainees will learn how to protect devices, networks, and data from unauthorized access and cyber-attacks, which is now one of the most critical responsibilities of a modern telecom technician.

Say

Good Morning everyone!

Today, we will learn about IoT security, how to protect networks, how access is controlled, and how data moves safely through Ethernet, TCP/IP, and VPN.

Ask

Ask the participants:

- What happens if someone hacks into a smart camera or smart meter?
- Have you ever heard of a website crashing due to heavy traffic or hacking?

Write their answers on the whiteboard or flipchart.

Elaborate

In this session, we will discuss the following point:

- Importance of Authentication and Authorization in IoT
- Access Control System
- Software Interface Characteristics
- Software Used for Access Control Management
- Securing Wireless Connections in IoT
- Working of Ethernet, TCP/IP, and VPN in IoT Installations

Say

Now let us perform hands-on activities to understand how IoT systems are protected and how secure communication is established.

Activity

- Duration: 30 minutes
- Resources: Wi-Fi router, laptop, gateway, projector.
- Steps:
 1. Demonstrate how to change Wi-Fi password.
 2. Enable WPA2/WPA3 security.
 3. Disable default login credentials.
 4. Show firewall enablement.
 5. Connect an IoT gateway securely to the network.

Do

- Ask trainees to repeat the steps.
- Correct weak password selections.
- Explain why changing default credentials is critical.
- Emphasize regular firmware updates.

Notes for Facilitation

- Avoid deep cybersecurity theory—keep explanations technician-focused.
- Continuously remind trainees that weak security = service failure + financial loss.
- Use simple real-life hacking examples.
- Emphasize strong passwords, regular updates, and firewall usage.
- Encourage safe digital habits both at work and home.

UNIT 2.5: Authentication and Access Control Mechanism

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, sample IoT gateway, internet connection, cybersecurity case study handouts, notepad, pens.

Note

This unit helps trainees understand real-world cyber threats in IoT systems and how to protect against them using standard security practices and global compliance frameworks. This knowledge is essential for anyone working with broadband, telecom networks, and IoT-enabled systems.

Say

Good Morning everyone!

Today, we go one step deeper. We will understand the most common cybersecurity threats faced by IoT systems and also learn about international security standards like ISO 27001, GDPR, and NIST that guide how data and networks should be protected.

Ask

Ask the participants:

- Why do hackers mostly target connected devices instead of isolated systems?
- What could happen if customer data from a smart meter or CCTV camera gets leaked?

Write their answers on the whiteboard or flipchart.

Elaborate

In this session, we will discuss the following point:

- Common IoT Cybersecurity Threats
- Preventive Measures Against IoT Cyber Threats
- Importance of Security Standards and Compliance
- ISO 27001 – Information Security Management System (ISMS)
- GDPR – General Data Protection Regulation
- NIST – National Institute of Standards and Technology (Cybersecurity Framework)

Say

Now let us move into activity where you will identify real cyber threats and link them with proper security standards and preventive measures.

Activity

- Duration: 30 minutes
- Resources: Case study handouts, whiteboard.
- Steps:
 1. Divide learners into small groups.
 2. Provide one cyber-attack scenario to each group.
 3. Ask them to identify:
 - Type of threat
 - Possible cause
 - Preventive action
 4. Groups present their answers.

Do

- Correct misclassification of cyber threats.
- Relate each preventive step to real telecom practices.
- Emphasize documentation and security logging.

Notes for Facilitation

- Use real-life hacking examples to keep trainees engaged.
- Avoid heavy legal language—explain standards in simple, practical terms.
- Emphasize that cybersecurity is everyone's responsibility, not only IT teams.
- Always relate security breaches to customer trust and business loss.
- Encourage safe digital habits inside and outside the workplace.

UNIT 2.6: Mounting Devices at Desired Locations

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, sample IoT sensors, smart meter demo unit, IP camera, industrial IoT device sample, microcontroller boards (Arduino, Raspberry Pi, ESP32, etc.), mounting brackets, screws, anchors, drill machine, screwdriver set, multimeter, network cables, power adapters, PPE (gloves, helmet), notepad, pens.

Note

This unit focuses on real-world physical installation skills required by IoT and telecom technicians. Trainees will learn how to mount devices safely, identify microcontroller boards, verify pin configurations, and install commonly used IoT field equipment such as smart meters and IP cameras.

Say

Good Morning everyone!

Today, you will learn how to mount IoT devices securely, identify microcontroller boards, check their pin configurations, and install real devices used in homes, cities, and industries.

Ask

Ask the participants:

- What could happen if an IoT device is mounted loosely or at a wrong location?
- Have you ever seen a CCTV camera stop working due to water or dust?

Use their answers to introduce safe installation and mounting importance.

Elaborate

In this session, we will discuss the following point:

- Secure Mounting of IoT Devices Using Industry-Approved Techniques
- Identification of Microprocessor Boards and Microcontrollers
- Checking Components, Pin Configuration, and Interconnectivity
- Installation and Configuration of Smart IoT Devices

Say

Now let us move to the most important part—hands-on installation and board identification practice, just like you will do at real customer and industrial sites.

Activity

- Duration: 30 minutes
- Resources: Camera, sensor, bracket, drill tools.
- Steps:
 - Demonstrate correct wall and pole mounting.
 - Show the use of anchors and fasteners.
 - Explain outdoor weatherproof installation.
 - Allow trainees to perform mounting in pairs.

Do

- Observe grip strength and bracket alignment.
- Correct unsafe drilling practices immediately.
- Ensure PPE usage during drilling.
- Reinforce weatherproof sealing importance.

Notes for Facilitation

- Emphasize that installation mistakes cause maximum after-sales complaints.
- Reinforce tool handling safety and PPE use repeatedly.
- Always teach trainees to read datasheets before connections.
- Link every activity to real telecom + IoT field conditions.
- Encourage teamwork and confidence during practical handling.

UNIT 2.7: Performing Checks and Connections

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, RF signal strength meter, spectrum analyzer (or mobile RF analyzer app), IoT sensors and gateway, antennas, power adapters, grounding wire, earthing rod sample, multimeter, PPE (helmet, gloves), warning signboard, notepad, pens.

Note

This unit focuses on radio frequency (RF) performance, interference issues, radiation safety, and safe installation practices. These factors directly affect the reliability, safety, and long-term performance of IoT and telecom systems, especially in real field environments.

Say

Good Morning everyone!

Today, we will understand how signal strength, RF interference, radiation safety, and grounding directly impact IoT performance and technician safety.

Ask

Ask the participants:

- Have you ever experienced dropped calls or slow internet despite having network coverage?
- What do you think happens to an IoT system when the signal is weak or power fails suddenly?

Use their answers to introduce safe installation and mounting importance.

Elaborate

In this session, we will discuss the following point:

- Impact of Signal Interference, Packet Loss & Power Failures on IoT Performance
- Tools & Techniques for RF Signal Strength Measurement & Spectrum Analysis
- Hazards of RF Radiation Exposure & Safety Procedures
- Performing Signal Strength Testing & RF Spectrum Analysis
- Proper Handling, Grounding & Safety Measures During IoT Installation

Say

Now let us move into practical signal testing, interference detection, and grounding demonstration, just like you would do at actual deployment sites.

Activity

- Duration: 30 minutes
- Resources: RF meter, IoT gateway, mobile analyzer app.
- Steps:
 - Demonstrate how to turn ON the RF meter.
 - Measure signal at multiple locations inside the room.
 - Record dBm values.
 - Compare results and identify the strongest position.

Do

- Help trainees interpret dBm readings.
- Explain why negative values are normal.
- Highlight safe antenna placement.

Notes for Facilitation

- Emphasize that RF issues are invisible but extremely damaging.
- Avoid heavy electromagnetic theory—keep focus on practical testing and placement.
- Repeatedly highlight that grounding is not optional, it is mandatory.
- Always connect RF safety with personal health and legal compliance.
- Encourage careful documentation of signal measurements during site work.

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

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, flipchart, markers, laptop, projector, microcontroller boards (Arduino, ESP32, Raspberry Pi), sensors (temperature, motion, gas), actuators (relay, motor, buzzer), jumper wires, USB cables, Ethernet cables, Wi-Fi router, SIM card, IoT gateway, power adapters, dashboard software/app, multimeter, notepad, pens, PPE.

Note

This unit focuses on the core technical skill of connecting IoT hardware, selecting the correct communication protocol, linking devices to interfaces, and validating real-time data flow. These skills are critical for successful IoT deployment at customer and industrial sites.

Say

Good Morning everyone!

Today, we bring everything together by configuring connectivity on microcontroller boards, selecting the right protocols, connecting sensors and actuators, and finally validating that real data is actually flowing through the system—just like in real projects.

Ask

Ask the participants:

- What happens if the sensor is connected correctly but data still does not appear on the dashboard?
- Do you think Bluetooth and LoRa are used for the same distance?

Use their responses to lead into connectivity setup, protocol selection, and data validation.

Elaborate

In this session, we will discuss the following point:

- Setting Up Connectivity Options on Microcontroller Boards
- Using Compatible Cable Connectors & Interfaces
- Selecting Appropriate Communication Protocols
- Functions and Applicability of Sensors & Actuators
- Validating Data Transfer Between Devices

Say

Now let us move into practical connectivity setup, protocol selection, and live data verification, exactly how you will do at real customer or industrial sites.

Activity

- Duration: 30 minutes
- Resources: ESP32/Arduino, laptop, USB cable, Wi-Fi router.
- Steps:
 - Power ON the board using USB.
 - Upload demo code.
 - Connect the board to Wi-Fi.
 - Display connection status on serial monitor.

Do

- Check that each trainee establishes Wi-Fi successfully.
- Help with SSID/password errors.
- Explain LED blink patterns clearly.

Notes for Facilitation

- Emphasize that correct connectivity + correct protocol = successful IoT deployment.
- Always preach “test before you leave the site”.
- Encourage trainees to use log files and LED indicators for quick troubleshooting.
- Relate every mistake to actual field errors that cause service failure.
- Keep confidence-building during hands-on sessions.

UNIT 2.9: Installing Suitable Framework

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, whiteboard, laptop, projector, internet connection, microcontroller boards (ESP32/Arduino/Raspberry Pi), USB cables, firmware files, IoT cloud platform (AWS IoT, ThingsBoard, Blynk, Azure IoT), dashboard software, routers, power adapters, multimeter, notepad, pens, PPE.

Note

This unit develops core commissioning and deployment skills. Trainees learn how to flash firmware, connect devices to the cloud, visualize live data, and troubleshoot real-world connectivity and configuration errors.

Say

Good Morning everyone!

Today's unit is where your device officially becomes part of the cloud. You will learn how to install firmware, configure cloud dashboards, and fix common problems that happen during real field installations.

Ask

Ask the participants:

- What happens if firmware is outdated?
- Has anyone faced issues where hardware was working but data never appeared on the dashboard?

Use these answers to introduce the importance of firmware–cloud synchronization.

Elaborate

In this session, we will discuss the following point:

- Firmware / Software Framework Installation for IoT Devices
- Cloud-Based IoT Platform Configuration
- Troubleshooting Cloud-Based IoT Platforms

Say

Now we will move into the hands-on cloud integration process, where you will flash firmware, link it to a cloud platform, and troubleshoot errors like a real IoT field technician.

Activity

- Duration: 30 minutes
- Resources: Microcontroller board, USB cable, laptop, firmware file, IDE.
- Steps:
 1. Connect the board to the laptop.
 2. Open IDE and select correct board and port.
 3. Load provided firmware code.
 4. Flash firmware to device.
 5. Open serial monitor and verify device boot status.

Do

- Check that every trainee successfully uploads firmware.
- Help with driver or COM port issues.
- Explain flashing errors and resets.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.10: Transferring Software Code to On-board Microprocessor & Compiling code to On Board Microprocessor

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Laptop, Arduino IDE / PlatformIO / ESP-IDF, USB programming cables, ESP32 / Arduino / Raspberry Pi Pico boards, sensors, actuators, serial monitor, Wi-Fi router, SIM module (optional), sample code files, multimeter, projector, whiteboard, PPE.

Note

This unit focuses on the core software skill required for IoT deployment—writing correct code, compiling without errors, uploading to hardware successfully, and debugging real-time field issues. A telecom IoT technician must be able to quickly identify and correct software faults during installation and commissioning.

Say

Good Morning everyone!

Today, you will learn how to take your IoT project from hardware to software reality. A perfectly connected device is useless if the software is incorrect.

Ask

Ask the participants:

- What happens if the wrong board is selected during code upload?
- Have you ever seen “Upload Failed” errors?

Use responses to transition into software–hardware compatibility and debugging discipline.

Elaborate

In this session, we will discuss the following point:

- Compiling and Uploading Code to Microcontrollers
- Best Practices for Writing IoT Microcontroller Code
- Debugging Techniques for IoT Microcontrollers

Say

Now you will practically compile, upload, and debug real IoT programs the way it is done during site commissioning and customer handover.

Activity

- Duration: 30 minutes
- Resources: Arduino/ESP32, Laptop, USB cable.
- Steps:
 - Open a sample Wi-Fi sensor code
 - Select correct board and port
 - Compile the code
 - Upload to microcontroller
 - Open serial monitor and confirm execution

Do

- Observe each trainee's board detection
- Fix COM port errors
- Reinforce safe USB handling

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.11: Understanding Error Codes and Debug Software

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Laptop, IoT emulator/simulator software (Proteus / Cisco Packet Tracer IoT / MATLAB IoT toolkit), serial monitor, Wireshark network analyzer, cloud IoT dashboard, microcontroller boards, sensors, router, internet connection, projector, whiteboard, markers, notepad, PPE.

Note

In this unit, trainees will learn how modern telecom and IoT systems are monitored, optimized, and maintained remotely using software tools. This is a critical skill required for Network Operations Centers (NOC), field troubleshooting, and preventive maintenance teams.

Say

Good Morning everyone!

Today, you will learn how professionals: Debug systems remotely, Monitor performance in real-time, and Predict failures before breakdown happens

Ask

Ask the participants:

- What happens if an IoT device fails at midnight in a remote location?
- Can we physically visit every site every time?

Use responses to transition into software–hardware compatibility and debugging discipline.

Elaborate

In this session, we will discuss the following point:

- Debugging Using Emulators and Network Testing Tools
- Remote Diagnostics & Monitoring Tools
- Predictive Maintenance Methodologies

Say

You will now practice how professionals analyze live IoT data, detect problems early, and prevent breakdowns before customers are affected.

Activity

- Duration: 30 minutes
- Resources: Laptop, emulator software, sample IoT code.
- Steps:
 - Load sample IoT configuration in emulator
 - Run sensor simulation
 - Observe output data
 - Introduce a fault in the code
 - Identify the error using simulation logs
 - Correct and re-run

Do

- Ensure all trainees operate the emulator
- Explain simulation vs real hardware differences
- Encourage logical troubleshooting instead of guessing

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.12: Functioning of Microcontroller and Attached Devices

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Microcontroller boards (Arduino, ESP32, Raspberry Pi), IoT nodes and gateways, sensors and actuators, Ethernet cables, Wi-Fi router, backend server or cloud dashboard, laptop, serial monitor, network testing tools (ping/traceroute), projector, whiteboard, markers, notepad, pens, PPE.

Note

This unit focuses on the final step of IoT deployment—ensuring that devices, software, and network connectivity are functioning as expected. This step is critical for commissioning, quality assurance, and customer satisfaction.

Say

Good Morning everyone!

Today, we will learn how to verify that all installed software and devices are working perfectly.

Ask

Ask the participants:

- How can we be sure that our IoT installation is working before leaving the site?
- What should be done if data is not appearing on the backend dashboard?

Use their responses to emphasize verification, troubleshooting, and escalation procedures.

Elaborate

In this session, we will discuss the following point:

- Setting Up Nodes and Gateways for Verification
- Confirming Data Reception at Backend Server
- Confirming Data Reception at Backend Server

Say

Now we will practice verifying software execution, checking data flow, and handling unresolved connectivity issues, exactly as done in professional field deployments.

Activity

- Duration: 30 minutes
- Resources: Nodes, gateways, sensors, actuators.
- Steps:
 - Power ON nodes and gateways.
 - Confirm correct network configuration.
 - Check LED indicators on devices.
 - Ensure communication between node and gateway.

Do

- Observe and correct incorrect network settings.
- Reinforce proper identification of nodes and gateways.
- Encourage trainees to note observations in logbook.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.13: Initializing Nodes and Gateways

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

IoT nodes, IoT gateways, sensors, actuators, microcontroller boards, laptop, USB cables, Ethernet cables, Wi-Fi router, SIM modules (if applicable), backend/cloud dashboard, serial monitor, network testing tools (ping, traceroute), projector, whiteboard, markers, notepad, pens, PPE.

Note

In this unit, trainees will learn how to perform the very first operational setup of IoT devices. This is a critical stage because incorrect initial configuration leads to repeated failures, no data flow, and poor network performance.

Say

Good Morning everyone!

Today, we are going to learn how to prepare IoT nodes and gateways for real operation. This is the moment where your hardware, software, and network finally come together. If the initial configuration is correct, everything becomes smooth. If it is wrong, nothing will work properly.

Ask

Ask the participants:

- What is the first thing you should configure when you power ON a new IoT device?
- Why do you think initial configuration is more important than later troubleshooting?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Initial Configuration of IoT Nodes
- Initial Configuration of IoT Gateways
- Validating Communication Flow During Initialization
- Common Initialization Failures and Corrections

Say

Now, you will practically configure real nodes and gateways, validate their communication, and confirm that your IoT system is fully operational from the very first moment.

Activity

- Duration: 30 minutes
- Resources: Nodes, laptop, USB cables, serial monitor.
- Steps:
 - Power ON each node.
 - Configure device ID and network settings.
 - Set sensor parameters.
 - Save configuration and reboot.
 - Verify output on serial monitor.

Do

- Check each trainee's configuration values.
- Correct duplicate IDs immediately.
- Reinforce clean and documented configuration steps.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.14: Launching the Software on Nodes and Gateways

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

IoT nodes, IoT gateways, microcontroller boards (ESP32/Arduino/Raspberry Pi), laptop, USB programming cables, Ethernet cables, Wi-Fi router, SIM cards (for cellular gateways), cloud/IoT platform dashboard, serial monitor, network testing tools (ping), power adapters, projector, whiteboard, markers, notepad, pens, PPE.

Note

This unit focuses on making IoT devices operational at the software level. Even if hardware connections are perfect, a device becomes fully functional only after correct software modules are configured, activated, registered, and joined to the network.

Say

Good Morning everyone!

Today, we take the next important step—activating the software brains of your IoT devices. This is where devices actually come alive, register on the network, and start communicating like real smart systems.

Ask

Ask the participants:

- What happens if an IoT device powers ON but does not join the network?
- Why do we need software modules in addition to hardware?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Configuring IoT Software Modules on Nodes
- Activating Software Modules on Gateways
- Ensuring Proper Boot-Up of IoT Devices
- Device Registration and Network Joining Process

Say

Now you will activate real IoT software modules, observe the boot-up process, and watch your devices successfully join the network just like in live telecom deployments.

Activity

- **Duration:** 30 minutes
- **Resources:** Nodes, laptop, USB cables.
- **Steps:**
 - Connect node to laptop.
 - Configure protocol and network settings.
 - Upload software.
 - Observe boot-up on serial monitor.
 - Confirm module activation messages.

Do

- Check configuration files of each trainee.
- Correct library conflicts and wrong board selections.
- Reinforce orderly and documented configuration practices.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.15: Confirming Communication & Establishing Connectivity

Unit Objectives



After the completion of this unit, the participant 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.

Resources to be Used



IoT nodes and gateways, microcontroller boards, sensors, laptop, Wi-Fi router, Ethernet cables, USB cables, internet connection, backend/cloud dashboard, network testing tools (Ping, Traceroute, iPerf, Wireshark), serial monitor, projector, whiteboard, markers, notepad, pens, PPE.

Note



This unit focuses on ensuring network reliability and data integrity before final deployment. Even if devices are installed and configured correctly, poor network performance can cause delays, data loss, and customer complaints. Therefore, testing latency, packet loss, interference, and backend data reception is mandatory before system handover.

Say



Good Morning everyone!

Today, we will verify something extremely important — how well your network is actually performing. A slow or unstable network can make even the best IoT system fail. So today, you will learn how to test the network like real telecom engineers and confirm that data is safely reaching the backend server.

Ask



Ask the participants:

- What happens if network latency becomes very high?
- Can we trust data if packets are getting lost during transmission?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Network Performance Parameters in IoT Systems
- Tools Used for Network Performance Testing
- Performing Network Performance Testing
- Detecting Interference Issues

Say

Now, you will test your network like a field engineer, analyze performance like a NOC technician, and confirm live data at the backend just like during real project commissioning.

Activity

- Duration: 30 minutes
- Resources: Laptop, gateway, internet, Ping, Traceroute.
- Steps:
 - Run Ping from laptop to gateway and server.
 - Measure latency values.
 - Observe packet loss percentage.
 - Run Traceroute to identify delay points.
 - Record observations.

Do

- Help trainees interpret latency values.
- Explain causes of abnormal packet loss.
- Reinforce structured test recording.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 2.16: Controlling Edge Appliances and Hubs

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

IoT nodes, gateways, edge appliances, sensors and actuators, laptop, backend/cloud dashboard, serial monitor, gateway logs, network monitoring tools (Ping, Wireshark), internet connection, projector, whiteboard, markers, notepad, pens, PPE.

Note

This unit focuses on real-time operational monitoring of the entire IoT communication chain—from field devices to the backend. It teaches trainees how to track live data movement, verify system responsiveness, and confirm healthy communication status using professional monitoring tools as done in NOC and enterprise IoT operations.

Say

Good Morning everyone!

Today, you will learn how to continuously monitor what is happening inside the network. A working system is not enough — a professional technician must be able to see data flowing, detect slow responses, and verify that every layer of the system is healthy in real time.

Ask

Ask the participants:

- How will you know if a device is sending data but the gateway is not forwarding it?
- What signs will tell you that the system is slow or unresponsive?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Monitoring Data Flow Across Nodes, Gateways, and Edge Appliances
- Verifying Seamless End-to-End Data Transfer and System Responsiveness
- Checking Communication Status Using Dashboards, Logs & Performance Indicators
- Common Monitoring Issues and Field Corrections

Say

Now, you will monitor live data flowing across real IoT layers, test full system responsiveness, and verify communication health just like NOC and enterprise monitoring engineers.

Activity

- Duration: 30 minutes
- Resources: Nodes, gateway, edge appliance, dashboard, serial monitor
- Steps:
 - Observe live sensor data at the node terminal.
 - Track same data on gateway logs.
 - Confirm arrival and processing on edge appliance.
 - Verify final display on backend dashboard.

Do

- Ensure every trainee traces one full data cycle.
- Correct gaps in data flow visibility.
- Reinforce systematic tracking from source to destination.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

Exercise

Answers to exercises for PHB

A. Short Answer Questions:

1. Gateways collect data from IoT nodes, process or filter it, and securely transmit it to backend servers or cloud platforms.
2. Short-range protocols offer high speed over small distances, while long-range protocols support low power communication over large distances.
3. It ensures proper device placement, reliable connectivity, and reduces communication failure.
4. By processing data locally, reducing latency, saving bandwidth, and enabling faster real-time responses.
5. Unauthorized access and data breaches; prevented through strong authentication, encryption, and regular firmware updates.

B. Multiple Choice Questions (MCQs):

1. b. Microcontroller
2. b. Long-range low-power communication
3. c. Remote diagnostics and monitoring
4. c. Information security management
5. c. Network testing tools

C. Fill in the Blanks:

1. Edge
2. Node
3. LoRaWAN
4. Latency and packet loss
5. Flashing

Notes



Notes



3. Configuring Equipment and Establishing Wireless Network Connectivity



- Unit 3.1 - Network Topologies
- Unit 3.2 - Establishing Connectivity
- Unit 3.3 - Establishing Connectivity
- Unit 3.4 - Configuration Testing
- Unit 3.5 - Comprehension and Interpretation of Technical Data
- Unit 3.6 - Executing Speed Test and Analyze



Key Learning Outcomes

After the completion of this module, the participant 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

After the completion of this unit, the participant 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.

Resources to be Used

Broadband CPE router, Wi-Fi access point, Ethernet cables, laptop, PoE switch, mobile phones, smart speaker device (Alexa/Google Home), firewall-enabled router, VPN software, network testing tools, projector, whiteboard, markers, notepad, pens, PPE.

Note

This unit focuses on real-world broadband deployment and security operations, covering everything from CPE configuration and advanced Wi-Fi security to VPN, IPv6, smart home integration, cybersecurity protection, and escalation handling in major network failures.

Say

Today you will learn how broadband networks actually work in homes, offices, and enterprises. You will configure CPE devices, secure Wi-Fi networks, understand VPN and ILL links, integrate smart home systems, and apply cybersecurity protection. You will also learn how professionals escalate critical failures using structured emergency procedures.

Ask

Ask the participants:

- What happens if the home Wi-Fi is hacked?
- How do enterprises securely connect remote users? Who handles the issue if the entire broadband network goes down?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Wired and Wireless CPE Configurations (VLAN, NAT, QoS)
- VPN and Internet Leased Line (ILL)
- IPv6 Addressing, Subnetting, NAT & QoS in Broadband
- Connectivity Options & Advanced Wi-Fi Security and Smart Home Integration with Broadband Networks

Say

Now, you will configure CPE devices, secure networks, integrate smart systems, and understand how network professionals respond to critical emergencies and large-scale failures.

Activity

- Duration: 30 minutes
- Resources: CPE router, laptop, Ethernet cables
- Steps:
 - Log into CPE admin paneal
 - Configure VLAN
 - Enable NAT
 - Set QoS for video and voice traffic
 - Test internet performance

Do

- Ensure every trainee understands CPE admin panel
- Ask them to show how to configure VLAN.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 3.2: Establishing Connectivity

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Laptop, broadband router/CPE device, Ethernet cables, Wi-Fi-enabled mobile phone, internet connection, command prompt/terminal access, speed test tools, projector, whiteboard, markers, notepad, pens.

Note

This unit focuses on hands-on network troubleshooting and configuration, enabling trainees to test real-time connectivity using ping, speed tests, packet loss analysis, and to configure secure LAN and Wi-Fi networks in residential and enterprise environments.

Say

Today, you will learn how to test internet connectivity from the customer side, identify delays and packet loss, and configure secure LAN and Wi-Fi networks. These skills are essential for field technicians, network support engineers, and broadband installation teams.

Ask

Ask the participants:

- What does it mean if a website loads slowly but does not disconnect?
- How can we check whether the fault is at customer side or service provider side?
- What happens if Wi-Fi is not properly secured?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Pinging the Service Provider Gateway & Response Time Analysis
- Analyzing Connectivity Test Results
- LAN and Wi-Fi Configuration (SSID & Security Settings)

Say

Now, you will perform real-time ping testing, network performance analysis, and Wi-Fi/LAN configuration as done by professional broadband technicians.

Activity

- Duration: 30 minutes
- Resources: Laptop, router, internet connection
- Steps:
 1. Identify the gateway IP address
 2. Run ping command
 3. Record:
 - Minimum time
 - Maximum time
 - Average time
 4. Identify if packet loss exists

Do

- Ask one trainee to operate the router
- Another to perform ping and speed test
- Another trainee records results on the board

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 3.3: Connectivity of CPE and End User Devices

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Broadband CPE/router, laptop/PC, smart TV/IP TV, smartphones, IoT devices (smart bulb/switch/camera), Ethernet cables, fiber patch cord, power adapters, Wi-Fi router, VPN configuration file/credentials, projector, whiteboard, markers, notepad, pens, internet connection.

Note

This unit focuses on end-to-end customer-side broadband activation, from physical cable checking to CPE configuration, secure Wi-Fi setup, advanced VPN/ILL provisioning, and smart home integration. These are the final delivery steps that decide customer satisfaction.

Say

Today, you will learn how to connect customer devices, configure the CPE, secure the network, and even integrate smart home systems. After this unit, you will be able to confidently hand over a fully functional and secure broadband connection to any customer.

Ask

Ask the participants:

- What happens if a cable is loosely connected at the customer site?
- Why is basic cybersecurity necessary even for home users?
- Has anyone used Alexa, Google Home, or smart lights at home?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Verifying Cables, Connectors & Physical Connectivity
- Connecting Customer Devices to the CPE
- Base CPE Configuration (IP, Gateway, Mask, NAT, QoS & IPv6)
- VPN & Internet Lease Line (ILL) Setup
- Applying Basic Cybersecurity Settings

Say

Now you will perform the complete customer handover setup, just like in real broadband field installations — from cables to cybersecurity to smart home integration.

Activity

- Duration: 30 minutes
- Resources: CPE, PC, TV, mobile phone, LAN cables
- Steps:
 1. Check all power and LAN cables
 2. Connect PC via LAN
 3. Connect mobile via Wi-Fi
 4. Connect Smart TV to internet
 5. Verify internet access on all devices

Do

- Ask one trainee to demonstrate full CPE configuration on the projector.
- Ask another trainee to connect a smart TV and show live streaming.
- Ask another trainee to control a smart bulb using voice command.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 3.4: Configuration Testing

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Broadband CPE/router, laptop/PC, smartphone, Ethernet cables, internet connection, command prompt/terminal access, speed test tools, VPN/ILL sample configuration, projector, whiteboard, markers, notepad, technical documentation formats, pens.

Note

This unit focuses on three critical field competencies—live network testing and performance analysis, traffic prioritization using QoS, and professional technical documentation for future troubleshooting and audits—all of which are mandatory for effective NOC coordination and maintaining ISP service quality standards.

Say

In today's session, you will learn how to test real network health, optimize performance for important applications using QoS, and document every configuration properly. Remember — a good technician not only fixes issues but also leaves behind clear records for future troubleshooting.

Ask

Ask the participants:

- Why do we test ping even when internet is working?
- What happens if gaming traffic gets the same priority as video calls?
- Why is documentation important after a site visit?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Pinging the Service Provider Gateway & Response Analysis
- Analyzing Connectivity Test Results (Latency, Throughput & Packet Loss)
- Pinging the CPE from End-User Device & Stability Optimization
- Enabling Quality of Service (QoS) for Traffic Prioritization
- Documenting End-User Device Configurations

Say

Now you will perform real troubleshooting tests, enable QoS priorities, and create professional technical documentation just like certified broadband engineers.

Activity

- Duration: 30 minutes
- Resources: CPE, PC, TV, mobile phone, LAN cables
- Steps:
 - Ping ISP gateway
 - Ping local CPE
 - Record: Latency and Packet loss
 - Identify performance category

Do

- Ask one trainee to demonstrate how to ping ISP gateway.
- Ask another trainee to ping local CPE.
- Ask another trainee to identify performance category.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 3.5: Comprehension and Interpretation of Technical Data

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Router, modem, IoT gateway, mobile phone, laptop, customer dashboard app, firmware update files, internet connection, projector, whiteboard, markers, notepad, pens, cybersecurity awareness posters, PPE.

Note

Today, you will learn how to guide customers to handle small issues themselves, stay safe from cyber threats, and keep their devices updated for better performance.

Say

Today, you will learn how to connect customer devices, configure the CPE, secure the network, and even integrate smart home systems. After this unit, you will be able to confidently hand over a fully functional and secure broadband connection to any customer.

Ask

Ask the participants:

- What do customers usually do when the internet suddenly stops working?
- Do customers update their router or IoT device firmware regularly?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Basic Troubleshooting Steps for Customers (Self-Help Techniques)
- Cybersecurity Best Practices for Customers
- Cybersecurity Best Practices for Customers
- Firmware Updates for Security and Performance

Say

Now, you will practice how to explain Cybersecurity Awareness Demonstration

Activity

- Duration: 30 minutes
- Resources: Posters, slides, mobile phone
- Steps:
 - Show common cyber attack examples.
 - Ask trainees to explain security precautions in simple words.
 - Demonstrate password change on router app.
 - Show how to log out from admin dashboard.

Do

- Ensure trainees use non-technical language.
- Reinforce “Never share passwords or OTPs”.
- Highlight real-life cyber fraud examples.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 3.6: Executing Speed Test and Analyze

Unit Objectives

After the completion of this unit, the participant will be able to:

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

Resources to be Used

Laptop, smartphone, broadband modem/ONT, Wi-Fi router, Ethernet cables, internet connection, speed test applications/websites (Ookla, Fast.com), notepad, pens, projector, whiteboard, markers, customer plan chart (mock), PPE.

Note

This unit focuses on validating real customer experience by checking whether the actual internet speed matches the subscribed broadband plan. Speed testing is a final acceptance step during installation, troubleshooting, and customer handover.

Say

In this session, you will learn how to test internet speed professionally, interpret results correctly, and prove network performance as per the customer's subscribed plan.

Ask

Ask the participants:

- Have you ever faced slow internet even after taking a high-speed plan?
- Is download speed the only factor that defines good internet performance?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Understanding Broadband Speed Parameters
- What Is Throughput?
- Tools Used for Network Speed Testing
- Interpreting Test Results against Subscribed Plan
- Customer Demonstration & Documentation

Say

Now you will perform live speed tests, record throughput data, and verify whether the broadband service truly matches the customer's subscribed plan — just like during real installation and troubleshooting jobs.

Activity

- Duration: 30 minutes
- Resources: Smartphone, laptop, Wi-Fi router, internet
- Steps:
 - Connect smartphone to Wi-Fi.
 - Run Speedtest app.
 - Note: Download, Upload, and Ping
 - Repeat test using laptop.
 - Compare mobile vs laptop results.

Do

- Help trainees understand result differences across devices.
- Highlight impact of Wi-Fi strength on speed.
- Ensure every trainee records results properly.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

Exercise

Answers to exercises for PHB

A. Short Answer Questions:

1. Access via browser using the CPE IP address (e.g., 192.168.1.1) or through command-line via SSH/Telnet; updating default credentials prevents unauthorized access and security breaches.
2. VLAN separates network traffic into virtual segments, while NAT translates private IPs to public IPs, helping manage traffic and enhance security.
3. IPv6 provides a larger IP address space, improves routing efficiency, and ensures future network scalability.
4. QoS prioritizes important traffic such as video calls and gaming, reducing lag and buffering for better user experience.
5. Level 1: Check cables, power, IP settings, and reboot devices. Level 2: Use ping/tracert, check CPE configuration, signal levels, and backend logs.

B. Multiple Choice Questions (MCQs):

1. b) Enabling MAC filtering and firewalls
2. b) Provide secure communication over the internet
3. b) ping
4. c) Compatibility and secure network access settings
5. b) Variations in packet delay affecting real-time applications

C. Fill in the Blanks:

1. Ping
2. Password
3. VLAN
4. Jitter
5. Network settings / Wi-Fi configuration

- Notes

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.





4. Troubleshoot and Rectify Faults

Unit 4.1 - Escalation Matrix

Unit 4.2 - Problem Solving

Unit 4.3 - Identifying and Repairing Faulty Cables and Connectors

Unit 4.4 - Electro Magnetic Interference (EMI) and Electro Magnetic Compatibility (EMC)

Unit 4.5 - Crimping and Soldering

Unit 4.6 - Troubleshooting of Cable and Connector

Unit 4.7 - Troubleshooting of CPE (Modem, Router, Switch)

Unit 4.8 - Troubleshooting of Configuration and Connectivity CPE faults

Unit 4.9 - Troubleshooting and Repairing of Client's Broadband Service

Key Learning Outcomes



After the completion of this module, the participant will be able to:

1. Explain about workplace health and safety
2. understand different types of health hazards
3. Demonstrate various first-aid techniques
4. Understand the importance of safety at workplace
5. understand basic hygiene practices and hand washing techniques
6. Explain the need for Social Distancing
7. Understand the hazard reporting methods at workplace
8. Explain e-waste and process of disposing them
9. Explain the greening of jobs

UNIT 4.1: Escalation Matrix

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Laptop, sample trouble ticket formats, escalation matrix chart, call flow scripts, mobile phone (for role play), projector, whiteboard, markers, flipchart, notepad, pens.

Note

In this unit, trainees will learn how to professionally handle broadband faults that cannot be resolved at the first level, how to document every technical action, and how to communicate clearly and confidently with customers during remote troubleshooting. These skills are essential for customer satisfaction, SLA compliance, and smooth NOC coordination.

Say

In this session, you will learn when and how to escalate an issue, why proper documentation protects both the technician and the company, and how to communicate calmly and professionally with customers during remote support.

Ask

Ask the participants:

- What happens if a customer issue is not resolved for many hours?
- Have you ever spoken to a frustrated customer on a phone call?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Escalation Procedures for Unresolved Broadband Issues
- Importance of Documentation in Broadband Troubleshooting
- Best Practices for Customer Communication
- Remote Troubleshooting Assistance Flow

Say

Now, you will practice how real technicians escalate faults, document work properly, and communicate professionally with customers during live troubleshooting.

Activity

- Duration: 30 minutes
- Resources: Fault scenarios, escalation matrix
- Steps:
 - Trainer gives a fault scenario
 - Trainees decide: Can it be resolved at field level? Or should it be escalated?
 - Identify correct escalation level
 - Justify their decision

Do

- Correct wrong escalation decisions
- Reinforce SLA-based thinking
- Highlight consequences of delay

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 4.2: Problem Solving

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Laptop, broadband modem/router, fiber/DSL test setup, mobile hotspot, LAN cables, speed test websites/apps, command prompt/terminal, ping & tracert tools, Wireshark (optional), projector, whiteboard, flipchart, markers, notepad, pens, PPE.

Note

In this unit, trainees will learn how to identify real broadband faults, understand their technical causes, and apply both traditional and AI-based modern troubleshooting tools. This unit prepares trainees for field-level fault rectification and NOC-level diagnostics.

Say

In this session, you will learn why broadband services fail, how to accurately identify the exact fault, and how modern AI tools can detect problems even before customers experience them.

Ask

Ask the participants:

- What does a customer usually say when the internet stops working?
- Have you ever experienced slow internet even when the network shows “connected”?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Common Broadband Network Faults and Their Root Causes
- Causes of Broadband Service Disruptions
- Network Troubleshooting Techniques
- AI-Based Predictive Maintenance & Remote Diagnostics

Say

Now, you will practically identify different broadband faults, test real network performance, and observe how modern tools help engineers detect problems even before failures happen.

Activity

- Duration: 30 minutes
- Resources: Modem, router, LAN cables, simulated faults
- Steps:
 - Trainer simulates one fault (no service / slow speed / disconnection).
 - Trainees observe indicators.
 - Identify fault type and possible root cause.
 - Present findings to the class.

Do

- Encourage logical fault identification.
- Correct wrong assumptions with real field explanations.
- Link symptoms to root causes.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 4.3: Identifying and Repairing Faulty Cables and Connectors

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, damaged and good-condition cables, connectors, crimping tool, stripper, cutter, splitter, signal meter, multimeter, PPE (gloves), router, laptop, whiteboard, flipchart, markers, projector.

Note

In this unit, trainees will learn practical techniques for identifying and correcting physical layer faults in a broadband network.

Say

In today's session, we will focus on one of the most important skills for a Broadband Technician—identifying physical faults in cables and connectors and fixing signal-related issues that directly affect customer connectivity.

Ask

Ask the participants:

- What are the common reasons for cable damage at customer premises?
- What happens if a connector is loosely fixed?
- Has anyone seen signal fluctuation issues during internet usage?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Types of connectors used in broadband networks
- Signs of faulty connectors and damaged cables
- Step-by-step method of safe cable replacement
- Use of signal meters and multimeters
- Final testing after rectification

Say

Let us now perform a hands-on activity to practice these real field operations.

Activity

- Duration: 40 minutes
- Resources: Faulty cables, connectors, splitter, signal meter, crimping tools, PPE, router, laptop.
- Steps:
 1. Divide the class into small groups.
 2. Provide each group with one damaged cable and one faulty connector.
 3. Ask them to:
 - Identify the fault
 - Replace the damaged section
 - Re-terminate the connector properly
 4. Then, allow them to:
 - Take signal readings at the splitter
 - Measure readings again at the terminated ends
 5. Introduce an artificial interference source and ask them to locate and rectify it.

Do

- Observe each group and guide them during connector replacement.
- Correct improper tool handling immediately for safety.
- Encourage every trainee to take at least one signal reading.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

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

Unit Objectives

After the completion of this unit, the participant will be able to:

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

Resources to be Used

Participant handbook, pen, pencil, notepad, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, sample cables (coaxial, optical fiber, Ethernet), router, splitter, signal meter.

Note

In this unit, we will discuss the fundamentals of broadband communication and how signals travel through different transmission media. We will also understand why signal quality degrades and what factors affect network performance.

Say

In today's session, we will understand how broadband signals actually travel from the service provider to the customer's device. Once you clearly understand this concept, it becomes much easier to identify faults and maintain strong network performance in the field.

Ask

Ask the participants:

- What do you understand by the term "signal"?
- Which types of cables have you seen being used for internet connections?
- Why do you think internet speed sometimes slows down?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Meaning of broadband communication system
- Components of a broadband network
- Types of transmission media
- Basics of signal transmission
- Effects of signal degradation on network performance

Say

Let us now participate in a simple demonstration activity to understand signal strength and loss in a practical way.

Activity

- Duration: 30 minutes
- Resources: Router, splitter, signal meter, sample cables of different lengths, laptop, projector.
- Steps:
 - Connect a short cable between the router and signal meter and note the signal strength.
 - Replace it with a longer cable and again note the reading.
 - Introduce a splitter in between and observe the change in signal strength.
 - Slightly loosen a connector and observe the effect on signal quality.
 - Discuss the results with the trainees.

Do

- Encourage trainees to take readings one by one.
- Note down all readings on the whiteboard.
- Guide students to compare strong and weak signal readings.
- Explain how distance, poor connections, and splitters affect performance.
- Ask one trainee to summarize what they observed during the demonstration.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 4.5: Crimping and Soldering

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, damaged and fresh cables (Ethernet/coaxial), RJ-45 connectors, coaxial connectors, crimping tool, wire stripper, cutter, soldering iron, solder wire, flux, insulation tape, heat-shrink sleeves, multimeter, PPE (gloves, safety glasses), whiteboard, flipchart, markers, laptop, projector.

Note

In this unit, we will focus on one of the most essential practical skills for a Broadband Technician—proper re-connectorization, crimping, and soldering to ensure strong and reliable network connectivity.

Say

In this session, you will learn how to fix one of the most common field-level problems—faulty connectors and broken cable ends. A small mistake in crimping or soldering can completely disrupt broadband service, so today's hands-on practice is extremely important for your real-world work.

Ask

Ask the participants:

- What problems can occur if a connector is not crimped properly?
- Have you ever seen a loose or broken cable connector at home or in the field?
- Why do you think soldering is sometimes preferred over twisting wires?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Meaning of re-connectorization and when it is required
- Types of connectors used in broadband networks
- Step-by-step re-connectorization process
- Basics of soldering and its application in telecom
- Testing connectivity using a multimeter or LAN tester

Say

Let us now move on to a hands-on activity where you will perform re-connectorization, crimping, and soldering by yourself.

Activity

- Duration: 30 minutes
- Resources: Ethernet/coaxial cables, connectors, crimping tool, soldering iron, solder wire, flux, insulation tape, multimeter, PPE.
- Steps:
 1. Divide the class into small groups.
 2. Provide each group with a damaged cable end and a set of tools.
 3. Ask them to:
 - Cut the damaged portion and strip the insulation neatly
 - Arrange the cable pairs using proper color coding
 - Insert the pairs into the connector
 - Perform proper crimping
 4. Next, demonstrate where soldering is required and ask trainees to: i. Heat the soldering iron safely, ii. Apply flux and solder the joint, and iii. Insulate the joint properly
 5. Finally, test the connectivity using a multimeter or LAN tester.

Do

- Encourage trainees to take readings one by one.
- Note down all readings on the whiteboard.
- Guide students to compare strong and weak signal readings.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 4.6: Troubleshooting of Cable and Connector

Unit Objectives

After the completion of this unit, the participant 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).

Resources to be Used

Participant handbook, signal level meter, OTDR machine (demo unit), router, modem, laptop, Ethernet cables, software tools for CPE log analysis, internet connection, whiteboard, flipchart, markers, projector, PPE.

Note

In this unit, trainees will learn how to measure signal quality, analyze device logs, and use advanced network diagnostic tools to accurately identify broadband faults.

Say

In today's session, you will learn how to move beyond visible physical faults and detect hidden broadband issues using professional diagnostic tools. These skills will help you quickly identify the real root cause of network problems in the field.

Ask

Ask the participants:

- Have you ever faced slow internet even when all cables were properly connected?
- How do you usually check if the internet connection is alive?
- Have you heard about tools like ping or traceroute before?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Meaning of signal loss, attenuation, and interference
- Role of signal level meters in broadband testing
- What are CPE logs and why they are important
- Types of fault messages found in modem/router logs
- Using software tools to access and analyze CPE logs

Say

Let us now move into a practical activity where you will test signal quality and diagnose network faults using real diagnostic tools.

Activity

- Duration: 45 minutes
- Resources: Signal meter, OTDR (demo), router, modem, laptop, Ethernet cables, diagnostic software, internet connection.
- Steps:
 1. Divide the class into small groups.
 2. Provide each group with a router, modem, and testing instruments.
 3. Ask them to:
 - Measure signal levels using a signal meter
 - Identify if signal levels indicate loss or interference
 - Access CPE logs through the software tool
 - Identify warning and error messages
 - Perform ping tests & use trace route for path analysis
 - Observe OTDR results (demonstration if equipment is limited)
 4. Discuss the fault conclusions drawn by each group.

Do

- Help trainees understand actual meaning of log error messages.
- Encourage each trainee to run at least one diagnostic test.
- Ask each group to explain the fault detected and the reasoning behind it.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

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

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, signal level meter (SLM), OTDR (demo unit), router, modem, laptop, Ethernet cables, internet connection, CPE diagnostic software, AI-based troubleshooting software/dashboard (demo), whiteboard, flipchart, markers, projector, PPE.

Note

In this unit, we will focus on advanced diagnostic tools, CPE software access, firmware management, and AI-based remote troubleshooting techniques used in modern broadband networks.

Say

In today's session, we are moving one step ahead into advanced diagnostics. You will learn how technicians use professional tools and smart AI-based systems to detect problems, correct CPE issues, and even support customers remotely without visiting the site.

Ask

Ask the participants:

- Have you ever reset your Wi-Fi router at home? Did it solve the problem?
 - What do you think firmware means in a router or modem?
 - Do you think it is possible to fix internet problems without visiting the customer's home?
- Write their responses on the whiteboard.

Elaborate



In this session, we will discuss the following point:

- Overview of modern broadband diagnostic tools
- Working principle of Signal Level Meters (SLMs)
- Role of OTDR in fiber fault detection
- Understanding fiber breaks, reflection, and attenuation using OTDR
- Reconfiguration of CPE settings after reset

Say



Let us now move into a practical activity where you will use CPE software, perform firmware actions, and experience AI-based remote troubleshooting.

Activity



- Duration: 45 minutes
- Resources: Router, modem, laptop, internet connection, CPE software interface, AI diagnostic dashboard, Ethernet cables.
- Steps:
 1. Divide the class into small groups.
 2. Provide each group with a router/modem and a laptop.
 3. Ask them to:
 - Access the CPE software using browser or application
 - View device status and logs
 - Reconfigure Wi-Fi and network settings
 - Demonstrate how an AI tool detects abnormal patterns and how faults are suggested automatically
 4. Ask trainees to simulate a remote customer support case using AI tools.

Do



- Explain every firmware step clearly to avoid confusion.
- Encourage each trainee to perform at least one CPE operation.
- Ask one trainee from each group to describe how AI helped in detecting or resolving a fault.

Notes for Facilitation



- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

UNIT 4.8: Troubleshooting of Configuration and Connectivity CPE faults

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, router, modem, laptop, Ethernet cables, internet connection, CPE access credentials (demo), speed test tools, ping and traceroute utilities, whiteboard, flipchart, markers, projector.

Note

In this unit, trainees will learn how to properly configure CPE devices, secure the network, analyze internet performance, and manage traffic using QoS for better user experience.

Say

In today's session, we will focus on how to correctly configure customer devices, secure the home network, test real internet performance, and manage network traffic efficiently. These skills directly impact customer satisfaction and service quality.

Ask

Ask the participants:

- Have you ever changed your Wi-Fi name or password at home?
- Why do you think some users experience buffering while others work smoothly on the same network?
- What do you understand by network security?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Importance of changing default usernames and passwords
- Secure firmware update practices
- Backup and restore of CPE configurations
- Network security basics
- Introduction to Quality of Service (QoS)

Say

Let us now move into a practical activity where you will configure a router, test connectivity, and apply QoS settings.

Activity

- Duration: 45 minutes
- Resources: Router, modem, laptop, Ethernet cables, internet connection, speed test tools, CPE interface.
- Steps:
 1. Divide the class into small groups.
 2. Provide each group with one router and a laptop.
 3. Ask them to:
 - Access the CPE interface
 - Change the default Wi-Fi SSID and password
 - Configure LAN and Wi-Fi security
 - Guide them to: Perform speed test, Run a ping test, Observe latency and packet loss
 - Ask them to: Enable QoS, Assign high priority to a video call application, and assign low priority to downloads
 4. Compare internet performance before and after applying QoS.

Do

- Ensure that security settings are applied correctly.
- Guide trainees in correctly interpreting test results.
- Encourage every trainee to perform at least one configuration step.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

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

Unit Objectives

After the completion of this unit, the participant 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.

Resources to be Used

Participant handbook, router, modem, laptop, Ethernet cables, internet connection, speed test websites/apps, ping utility, sample fault scenarios, system database/demo CRM software, whiteboard, flipchart, markers, projector.

Note

In this unit, we will focus on identifying common broadband service faults, testing actual internet performance, and correctly documenting all troubleshooting activities in the system.

Say

In today's session, you will learn how to clearly identify different types of broadband faults, check real internet speed, and most importantly, record your work properly in the system. Good documentation is just as important as good troubleshooting in a technician's job.

Ask

Ask the participants:

- Have you ever faced a situation where the internet was completely down?
- Have you experienced slow internet even though the connection was active?
- Why do you think documentation is important after fixing a customer issue?

Write their responses on the whiteboard.

Elaborate

In this session, we will discuss the following point:

- Types of broadband service faults
- Common causes of each fault condition
- Visual and technical checks for fault identification
- Indicators on modem/router LEDs and their meanings
- Introduction to broadband speed testing

Say

Let us now move into a practical activity where you will configure a router, test connectivity, and apply QoS settings.

Activity

- Duration: 45 minutes
- Resources: Router, modem, laptop, internet connection, speed test tool, sample fault cases, system database/demo CRM.
- Steps:
 1. Divide the class into small groups.
 2. Provide each group with a simulated fault scenario, such as: No internet connection, Slow speed, and Frequent disconnections.
 3. Ask them to:
 - Observe modem/router indicators
 - Identify the fault type
 - Perform a broadband speed test
 - Compare the result with the assigned plan speed
 - Interpret whether the results are acceptable or faulty
 - Enter the fault details, test results, and resolution steps into the system database or demo CRM.

Do

- Assist trainees in interpreting speed test values accurately.
- Ensure each trainee gets a chance to enter details into the system.
- Ask one trainee from each group to explain the fault handled and how it was documented.

Notes for Facilitation

- Encourage active participation from all trainees.
- Promote peer learning and group discussions.
- Clarify doubts immediately to ensure concept clarity.
- Relate topics to real-field and industry scenarios.
- Ensure safety practices are followed during practical sessions.

Exercise

Answers to exercises for PHB

A. Short Answer Questions:

1. OTDR identifies the exact location of fiber faults and losses, while Signal Level Meters measure the strength and quality of broadband signals.
2. Loose or damaged cables, interference, poor line quality, faulty CPE, and network congestion.
3. They analyze network data to predict failures, detect anomalies early, and enable proactive maintenance.
4. Log in to the CPE interface, back up settings, upload the latest firmware, perform the update, and reboot the device.
5. It ensures accountability, helps in future fault analysis, supports audits, and improves maintenance efficiency.

B. Multiple Choice Questions (MCQs):

1. d) All of the above
2. b) Identify the path taken by packets and locate network delays
3. b) OTDR
4. b) CPE configuration and connectivity
5. c) Predict potential faults and assist remote troubleshooting

C. Fill in the Blanks:

1. Intermittent fault
2. OTDR
3. Speed / Performance
4. Crimping / Termination
5. Accountability

- Notes

This image shows a single sheet of white paper with horizontal ruling lines. The lines are evenly spaced and run across the width of the page. There are no margins, text, or other markings on the paper.



TEL/N9105

Key Learning Outcomes



After the completion of this module, the participant 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 5.1: Environmental Sustainability and Waste Management in the Telecommunications Industry

Unit Objectives

After the completion of this unit, 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.

Resources to be Used

Participant handbook, pen, pencil, notepad, whiteboard, flipchart, markers, laptop, overhead projector, laser pointer, sample e-waste bins, labels, PPE (gloves, masks), and demonstration components.

Notes For Facilitation

In this unit, we will discuss environmental sustainability practices and waste management procedures followed in the telecom sector.

Say

Good Morning everyone, and welcome back!

In this session, we will explore how the telecom industry is adopting sustainable practices and managing waste responsibly. As future broadband technicians, your role in keeping our environment clean and safe is extremely important.

Ask

Ask the participants the following questions:

- Why do you think sustainability is important in the telecom sector?
- Have you ever seen or handled e-waste before?

What challenges did you notice? Write down the trainees' answers on the whiteboard or flipchart.

Use their responses as a starting point to explain today's lesson.

Elaborate

In this session, we will discuss the following points:

- Environmental Sustainability in Telecom Industry
- Environmental Laws and Regulations in Telecommunications.
- E-Waste in the Telecom Industry
- E-Waste Management Process in the Telecom Industry
- Occupational Safety in Environmental Practices for Telecom E-Waste Management
- Energy Optimization in Telecom Operations
- Reducing the Carbon Footprint in Telecom
- Documentation and Compliance Tracking in Telecom Environmental Management

Say

Let us now participate in an activity to explore these topics more deeply.

Activity



Duration: 30 minutes

Resources: Sample components (cables, adapters, packaging materials), e-waste bins, labels, gloves, markers, projector, laptop, whiteboard.

Steps:

1. Divide the class into small groups.
2. Give each group a mix of telecom-related items (e.g., cable scraps, old router parts, batteries, plastic packaging).
3. Ask them to sort the items into:
 - Recyclable
 - Refurbishable
 - Hazardous waste
 - General waste
4. Display a checklist on the projector for guidance.
5. After all groups finish, reveal the correct sorting categories and explain the reasoning behind each decision.

Do



- Ask a student to maintain scores or observations on the whiteboard.
- Write down important points shared by trainees.
- Add your own insights based on industry best practices.
- Encourage every student to engage in discussions and participate in sorting activities.
- Ask one participant to summarize the key learnings of the session.
- Maintain positive energy and show enthusiasm for sustainability practices.

Activity



Duration: 25 minutes

Resources: Laptop, projector, sample telecom equipment (router/ONT), power meter (if available), pictures/videos of solar-powered telecom sites, whiteboard, markers.

Steps:

1. Divide the class into small groups.
2. Play a short video or show images demonstrating energy-efficient telecom practices such as:
3. Use of solar panels
 - Smart cooling techniques
 - Low-power CPE devices
 - Optimized equipment placement to reduce heat load Provide each group with a scenario—for example: “A broadband installation site has high energy consumption due to poor equipment placement. Suggest three improvements.”
 - Ask the groups to discuss and write down their solutions.
4. Invite one member from each group to present their recommendations.
5. Summarize the key practical techniques used in the industry to save energy.

Do

- Ask a trainee to note down the key energy-saving suggestions shared by each group on the whiteboard.
- Highlight the practical feasibility of each idea and relate them to real telecom installation scenarios.
- Add your own insights—especially where small changes (like repositioning equipment or using smart adapters) can lead to big energy savings.
- Encourage quieter students to share their thoughts or add to the discussion.
- Ask one participant to briefly recap the energy-efficiency techniques discussed in the activity.
- Reinforce the importance of using energy-efficient tools and practicing mindful consumption during field installations.

Notes for Facilitation

- Ask trainees if they have any questions or doubts regarding waste handling or environmental laws.
- Encourage peer learning by inviting other trainees to answer queries.
- Remind participants to read the related section in their participant manual.
- Reinforce the importance of safe handling, labeling, and correct segregation while working on telecom sites.

Exercise



Answers to exercises for PHB

Multiple-Choice Questions (MCQs)

- b) To avoid damage to the cable core c) Duct laying method
- b) Cable winch machine
- b) To avoid excessive friction and damage
- b) Using approved cable ties or clamps

Descriptive Questions

1. Step-by-step procedure for direct burial cable laying

- Conduct a site survey and mark the cable route.
- Excavate the trench to the required depth.
- Lay a layer of sand or soft soil at the base.
- Place the cable carefully without exceeding bend radius.
- Cover the cable with sand and protective tiles/warning tape.
- Backfill the trench and compact the soil.
- Test cable continuity and performance after installation.

2. Safety precautions during underground cable laying

- Ensure all underground utilities (water, gas, electricity) are identified before digging.
- Use PPE: gloves, safety shoes, helmets, eye protection.
- Maintain safe distance from live electrical cables.
- Use proper tools for excavation and lifting.
- Avoid working in wet or unstable soil conditions.
- Ensure trench shoring to prevent collapse.

3. Difference between aerial and underground cable laying

- Cost: Aerial is cheaper; underground is more expensive due to excavation and protection materials.
- Durability: Underground cables are safer from weather and vandalism; aerial cables are more exposed.
- Maintenance: Aerial cables are easy to access and repair; underground maintenance is difficult, costly, and time-consuming.

4. Role and importance of cable jointing and termination

- Ensures continuity and reliable signal/power transfer.
- Provides mechanical and environmental protection at connection points.
- Reduces losses, electrical faults, and downtime.
- Maintains safety by insulating and securing conductors properly.

5. Common challenges in urban cable laying & solutions

- Limited space: Use micro-trenching and duct methods.
- Traffic congestion: Work during off-peak hours and use proper barricading.
- Utility congestion: Conduct detailed utility mapping and use cable locators.
- Permission and coordination issues: Work closely with local authorities and utility providers.
- Obstructions like buildings, pipelines: Use directional drilling or rerouting techniques.

Notes



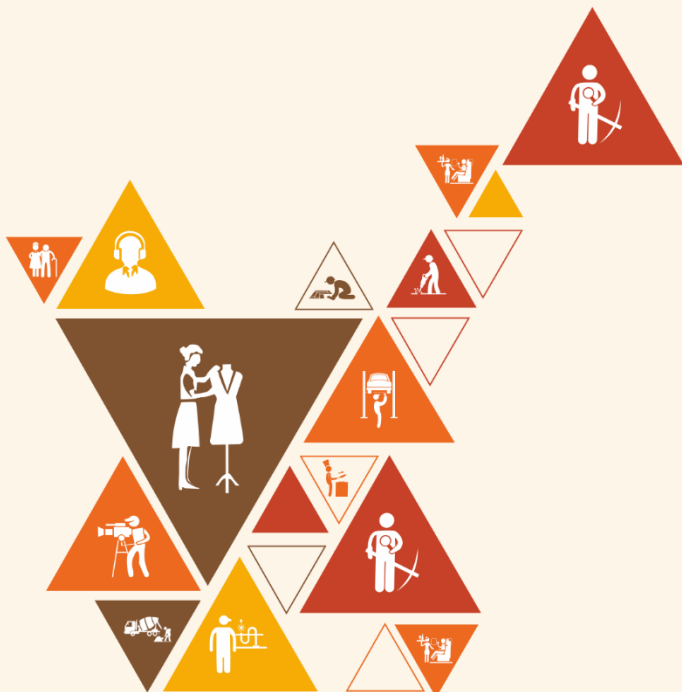
This image shows a full page of white paper with horizontal blue or grey ruling lines. The lines are evenly spaced and run across the width of the page. In the top left corner, there is a small orange icon consisting of three horizontal bars, resembling a simplified staircase or a set of steps. The rest of the page is empty, with no text or other markings.





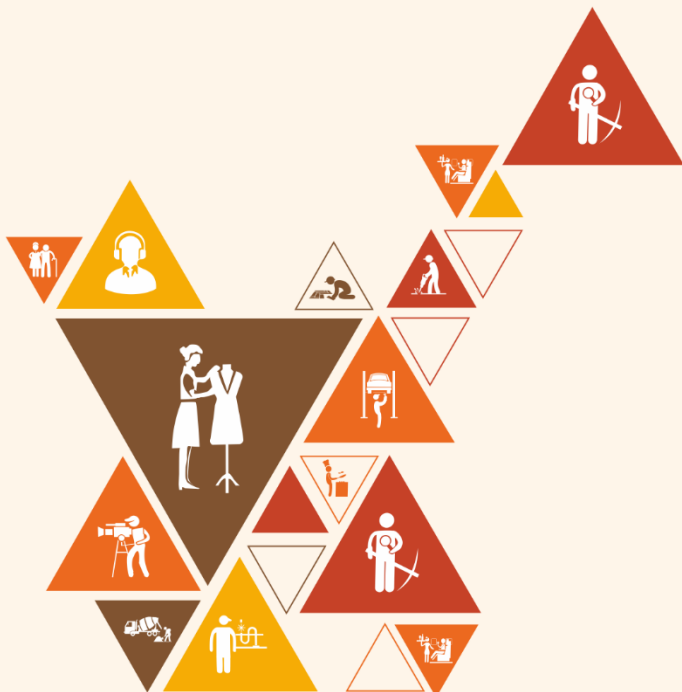
6. Employability Skills (60 Hours)

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





Annexure - I

Training Delivery Plan

Training Delivery Plan			
Program Name:	Telecom Technician – IoT Devices/Systems		
Qualification Pack Name & Ref. ID	Telecom Technician – IoT Devices/Systems (TEL/Q6210)		
Version No.	4.0	Version Update Date	27-01-2022
Pre-requisites to Training	10 + 2 preferably		
Training Outcomes	<p>After completing this programme, participants will be able to:</p> <ol style="list-style-type: none"> 1. Install IoT Devices at Customer Premises/equipment: List IoT devices (nodes and gateways) and identify suitable points/locations for installing them. 2. Configure IoT devices and establish communication: Connect nodes and gateways (hardware pre-configured) to data transfer devices (PC/Laptop) for software upload to micro-controllers, on-board compilation and debugging of software. 3. Troubleshoot the IoT devices: Troubleshoot IoT nodes and gateways over different modes of communication (Bluetooth, Zigbee, Wi-Fi etc.) 4. Demonstrate health and safety measures: Work in accordance with emergency procedures, standards and guidelines for health and safety in the organization 		

Sl. No.	Module Name	Session Name	Session Objectives	NOS Reference	Methodology	Training Tools/Aids	Duration (hours)
1	Module 1: Introduction to the sector and the job role of a Telecom Technician - IoT Devices/Systems (Theory-05:00)	Introduction to IoT Ecosystem	<ul style="list-style-type: none"> Explain the role of IoT technicians in telecom sector Describe IoT architecture and components Identify IoT applications across different industries 	KU1, KU2	Lecture, Case Studies, Group Discussion	Presentation slides, IoT application videos, industry case studies	T: 03:00 P: 00:00
		IoT Hardware Fundamentals	<ul style="list-style-type: none"> Identify various types of microprocessor boards and microcontrollers Differentiate between IoT nodes and gateways 	PC1, PC5, KU1	Demonstration, Hands-on Exploration	Arduino, Raspberry Pi, microcontroller samples, node/gateway models	T: 02:00 P: 00:00
2	Module 2: Analyze Requirements and Install IoT Devices (Theory-25:00 Practical-50:00)	IoT Sensors, Actuators & Communication Protocols	<ul style="list-style-type: none"> Determine functions and applicability of different IoT sensors and actuators 	PC2, PC3, KU3, KU6, KU7	Hands-on Workshop, Comparative Analysis	Temperature, humidity, motion sensors; Bluetooth, Zigbee, Wi-Fi, LoRaWAN modules	T: 02:30 P: 05:00
			<ul style="list-style-type: none"> Select appropriate communication protocols for IoT applications 				T: 02:30 P: 05:00
		Hardware Analysis & Installation Planning	<ul style="list-style-type: none"> Check microcontroller components and pin configurations 	PC4, PC6, KU11, KU16	Practical Lab, Site Simulation	Microcontroller boards, multimeters, installation planning tools, signal strength meters	T: 02:30 P: 05:00
			<ul style="list-style-type: none"> Determine optimal installation points based on environmental factors 				T: 02:30 P: 05:00
		Physical Installation & Power Management	<ul style="list-style-type: none"> Mount IoT devices securely using industry-approved techniques 	PC8, PC9, KU13, KU16	Hands-on Practice, Safety Demonstration	Mounting tools, power supplies, grounding equipment, safety gear	T: 02:30 P: 05:00
			<ul style="list-style-type: none"> Connect and secure power supply with proper grounding 				T: 02:30 P: 05:00
		Connectivity Establishment & Optimization	<ul style="list-style-type: none"> Establish communication line connectivity using suitable networks 	PC7, PC10, KU11, KU14	Field Simulation, Testing Practice	Network simulators, RF spectrum analyzers, signal strength testers	T: 02:30 P: 05:00
			<ul style="list-style-type: none"> Implement signal strength testing and RF spectrum analysis 				T: 02:30 P: 05:00
		IoT Installation Project	<ul style="list-style-type: none"> Complete end-to-end IoT device installation project 	PC6-PC10	Project-based Learning	Full IoT installation kit, project scenarios, assessment checklists	T: 02:30 P: 05:00
			<ul style="list-style-type: none"> Apply all installation principles in integrated scenario 				T: 02:30 P: 05:00

3	Module 3: Configure IoT Devices and Test Connectivity (Theory-30:00 Practical-50:00)	Microcontroller Configuration & Programming	• Set up connectivity options on microcontroller boards	PC11, PC14, KU17	Hands-on Programming Lab	Microcontrollers, programming IDE, sample code, debuggings tools	T: 03:00 P: 05:00
			• Compile and upload software code to microcontrollers				T: 03:00 P: 05:00
		Device Connectivity & Cloud Integration	• Link IoT devices with data transfer interfaces	PC12, PC13, KU9, KU22	Cloud Platform Workshop	AWS IoT Core/Azure IoT Hub access, gateway devices, interface cables	T: 03:00 P: 05:00
			• Install and configure firmware/software frameworks for cloud platforms				T: 03:00 P: 05:00
		Software Debugging & Performance Optimization	• Debug software errors and optimize system performance	PC15, KU17, KU18	Troubleshooting Lab	Debugging tools, emulators, performance monitoring software	T: 03:00 P: 05:00
			• Apply edge computing and AI integration principles				T: 03:00 P: 05:00
		Network Testing & Connectivity Validation	• Verify software execution and validate data transfer	PC16, PC17, PC18, KU15	Testing Laboratory	System logs dashboards, LED indicators, network testing tools	T: 03:00 P: 05:00
			• Establish connectivity between gateways and backend platforms				T: 03:00 P: 05:00
		Performance Testing & Issue Resolution	• Perform network performance testing for latency and packet loss • Confirm data reception and escalate unresolved issues	PC19, PC20, KU14, KU15	Advanced Testing Workshop	Network analyzers, packet loss simulators, escalation procedures	T: 03:00 P: 05:00
		IoT Data Protocols & Security	• Implement IoT data transfer protocols (MQTT, CoAP, HTTP) • Apply cybersecurity measures and preventive techniques	KU4, KU10, KU12	Security Workshop, Protocol Implementation	Protocol implementation tools, security testing software, compliance checklists	T: 03:00 P: 05:00

3	Module 4: Perform level 1 troubleshooting of IoT devices (Theory- 50:00 Practical- 90:00)	Fundamentals of IoT Troubleshooting	<ul style="list-style-type: none"> Establish structured troubleshooting methodologies 	PC1, KU2, KU5	Lecture, Case Studies, Planning Workshops	Troubleshooting flowcharts, test environment setups, diagnostic planning templates	T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Set up test environments for systematic diagnosis 				T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Create troubleshooting plans for common IoT failures 				T: 03:00 P: 05:00
		Hardware Connectivity Diagnosis	<ul style="list-style-type: none"> Verify connectivity between sensors, microcontrollers, and components 	PC2, PC3, KU4	Hands-on Lab, Fault Simulation, Diagnostic Practice	Multimeters, continuity testers, pinout diagrams, faulty hardware samples	T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Inspect wiring, pin configurations, and power supply connections 				T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Use diagnostic tools for hardware fault detection 				T: 03:00 P: 05:00
		Software Debugging & Performance Optimization	<ul style="list-style-type: none"> Debug software errors and optimize system performance 	PC15, KU17, KU18	Troubleshooting Lab	Debugging tools, emulators, performance monitoring software	T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Apply edge computing and AI integration principles 				T: 03:00 P: 05:00
		Software & Firmware Troubleshooting	<ul style="list-style-type: none"> Reload or update software/firmware on IoT nodes and gateways 	Software Lab, Firmware Update Workshops, Memory Analysis	Testing Laboratory	Firmware update tools, memory analyzers, data validation software, update logs	T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Check onboard memory storage and validate sensor data Apply best practices for firmware updates and security patching 				T: 03:00 P: 05:00
		Communication Module Diagnostics	<ul style="list-style-type: none"> Inspect and verify functionality of communication modules (Wi-Fi, 5G, NB-IoT, LoRaWAN) 	PC7, PC8, PC9, KU2	Communication Lab, Signal Analysis, Reconfiguration Practice	Spectrum analyzers, signal strength meters, communication modules, reconfiguration tools	T: 03:00 P: 05:00
			<ul style="list-style-type: none"> Measure communication link performance between nodes and gateways 				T: 02:00 P: 05:00
			<ul style="list-style-type: none"> Reconfigure device credentials and network authentication 				T: 02:00 P: 05:00

		Protocol-Level Debugging	<ul style="list-style-type: none"> Perform protocol-level debugging for MQTT, CoAP, HTTP Reset network configurations and conduct connectivity tests Use diagnostic software for network performance interpretation 	PC10, PC11, KU10	Protocol Analysis Workshops, Network Debugging Labs	Protocol analyzers, network simulators, debugging software, log analysis tools	T: 03:00 P: 05:00
		IoT Cybersecurity in Troubleshooting	<ul style="list-style-type: none"> Apply cybersecurity measures during troubleshooting Implement device authentication, encryption (AES-256), and secure access controls Ensure compliance with IoT security standards 	KU1, KU6, KU9	Security Workshops, Compliance Exercises, Encryption Practice	Security testing tools, encryption software, compliance checklists, authentication systems	T: 03:00 P: 05:00
		Advanced Diagnostic Tools & Remote Monitoring	<ul style="list-style-type: none"> Utilize remote monitoring tools for predictive maintenance 	KU3, KU4, KU7	Tool Configuration Labs, Remote Monitoring Setup, Performance Analysis	Remote monitoring platforms, cloud troubleshooting tools, latency measurement equipment	T: 02:00 P: 05:00
			<ul style="list-style-type: none"> Configure cloud-based IoT troubleshooting tools Diagnose network latency and interference issues 				T: 02:00 P: 05:00
		Documentation & Escalation Procedures	<ul style="list-style-type: none"> Maintain accurate logs of performance tests and corrective actions Document troubleshooting processes systematically Apply escalation procedures for unresolved issues 	PC6, PC12, KU5	Documentation Workshops, Escalation Role-plays, Logging Practice	Log templates, escalation procedure documents, case study scenarios, reporting systems	T: 03:00 P: 05:00
5	Follow sustainable practices in telecom infrastructure installation	Segregate recyclable and refurbishable components	<ul style="list-style-type: none"> Identify telecom components suitable for recycling or refurbishment Explain how to sort electronic and non-electronic waste based on disposal protocols Show how to label and store recyclable and refurbishable components separately 	TEL/N9105 PC1, PC2, PC3	Classroom lecture / PowerPoint Presentation / Question & Answer / Group Discussion	Green installation toolkit, waste segregation and e-waste disposal bins, energy audit and power measurement devices, environmental safety PPE kit, sustainability SOP charts and visual posters, simulation videos and interactive case studies	T: 02:30 P: 05:00
		Dispose of waste & Use Energy-Efficient Methods	<ul style="list-style-type: none"> Explain how to follow approved procedures for the safe disposal of hazardous and non-hazardous waste Discuss how to coordinate with authorized e-waste recycling units or certified disposal agencies Show how to select and use energy-efficient tools and equipment during telecom installations 	TEL/N9105 PC4, PC5, PC7			T: 02:30 P: 05:00
		Follow environmental standards and compliance guidelines	<ul style="list-style-type: none"> Discuss how to adhere to national and international environmental regulations for telecom infrastructure installation Explain how to maintain records of waste disposal, recycling, and sustainability measures 	TEL/N9105 PC10, PC11, PC12, PC13			T: 02:30 P: 05:00
		Guide team members	<ul style="list-style-type: none"> Explain how to guide team members on sustainable telecom installation guidelines and practices Discuss how to encourage environmentally responsible work habits 	TEL/N9105 PC14, PC15			T: 02:30 P: 05:00

Annexure II

Assessment Criteria

CRITERIA FOR ASSESSMENT OF TRAINEES







Assessment Criteria for	
Job Role	Telecom Technician - IoT Devices/Systems
Qualification Pack	TEL/Q6210, V.5.0
Sector Skill Council	Telecom Sector Skill Council




S. No.	Guidelines for Assessment
1	The assessment for the theory part will be based on knowledge bank of questions approved by the SSC.
2	Assessment will be conducted for all compulsory NOS, and where applicable, on the selected elective/option NOS/ Set of NOS.
3	Individual assessment agencies will create unique question papers for theory part for each candidate at each examination/training centre (as per assessment criteria below).
4	Individual assessment agencies will create unique evaluations for skill practical for every student at each examination/training centre based on this criterion.
5	To pass the Qualifications File, every trainee should score a minimum of 70% of aggregate marks.
6	In case of unsuccessful completion, the trainee may seek reassessment on the Qualification File.

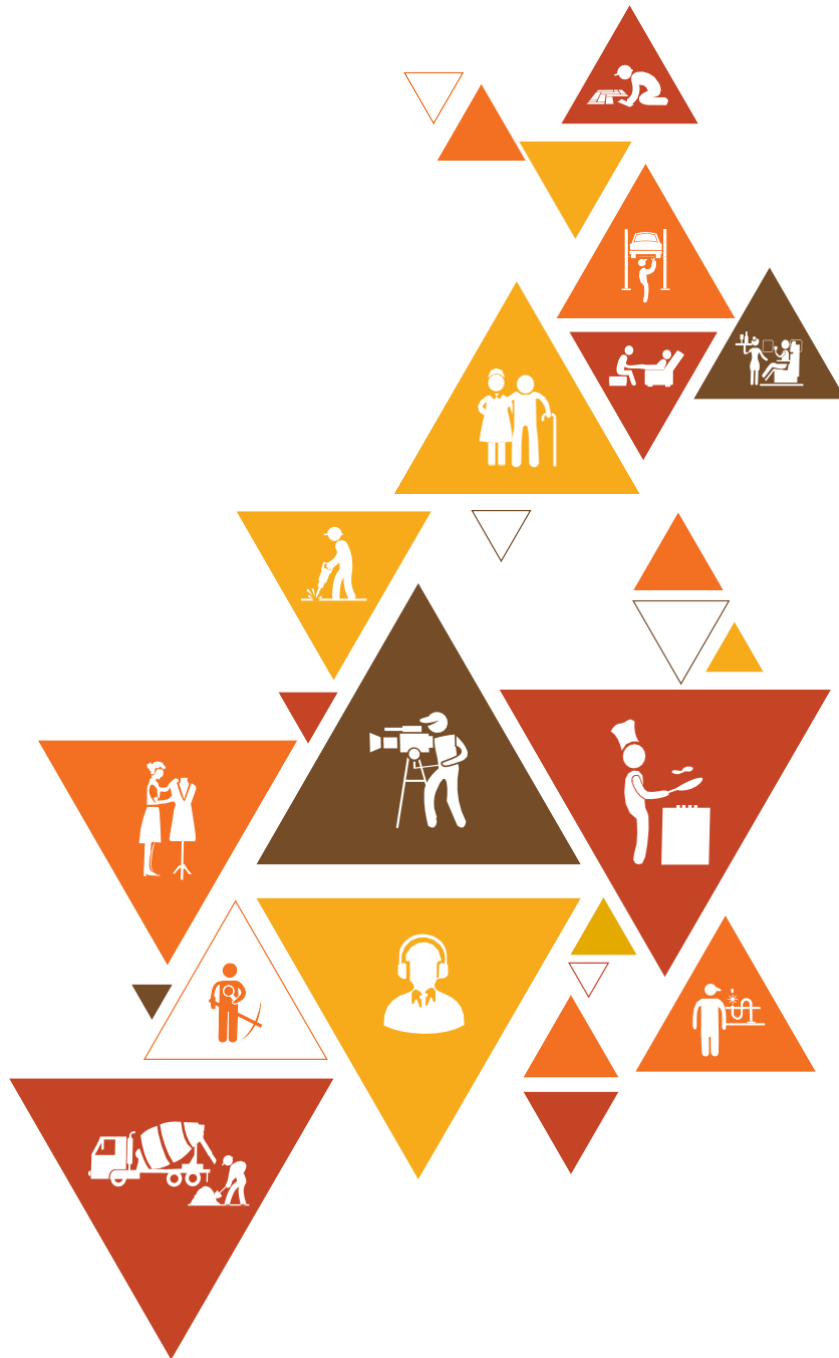
National Occupational Standards	NOS Code & Version	Theory Marks	Practical Marks	Project Marks	Viva Marks	Total Marks	Weightage
Install and configure IoT devices at customer premises	TEL/N62 34, v4.0	30	50	-	20	100	40
Perform level 1 troubleshooting of IoT devices	TEL/N62 36, v4.0	30	50	-	20	100	40
Follow sustainable practices in telecom infrastructure installation	TEL/N91 05, v1.0	30	50	-	20	100	10
Employability Skills (30 Hours)	DGT/VS Q/N010 1, v1.0	20	30	-	-	50	10
Total		110	180	-	60	350	100

Annexure - I

QR Codes –Video Links

Chapter No.	Unit Name	Topic	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	https://www.youtube.com/watch?v=D7J37mbEj0M	
	Unit 2.11 - Understanding Error Codes and Debug Software	Understanding Edge Devices	https://www.youtube.com/watch?v=LlhmzVL5bm8	
Chapter 3: Configuring Equipment and Establishing Wireless Network Connectivity	Unit 3.1 - Network Topologies	Network Topology	https://www.youtube.com/watch?v=uSKdjjw5zow	
	Unit 3.5 - Comprehension and Interpretation of Technical Data	Interpreting Technical Data	https://www.youtube.com/watch?v=Hm6Urf8ng3M	
	Unit 3.6 - Executing Speed Test and Analyze	How to perform speed x test	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?	https://www.youtube.com/watch?v=opB5oOvB3cl	

Chapter No.	Unit Name	Topic	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	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	https://www.youtube.com/watch?v=l88Qzdahn_o	
	Unit 4.7 - Troubleshooting of CPE (Modem, Router, Switch)	Modem, Router, Switch, Hub and Access Point: What's the Difference?	https://www.youtube.com/watch?v=39zXmf61Mcl	





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