NCVET
कौशल गुणवत्ता प्रगति

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
RE IMAGINE FUTURE

Telecom Sector Skill Council

Participant Handbook

Sector
Telecom

Sub-Sector
Passive Infrastructure

Occupation
Customer Service - Passive Infrastructure

Reference ID: **TEL/Q0102,** Version **5.0**
NSQF level **4**

Broadband Technician

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

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

Shri Narendra Modi
Prime Minister of India

Certificate

COMPLIANCE TO QUALIFICATION PACK– NATIONAL OCCUPATIONAL STANDARDS

is hereby issued by the

TELECOM SECTOR SKILL COUNCIL

for

SKILLING CONTENT : PARTICIPANT HANDBOOK

Complying to National Occupational Standards of

Job Role/ Qualification Pack: **"Broadband Technician"** QP No. **"TEL/Q0102, NSQF Level 4.0"**

Date of Issuance: 8th May 2025

Valid up to*: 30th April 2028

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

Authorised Signatory
(Telecom Sector Skill Council)

Acknowledgements

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

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

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

About this book

Welcome to the "Broadband Technician" training programme. This PHB intends to facilitate the participants with detailed knowledge about the concept of Telecom industry, Communication Electronics profession and their functioning. This Participant Handbook is designed based on the Qualification Pack (QP) under the National Skill Qualification framework (NSQF) and it comprises of the following National Occupational Standards (NOS)/ topics and additional topics.

1. TEL/N0111: Lay cable/system wiring and install equipment at customer premises
2. TEL/N0112: Configure customer premises equipment and establish broadband connectivity
3. TEL/N0113: Troubleshoot and rectify faults
4. TEL/N9105: Follow sustainable practices in telecom infrastructure installation
5. DGT/VSQ/N0101: Employability Skills (30 Hours)

We trust this Participant Handbook will offer strong learning support and help budding professionals carve out engaging and rewarding careers in India's dynamic telecom industry.

Symbols Used


Key Learning Outcomes


Steps


Notes


Practical


Unit Objectives

Table of Contents

Table of Contents

1. Introduction to the Sector and the Job Role of a Broadband Technician

Unit 1.1 - Introduction to Telecom Sector and Role of a Broadband Technician

TEL/N0111

Key Learning Outcomes

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

1. Explain the importance of Telecom Sector.
2. Discuss the roles and responsibilities of a Broadband Technician.

UNIT 1.1: Introduction to Telecom Sector and Role of a Broadband Technician

Unit Objectives

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

1. Explain the role of a Broadband Technician in deploying, maintaining, and troubleshooting wired and wireless broadband networks.
2. Describe the key components of broadband infrastructure and customer premises equipment (CPE).
3. Identify different types of broadband connections, such as fiber-to-the-home (FTTH), digital subscriber line (DSL), cable internet, and fixed wireless access (FWA)..
4. Elucidate the importance of network performance metrics, such as bandwidth, latency, jitter, and packet loss, in broadband service quality.
5. Explain the importance of customer service skills in assisting end-users with troubleshooting, configuring network devices, and resolving connectivity issues.
6. Discuss safety protocols, grounding techniques, and personal protective equipment (PPE) required for handling broadband installation and maintenance tasks.
7. Explain the career opportunities available for a Broadband Technician.

1.1.1 Overview of the Training Program

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

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

Fig. 1.1.1 Telecom Industry

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

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

Sector growth and infrastructure expansion:

Telecom infrastructure continues to expand rapidly, with the number of towers and mobile base transceiver stations (BTS) steadily increasing. This expansion has helped improve connectivity and service quality, especially in urban regions, though rural areas still face gaps.

Policy targets and initiatives:

The Government has launched the National Broadband Mission 2.0 (2025–30), aiming to provide optical fibre connectivity to all Gram Panchayats and key institutions, with at least 95% uptime, and to raise average fixed broadband speeds to 100 Mbps by 2030. In parallel, the Draft National Telecom Policy 2025 sets ambitious goals such as achieving 100% 4G coverage, 90% 5G coverage, 80% tower fibreisation, broadband access to 100 million households, and the rollout of 1 million public Wi-Fi hotspots by 2030.

Subscriber trends and market dynamics:

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

(Source: https://www.investindia.gov.in/sector/telecom)

1.1.2 Wi-Fi Broadband Industry in India

Wi-Fi broadband services in India have become increasingly popular in recent years as more and more people rely on the internet for work, education, entertainment, and communication. Wi-Fi broadband services provide high-speed internet connectivity over a wireless network, allowing users to access the internet from multiple devices simultaneously without the need for wired connections.

Wi-Fi broadband services are offered by a range of service providers in India, including private telecom companies such as Bharti Airtel, Reliance Jio (which currently leads the broadband market with over 497 million subscribers), and Vodafone Idea, as well as internet service providers (ISPs) such as Hathway, Spectra, and ACT Fibernet (which holds 2.33 million wired broadband subscribers as of June 2025). These companies offer various plans with different speeds, data limits, and prices, catering to the needs of different users.

One of the advantages of Wi-Fi broadband services is that they offer faster and more reliable internet connectivity than mobile networks. Wi-Fi networks can deliver speeds of up to 1 Gbps, which is significantly higher than the speeds offered by mobile networks. This makes Wi-Fi broadband services ideal for applications that require high-speed internet connectivity, such as video streaming, online gaming, and video conferencing.

Another advantage of Wi-Fi broadband services is that they offer more flexibility in terms of usage. Unlike mobile networks, which have data caps and can be expensive to use for heavy data consumption, Wi-Fi broadband services offer unlimited data plans, allowing users to consume as much data as they need without worrying about extra charges.

However, there are also some challenges associated with Wi-Fi broadband services in India. One of the biggest challenges is the lack of infrastructure in many areas, especially in rural areas, where access to high-speed internet connectivity is limited. Another challenge is the high cost of installation and maintenance of Wi-Fi networks, which can make it difficult for smaller service providers to compete with larger players in the market.

The top five broadband providers—Reliance Jio, Bharti Airtel, Vodafone Idea, BSNL, and Hathway—collectively account for approximately 99% of the broadband subscriber base in India. In the wired broadband segment, JioFiber leads with 13.93 million subscribers, followed by Airtel Xstream Fiber with 9.41 million, BSNL with 4.35 million, and Hathway with around 0.2 million. The remaining market share is distributed among regional and smaller ISPs grouped under "Others."

BSNL, once a major Wi-Fi player, has experienced a significant decline in its Wi-Fi user base—from 1.09 million in 2020 to just 0.41 million in 2024.

The market share of Wi-Fi broadband players in India is constantly evolving and is subject to change. However, based on recent reports and surveys, some of the leading players in the Wi-Fi broadband market in India and their respective market shares are:

As of 2025, Reliance Jio leads the Indian broadband market with a dominant 51.5% share, followed by Bharti Airtel at 31.5%, Vodafone Idea at 13.2%, BSNL at 2.6%, Hathway at 0.2%, and other players collectively holding the remaining 1% of the total 965 million broadband subscribers.

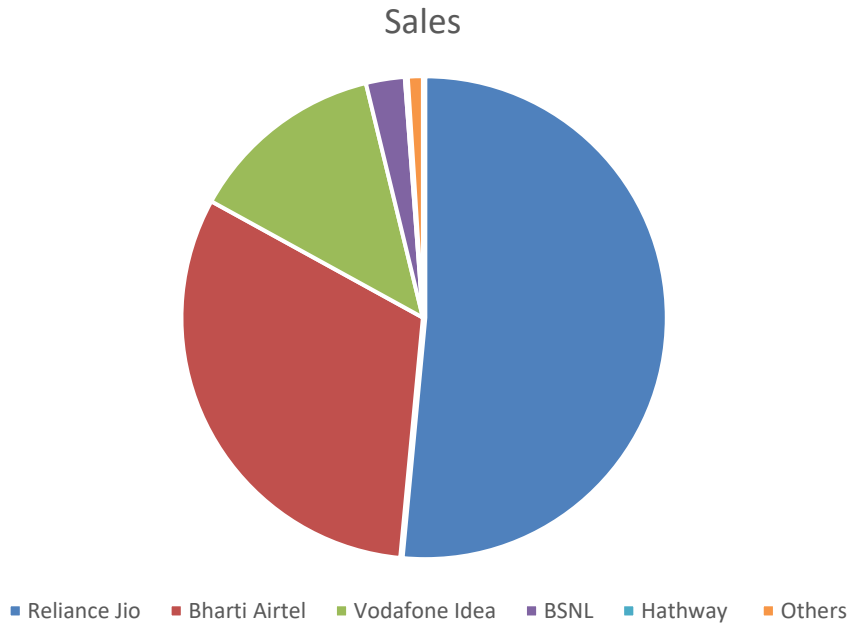


Fig 1.1.2 Market share of Wi-Fi broadband players in India

(Source: https://www.investindia.gov.in/sector/telecom)

By 2030, Reliance Jio is expected to continue leading the Wi-Fi broadband market in India, maintaining a stronghold with a projected market share of over 50%, driven by its expansive fiber network and competitive pricing under the JioFiber brand. Bharti Airtel is likely to remain the second-largest player, growing its footprint through Airtel Xstream Fiber, offering speeds from 100 Mbps to 1 Gbps with enhanced digital services bundled in.

Vodafone Idea, though facing stiff competition, may stabilize its presence in the Wi-Fi broadband segment through Vodafone Fiber, potentially holding around 10–12% market share, depending on its infrastructure investments and customer retention strategies.

The Wi-Fi broadband landscape in India is expected to evolve rapidly by 2030 due to ongoing competition, entry of new regional ISPs, and the increasing shift in user behaviour toward hybrid work, digital education, smart homes, and 4K/8K streaming services.

As India moves deeper into the digital economy, the demand for ultra-fast and reliable internet is anticipated to rise sharply. By 2030, urban centers and tier-II cities will see widespread fiber penetration, and smart city initiatives are likely to integrate public Wi-Fi infrastructure across transportation, healthcare, and education sectors.

According to revised projections, India's Wi-Fi hotspot and broadband market could witness a compound annual growth rate (CAGR) of 25–30%, reaching an estimated market value of $6–7 billion by 2030, fueled by expanding digital infrastructure, government support, and rising consumer dependence on high-speed internet. Some of the key factors that are likely to shape the future of Wi-Fi broadband in India are:

- Increasing penetration: The penetration of Wi-Fi broadband services in India is expected to increase in the coming years as more and more people become aware of the benefits of high-speed internet connectivity. The increasing availability of Wi-Fi hotspots in public places, such as airports, cafes, and malls, is also expected to contribute to the growth of Wi-Fi broadband in India.
- Government policies: The Indian government's initiatives, such as the National Broadband Mission, National Digital Communications Policy, Digital India, BharatNet and Wi-Fi Access Network Interface (WANI), are expected to play a key role in driving the growth of the Wi-Fi broadband industry in India. These initiatives aim to provide high-speed internet connectivity to all citizens across the country, especially in rural areas.
- Infrastructure development: The development of infrastructure for Wi-Fi broadband, including the installation of fibre optic cables and the deployment of Wi-Fi hotspots, is likely to improve the quality and reliability of internet connectivity in India. The government's initiatives, such as the National Broadband Mission, are expected to play a significant role in the development of infrastructure for Wi-Fi broadband in India.
- Advancements in technology: Advancements in technology, such as 5G and Wi-Fi 6, are likely to further enhance the capabilities of Wi-Fi broadband services in India. These technologies are expected to deliver higher speeds, lower latency, and improved connectivity, making Wi-Fi broadband even more attractive to consumers.
- Increased competition: The Wi-Fi broadband market in India is highly competitive, with a large number of players vying for market share. This is likely to drive innovation and improvements in service quality as companies compete to offer better plans, speeds, and customer service.

1.1.3 Broadband

The technique which lets any user access the Internet services at higher speeds as compared to a dial-up connection is called Broadband. The speeds vary, subject to the technology set up and the distribution of the levels. Residential services have quicker download speeds when compared to upload speeds.

Information via the Internet is allowed for users through high -speed technology transmission, which is digital, while images, sounds, and text are transmitted as "bits" of data.

1.1.4 Broadband Platform

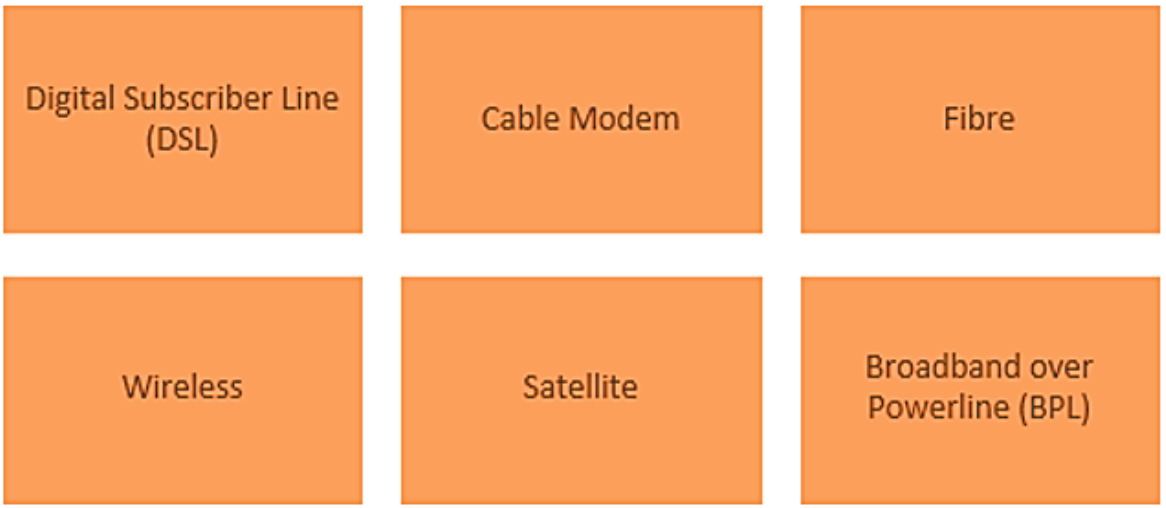


Fig 1.1.2 Market share of Wi-Fi broadband players in India

Unlike the copper lines installed in homes and businesses, the DSL line transmits data in much faster way. Its transmission speed ranges from several hundreds kbps to millions of bits per second (Mbps)

Digital Subscriber Line (DSL)

Unlike the copper lines installed in homes and businesses, the DSL line transmits data in much faster way. Its transmission speed ranges from several hundreds kbps to millions of bits per second (Mbps)

DSL transmission technologies are as follows:

- ASymmetrical Digital Subscriber Line (ADSL): Mainly used in homes (Refer Fig.1.1.1). ADSL provides faster downstream rather than upstream. This sanctions faster data transmission toward the end end-user the same line used for voice service.

Fig 1.1.4 ADSL modem

Cable modem

This allows the operators to deliver Internet (using broadband) at the same time allowing the users to watch TV with a cable connection. Thespeed and transmission are subject to the quality of cable used, modem, network and the number of users at a given time. Generally, the speeds are equivalent or sometimes surpass the classic residential DSL.

Fibre

Fibre optic cables are used to carry data, which are carried by electric signals to light and sends them to transparent glass fibres. These fibres transform or transfers the data at much higher speeds than DSL or cable modems. The end user speed may fluctuate subject to the distance between the fibre cables and the computer, and also how the service provider has set up the configurations of the service. The fibres, which allow you to access broadband, can also be utilized for delivering voice through VoIP and video services.

Wireless

When a device is connected to the Internet by short-range wireless is called Wireless Fidelity (Wi-Fi). This allows movement to a limited range within a home or business, or can be used in many public places through "hotspots".

A fixed wireless technology when connected with equipment that has a longer range can provide cost-effective Internet service to remote areas.

Mobile service providers also provide mobile wireless broadband services to their customers, although services as compared to a wired or fixed connection is slow.

Satellite

Substituting the wireless broadband is satellite service which is commonly used in remote or thinly populated areas. The speed varies on few dynamics like the provider, service plan, etc. Extreme weather conditions can be a major reason for disruption of satellite service. As compared to dial-up connection speed is faster, however lower if compared to DSL and cable modem.

The key requirements for having satellite service are:

- a base station or dish which should be at least 3 feet
- a clear line of sight (LOS) to the satellite
- a modem

Broadband over Powerline (BPL)

BPL is coming up as a promising technology, which uses existing electrical connections for providing Internet to customer. It has great prospects as the power lines are needed everywhere, mitigating the necessity to set up a broadband for every customer.

1.1.5 Broadband Industry

Telecommunication plays a major role in economic and social development and has its scope across all technical fields. It integrates all telecommunication-related services in India and acts as a backbone for digital transformation.

The rapid improvement of internet and mobile technologies has had a significant impact on India's economic growth. Recognising this, the Government of India has placed strong emphasis on the development of the telecom industry. India continues to be the world's second-largest telecom market, after China.

However, broadband penetration and fixed broadband speeds in India still lag behind those of China. Strengthening broadband connectivity remains a key driver for digitalisation, economic inclusion, and innovation. The government has therefore prioritised expanding both mobile and fibre-based internet services to bridge the gap.

A major focus is on enhancing network connectivity in rural and semi-urban areas. The primary aim is to provide broadband access to every citizen of the country. Under the National Broadband Mission 2.0 (2025–30), the Government is targeting optical fibre connectivity for all Gram Panchayats and key institutions, ensuring at least 95% uptime. The mission also aims to raise average broadband speeds to 100 Mbps by 2030.

In line with this, rural and village-level networks are being upgraded to support high-speed internet, including the rollout of affordable 100 Mbps connections in villages through Panchayat-level initiatives. By doing so, India is working towards narrowing the rural-urban digital divide.

The Draft National Telecom Policy 2025 further outlines ambitious goals such as 100% 4G coverage, 90% 5G coverage by 2030, 80% fibreisation of towers, and 1 million public Wi-Fi hotspots across the country. These steps not only aim to improve connectivity but also attract foreign investment into the telecom sector, thereby creating new avenues for employment and skill development.

5G adoption and economic impact:

India has already rolled out 5G services across major cities and industrial hubs, with rapid expansion into smaller towns and rural regions underway. The adoption of 5G is expected to drive innovation in sectors like smart manufacturing, healthcare, education, transport, and agriculture, enabling applications such as IoT, automation, and AI-driven services. According to projections, 5G technology could contribute around USD 450 billion to India's economy between 2023 and 2040. This transformative impact will strengthen India's digital ecosystem, enhance productivity, and support the government's vision of a digitally empowered society and knowledge economy. With these initiatives, India is positioning itself strongly in the global telecom space and aspires to move closer to the top rank worldwide.

1.1.6 Role and Responsibilities of a Wireless Technician

A Broadband Technician is a skilled professional responsible for the installation, maintenance, and repair of broadband network infrastructure. They work with both wired (such as fiber optic cables, coaxial cables, DSL) and wireless (such as Wi-Fi, LTE, and other radio frequency-based networks) systems to ensure uninterrupted internet connectivity, optimal network performance, and efficient data transmission for residential, commercial, and industrial clients.

Role of a Broadband Technician:

1. Deployment of Broadband Networks

- Site Survey & Planning: Assess the physical environment to determine the best locations for equipment, cables, and antennas, considering interference, signal strength, and safety standards.
- Installation of Equipment:
  - Wired Networks: Lay cables, splice fiber optics, terminate connections, and install routers, modems, switches, and distribution frames.
  - Wireless Networks: Install antennas, access points, and base stations ensuring correct alignment and signal coverage.
- Configuration: Set up hardware and software configurations, including IP addressing, network settings, encryption protocols, and access controls.
- Compliance & Safety: Ensure adherence to electrical codes, network standards, and safety protocols to protect users and equipment.

2. Maintenance of Broadband Networks

- Regular Inspections: Conduct scheduled checks on cables, routers, antennas, and other devices to ensure they function properly.
- Firmware & Software Updates: Keep devices and systems updated to the latest versions to prevent vulnerabilities and enhance performance.
- Signal Optimization: Monitor and fine-tune signal strength, bandwidth allocation, and network load to ensure users receive stable and fast internet connections.
- Documentation: Maintain accurate records of installations, service reports, and inventory for tracking network health and troubleshooting.

3. Troubleshooting Broadband Networks

- Problem Identification: Use diagnostic tools such as OTDR (Optical Time-Domain Reflectometer), spectrum analyzers, or ping tests to locate faults.
- Fault Rectification:
  - Wired: Repair damaged cables, replace connectors, or reroute lines.
  - Wireless: Resolve interference issues, realign antennas, and replace malfunctioning equipment.
- User Support: Assist customers experiencing connectivity issues, explaining solutions and providing guidance on usage.
- Emergency Response: Quickly address outages or critical faults to minimize downtime and restore services efficiently.

1.1.7 Types of Broadband Connections

Broadband connections provide high-speed internet access to homes, businesses, and other facilities. There are various technologies used to deliver broadband, each with its own characteristics, advantages, and limitations. Below are the commonly used broadband connection types explained in detail:

1. **Fiber-to-the-Home (FTTH):** Fiber-to-the-home (FTTH) is a broadband technology that delivers internet connectivity directly to residential premises using fiber optic cables. It is one of the fastest and most reliable types of internet connections available today.

How it works:

In FTTH networks, data is transmitted as pulses of light through ultra-thin strands of glass or plastic. The fiber optic cables run from a central network hub directly to the customer's premises, providing a dedicated and uninterrupted data path.

Advantages:

- Extremely high-speed internet access (often up to 1 Gbps or higher).
- Low latency, making it suitable for real-time applications like gaming, video conferencing, and streaming.
- High bandwidth allows multiple users and devices to operate simultaneously without speed degradation.
- Less signal interference compared to copper-based connections.

Limitations:

- Installation costs can be high, especially in rural or remote areas.
- Requires professional installation and maintenance.

Use Cases:

- Smart homes and offices
- Streaming services and entertainment platforms
- Cloud computing and large data transfers
- Educational institutions and healthcare facilities

2. **Digital Subscriber Line (DSL):** Digital Subscriber Line (DSL) is a broadband connection that transmits digital data over traditional copper telephone lines. It allows simultaneous voice and internet usage without interference.

How it works:

DSL technology separates the telephone line into multiple channels using frequency division. This allows both internet and voice services to operate at the same time, utilizing different parts of the frequency spectrum.

Types of DSL:

- **ADSL (Asymmetric DSL):** Offers higher download speeds compared to upload speeds, suitable for typical residential use.
- **SDSL (Symmetric DSL):** Provides equal upload and download speeds, beneficial for businesses and applications requiring data sharing.

Advantages:

- Uses existing telephone infrastructure, reducing installation costs.
- Provides decent internet speeds for everyday activities.
- Available in many regions where fiber networks are not present.

Limitations:

- Speed depends on distance from the telephone exchange; further distance reduces performance.
- Copper wires are prone to signal loss and interference.
- Limited bandwidth compared to fiber solutions.

Use Cases:

- Basic internet browsing, email, and streaming
- Small businesses with moderate internet requirements
- Residential areas not yet served by fiber-optic networks

3. Cable Internet: Cable internet delivers broadband service through coaxial cables, the same type of cables used for cable television. It provides faster speeds than DSL and is widely available in urban and suburban areas.

How it works:

Data signals are transmitted using radio frequency over coaxial cables, which consist of a core conductor, insulating layer, and shielding to prevent interference.

Advantages:

- Faster than DSL, with download speeds ranging from 100 Mbps to 1 Gbps depending on the provider.
- Supports simultaneous use by multiple users.
- Reliable for video streaming, online gaming, and telecommuting.

Limitations:

- Shared bandwidth among users in the same area can slow down performance during peak hours.
- Signal quality may degrade over long cable runs or outdated infrastructure.

Use Cases:

- Households requiring consistent internet speed for entertainment and work-from-home scenarios
- Streaming services, video conferencing, and large file downloads
- Apartment complexes and dense residential areas

4. Fixed Wireless Access (FWA): Fixed Wireless Access (FWA) provides broadband internet over radio signals instead of physical cables. It connects homes and businesses to the network through antennas mounted on buildings or towers.

How it works:

FWA transmits data wirelessly from a base station to customer premises using high-frequency radio signals. The connection is typically line-of-sight or near-line-of-sight between the service provider's antenna and the user's receiver.

Advantages:

- Faster deployment compared to wired solutions, as no cables need to be laid.
- Useful in areas where laying cables is impractical or expensive.
- Can offer speeds comparable to DSL and cable connections depending on network infrastructure.

Limitations:

- Performance may be affected by weather, physical obstructions, or distance from the base station.
- Security and interference concerns require advanced encryption and network management.

1.1.8 Key Components of Broadband Infrastructure and Customer Premises Equipment (CPE)

Broadband networks require a combination of infrastructure components and equipment at the customer's location to deliver seamless internet connectivity. These components ensure data is transmitted, received, and managed effectively across the network. Below is an explanation of the key elements involved in broadband deployment.

1. Key Components of Broadband Infrastructure

Broadband infrastructure refers to the systems, hardware, and network architecture that enable high-speed data transmission from service providers to customers. These components form the backbone of the broadband network.

a. Core Network

- The central part of the broadband infrastructure, consisting of high-capacity servers, routers, switches, and data centers.
- Routes internet traffic, manages data flow, and connects to global internet exchanges.
- Includes redundancy systems for backup in case of failure, ensuring uninterrupted service.

b. Access Network

- The intermediate layer that connects the core network to customer locations.
- Consists of distribution networks such as fiber optic cables, coaxial cables, or wireless towers.
- Handles the last-mile connection, which is critical for delivering broadband services.

c. Transmission Media

The physical or wireless channels used to carry data signals from the provider to the user.

Includes:

- Fiber Optic Cables – Provide ultra-fast data transfer using light signals.
- Coaxial Cables – Used for cable internet services, capable of handling large bandwidths.
- Twisted Pair Copper Cables – Used in DSL networks.
- Radio Waves – Used in wireless networks like FWA, Wi-Fi, or mobile broadband.

d. Network Elements

- Routers & Switches – Manage traffic between networks and distribute data to the correct destination.
- Optical Line Terminals (OLT) – Used in fiber networks to send signals to multiple users.
- Base Stations – Used in wireless networks to transmit and receive radio signals.
- Modems – Convert digital signals to analog and vice versa for communication over transmission media.

e. Power Supply and Backup Systems

- Ensure continuous operation by providing reliable power.
- Includes batteries, generators, and uninterrupted power supply (UPS) systems for redundancy.

f. Monitoring & Management Systems

- Tools and software that monitor network performance, detect faults, and optimize traffic flow.
- Helps service providers quickly respond to issues and maintain service quality.

2. Key Components of Customer Premises Equipment (CPE)

Customer Premises Equipment (CPE) refers to the devices installed at the user's location that interface with the broadband infrastructure to provide internet access and networking services.

a. Modem

The device that connects the customer's home or office to the broadband service.

Modulates and demodulates signals between the user's devices and the provider's network.

Types:

- DSL Modems – Connect via copper lines.
- Cable Modems – Connect via coaxial cables.
- Fiber Modems/ONT (Optical Network Terminals) – Connect via fiber lines.
- Wireless Gateways – Combine modem and router functions for wireless access.

b. Router

- Directs internet traffic between devices within the customer's premises and external networks.
- Provides security features like firewalls and encryption protocols.
- Manages local area networks (LAN) by assigning IP addresses and bandwidth priorities.

c. Wi-Fi Access Points

- Allow devices to connect wirelessly to the broadband network.
- Provide signal coverage throughout homes, offices, and outdoor areas.

d. Ethernet Switches

- Expand wired connectivity by allowing multiple devices to connect to the modem or router.
- Used in businesses or homes requiring several wir

1.1.9 Importance of Network Performance Metrics in Broadband Service Quality

Broadband networks are expected to deliver fast, reliable, and uninterrupted internet access. However, the quality of broadband service depends not only on the speed advertised by the service provider but also on how the network performs under real-world conditions. To evaluate and ensure optimal broadband service, several network performance metrics are used. These metrics—bandwidth, latency, jitter, and packet loss—play a critical role in assessing the health and efficiency of a network. Below is a detailed explanation of each metric and its importance:

Bandwidth: Bandwidth refers to the maximum amount of data that can be transmitted over a network connection in a given time period, usually measured in megabits per second (Mbps) or gigabits per second (Gbps).

Importance:

- Determines the internet speed available to the user.
- Affects how quickly websites load, files download, or videos stream.
- Higher bandwidth supports more users and devices simultaneously without performance degradation.
- Essential for activities that require heavy data use, such as video conferencing, online gaming, and cloud-based applications.

Impact of Poor Bandwidth:

- Slow download and upload speeds.
- Increased buffering in streaming services.
- Difficulty in handling multiple devices or tasks at once.

2. Latency:

Latency is the time it takes for data to travel from the source to the destination and back, measured in milliseconds (ms). It is often referred to as "ping time."

Importance:

- Affects how quickly data responds during real-time interactions.
- Critical for applications that require immediate feedback, such as video calls, online gaming, and virtual meetings.
- Low latency ensures smoother communication and faster response times.

Impact of High Latency:

- Delay in voice or video transmissions.
- Lagging during online gaming.
- Poor user experience in interactive applications.

3. Jitter: Jitter measures the variation in packet arrival times during data transmission. It indicates how consistent the network's response is.

Importance:

- High jitter affects the quality of streaming and voice services.
- Important for maintaining uninterrupted data flow, especially for video conferencing and VoIP (Voice over Internet Protocol).
- Consistent packet delivery ensures better synchronization and fewer disruptions.
- Impact of High Jitter:
- Choppy audio or video.
- Delays and out-of-sync communication.
- Interruptions in live streaming or webinars.

4. Packet Loss: Packet loss occurs when data packets traveling across the network fail to reach their destination. It is usually expressed as a percentage of lost packets.

Importance:

- Essential for data integrity and smooth communication.
- Even small amounts of packet loss can affect real-time services and large file transfers.

Helps identify network faults, congestion, or interference issues.

Impact of High Packet Loss:

- Broken or frozen video streams.
- Incomplete file transfers or corrupted data.
- Disruptions in online services and applications.

Why These Metrics Matter

1. **Service Reliability:**
   - These metrics help providers monitor the health of their networks and ensure uninterrupted service delivery.
2. **User Experience:**
   - A well-optimized network with sufficient bandwidth, low latency, minimal jitter, and negligible packet loss results in a seamless internet experience for end users.
3. **Troubleshooting and Optimization:**
   - By analyzing these metrics, network engineers can identify bottlenecks, predict failures, and improve network efficiency.

4. **Quality Assurance:**
   - Service providers use these metrics to meet service-level agreements (SLAs) and offer better customer satisfaction.
5. **Future Scalability:**
   - Monitoring performance helps in planning for increased demand, upgrading infrastructure, and implementing advanced services like smart homes, IoT devices, and telemedicine.

1.1.10 Importance of Customer Service Skills in Broadband Support

Broadband networks are technical systems that require proper setup, maintenance, and troubleshooting to ensure uninterrupted service. While technical expertise is essential, customer service skills are equally important when assisting end-users with troubleshooting, configuring network devices, and resolving connectivity issues. These skills ensure users receive not only the correct technical support but also a positive and reassuring experience. Below is a detailed explanation of why customer service skills are critical in broadband services:

1. Building Trust and Confidence

- Effective communication helps users feel heard and supported, especially when they are frustrated by connectivity issues.
- Providing clear, patient explanations builds trust, assuring customers that their problems will be handled professionally.
- A confident and empathetic approach reduces anxiety and helps users feel more in control.

2. Simplifying Complex Technical Information

- End-users may not be familiar with networking terms, devices, or settings.
- Customer service skills allow technicians to break down complicated concepts into simple steps that users can follow.
- Clear guidance during troubleshooting and configuration prevents confusion and mistakes, ensuring tasks are completed efficiently.

3. Enhancing User Satisfaction

- Prompt and courteous assistance improves customer satisfaction and loyalty.
- Listening carefully to user concerns before offering solutions ensures that the root problem is addressed.
- Providing step-by-step support, follow-ups, and reassurances creates a positive experience even when technical issues arise.

4. Resolving Issues More Effectively

- Troubleshooting requires asking the right questions, observing user descriptions, and confirming symptoms.
- Good customer service involves active listening, empathy, and patience, which help technicians gather accurate information and diagnose issues quickly.

- A calm, methodical approach helps users stay engaged, making it easier to guide them through repairs or reconfiguration.

5. Reducing Escalations and Repeat Calls

- Providing thorough support reduces the chances of unresolved problems or misunderstandings.
- Educating users on proper device usage and preventive maintenance empowers them to handle minor issues independently.
- Fewer escalations and repeated complaints improve service efficiency and reduce operational costs.

6. Promoting Brand Reputation and Customer Retention

- A helpful and friendly support experience encourages users to remain loyal to the service provider.
- Satisfied customers are more likely to recommend the service to friends and family.
- Excellent customer service can differentiate a provider in a competitive market, leading to long-term business growth.

7. Supporting Accessibility and Inclusion

- Not all users are equally tech-savvy; some may require additional support.
- Customer service skills ensure that users with limited technical knowledge, elderly users, or those with disabilities receive respectful and inclusive assistance.
- This strengthens relationships and broadens the provider's customer base.

1.1.11 Safety Protocols, Grounding Techniques, and Personal Protective Equipment (PPE) in Broadband Installation and Maintenance

Broadband installation and maintenance involve working with electrical systems, cables, antennas, and equipment in various environments. These tasks, if not performed safely, can result in accidents, injuries, or damage to equipment. Therefore, following proper safety protocols, using correct grounding techniques, and wearing suitable personal protective equipment (PPE) is essential for the safety of both technicians and end-users.

1. Safety Protocols in Broadband Installation and Maintenance

Safety protocols are procedures and guidelines designed to prevent accidents and ensure a safe working environment. Technicians must strictly adhere to these protocols during every broadband task.

Key Safety Protocols

1. Site Assessment Before Work
   - Inspect the area for potential hazards such as exposed wires, wet surfaces, or unstable structures.
   - Confirm that the work zone is safe and accessible.
2. Proper Handling of Tools and Equipment
   - Use insulated tools when working with electrical connections.
   - Avoid using damaged or malfunctioning equipment.

3. **Electrical Safety**
   - Switch off power sources before installing or repairing network equipment.
   - Verify circuits with appropriate testers to ensure no active current.
4. **Working at Heights**
   - Use harnesses, ladders, and scaffolding safely when installing antennas, towers, or cables on poles or rooftops.
   - Secure tools to prevent falling objects.
5. **Weather Considerations**
   - Avoid working during storms, heavy rain, or strong winds.
   - Protect equipment from moisture or lightning risks.
6. **Emergency Preparedness**
   - Keep first aid kits and emergency contact numbers on-site.
   - Train technicians in basic first aid and emergency procedures.

Best Practices
- Use corrosion-resistant materials like copper or galvanized steel for grounding.
- Periodically inspect grounding connections to ensure they are secure and effective.
- Follow national and local electrical codes during installation.

3. **Personal Protective Equipment (PPE) Required**

PPE protects technicians from hazards encountered during broadband installation and maintenance.

Essential PPE

1. **Insulated Gloves**
   - Protect against electric shocks when handling wires and connectors.
2. **Safety Helmets**
   - Protect the head from falling objects or accidental impacts.
3. **Safety Glasses or Goggles**
   - Prevent dust, debris, and sparks from damaging the eyes.
4. **Protective Footwear**
   - Insulated and slip-resistant shoes prevent electric shocks and provide stability.
5. **High-Visibility Clothing**
   - Ensures the technician is visible in outdoor or low-light environments.
6. **Fall Protection Equipment**
   - Harnesses, lanyards, and anchor points for work at heights.
7. **Hearing Protection**
   - Earplugs or earmuffs are used when working near loud machinery or tools.
8. **Respiratory Protection**
   - Masks may be required in dusty environments or areas with chemical fumes.

Additional Safety Gear
- Tool belts for easy access to equipment.
- Fire-resistant clothing for working near electrical panels.

1.1.12 Career Opportunities for a Broadband Technician

A Broadband Technician plays an essential role in ensuring internet connectivity through the installation, maintenance, and troubleshooting of broadband networks. With the growing demand for high-speed internet in homes, businesses, and industries, the career prospects for broadband technicians are strong and expanding. Below is a detailed explanation of the career opportunities available in this field:

1. Entry-Level Opportunities

Field Technician / Installer

- Install and set up broadband services for residential and commercial customers.
- Perform on-site surveys, equipment installation, and basic troubleshooting.
- Gain hands-on experience in handling network devices and customer interactions.

Service Technician / Maintenance Technician

- Perform routine inspections and maintenance of broadband infrastructure.
- Troubleshoot and resolve service outages, wiring issues, and equipment failures.
- Assist senior technicians in implementing upgrades and system improvements.

Help Desk Support / Technical Support Representative

- Provide remote assistance to customers facing internet connectivity issues.
- Guide users in configuring routers, modems, and other devices.
- Educate customers on proper network use and troubleshooting steps.

2. Mid-Level Opportunities

Network Engineer / Broadband Engineer

- Design, configure, and optimize broadband networks for efficient performance.
- Handle network expansions, upgrades, and integration with new technologies.
- Work with internet service providers (ISPs) and infrastructure companies to ensure reliable service delivery.

Field Supervisor / Team Lead

- Lead teams of technicians in managing large-scale installation and maintenance projects.
- Ensure compliance with safety protocols and quality standards.
- Train and mentor new technicians.

System Analyst

- Monitor network performance using diagnostic tools.
- Analyze network metrics such as bandwidth, latency, and packet loss to enhance service quality.
- Implement improvements to optimize traffic management and system resilience.

3. Advanced Career Paths

Network Architect

- Plan and develop large broadband networks with long-term scalability in mind.
- Work on complex designs involving fiber optics, wireless systems, and cloud integration.
- Collaborate with stakeholders to align technical infrastructure with business goals.

Project Manager

- Oversee broadband infrastructure projects from planning through deployment.
- Manage budgets, timelines, and technical teams to ensure successful implementation.
- Coordinate with clients, vendors, and regulatory bodies.

Cybersecurity Specialist

- Protect broadband networks from threats such as hacking, malware, and data breaches.
- Implement security protocols, encryption techniques, and monitoring systems.
- Educate users on safe practices and compliance standards.

4. Opportunities in Specialized Fields

Telecommunication Companies

- Work on large-scale broadband services for residential and enterprise customers.
- Engage in installation, maintenance, network planning, and customer support.

Data Centers

- Manage network infrastructure that supports cloud computing, hosting, and storage solutions.
- Ensure redundancy, power management, and secure connectivity.

Government and Public Sector

- Support broadband expansion initiatives in rural or underserved areas.
- Assist in implementing national digital infrastructure projects.

Smart City Projects and IoT

- Work on interconnected broadband networks for smart homes, healthcare systems, transportation, and urban management**.**
- Help integrate broadband services with automation and artificial intelligence platforms.

5. Freelancing and Entrepreneurship

- Start an independent broadband installation and maintenance service.
- Offer consulting services to small businesses or residential complexes.
- Provide specialized support such as network security audits or system upgrades.

Exercise

Short Answer Questions:

1. Explain the primary responsibilities of a Broadband Technician in deploying and maintaining broadband networks.
2. List the key components found in broadband infrastructure and customer premises equipment (CPE).
3. Compare and contrast at least two types of broadband connections and their advantages.
4. Why are network performance metrics such as latency and packet loss critical in ensuring broadband service quality?
5. Describe the role of safety protocols and PPE in broadband installation and maintenance tasks.

Multiple Choice Questions (MCQs):

1. Which of the following is considered customer premises equipment (CPE)?
   a) Fiber optic cables
   b) DSL modem
   c) Router switch in the central office
   d) Fiber distribution hub

2. Which broadband connection type uses existing telephone lines for high-speed internet?
   a) FTTH
   b) DSL
   c) Cable Internet
   d) Fixed Wireless Access

3. Which of these metrics measures the delay between sending and receiving data in a network?
   a) Bandwidth
   b) Latency
   c) Jitter
   d) Packet loss

4. A Broadband Technician is configuring a router for a customer. Which skill is most critical?
   a) Knowledge of fiber splicing
   b) Customer service and troubleshooting skills
   c) Ability to design network topologies
   d) Programming network devices from scratch

5. Which PPE item is essential when handling fiber optic cables?
   a) Safety gloves
   b) Hard hat
   c) Reflective vest
   d) Ear plugs

Fill in the Blanks:

1. The type of broadband connection that delivers fiber directly to a customer's home is called _____.
2. _____ refers to the variation in delay of received packets in a network.
3. Broadband infrastructure typically includes components such as routers, switches, optical line terminals, and _____.
4. Proper grounding techniques and _____ are essential to ensure safety during broadband installation.
5. Career opportunities for a Broadband Technician include network support, field installation, and _____.

Notes

2. Lay Cable/System Wiring and Install Equipment at Customer Premises

Telecom Sector Skill Council

TEL/N0111

Key Learning Outcomes

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

1. Explain the types, specifications, and selection criteria of network cables and PoE devices.
2. Demonstrate the process of assessing site feasibility and selecting appropriate installation locations.
3. Explain the functions, configurations, and troubleshooting methods for customer premise equipment (CPE).
4. Demonstrate structured wiring installation, device configuration, and power management techniques.
5. Explain post-installation site restoration, documentation, and customer communication procedures.
6. Demonstrate proper cleanup, record-keeping, and customer sign-off processes.

UNIT 2.1: Cable and Connectors

Unit Objectives

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

1. Explain the specifications of network cables, PoE devices, and network equipment.
2. Identify different sizes, colors, and categories of network cables, including CAT5e, CAT6, CAT6A, and fiber optic cables.
3. Describe the types of cables (OFC, UTP, STP, Twisted Pair, etc.) and connectors (RJ-45, RJ-11, SC, LC, etc.).
4. Explain the proper use of hand tools and power tools for cable installation, routing, and device mounting.
5. Demonstrate how to select and use appropriate connectors, ensuring PoE-supported devices receive stable power and data signals.
6. Show how to collect and organize the required tools, equipment, and PoE-compatible components for installation.

2.1.1 Networking Cables

The medium through which information travels from a specific network to another network is called cable. The cables that are used to connect a specific device to another device within a network are called networking cables. The type of cable chosen for a network depends upon protocol, network's topology and size.

The following figures shows UTP cable:

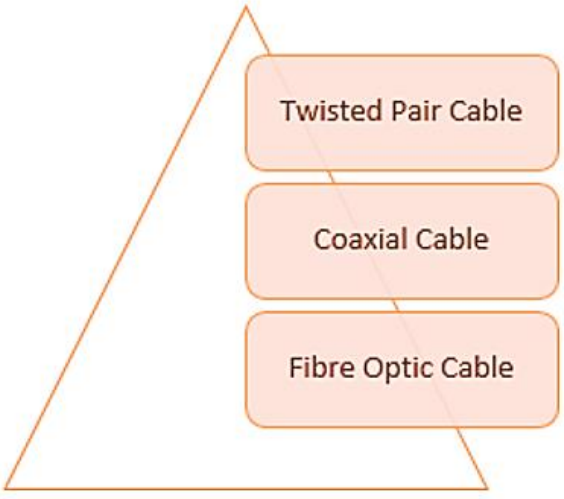


Fig 2.1.1 Classification of network cable

Twisted Pair Cable

In twisted-pair cables, copper wired cables are twisted together to reduce inter and intra Electro Magnetic Interference (EMI). These cables are mostly used for Ethernet networks.

These can further be classified as follows.

Unshielded Twisted Pair (UTP) Cable

UTP Cable has two undefended wires twisted around each other. Being cost effective this type of wire is widely used for local-area networks (LANs) and telephone connections. The quality of UTP varies from telephone wires to high-speed. To eliminate intrusion with neighboring pairs and other devices each UTP cable is twisted with a different number of rotations per inch. The better the twisting, the higher the transmission rate and cost/foot.

The following figures shows UTP cable:

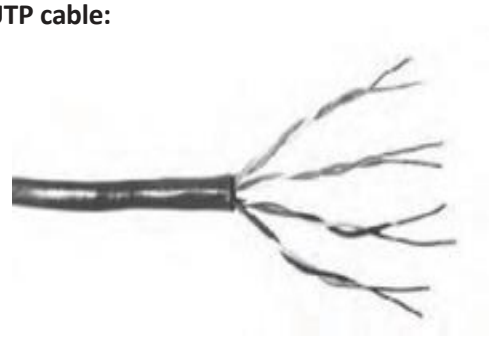


Fig 2.1.2: UTP Cable

Shielded TWISted Pair (STP) Cable

STP has wiring of copper wherein each of the two copper wires are twisted and coated with insulating coating and every pair of wire is individually shielded with foil that functions as a ground for the wires. STP cabling is majorly used for Ethernet networks, specifically for fast data rate Ethernets.

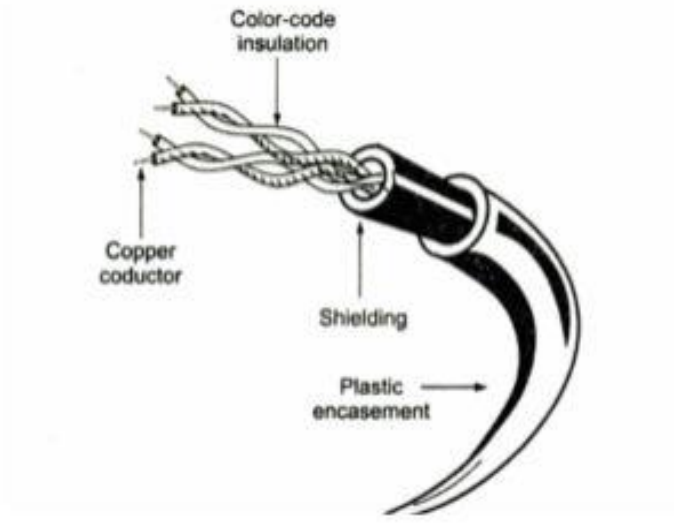


Fig 2.1.3: Shielded Twisted Pair Cable

Coaxial Cable

Coaxial cabling consists of copper conductor surrounded by dielectric insulator which is surrounded by braided metallic shield. Metallic shield is covered by layer of plastic which provides insulation between metal shield and the conductor. It is helpful in blocking intrusion from outside.

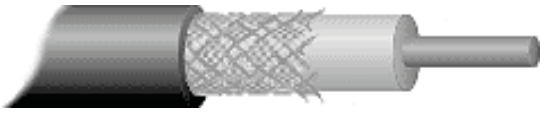


Fig 2.1.4: Coaxial Cable

There are two types of coaxial cables:

1. Thick coaxial cable
2. Thin coaxial cable

Thick coaxial cable

The specification of thick coaxial cable is 10Base5. The number 5 signifies the length of the segment as 500meters. The outer plastic covering prevents the moisture to get in contact with the conductor; because of this it is preferred for long-running lengths. These cables do not twist easily and is difficult to mount.

Thin coaxial cable

The specification of thin coaxial cable is 10 Base2. The number 2 signifies the length of the segment as 200 meters. They are commonly used in school network.

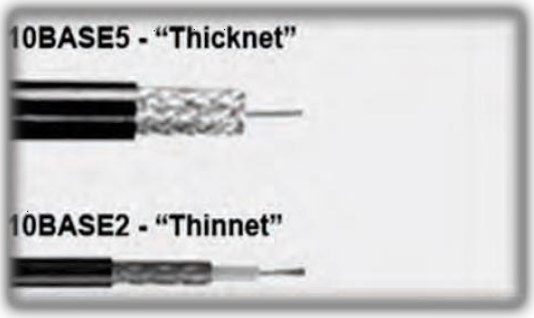


Fig 2.1.5:Thick and Thin Coaxial Cable

Fibre Optical Cable

To prevent interference, any optical fibre has a glass core in center, surrounded by numerous coatings of material for protection which is further topped with an outer layer of PVC jacket or insulating Teflon. This is for sure an expensive method when compared to others available in the market, but it has proven to be efficient in transmitting data in longer distances while ensuring good speed. This further in helpful in video conferencing and different interactive facilities.

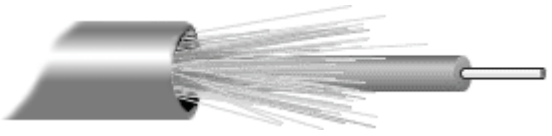


Fig 2.1.6 Fibre Optic Cable

The two types of fibre optic cables are as follows:

1. Single mode
2. Multimode

Single mode cables can provide more distance in comparison to multimode cables and is expensive, whereas, Multimode cables has larger diameter than single mode cables, however, both cables provide high bandwidth at high speeds.

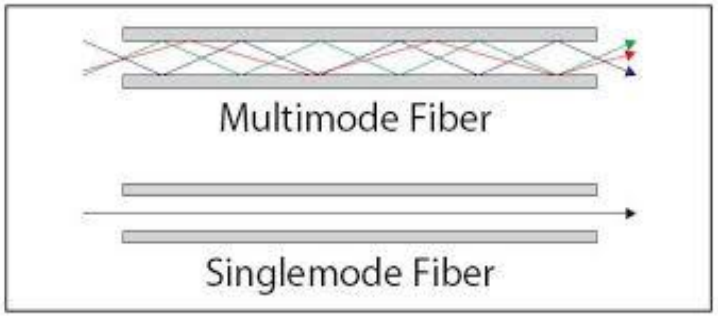


Fig 2.1.7: Single mode and Multimode Fibre

2.1.2 Connectors

A connector is a device required for connecting one device to another through interfacing of cable that plugs into a port.

Commonly used connectors are as follows:

- Registered Jack 45 (RJ45)
- Straight Tip (ST) Connector
- Lucent Connector (LC)
- Multi-fiber Push On (MPO)

RJ-45 Connector

It is an eight-wire telephone-type connector used with twisted-pair cabling for connecting computers, wall plates, patch panels, and other networking components. It is generally used with unshielded twisted-pair (UTP) and shielded twisted-pair (STP) cabling in star-topology Ethernet networks.

Fig 2.1.8: RJ-45 Connector

Straight Tip (ST) Connector

This is a straight tip, a high-performance fiber-optic connector with round ceramic ferrules and bayonet locking features. It is more commonly used than subscriber connector. These are getting slowly replaced by multi-fiber connectors (Lucent Connector and Multi-fiber Termination Push-on)

Fig 2.1.9: ST Connector

Lucent Connector

To terminate multiple fibers from high-density positioning, Lucent Connector (LC) was manufactured. LC connector is twofold connecting a pair of fibres.

Fig 2.1.10: LC Connector

Multi-fiber Push On (MPO)

MPO is also duplex connector for easy connections as it is designed to connect several times without any challenges. It is also known as Multi – Fibre Termination (MTP).

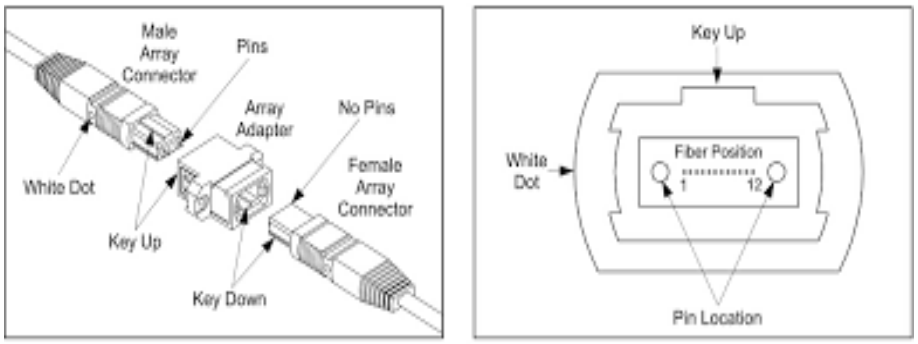


Fig 2.1.11: MPO Connector

2.1.3 PoE Devices and Network Equipment

Power over Ethernet (PoE) is a technology that enables both data and electrical power to be transmitted over the same Ethernet cable, simplifying the installation of network devices by reducing the need for separate power supplies. Understanding the specifications of PoE devices and network equipment is important for selecting, installing, and maintaining broadband networks safely and effectively.

Below is a detailed explanation of the key specifications related to PoE devices and other network equipment.

1. Specifications of PoE Devices

PoE devices are powered over Ethernet cables and are classified by their power requirements, compatibility standards, and supported features.

a. Power Standards: PoE devices follow standardized protocols to ensure compatibility between power sources (switches or injectors) and powered devices (PDs).

Fig 2.1.12: PoE Device

i. IEEE 802.3af (PoE)

- Maximum power supplied: 15.4 Watts per port.
- Voltage range: 44 – 57 V DC.
- Suitable for devices like IP phones, simple wireless access points, and basic security cameras.

ii. IEEE 802.3at (PoE+)

- Maximum power supplied: 30 Watts per port.
- Voltage range: 50 – 57 V DC.
- Supports more power-demanding devices such as advanced wireless access points and pan-tilt-zoom cameras.

iii. IEEE 802.3bt (PoE++ or 4PPoE)

- Two types: Type 3 (60 Watts) and Type 4 (90–100 Watts) per port.
- Designed for devices like LED lighting systems, video conferencing equipment, and high-performance access points.

b. Power Classification

- Devices are categorized into classes (0 to 4 or higher in newer standards) that define how much power they require.
- Example:
  - Class 0: 0.44 – 12.95 W (default classification).
  - Class 4: 12.95 – 25.5 W (higher power applications).

c. Data Transmission Speeds

- PoE devices support various Ethernet standards, depending on their purpose:
  - 10 Mbps (Ethernet) – Used in older systems.
  - 100 Mbps (Fast Ethernet) – Suitable for basic setups.
  - 1 Gbps (Gigabit Ethernet) – Common in modern networks.
  - 10 Gbps (10GBase-T) – Used for high-performance networks requiring greater bandwidth.

d. Connector Types

- Typically uses RJ45 connectors with Cat5e, Cat6, or higher-rated cables to support power and data.
- Cable quality and length affect performance; maximum recommended length is 100 meters (328 feet).

e. Protection Features

- Overcurrent Protection – Prevents damage from excessive current flow.
- Short-Circuit Protection – Detects and isolates faulty connections.
- Surge Protection – Protects against voltage spikes from lightning or other sources.
- Temperature Monitoring – Ensures devices operate within safe thermal ranges.

2. Specifications of Network Equipment

Network equipment refers to the devices that facilitate data communication and power distribution in a broadband network.

a. Switches

Fig.2.1.13: Network Switch

- Port Density: Number of Ethernet ports (typically 8, 24, 48, or more).
- PoE Support: Indicates if the switch supplies power and at what standard (802.3af/at/bt).
- Data Rate: Fast Ethernet (100 Mbps), Gigabit Ethernet (1 Gbps), or 10 Gigabit Ethernet.
- Management Type:
  - Unmanaged: Simple plug-and-play devices.
  - Managed: Offers configuration, monitoring, and advanced security features.
- Layer Type:
  - Layer 2: Handles data link layer tasks like MAC address filtering.
  - Layer 3: Supports routing functions, including IP addressing.

b. Routers

- WAN/LAN Ports: Number and type of input/output interfaces.
- Firewall and Security: Built-in protections against cyber threats.
- VPN Support: Secure remote access for users.
- Quality of Service (QoS): Prioritizes certain types of traffic for optimized performance.
- Throughput Capacity: Measures how much data can be processed per second.

Fig.2.1.14: Routers

c. Access Points (APs)

- Radio Frequency Bands:
  - Single-band (2.4 GHz) for basic coverage.
  - Dual-band (2.4 GHz and 5 GHz) for better speed and less interference.
  - Tri-band or more for high-density environments.
- Maximum Connections: Number of users or devices that can connect simultaneously.
- Security Protocols: WPA3, WPA2 encryption for secure communication.

d. Media Converters

- Convert signals between different cable types, such as fiber to copper.
- Support various network speeds and standards.
- Include features like link fault pass-through and auto-negotiation.

3. Installation and Compatibility Considerations

- Ensure PoE standards of the switch match the power requirements of connected devices.
- Use cables that meet the required category (Cat5e or higher for PoE).
- Verify that equipment can handle the total power load to avoid overloading circuits.
- Check for certifications such as IEEE compliance, safety approvals, and environmental ratings.

2.1.4 Sizes, Colors, and Categories of Network Cables

1. Different Sizes of Network Cables

- Diameter/Conductor Size:
  - Common sizes include 22 AWG, 24 AWG, and 26 AWG (American Wire Gauge).
  - 24 AWG is standard for Ethernet cables like CAT5e, CAT6.
- Outer Diameter:
  - CAT5e: ~5.0 – 6.0 mm
  - CAT6: ~6.0 – 7.0 mm
  - CAT6A: ~7.0 – 8.5 mm
- Fiber optic cables vary depending on type and layers; typical outer diameters range from 3 mm to 10 mm depending on protection layers.

2. Cable Colors

Different colors are often used for identification and organization in installations:

- Ethernet cables:
  - Blue, Gray, Black, White, Red, Yellow, Green, Orange
- Fiber optic cables:
  - Orange, Yellow, Aqua, Black, Blue
  - Some cables use industry-standard color codes to distinguish between single-mode and multimode fibers.

Note: Color does not necessarily indicate performance but is used for ease of installation and troubleshooting.

3. Categories of Network Cables

Category	Speed & Bandwidth	Shielding	Typical Use
CAT5e (Category 5e)	Up to 1 Gbps, 100 MHz	Unshielded	General office networks, home use
CAT6 (Category 6)	Up to 10 Gbps (55m), 250 MHz	Sometimes shielded	Professional networks, data centers
CAT6A (Category 6A)	Up to 10 Gbps (100m), 500 MHz	Shielded	High-performance installations, PoE networks
Fiber Optic (Single-mode, Multimode)	Up to 100 Gbps+, several kilometers	N/A	Backbone links, long-distance or high-bandwidth networks

4. Fiber Optic Cables Types

- **Single-mode Fiber (SMF):**
  - Small core (~8-10 µm)
  - Used for long-distance and high-speed communication
- **Multimode Fiber (MMF):**
  - **Larger core (50 µm or 62.5 µm)**
  - **Suitable for shorter distances such as within buildings**

2.1.5 Proper Use of Hand Tools and Power Tools in Broadband Installation

Broadband installation requires the correct use of tools to ensure efficiency, safety, and reliability. Using the appropriate hand tools and power tools for cable installation, routing, and device mounting helps prevent damage, reduce installation time, and maintain safety for technicians and end-users.

1. Hand Tools Used in Broadband Installation

Hand tools are essential for precision tasks and are typically used in environments where control and safety are paramount.

Fig. 2.1.15: Hand Tools

a. Cable Cutters

- Used to cut cables to required lengths.
- Ensure clean cuts to prevent frayed wires.
- Use insulated handles for safety when working near power lines.

b. Wire Strippers

- Remove the outer jacket or insulation from cables without damaging the internal wires.
- Adjustable stripper sizes allow use on different cable types like Cat5e, Cat6, or coaxial cables.

c. Crimping Tools

- Attach connectors (such as RJ45 plugs) to cables by compressing metal pins onto conductors.
- Requires careful alignment to ensure proper electrical contact.
- Specialized crimpers are used for Ethernet, coaxial, and fiber optic cables.

d. Screwdrivers and Nut Drivers

- Used to mount equipment like routers, switches, and wall plates.
- Insulated versions protect against accidental electrical shocks.

e. Pliers

- Grip, bend, twist, and pull cables during routing.
- Used for holding wires securely during stripping or termination.

f. Punch-Down Tools

- Insert wires into patch panels or keystone jacks.
- Ensures a secure and uniform connection without damaging the wires.

2. Power Tools Used in Broadband Installation

Power tools speed up installation tasks and are used for heavier work, such as drilling and fastening.

a. Electric Drill

- Used for mounting devices on walls, ceilings, or poles.
- Drill bits must match surface material (wood, concrete, metal).
- Always wear safety glasses when drilling to protect from flying debris.

b. Power Screwdriver

- Speeds up fastening of brackets, clamps, or mounting plates.
- Adjustable torque prevents over-tightening, which can damage equipment.

c. Cable Pullers and Fish Tapes

- Assist in routing cables through conduits, ceilings, or walls.
- Reduces strain and helps navigate long or complex pathways.

d. Heat Guns

- Used to shrink tubing or heat seals for protecting wire joints and terminations.
- Should be used with care to avoid burns or overheating cables.

Notes

UNIT 2.2: Cable Laying and Connectorisation

Unit Objectives

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

1. Define methods for accurately measuring distances to maintain permissible limits for network performance and PoE voltage drop.
2. Explain structured cabling standards for conventional and PoE-supported installations.
3. Explain the criteria for selecting suitable installation.
4. Describe crimping, splicing, and termination techniques for various cable types, ensuring proper power delivery for PoE.
5. Demonstrate how to perform cable splicing and crimping, ensuring proper termination for both standard and PoE-enabled cables.
6. Show neat wiring and clipping techniques within customer premises while following structured cabling norms.
7. Demonstrate how to test cables and joints for transmission loss and signal strength, and re-terminate if loss exceeds permissible limits.
8. Show how to properly dispose of installation waste and restore the worksite to its original condition.

2.2.1 Structured Cabling

A Structured Cabling system comprises of a set of transmission items that are collaborated with Engineering design rules. This assists in applying voice, data, and signals to maximize data rates. This technology divides the infrastructure into controllable blocks to get high-performance Network system, which is currently prevalent.

This is the most effective technology to cater to the requirement of telephone and data communication currently and will prevail in future.

The following figure lists the components of structured cabling system:

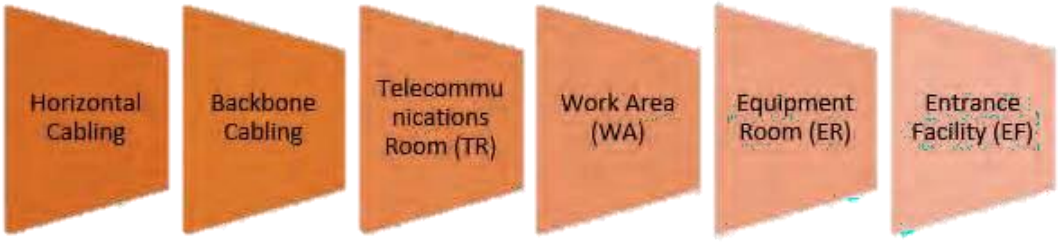


Fig 2.2.1: Components of structured cabling system

Horizontal Cabling

Any cabling, which connects floor's wiring, closed to wall plates to furnish local area network for connecting end user system to network. It is generally installed in star topology.

Backbone Cabling

It lays an association between telecommunication rooms, equipment rooms and entrance facilities. It is also called vertical cabling.

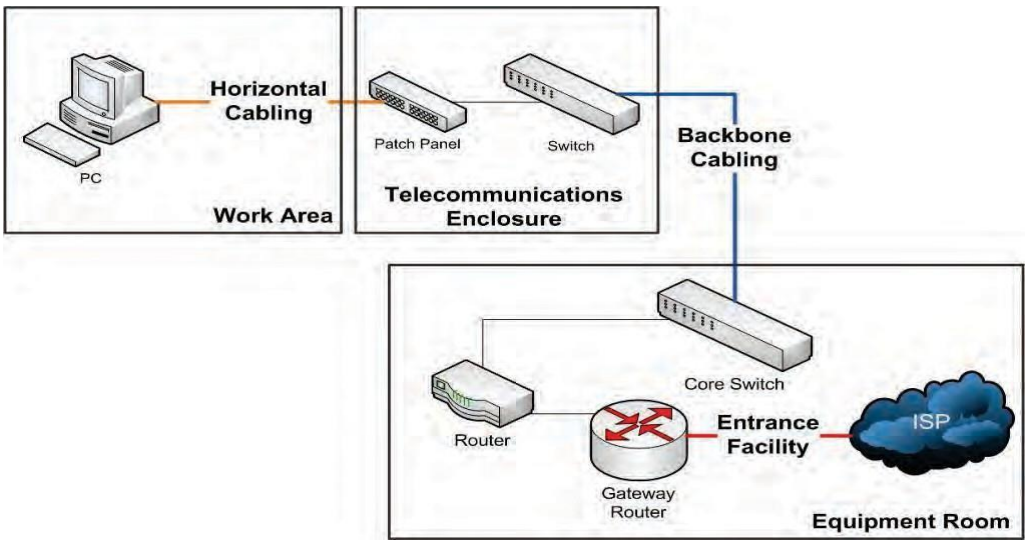


Fig 2.2.2: Structured Cabling Diagram

- **Telecommunication Room:** The area where the horizontal wiring and the backbone wiring are connected is called as telecommunications room. Each structure should have a minimum of one telecommunications room, preferably per floor where it's providing the connection.
- **Work Area:** This includes all components between the outlets of a telecommunication room to the user's workstation. It is where an individual works on his system with an attached peripheral.
- **Equipment Room:** As the name suggest, it's a room where the cables and other accessories connects with its respective electronic equipment. The complexity of the components in equipment room makes it different than telecommunications room.
- **Entrance Facility:** The area where internal and external cables connect. External cabling like, telecommunication providers, inter-building cables and antennae pathways.

2.2.2 Decision Factors in Choosing Cable for a Network

- Topology plays a critical factor in determining hardware and cables types to set up networking infrastructure
- Bandwidth is the amount of data that needs to be transferred at a given time. In any specific network, the cable with greater bandwidth provides faster information transmission
- To send the information without the use of equipment, a cable with higher signal attenuation is required in order to increase electric signal
- To avoid EMI (Electro-Magnetic Interference) while using appliances like photocopiers, fluorescent lights, and electrical wiring EMI resistant cables are preferred
- Easy installation and need for setting up additional equipment define expansion capabilities

2.2.3 Connectorisation

TIA/EIA 568A Wiring Sequence

- In both the 568A and 568B sequences, pair 1 and pair 4 refer to the blue wires and brown
- wires respectively. The following figures show the connections:

Pair 1 is allocated to pins 4 and 5.

- Blue wire connects to pin 4, as a ring (R) wire
- White wire of the blue pair connects to pin 5, as an IP (T) wire.

Pair 4 is allocated to pins 7 and 8 of the connector.

- The white wire of the brown pair connects to pin 7, as the IP wire
- The brown wire connects to pin 8, as the ring wire.

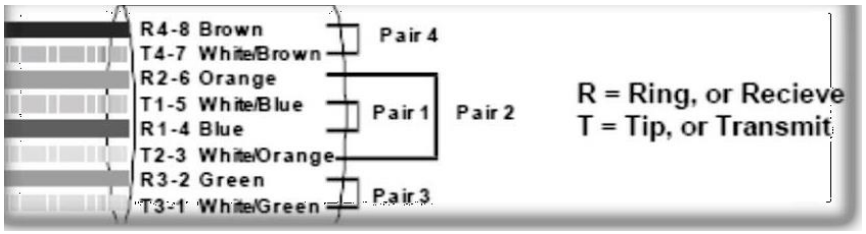


Fig 2.2.3: Wiring Sequence 1

The terms IP and ring are classic terms used for labelling the IP and ring (The retort is what is heard on the recipient end once the number is dialed).

If the network is set in a way that it uses 10 Mbps bandwidth, you may not need to use the blue and brown sets. In a scenario like this you may use the blue pair for transmission of voice and for network roles, use the brown pair. The position of pins numbering 1,2,3 and 6 which are the green and orange sets are categorically used for transmitting Ethernet through Pin 1 and pin 2 for receiving, number 3 and 6 pins sets are used.

TIA/EIA 568B Wiring Sequence

In the T568A arrangement, pin number 1 and 2 is allocated to the green pair while the orange pair is divided between pin 3 and 6. In T568B order is an opposite arrangement of T568A where the green pair splits between 3 and 6 pin, and the orange pair is allotted to pins 1 and

Fig 2.2.3: Wiring Sequence 1

PairS 2 and 3 are ASSIGNED to Different PINS

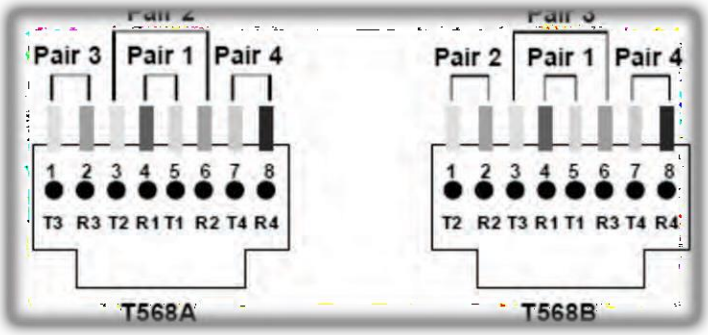


Fig 2.2.5: Wiring Sequence 3

We will discuss this topic further in coming sessions as well.

Crimping Cable

Cut, stripe, and crimp an exposed pair of category 5 cable, and attach to RJ-45 connector. After the completion of this task, you will be required to test your cables for connection.

Required Materials

- Category 5 UTP Cable
- Two (2) RJ-45 Connectors Crimping Tool (model 24 -4680P, or equivalent)
- Cable Tester (Brand and model in equipment package, or equivalent)

Procedure

Keep a record for portfolio. While following these steps record problems and major observations.

To become a suitable candidate for employment one must be aware of the conversing issues and solutions, using the following steps:

1. Compare individual crimping tool with the one illustrated below:

The image shows a tool with blades for cutting and stripping and connectors RJ-45 and RJ -11, which is used mainly for six wire telephone cable. In case all the given features are not available in a particular crimping tool, then in such situation one may need to use two or more tools, for example, a separate wire cutter and/or stripper.

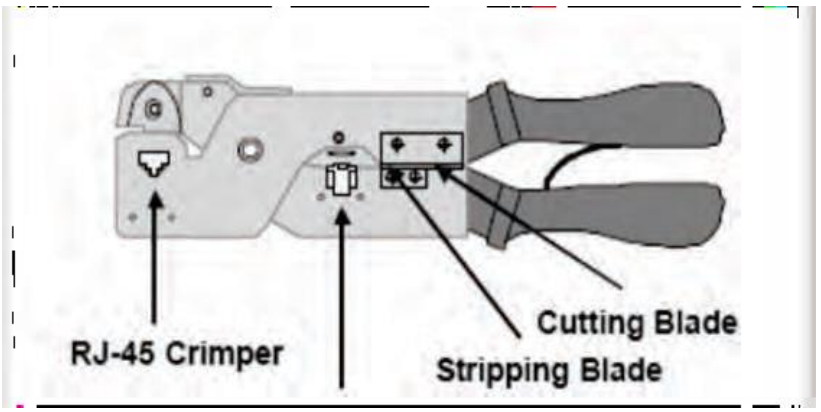


Fig 2.2.6: Crimping tool – Parts

2. Cut the category 5 UTP is specified length.
Ends should be cut in square rather than diagonal. Insert the cable in between the cutting blades and close the blades after squeezing the crimper handle firmly.

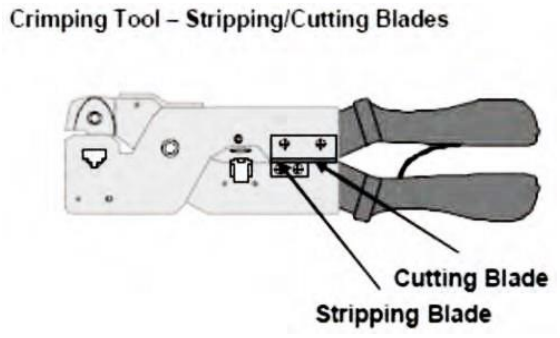


Fig 2.2.7: Crimping tool – Blades

3. To strip of the outer covering, one must pull -out the end of the cable with the backstop. The stop plays an important role in averting more insulation from the cable. Now jam with an uninterrupted pressure but be careful while applying the pressure as to much of it will cut the wires. Next the plastic insulation shield should be revolved to cut the wire.

4. You should have four pairs of wires which makes a total of eight single wires, if you don't have these number then the missing number was accidentally cut while stripping and, in such case, you will have to repeat point number 3.

5. Carefully observe the RJ-45 connector. One will be able to see the two sides:
- one side shows the plastic locking clip
- other side will show eight metallic pins.
- The pins will be marginally raised above the surface.

6. Be careful and observant while inserting these eight wires into the connector.

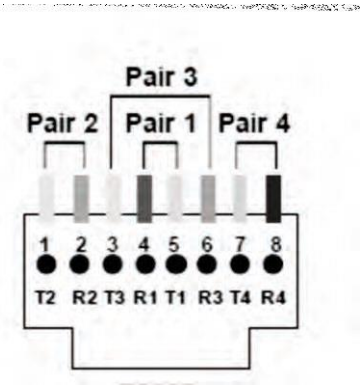


Fig 2.2.8: T568B Wiring Sequence

7. Ensure every wire fits in their eight separate respective slots. To ease this process, separating the wires is recommended.

7. Insert the cables with a firm and steady pressure. Each wire at the end must reach the metal pin of the connector.

8. The complete assembly of connector should reach RJ-45 slot. In order to fold these wires one can use the teeth of the crimper.

We will discuss crimping further in coming sessions as well.

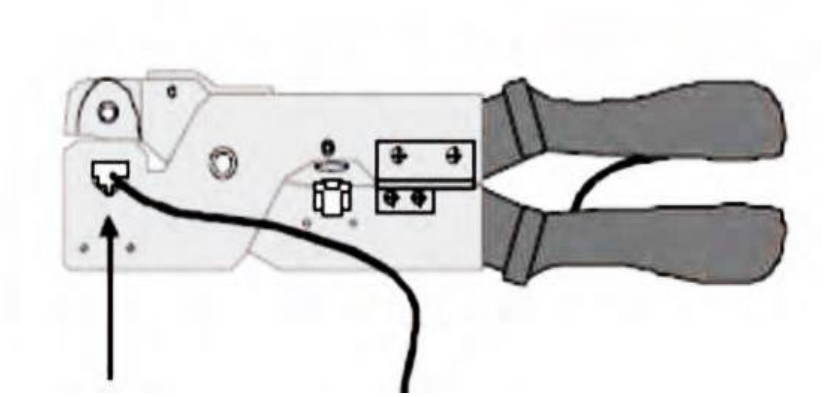


Fig 2.2.9: RJ-45Crimper

9. To check if the respective wire is crimped as desired, check the metal pins. If they are not raised on the connector that means they are cut in the desired manner, if not then redo the same process.

10. Be sure to record the colour sequence of these wires on the sheet with the right sequence. Use the portfolio-recording sheet for filling the colour sequence as revealed in below table. Hold the connector in such a way that the metal contact pins are facing you and the locking clip are on the other side. Record the wire colours from each end.

Pin 1 Colour	Pin 2 Colour	Pin 3 Colour	Pin 4 Colour	Pin 5 Colour	Pin 6 Colour	Pin 7 Colour	Pin 8 Colour

Fig 2.2.9: Recording the colours

11. For the other end of the cable, repeat steps 3 through 11.

Pin 1 Colour	Pin 2 Colour	Pin 3 Colour	Pin 4 Colour	Pin 5 Colour	Pin 6 Colour	Pin 7 Colour	Pin 8 Colour

Fig 2.2.10: Re-recording the colours

12. Present your cable along with the table for the wire colour to your instructor for inspection and clearance for testing using the cable tester.

2.2.4 Structured Cabling Standards

Structured cabling is governed by widely accepted standards such as:

- TIA/EIA-568: Telecommunications Industry Association and Electronic Industries Alliance standards defining commercial building cabling specifications.
- ISO/IEC 11801: International standard for generic cabling systems.
- NEC (National Electrical Code): Guidelines for electrical safety during installation.

These standards ensure uniform installation practices across buildings and data centers.

1. Conventional Installations

In conventional structured cabling:

- Cable Types: CAT5e, CAT6, or fiber optic cables are commonly used.
- Topology: Star topology is preferred, where cables run from a central patch panel or network closet to individual devices.
- Cable Pathways: Includes conduits, trays, or cable management systems to avoid interference and ensure safety.
- Patch Panels and Jacks: Used for managing connections and rerouting signals easily.
- Performance Specifications:
  - Bandwidth requirements up to 1 Gbps or 10 Gbps depending on the cable type.
  - Distance limits (e.g., Ethernet cables are typically restricted to 100 meters per link).
- Testing: Includes signal continuity, crosstalk, and attenuation checks.

2. PoE (Power over Ethernet) Supported Installations

PoE-supported structured cabling builds upon conventional installations but adds power delivery through the same cable that carries data.

Key Considerations:

- Standards:
  - IEEE 802.3af (PoE) – up to 15.4W
  - IEEE 802.3at (PoE+) – up to 30W
  - IEEE 802.3bt (PoE++) – up to 60W/100W depending on implementation.
- Cable Requirements:
  - CAT5e or higher is required for better power handling and reduced heating.
  - Shielded cables may be used in environments with higher interference.
- Installation Guidelines:
  - Ensure cable runs are within permissible lengths to avoid voltage drops.
  - Avoid sharp bends or excessive strain that can damage cables or reduce power efficiency.
  - Proper grounding and separation from high-voltage lines are critical to prevent interference and hazards.
- Equipment Compatibility:
  - Use PoE switches, injectors, and powered devices (IP cameras, phones, access points) that comply with IEEE standards.
- Testing and Certification:
  - Validate power delivery, signal integrity, and safety compliance using specialized PoE testers.

3. Differences Between Conventional and PoE Installations

Aspect	Conventional Cabling	PoE-Supported Cabling
Purpose	Data transmission only	Data and power transmission
Cable Type	CAT5e, CAT6, fiber	CAT5e or higher with PoE compliance
Standards	TIA/EIA-568, ISO/IEC 11801	IEEE 802.3af/at/bt in addition to cabling standards
Installation	Basic pathways and connectors	Enhanced planning for power delivery, grounding, and heat management
Testing	Signal continuity and interference	Includes power tests and voltage drop verification

2.2.5 Cable Installation, Routing, and Device Mounting Guidelines

1. Planning the Route

- Map out cable pathways before installation.
- Avoid sharp bends and interference from power lines or metal objects.
- Keep cables organized using cable ties, clips, or trays.

2. Routing Cables

- Use fish tape to pull cables through confined spaces.
- Avoid tight bends (maintain a bend radius at least four times the cable diameter).
- Label cables clearly to identify endpoints.

3. Device Mounting

- Secure mounting brackets firmly using appropriate anchors.
- Keep devices elevated and ventilated to prevent overheating.
- Use protective covers in outdoor installations to shield from weather.

4. Safety Precautions

- Always wear PPE such as gloves, safety glasses, and helmets.
- Power off circuits before working with cables carrying current.
- Use insulated tools when handling live components.

2.2.6 Crimping, Splicing, and Termination Techniques

Proper cable termination ensures signal integrity and power delivery, especially for PoE applications where data and power share the same line.

1. Crimping Techniques

Crimping secures connectors to the cable ends by compressing them tightly.

Steps:

- Strip the cable jacket and untwist the wire pairs.
- Insert the wires into the connector following the correct pinout (e.g., T568A or T568B standard).
- Use a crimping tool to press the pins firmly into the wires.
- Inspect the connection for proper seating and secure locking.

Important Considerations:

- Ensure wires are fully inserted before crimping.
- Use the right crimping tool for the connector type.
- Verify continuity with a cable tester.

2. Splicing Techniques

Splicing joins two or more wires when cables are extended or repaired.

Steps:

- Strip the cable insulation on both ends.
- Align wires by color coding or number.
- Twist wires together and wrap with electrical tape, or use wire nuts or gel-filled splice kits for protection.
- Apply heat shrink tubing over the joint to seal and protect the splice.

Best Practices:

- Ensure no exposed wires remain after splicing.
- Use moisture-resistant materials for outdoor installations.
- Avoid unnecessary splices to reduce signal degradation.

3. Termination Techniques

Termination refers to connecting cables to devices like patch panels, switches, or connectors.

For Ethernet Cables:

- Use punch-down tools to press wires into insulation displacement connectors.
- Follow wiring standards consistently to ensure cross-device compatibility.

For Coaxial Cables:

- Trim the outer jacket and shield to expose the inner conductor.
- Slide the connector over the prepared cable and crimp the ferrule to secure the shield and conductor.

For Fiber Optic Cables:

- Clean and prepare the fiber by stripping the protective layers.
- Use specialized connectors and polishing techniques to ensure minimal signal loss.
- Test the termination with an optical power meter.

Ensuring Proper Power Delivery for PoE

1. **Selecting the Right Cable**
   - Use Cat5e or higher-rated cables to support PoE power levels.
   - Ensure cables are certified for PoE applications to handle voltage and current without overheating.
2. **Maintaining Correct Termination**
   - Crimp connections must be tight to prevent resistance and power loss.
   - Avoid loose or misaligned connectors, which can reduce power efficiency.
3. **Minimizing Signal Interference**
   - Keep data and power lines separated from electrical cables.
   - Avoid sharp bends or compressions that could damage insulation.
4. **Testing the Installation**
   - Use a PoE tester to confirm power is delivered correctly to the device.
   - Verify data transmission by testing continuity and signal strength.

2.2.7 Accurately Measuring Distances to Maintain Permissible Limits for Network Performance and PoE Voltage Drop

In broadband installations, it is essential to accurately measure cable lengths and distances to ensure network performance, signal integrity, and proper power delivery—especially in Power over Ethernet (PoE) systems. Exceeding distance limits can result in excessive voltage drop, data degradation, and network failures. This section explains methods for measuring distances accurately to maintain permissible limits.

1. Importance of Accurate Distance Measurement

- Network Performance: Excessive cable lengths can introduce latency, signal attenuation, and crosstalk, which degrade data transmission quality.
- PoE Voltage Drop: Power losses occur due to resistance in cables. Longer distances cause higher voltage drops, potentially resulting in insufficient power at devices like IP cameras or access points.
- Compliance with Standards: Industry standards, such as 100 meters (328 feet) for Ethernet cables, ensure consistent and reliable network installations.

2. Methods for Measuring Distances

Physical Measurement with Tape or Laser Distance Meter

Description:

A tape measure or laser distance meter is used to physically measure the length of cable runs or the distance between network devices.

Usage Steps:

1. Stretch the tape measure along the cable path, accounting for bends or corners.
2. For complex installations, a laser distance meter offers greater accuracy by measuring straight-line distances, which can then be adjusted to the actual routing path.

Advantages:

- Simple, cost-effective.
- Easy to use in confined or open spaces.

Best Practices:

- Account for bends, corners, or obstacles that increase the effective cable length.
- Confirm measurements before cable installation.

b. Cable Length Testers (Time-Domain Reflectometers - TDR)

Description:

A TDR measures the time it takes for an electrical signal to travel through the cable and reflect back from the endpoint.

Usage Steps:

- Connect the tester to one end of the cable.
- Send a test signal and observe the time delay.
- The tester calculates the cable length based on signal speed.

Advantages:

- Provides accurate measurements without physically inspecting the entire run.
- Can detect faults, breaks, and impedance changes.

Best Practices:

- Use TDRs that support the specific cable type (Cat5e, Cat6, etc.).
- Regularly calibrate the device for accurate readings.

c. Optical Time-Domain Reflectometer (OTDR) for Fiber Links

Description:

Used for fiber optic cables, the OTDR sends light pulses and measures reflections to determine length and detect faults.

Usage Steps:

- Connect the OTDR to the fiber cable.
- Launch test pulses and review the reflection profile.
- Identify distance to connectors, splices, and faults.

Advantages:

- Highly precise for long-distance fiber networks.
- Detects signal loss, bends, and breaks.

Best Practices:

- Clean connectors before testing.
- Verify test results at multiple points for consistency.

d. Manufacturer-Supplied Distance Limits and Specifications

Description:

Device manuals or installation guides often specify maximum allowable cable lengths for both data and power delivery.

Usage Steps:

- Refer to the product documentation.
- Cross-check planned distances against permissible limits.
- Factor in safety margins (typically 10% to 20% less than the maximum limit).

Advantages:

- Ensures compatibility and avoids guesswork.
- Helps in planning installations ahead of time.

Best Practices:

- Confirm standards for both Ethernet data and PoE power requirements.
- Avoid routing near sources of interference that may reduce effective distance.

e. Software Tools and Network Mapping

Description:

Network design tools and mapping software allow technicians to plan cable routes and calculate lengths before installation.

Usage Steps:

- Use architectural drawings or floor plans.
- Trace cable paths and input measurements.
- Automatically compute distances and check compliance.

Advantages:

- Helps in planning complex installations.
- Provides documentation for audits and maintenance.

Best Practices:

- Incorporate real-world obstacles like walls, ducts, and furniture.
- Update maps after installation for future troubleshooting.

3. Maintaining Permissible Limits for PoE Voltage Drop

Key Considerations

1. Cable Type and Gauge

- Higher gauge cables (thicker wires) reduce resistance and voltage drop.
- Cat6 or Cat6a cables are preferred for longer runs requiring PoE.

2. Total Length

- Keep cable runs within the recommended maximum of 100 meters (328 feet).
- For distances nearing the limit, consider using PoE extenders or mid-span injectors.

3. Power Classification

- Match device power requirements with available PoE power at the distance in question.
- Use lower power devices or multiple power sources for longer runs.

4. Monitoring Tools

- Use PoE testers to measure voltage and current at endpoints.
- Detect excessive drops before they result in failures.

2.2.8 Selecting Suitable Installation in Broadband Networks

Choosing the correct installation approach is critical to ensuring that broadband networks operate efficiently, safely, and reliably. A poorly planned or executed installation can lead to signal degradation, power loss, equipment damage, and customer dissatisfaction. The selection of a suitable installation depends on various technical, environmental, and operational factors. Below is a structured explanation of the key criteria for selecting the most appropriate installation method in broadband networks.

1. Network Requirements and Performance Goals

a. Bandwidth and Data Rate Needs

- Evaluate the expected data load, number of users, and types of applications (e.g., streaming, cloud computing).
- Choose cables and devices that support the required throughput without bottlenecks.

b. Power Requirements (Especially for PoE Installations)

- Determine the power consumption of devices like IP cameras, wireless access points, or sensors.
- Select installation methods that ensure proper power delivery over the intended cable length without excessive voltage drop.

c. Reliability and Uptime

- Consider whether the network needs to operate continuously, such as in hospitals or financial institutions.
- Choose installation methods that minimize interference, downtime, and maintenance requirements.

2. Cable Type and Distance Constraints

a. Cable Category

- Select Cat5e, Cat6, Cat6a, or fiber optic cables based on speed requirements and expected interference.
- Higher categories offer better shielding and support for longer distances.

b. Maximum Cable Length

- Ensure cable runs do not exceed recommended distances (e.g., 100 meters for Ethernet).
- For longer runs, consider using signal boosters, PoE extenders, or alternate routing.

3. Environmental Factors

a. Indoor vs Outdoor Installation

- Indoor environments require protection from furniture, moisture, and electrical interference.
- Outdoor installations must account for weather, UV exposure, temperature variations, and rodents.

b. Physical Obstacles

- Walls, ceilings, floors, ducts, and existing infrastructure can affect routing options.
- Installations should avoid sharp bends and ensure cable protection through conduits or trays.

c. Electromagnetic Interference (EMI)

- Identify sources like power lines, motors, or heavy equipment that may disrupt signals.
- Use shielded cables or reroute pathways to reduce interference.

4. Safety and Compliance

a. Electrical Safety

- Ensure that installations meet grounding, surge protection, and insulation standards.
- Avoid routing cables near high-voltage lines without proper shielding.

b. Regulatory Compliance

- Follow national and local codes such as NEC, ISO/IEC standards, or telecommunications regulations.
- Obtain required permits for outdoor or large-scale installations.

c. Worker Safety

- Plan installations that reduce risks from heights, confined spaces, or hazardous conditions.
- Use appropriate PPE and tools for secure and compliant installation.

5. Scalability and Future Growth

a. Anticipated Expansion

- Install with additional capacity for future devices and increased bandwidth.
- Use modular designs and structured cabling systems to facilitate upgrades.

b. Ease of Maintenance

- Select installation paths that are accessible for troubleshooting and repairs.
- Label cables and document the layout for efficient network management.

6. Cost and Resource Availability

a. Budget Constraints

- Balance installation quality with available financial resources.
- Prioritize critical areas for high-performance equipment while using cost-effective options elsewhere.

b. Availability of Skilled Personnel

- Choose installation methods that match the expertise of available technicians.
- Complex installations may require specialized training or external contractors.

7. Aesthetic and Structural Considerations

a. Concealed vs Exposed Installations

- Indoor setups often need to be aesthetically pleasing and blend with interior décor.
- Exposed installations require proper shielding and secure mounting.

b. Structural Integrity

- Avoid compromising walls, ceilings, or building infrastructure during installation.
- Use brackets, conduits, and clamps to secure cables without damaging surfaces.

8. Customer Expectations and Application Use

a. Residential vs Commercial Needs

- Residential users may prioritize ease of setup and minimal visible cabling.
- Commercial or industrial users may require robust networks for high usage and environmental resilience.

b. Type of Application

- High-definition video streaming, telemedicine, remote offices, or smart home systems demand tailored installation approaches.

2.2.9 Testing Cables and Joints for Transmission Loss and Signal Strength, and Re-Terminating if Loss Exceeds Permissible Limits

In broadband installations, ensuring proper signal strength and minimal transmission loss is critical for network performance and reliability. Cables and joints must be tested after installation and during maintenance to verify that they meet performance standards. If excessive loss is detected, corrective actions such as re-termination must be performed.

Below is a structured explanation suitable for textbook content covering how to test cables and joints and how to re-terminate if necessary.

1. Why Testing is Important

- Detects faults or weak connections that could cause intermittent signals or outages.
- Ensures compliance with industry standards, such as maximum allowable attenuation or signal loss.
- Prevents network downtime by addressing problems early.
- Verifies power delivery for PoE to avoid device malfunction due to insufficient voltage.

2. Tools Used for Testing

a. Cable Testers

- Check continuity, shorts, open circuits, and wire mapping.
- Suitable for Ethernet cables (Cat5e, Cat6, etc.).

b. Time Domain Reflectometer (TDR)

- Measures distance to faults, cable length, and impedance changes.
- Identifies breaks, splices, and discontinuities.

c. Optical Power Meter and Light Source (for Fiber Optic Cables)

- Measures signal strength and power loss across fiber links.
- Provides pass/fail indicators based on standards.

d. PoE Testers

- Measures voltage and current at powered devices.
- Ensures that power delivery meets device requirements.

3. Testing Procedure for Cables and Joints

Step 1 – Visual Inspection

- Check cable insulation for cuts, abrasions, or kinks.
- Inspect joints and connectors for loose or corroded contacts.

Step 2 – Continuity Test

- Use a cable tester to confirm that each wire is connected end-to-end.
- Verify that there are no open or short circuits.

Step 3 – Measure Transmission Loss (Attenuation)

- For Ethernet cables:
  - Use a TDR to send signals and measure reflections caused by impedance mismatches.
  - Compare results with permissible limits (e.g., ≤ 2 dB for certain frequencies).

- For fiber cables:
  - Connect a light source at one end and a power meter at the other.
  - Measure how much signal is lost over the length.
  - Check that the loss does not exceed specified limits (e.g., ≤ 0.3 dB/km).

Step 4 – Check Signal Strength

- Use appropriate testers to confirm that signals are within operating thresholds.
- For PoE installations, verify that voltage at the endpoint is sufficient (e.g., ≥ 44V for 802.3af).

Step 5 – Perform Functional Testing

- Run data traffic or ping tests to verify stable communication.
- Ensure that signal interruptions or latency issues are not present.

4. Interpreting Test Results

Parameter	Permissible Limit Example	Action if Exceeded
Ethernet attenuation	≤ 2 dB at 100 MHz	Re-terminate or replace cable
Fiber optic loss	≤ 0.3 dB/km	Clean connectors, re-terminate, or replace segment
PoE voltage	≥ 44V	Re-terminate, upgrade cabling, or shorten run

5. Re-Termination Procedure if Loss Exceeds Limits

Step 1 – Identify Faulty Segment

- Use TDR or visual inspection to pinpoint the location of signal degradation.

Step 2 – Prepare the Cable

- Cut off the defective portion ensuring at least a few inches are removed beyond visible damage.
- Strip the cable jacket carefully without nicking the wires inside.

Step 3 – Re-Terminate the Cable

- Align wires according to wiring standards (e.g., T568A or T568B).
- Insert wires into connectors and use a crimping tool to secure them.
- For fiber cables, clean the fiber ends, cleave them properly, and attach connectors following industry protocols.

Step 4 – Protect the Joint

- Use heat shrink tubing, tape, or enclosures to shield the joint from moisture, dust, and mechanical strain.

Step 5 – Retest the Cable

- Repeat the continuity, attenuation, and signal strength tests to ensure that performance is restored within permissible limits.
- Document the test results for quality assurance.

Notes

UNIT 2.3: Customer Premise Equipment

Unit Objectives

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

1. Describe the functions, features, and configurations of customer premise equipment, including modems, routers, PoE switches, IP cameras, and VoIP phones.
2. Explain troubleshooting methods for CPE, including resolving power and connectivity faults in PoE-supported devices.
3. List different diagnostic tools such as LAN testers, PoE testers, and network analyzers, and explain their safe handling and usage.
4. Demonstrate how to install and configure equipment such as modems, routers, PoE switches, IP cameras, and VoIP phones, ensuring proper functionality.
5. Demonstrate how to guide customers on using installed equipment, including PoE-enabled devices.

2.3.1 Modem

A modem is a hardware device that converts binary signals to analog auditory signals and allows transmission over the telephone lines. Data is transmitted in an intermittent packet and at the receiving end data is extracted from packets and reassembled.

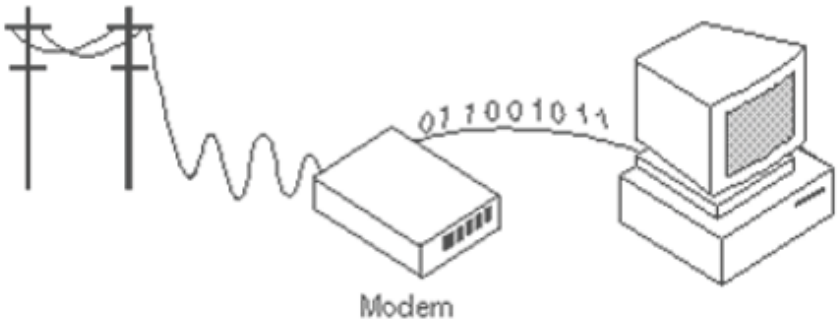


Fig 2.3.1: Modem

Modulation is converting to an analog signal. Demodulation is the reverse process of converting the analog signal back to binary signal.

For better understanding let's take the following example:

Consider a computer that has been given a command to view a website/webpage on a browser. A digital request is accepted by the modem from the computer, which further alters it to an analog signal. The answer to the request in analog form, returns to the modem, once the request is accepted. The answer signal is, converted to digital form by the modem, and finally sent it back to the computer. In simple words a modem converts an analog signal to digital.

It may strike you why there is idleness in converting analog to digital signals. The simple answer is– telephone lines have limitations while carrying digital signals and on the other hand our computers are limited to only understand 1s and 0s, as the digital signals. The solution is explained further.

Modem Types

- External - connected outside system using a serial cable
- Internal - mounted to an expansion slot of motherboard
- Wireless – connected without cable; uses radio frequency to transfer data
- Dial-up – connected through ISP to computer using telephone line
- Cable – system communicates with ISP over a landline connection
- DSL - connect to a computer or router through Ethernet or USB port
- Satellite – uses satellite technology for data transmission
- Half – duplex - sends and receives signals in an alternate fashion
- Full – duplex - capable of consecutively handling two separate signals at the same time while using two carriers each of which transmits and receives data

How does a modem work?

A modem holds the following three components:

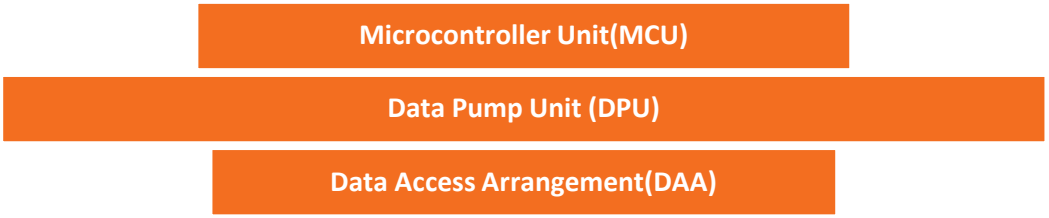


Fig. 2.3.2: Components of Modem

Microcontroller Unit (MCU) – It is required for data compression and error checking. It also converts parallel transmission to serial.

Data Pump Unit (DPU) - It communicates with ROM and receives commands and settings.

Data Access Arrangement (DAA) – It acts as an interface to Public switched telephone system (PS)

Fig. 2.3.3: Components of Modem

2.3.2 Router

Hardware that is used to route data from local area network to a specific network connection is called a Router. Data here refers to files, communications, and transmissions. Most of these routers keep logs of the activity of the particular network.

Routers yield information through broadband signals via a modem then decode it and further deliver it to the computer. It is capable of reading sender's details, data type, size, Internet Protocol address (IP address).

Since a router can connect two or more networks and runs on OSI (Open Systems Interconnection) model that's the reason it's called a Layer 3 gateway device.

Usually, residents use wireless or wired Internet protocol router. The home local area network (LAN) is connected to a wide-area network (WAN) via either a DSL or cable modem.

Types of Routers

- **Core router:** They are used by service providers (i.e., AT&T, Verizon, Vodafone) or cloud providers (i.e., Google, Amazon, Microsoft). Large enterprises use these routers as they have the capability of generating maximum bandwidth to connect across.
- **Edge router:** They are known as gateway as they are connected with external networks. They are used for optimizing bandwidth and connect to other routers for distributing data.
- **Distribution router:** It receives data from wired connection and shares it with users via Wi-Fi.
- **Wireless router:** It is a combination of edge routers and distribution routers. They are commonly used for home networks and access to Internet.
- **Virtual router:** To cater to large business needs where complexities are high, these routers provides services in the cloud.

2.3.3 Modem vS. Router

Parameters	Modem	Router
Definition	It is a device that modulates and demodulates the electrical signal and maintains a dedicated connection between the Internet and network	It is a networking device that enables multiple devices to connect to wired or wireless networks
Operating Layer of OSI model.	It works on the data link layer of the OSI model	It works on the physical, data-link, and network layers of the OSI model
How does it work?	It modulates the electrical signal to a digital signal and sends it to system, demodulates the signal from digital to analog, and sends it to the Internet	It follows routing table to transfer data packets from one source to another. It permits several network devices to connect over the network

Security	There is no authentication check happens for the data	There is complete security through passwords to transmit data packets over a network.
Cable Used	RJ45 is used to connect with router and RJ11 to connect to telephone line	RJ45 cable is required
Placed	Between the telephone line and computer or router	Between modem and other networking devices
Internet Access	Essential to access the Internet as it connects the ISP to system	One can access Internet without using a router
Number of connected devices	Connected to only one device that can be either a computer or a router	Can connect to multiple network devices using Ethernet cable or Wi-Fi
Ports	Essentially two ports are required	Can have 2 to 4 ports

Table 2.3.1 Modem vS. Router

2.3.4 Network Switches

Network switch is a hardware or software-based device that connect devices in a network to each other and transmit data packets. Devices such as printers, computers and servers, which are placed within premises or at a particular site. It acts as a controller, permitting networked devices to connect to each other efficiently, thereby increasing productivity of employees.

On an Ethernet LAN, from the physical address of a device, called MAC (Media Access Control) address in each incoming message frame, a switch determines which output port to forward it to. In Internet which can be considered as wide area packet - switched network, a switch figures out which IP to use for its next destination travel.

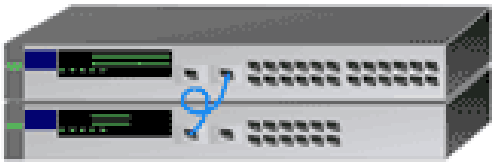


Fig 2.3.7: Network switches

In the Open Systems Interconnection (OSI) communications model, a switch makes the route easier by simply identifying the data unit through its physical address and moves it towards that device. Newer switches that start performing the routing functions are at times called as IP switches.

The number of routers passed by a data packet is called a hop. The time used in figuring the destination of a data unit is called latency. So that's why switches are considered to be the backbone of the gateway at the junction where once network is connected to another, known as core switches, and the sub levels where the transfer or travel of data is done to its origin or destination known as desktop switches.

Types of Ethernet Switches

- Unmanaged Switches: A switch that works for basic connectivity and doesn't need any configuration or installation is called unmanaged switched. Usually, these are used in home networks and they have partial network capacity when compared to managed switches.
- Managed Switches: A managed network can be configured and offers scalability and maximum security. Such switches permit monitoring and can be adjusted locally or remotely.
- LAN Switches: Switches that are used to connect points on LAN are termed as LAN switches. They are used to reduce network congestion by allocating data packets to its proposed receiver.
- PoE Switches: They are used for PoE technology that integrates data and power on same cable. Through these switches, greater flexibility is provided.

2.3.5 Network SwitcheS VS. Router

Network is created by switches that are further connected by routers. Router picks the most suited way for flow of information in a way that it is received swiftly.

Routers are more sophisticated devices when compared to a switch. Traditional routers are used in multiple area networks, i.e. LANs and WANs. The network traffic flows through routers.

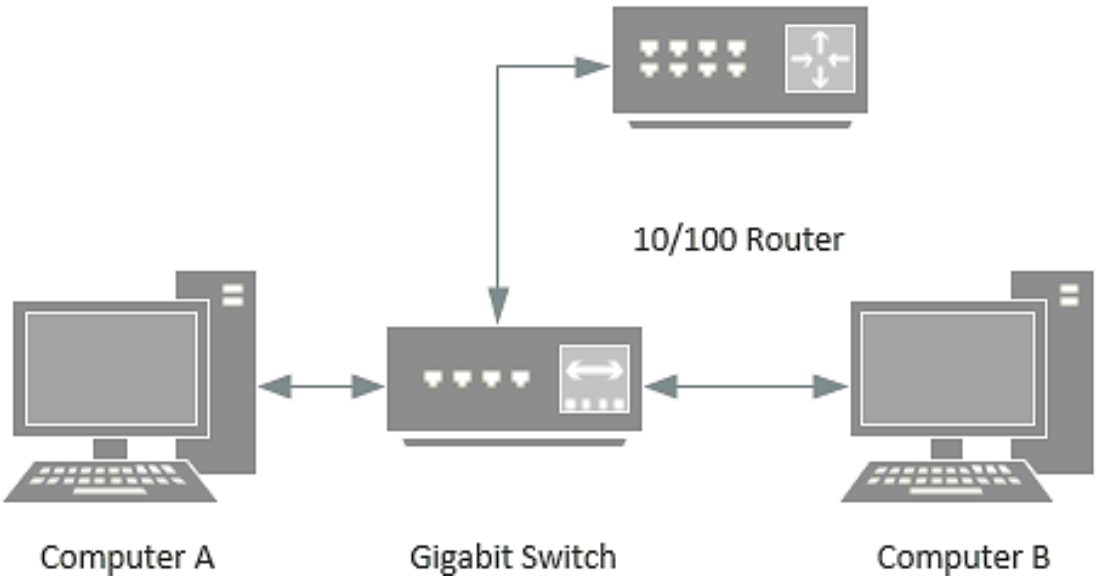


Fig 2.3.8: Network Connectivity through Switch and Router

Switch	Router
It connects multiple networked devices	It connects multiple switches & their respective networks.
It works on the data link layer of the OSI model	It works on the network layer of the OSI model
It is used within a LAN	It can be used in LAN or MAN
It cannot perform Network Address Translation	It can perform Network Address Translation.
The switch takes a long time while making complicated routing decisions	A router can take a routing decision much faster
It provides security to ports only	It provides security measures to protect the complete network
It works in either half or full-duplex transmission mode	It works in the full-duplex transmission mode and per need can be changed to half-duplex mode
It sends information in the form of Frames (for L2 switch) and the form of packets (for L3 switch)	It sends information in the form of data packets
Switches can only work with the wired network	Routers can work with both wired & wireless networks

Table 2.3.2 Switch vS. Router

2.3.6 Diagnostic Tools Used in Broadband Installation and Maintenance

In broadband networks, diagnostic tools are essential for testing, troubleshooting, and ensuring optimal performance. These tools help technicians detect faults, measure signal strength, and verify power delivery without guesswork. Below is a structured list of commonly used diagnostic tools and explanations of their safe handling and usage.

1. LAN Testers:

LAN testers are used to verify the integrity and connectivity of Ethernet cables. They check continuity, wiring order, shorts, open circuits, and crosstalk.

Fig 2.3.9: LAN Tester

Common Types

Basic Cable Tester – Verifies wiring and continuity.

Advanced Cable Analyzer – Measures signal strength, insertion loss, and noise interference.

Safe Handling and Usage

- Always disconnect the cable from live circuits before testing to prevent electrical damage or injury.
- Use insulated leads and ensure the tester is properly grounded.
- Follow manufacturer instructions for calibration and connection.
- Keep the device in a dry and clean environment to prevent moisture-related malfunctions.

2. PoE Testers:

PoE testers measure voltage, current, and power availability over Ethernet cables. They ensure that devices like IP cameras and wireless access points receive sufficient power.

Fig 2.3.10: PoE Tester

Functions

- Verify that power is present and within safe operating limits.
- Detect miswired or overloaded circuits.
- Confirm compatibility with PoE standards (802.3af, at, or bt).

Safe Handling and Usage

- Do not insert the tester into a live or unstable circuit unless specified by the manufacturer.
- Use devices with proper surge protection, especially in environments prone to voltage spikes.
- Handle connectors carefully to avoid damaging pins or sockets.
- Wear protective gloves when working in areas with exposed wiring.

3. Network Analyzers:

Network analyzers monitor data traffic, signal quality, bandwidth usage, and latency. They are used to diagnose network problems and optimize performance.

Fig 2.3.11: Network Analyzer

Common Types

- Packet Analyzers – Capture and inspect data packets.
- Throughput Analyzers – Measure data transfer rates.
- Latency and Jitter Testers – Identify delays and instability.

Safe Handling and Usage

- Ensure that test probes or interfaces are connected to the correct ports to prevent misrouting signals.
- Avoid installing analyzers in areas with electromagnetic interference unless shielded equipment is used.
- Do not expose the device to extreme temperatures or moisture, as it may impair functionality.
- Periodically update software and firmware to maintain security and accuracy.

4. Time-Domain Reflectometers (TDR):

A TDR is used to detect faults, measure cable length, and identify impedance mismatches by analyzing signal reflections.

Fig 2.3.12: Time-Domain Reflectometers

Safe Handling and Usage

- Do not connect to circuits carrying power unless the device is rated for such usage.
- Use only cables and connectors specified for testing.
- Avoid applying excessive force when connecting probes or leads.
- Store in a protective case when not in use to prevent physical damage.

5. Optical Power Meters and Light Sources (For Fiber Networks):

These tools measure the optical signal strength and attenuation in fiber optic cables.

Fig 2.3.13: Optical Power Meters and Light Sources

Safe Handling and Usage

- Never look directly into the fiber port while the light source is active; invisible laser beams can damage eyesight.
- Clean fiber connectors before and after testing to ensure accurate readings.
- Use dust caps when the device is idle to prevent contamination.
- Handle fiber cables gently to avoid breaking the delicate glass strands.

6. Multimeters:

Multimeters measure voltage, current, and resistance. They are useful for verifying PoE circuits and identifying faults in electrical pathways.

Fig 2.3.14: Multimeters

Safe Handling and Usage

- Select the correct measurement range before testing to prevent damage to the device.
- Use probes with insulated grips.
- Avoid contact with exposed wires or terminals.
- Store in a dry, shock-free environment.

7. Cable Tracers and Tone Generators:

These devices help trace cables through walls or conduits by sending signals and detecting their path.

Fig 2.3.15: Cable Tracers and Tone Generators

Safe Handling and Usage

- Ensure cables are de-energized before applying tracing signals.
- Avoid interference from nearby equipment that may disrupt signals.
- Do not force cables into tight spaces; use proper guides.

General Safety Guidelines for All Diagnostic Tools

- Verify Circuit Power Status: Always confirm that the cables or ports being tested are powered down unless the tool is designed to handle live circuits.
- Use Personal Protective Equipment (PPE):L Gloves, safety glasses, and insulated tools protect technicians from accidental shocks or injuries.
- Read Manufacturer Instructions: Each device may have specific calibration, connection, or handling requirements that must be followed.
- Keep Tools Clean and Dry: Moisture, dust, and debris can impair tool accuracy or cause malfunctions.
- 5Store Tools Properly: Use protective cases and keep tools organized to avoid accidental drops or damage.
- Test Tools Before Use: Perform self-tests or calibration checks to ensure the device is functioning correctly.

Notes

Scan the QR Code to watch the related videos

https://www.youtube.com/watch?v=1z0ULvg_pW8&ab_channel=PowerCertAnimatedVideos

Difference between hub, router, and switch

https://youtu.be/dm4d2LZC2dk

How to install a router

UNIT 2.4: Equipment Installation Procedures

Unit Objectives

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

1. Show how to conduct a site survey at customer premises to assess installation feasibility for PoE-supported devices.
2. Show how to analyze the installation environment and select appropriate cables, connectors, and PoE injectors/switches.
3. Demonstrate how to inspect indoor and outdoor cable routes to avoid electrical hazards and interference sources.
4. Show how to verify that cable lengths remain within permissible limits for signal continuity and PoE power transmission.
5. Demonstrate how to determine the correct placement of network equipment to ensure proper signal coverage and power efficiency.
6. Demonstrate real-time fault clearance techniques to resolve connectivity or power issues during installation.

2.4.1 Modem Installation

Modem Installation Process

Step 1: Ensure to check the following items before installing the modem:

Fig 2.4.1: Items to be checked before installing modem

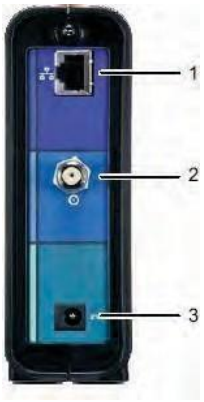
Step 2: Product Overview

It is important to check both front and rear panel.

Fig 2.4.2: Modem front panel

	ICON	FLASHING	ON
1	POWER	Not applicable — icon does not flash	**Green**: Power is properly connected
2	RECEIVE	Scanning for a downstream (receive) channel connection	**Green**: Non-bonded downstream channel is connected **Blue***: High-speed Internet connection with bonded downstream channels
3	SEND	Scanning for an upstream (send) channel connection	**Green**: Non-bonded upstream channel is connected **Blue***: High-speed Internet connection with bonded upstream channels
4	ONLINE	Scanning for an Internet connection	**Green**: Startup process completed
5	LINK	Transmitting or receiving data on Ethernet port	**Amber**: A device, computer, or hub is connected to the Ethernet (10Base-T) or Fast Ethernet (100Base-T) port **Blue***: High-speed Gigabit Ethernet (1000Base-T) connection from the SB6121 to your PC
6	ENERGY CONSERVATION SWITCH	Powers on and off the cable modem **Note**: The Energy Conservation switch may be an option that is not provided by your service provider.	

Fig 2.4.3: Modem icon table



Rear Panel

Fig 2.4.4: Modem rear panel(sample)

	ITEM	DESCRIPTION
1	ETHERNET	Ethernet port for connecting an Ethernet-equipped computer, hub, bridge, or switch using an RJ-45 cable
2	CABLE	Coaxial cable connector
3	POWER	+12VDC Power connector

Fig 2.4.5: Modem icon table

Step 3: Connecting the SB6121 Cable Modem

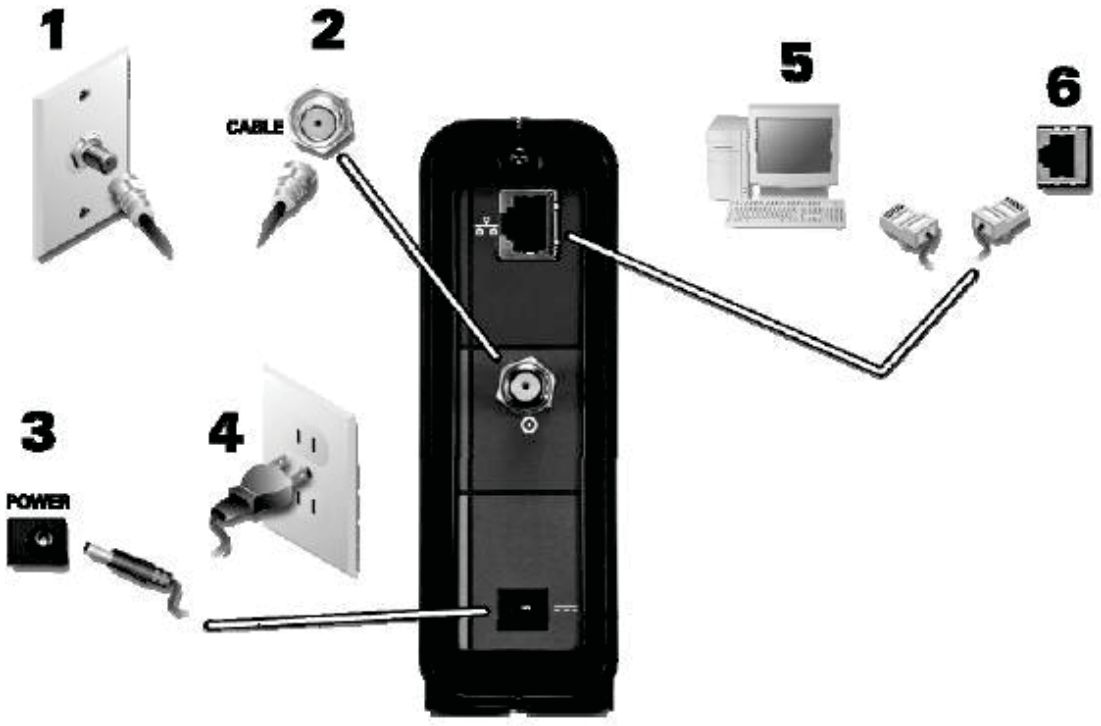


Fig 2.4.6: Ports to connect SB6121 to cable modem

1. Ensure that the coaxial cable is connected to a splitter or a cable outlet
2. Connect the other end of the cable to the input on your modem
3. Tighten the cables properly
4. Plug the end of the power cord to the modem's power port and other end into an electrical wall outlet
5. Connect the end of the Ethernet cable to the Ethernet port and the other end to the modem

Step 4: Wall Mounting the Modem (If required):

- Locate the unit as per the specifications of the local or national codes related to the residential or business cable TV and communications services.
- Follow the standards for the installation of a network interface unit (NIU) or network interface device (NID).
- Do not plug power cord to power outlet while mounting the modem.
- Ensure you have:
  - Wall-mounting template
  - Crosshead and flathead screwdriver
  - Two M3.5 (#6) screws with a flat underside. The maximum diameter of the screw head, required to mount the cable modem, is 9.0 mm

Note: Ensure that the modem is mounted on firm surface.

⚠	Before finalizing the area or wall for mounting, ensure that the area is checked for any water leakage, gas or electrical lines.

- Mark the holes on the wall, by positioning and securing the wall mounting template.
- Select the depth and diameter, to drill the holes. The depth of the holes should be at least 1½ inches (3.8 cm).

Note: The installer should determine the depth of the hole by the type of selected hardware.

The following diagram may be referred to, to determine the spacing needed in between the wall surface and underside of the screw head:

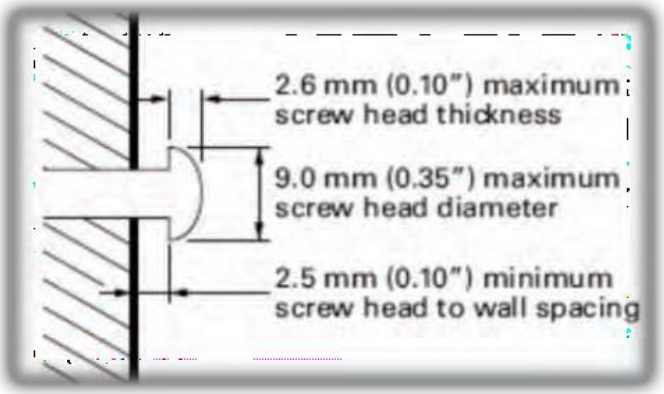
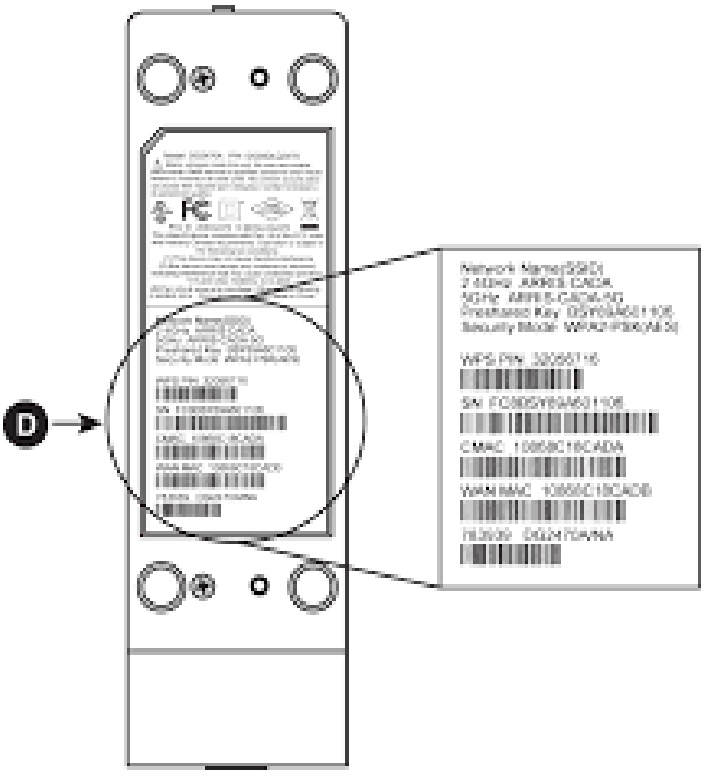


Fig 2.4.7: Spacing while wall mounting the modem

- Reconnect the coaxial and Ethernet cable, after mounting the cable modem.
- Connect the power cord into the power outlet on the wall and the +12VDC Power connector on the cable modem.
- Arrange the cables properly to avoid any safety hazards.
- Ensure that the cable modem is attached to the wall securely.



Step 5: Wireless instructions for connecting to Internet

- Using a wireless device (computer, tablet, smartphone, or other device), circumnavigate to the list of available Wi-Fi networks. Choose the TDS-named Wi-Fi network (SSID) that matches what is printed on the sticker on modem (D)
- Enter the key on the sticker. There will be need to update wireless devices with this Wi-Fi information in order to connect or can rename Wi-Fi network and change the password.
- In the address bar of an Internet browser, type http://192.168.0.1 and press enter
- On the modem's main screen, enter admin as the username and password as the password
- Click Login and check System Basic Setup Screen
- Update Network Name (SSID) field as required
- Enable WPA2-PSK
- Enter a new WPA key/Wi-Fi Password as desired
- Click Apply

2.4.2 Router Installation

Wireless Router Set Up

Step 1: Check the package of router for the items it is carrying in new pack. Normally any new router packet carries following items:

Wireless router	An AC power adapter (varies by company)	A blue Ethernet cable
Resource CD	User Manual	Warranty and Support Information cards

Fig 2.4.8: Router pack components

	Note: Contact the router dealer in case of missing, incorrect or any damaged part.

Step 2: Information such as serial number, status lights, port connectors and default login is available on a label, which is at the back of the router.

Fig 2.4.9: Port on router rear panel

Step 3: Before setting up a router check for the following:

- Internet service
- Information of Internet Service Provider (ISP) required for configuring the wireless router to access the Internet such as Internet Login Name and Password
- In case of antennas, extend them before installation
- If there are mobile applications provided, run the setup accordingly

Step 4: Use the indicator lights on the front of the wireless router to verify the status of various conditions:

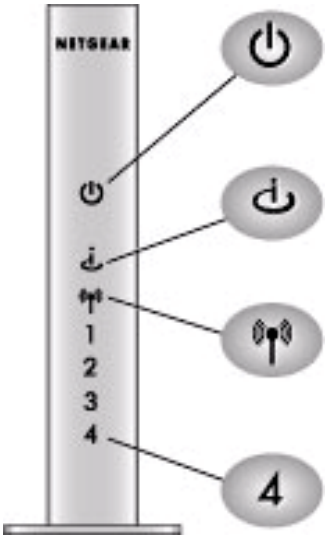


Fig 2.4.10: Icons on front panel of Netgear router

Status Light	Activity	Description
1. Power	On -- Amber On -- Green Fast blink -- Green Slow blink -- Green Off	The router integrity test is running. Power is on and the router is ready. Software update is in progress. There is a problem with the wireless router software. Power is not supplied to the router.
2. Internet	On -- Amber On -- Green Blink -- Green	The Ethernet cable is connected but the wireless router has not gotten an Internet address. The wireless router has an Internet address. Data is being communicated with the Internet.
3. Wireless	On	Indicates that the Wireless port is initialized.
4. LAN (Local Area Network) Lights 1-4	On (Green) Blink (Green) On (Amber) Blink (Amber) Off	The local port is connected to a 100 Mbps device. Data is being transmitted at 100 Mbps. The local port has detected a link with a 10 Mbps device. Data is being transmitted at 10 Mbps. No link is detected on this port.

Fig 2.4.11: Light indications on router

Step 5: Check the back of the wireless router

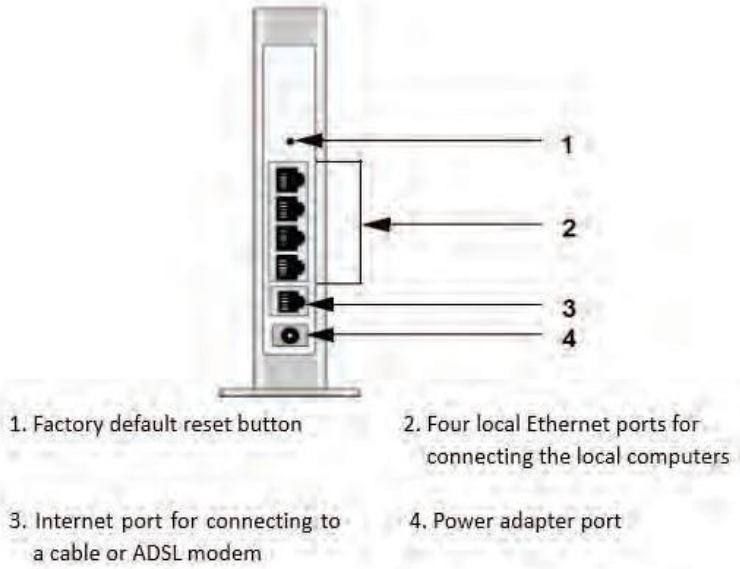


Fig 2.4.12: Rear panel of a router

2.4.3 Networking Switches Installation

Standalone network units are preferred for home and small office setups, while rack mounted switches are used for larger networks. In both setups, Cat5 or Cat6 Ethernet cables are used. Switches connect a single Internet connection to multiple computers. Switches are mostly installed in the similar fashion although their handling of network varies.

Steps for Installation

Step 1: Plug in the power supply.

Step 2: Connect the incoming network cable to the switch, preferably in the first slot. The incoming cable from the modem will be considered in case of home and small office.

Step 3: Connect a Cat5 or Cat6 cable to another slot in the network switch. Attach the other end to a computer that needs to be connected to the network.

Step 4: Repeat this process until all the computers are connected or all slots are filled.

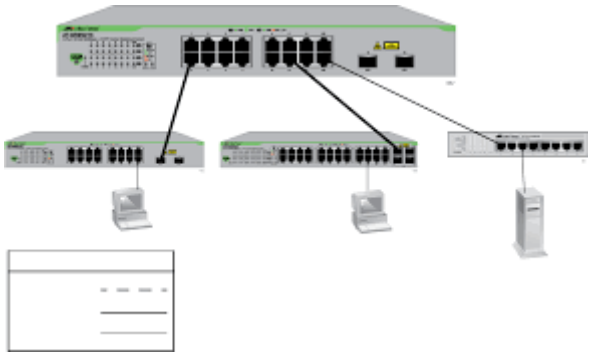


Fig.2.4.13: Switches

2.4.4 Real-Time Fault Clearance Techniques for Resolving Connectivity and Power Issues During Broadband Installation

During broadband installation, technicians often encounter real-time connectivity or power issues that can disrupt network performance or prevent devices from functioning properly. Efficient fault clearance ensures minimal downtime, maintains service quality, and safeguards equipment and personnel. This section provides a structured, textbook-style explanation of fault clearance techniques.

1. Understanding Common Faults

Broadband installations can experience several types of faults:

Connectivity Issues

- Open circuits or broken wires
- Miswiring at connectors or patch panels
- Signal attenuation due to long runs or poor-quality cables
- Crossed pairs or crosstalk in Ethernet cables

Power Issues (PoE)

- Insufficient voltage or current at the powered device
- Overloaded ports or circuits
- Faulty injectors or switches
- Voltage drop due to excessive cable length or poor termination

Environmental Faults

- Electromagnetic interference (EMI) from nearby electrical equipment
- Physical damage to cables or connectors
- Moisture or dust ingress in outdoor installations

2. Tools for Real-Time Fault Detection

- **LAN Cable Tester / Continuity Tester** – Checks wiring integrity and mapping.
- **PoE Tester** – Measures voltage and current at endpoints.
- **Network Analyzer / Packet Sniffer** – Detects traffic issues, signal loss, and latency.
- **Time Domain Reflectometer (TDR)** – Pinpoints breaks, short circuits, or impedance mismatches.
- **Multimeter** – Measures voltage, current, and resistance for PoE verification.
- **Fiber OTDR / Optical Power Meter** – Checks optical signal strength and fiber continuity.

3. Real-Time Fault Clearance Procedures

Step 1 – Identify the Fault

- Observe error indicators such as link lights on devices or switches.
- Use diagnostic tools to isolate the fault:
  - Run a continuity test for Ethernet cables.
  - Measure voltage at PoE endpoints.
  - Check signal strength for fiber optic links.
- Example: A wireless access point is not powering on. A PoE tester confirms insufficient voltage at the port.

Step 2 – Isolate the Faulty Segment

- Disconnect the suspected cable or device without affecting the rest of the network.
- Test individual segments or connectors to narrow down the problem area.
- Example: If an Ethernet run has intermittent connectivity, test each patch cable and wall jack individually.

Step 3 – Correct the Issue

Re-Terminate or Re-Crimp Connectors

- Strip the cable properly and align wires according to the standard (T568A/B).
- Crimp the connector using the appropriate tool and retest for continuity.

Replace Faulty Components

- Swap out defective cables, connectors, switches, or injectors.
- Use certified, high-quality replacement parts.

Adjust Cable Routing

- Avoid tight bends or interference sources.
- Use proper cable trays, conduits, or separation from high-power lines.

Verify Power Delivery for PoE

- Ensure voltage and current meet device requirements.
- For long runs, consider PoE extenders or mid-span injectors to maintain proper power.

Clean and Inspect Connectors (for Fiber)

- Remove dust or debris from fiber connectors using lint-free wipes and alcohol.
- Re-seat connectors and verify optical power levels.

Step 4 – Retest After Correction

- Re-run continuity, voltage, or signal tests to confirm that the fault is resolved.
- Check device functionality and monitor link stability.
- Document the fault and corrective actions for maintenance records.

4. Best Practices During Fault Clearance

Safety First

- Wear PPE (insulated gloves, safety glasses) when handling live circuits or PoE devices.
- Avoid contact with exposed wiring or energized equipment unless necessary.

Work Methodically

- Test and correct one segment at a time to prevent new issues.
- Label cables and maintain clear documentation.

Minimize Service Disruption

- Perform fault clearance during low-usage periods when possible.
- Use temporary bypasses if immediate connectivity is required.

Use the Right Tools

- Only use calibrated, manufacturer-approved diagnostic tools.
- Avoid makeshift solutions that could damage cables or equipment.

2.4.5 Inspecting Indoor and Outdoor Cable Routes to Avoid Electrical Hazards and Interference Sources

Proper inspection of cable routes is a critical step in broadband installation. It ensures safety, maintains signal integrity, and reduces the risk of equipment damage. Technicians must carefully plan and inspect both indoor and outdoor routes to avoid electrical hazards, interference, and physical damage to the cables.

1. Importance of Cable Route Inspection

- **Safety**: Prevents electric shocks, short circuits, and fire hazards.
- **Signal Integrity**: Reduces interference from electrical equipment and maintains network performance.
- **Reliability**: Minimizes wear and tear on cables caused by environmental factors.
- **Compliance**: Ensures adherence to electrical codes and industry standards.

2. Indoor Cable Route Inspection

a. Identify Potential Electrical Hazards

- Locate electrical wiring, outlets, and power distribution panels.
- Maintain a safe distance from high-voltage lines to prevent accidental contact.
- Avoid running data cables parallel to power cables over long distances, which can cause electromagnetic interference (EMI).

b. Inspect Physical Pathways

- Check walls, ceilings, and floors for conduits, ducts, and false ceilings suitable for cable routing.
- Ensure there are no sharp edges, nails, or screws that could damage cable insulation.
- Confirm that cable trays and conduits are free from dust, moisture, or debris.

c. Identify Interference Sources

- Locate fluorescent lights, motors, or HVAC systems that may introduce EMI.
- Keep network cables at least 12 inches away from electrical devices whenever possible.

d. Verify Accessibility

- Ensure the route allows easy access for installation, maintenance, and future upgrades.
- Avoid tight bends or overly long cable runs that could degrade signal quality.

3. Outdoor Cable Route Inspection

a. Assess Environmental Hazards

- Check for exposure to sunlight (UV), rain, snow, or flooding.
- Ensure cables are protected from rodents, vegetation, or sharp objects.
- Identify areas with high mechanical stress, such as near gates or doors, where cables could be pinched.

b. Identify Electrical Hazards

- Locate overhead power lines and underground electrical conduits.
- Maintain recommended separation distances:
  - Overhead lines: Keep a minimum clearance of 1 meter (3 feet) or as per local regulations.
  - Underground power lines: Maintain at least 150 mm (6 inches) horizontal separation or use conduits for physical isolation.

c. Check for Interference Sources

- Avoid routing near large motors, transformers, or broadcast antennas that may emit EMI.
- Use shielded cables (STP or coaxial) in areas with high electrical interference.

d. Evaluate Physical Route

- Prefer conduits, cable trays, or buried ducts to protect cables from mechanical damage.
- Avoid sharp bends; maintain minimum bend radius (usually 4–6 times the cable diameter for Ethernet).
- Ensure proper drainage for underground or outdoor installations to prevent water accumulation.

4. Tools and Techniques for Inspection

Tool/Method	Purpose
Visual Inspection	Identify obvious hazards, sharp edges, or interference sources.
Cable Route Maps / Floor Plans	Verify distances, pathways, and proximity to electrical sources.
Non-Contact Voltage Tester	Detect live electrical wires before handling.
EMF/Interference Detector	Locate sources of electromagnetic interference.
Tape Measure / Laser Measure	Ensure proper separation distances and avoid excessive cable length.

Notes

UNIT 2.5: UPS and Its Types

Unit Objectives

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

1. Describe the process of installing, replacing, and managing UPS systems to ensure a stable power supply for network infrastructure.

2.5.1 UPS

Uninterruptible Power Supply (UPS) is powered by a battery that gets self-activated in events of power cuts. UPS keeps the system running for a while providing time to the user to save data and eventually it shuts down.

Modern-day UPSs come enabled with software that keeps power levels consistent and avoids fluctuations, which can possibly harm the system and equipment.

UPS Types

UPS comes in lots of designs and in different varieties where each has its own diverse characteristics or performance. The most common are as follows:

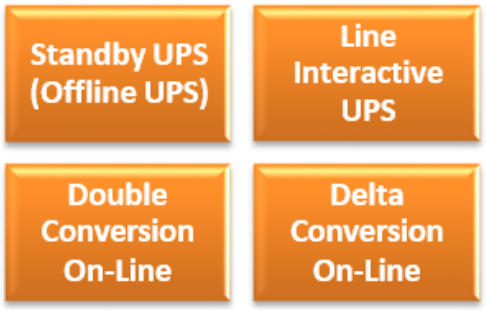


Fig 2.5.1: UPS types

UPS keeps monitoring the power supply and switches to battery power the moment system stops receiving power from the electrical switch. Although there is some time lapse between the time, power is interrupted to the time UPS gets started. Interactive UPS are sometimes referred to as a standby power system. UPS is also categorized into:

Parameters	Offline UPS	Online UPS
Operational Difference	The batteries of offline UPS are charged always. If the power fails, the inverter motorizes the load.	Online UPS takes the incoming AC mains supply and converts it to DC, which feeds the battery and the load through the inverter. If the main supply fails, then the batteries feed the load through the inverter.
Voltage distortion	More fluctuations lead to more offline UPS usage	Voltage alteration does not lessen the performance
Price	They are cheaper	These are costly
When to use	If cost is a major consideration and needs a lower operating temperature	If cost is a major consideration and needs a lower operating temperature

The following figure shows UPS connectivity:

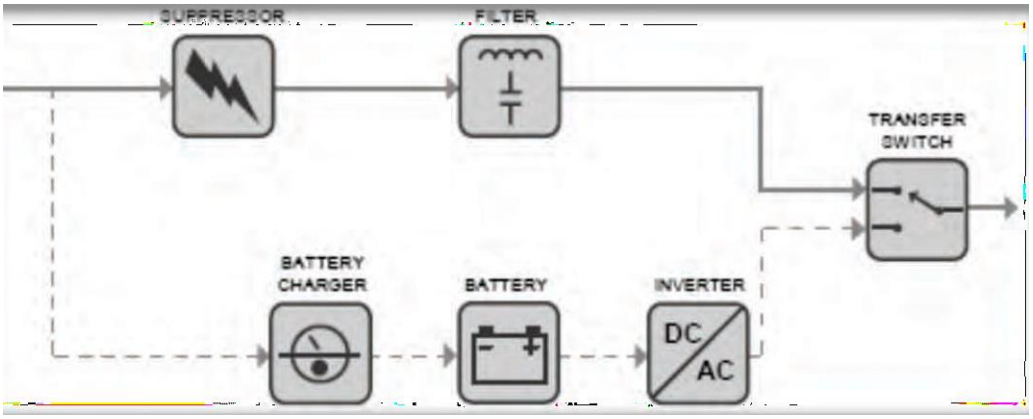


Fig 2.5.2: Illustration showing UPS connectivity

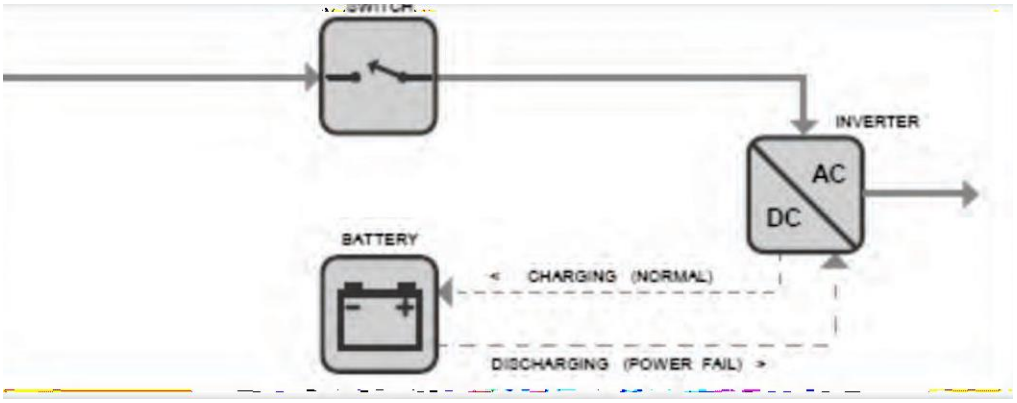


Fig 2.5.3: Online UPS

Notes

UNIT 2.6: Checking of Voltage, Current and Earthing

Unit Objectives

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

1. Show how to perform voltage, current, and earthing checks to ensure a stable and safe power supply.

2.6.1 Voltage and Current Checking

A device that is used for measuring voltage, resistance, and current in electronics and electrical equipment is called a multimeter.

Battery voltages, vehicle electrics and electronics, cables continuity, fuses, and home appliances can also be verified using a multimeter as it also tests continuity.

A multimeter is of two types, Analog and Digital:

- Needle style gauge is found in Analog multimeter
- LCD display is seen on Digital multimeter

Fig 2.6.1 Multimeter

A positive connection is confirmed once the red meter lead is firmly connected to an amperage port or Voltage/Resistance.

A negative connection is when a Black meter lead is connected to any common port.

2.6.2 Earthing

To avoid hazards and mis happenings, proper earthing is essential. The process of sharing the charges with the earth is called “Earthing”. It is important for protecting the devices from electric harm.

“Grounding” is a safety process that protects the entire power system from malfunctioning and is largely used to balance the load when the electric system overloads.

It protects the user against electric shock because, in case of any electrical fault, it ensures low resistance, by connecting it to the neutral circuit at the service panel. Ground wiring is always essential.

Any electrical appliance is capable of running without the ground wire; however, this is not an ideal way for connecting an appliance using direct mode. One can’t even make a difference if in case the ground wire is broken. Its working or importance comes only in a scenario when there is high voltage. In such a situation if the ground wire isn’t working it will cause an electric shock to the user.

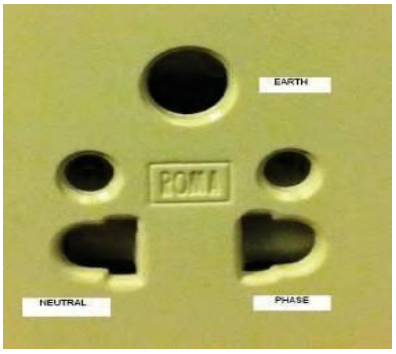


Fig 2.6.2 Electrical switch

Here is an image illustration of an electrical socket or receptacle used in India. The center hole is for earth, left hole is for neutral and the right hole is for phase. Phase is always positive, and this is where the switch is mostly installed.

Earthing Checking Procedure

Multimeter is used to check if there is grounded electrical socket. This is easily available for ~Rs.600 in markets.

Step 1: As shown in the image below, connect the probes and set the knob of the multimeter to 750V AC. Insert the red probe in phase hole and black probe in neutral hole. Here the reading is showing zero because the switch is off.

Fig 2.6.3: Connect multimeter knob

Step 2: Once the switch is turned the voltage across Phase and Neutral can be measured. Here the reading is 240V.

Fig 2.6.4: Turn the multimeter knob

Step 3: Insert the black test probe and red test probe, in earth and in phase respectively, and measure. Here the reading is 243V.

Fig 2.6.5: Connect black test probe to earth outlet

Step 4: Next, put the red probe and black probe in earth and neutral respectively, and measure. The reading should never be more than 2V. Here the reading is 1V.

Fig 2.6.6: Red probe and black in earth and neutral respectively

It protects the user against electric shock because, in case of any electrical fault, it ensures low resistance, by connecting it to the neutral circuit at the service panel. Ground wiring is always essential.

Any electrical appliance is capable of running without the ground wire; however, this is not an ideal way for connecting an appliance using direct mode. One can't even make a difference if in case the ground wire is broken. Its working or importance comes only in a scenario when there is high voltage. In such a situation if the ground wire isn't working it will cause an electric shock to the user.

Step 5: Calculate the voltage difference between Step 3 and Step 2 i.e., 243V - 240V = 3V.

Step 6: Calculate the difference in voltage received in Step 5 and Step 4 i.e., 3V - 1V = 2V. The acceptable value is 1V to 2V.

Please note, the testing is done here to check the existence of earthing circuit. To measure the actual earthing resistance, an Earth Resistance Tester is required.

Notes

Scan the QR Code to watch the related videos

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

Use of Multimeter and revise electricity basics

UNIT 2.7: Checking and Testing Battery

Unit Objectives

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

1. Demonstrate how to inspect and replace UPS batteries when required to maintain uninterrupted network operations.

2.7.1 Battery Checking and Testing

Battery checking and testing are critical to the continued performance of a UPS system. There is automatically built-in functionality to evaluate batteries timely and alert if there is any defect, in most power supplies. Merely testing voltage doesn't provide the correct picture of battery condition.

The best way to assess the correct condition is through external battery testing. For large battery sets, specific block testing can be more dependable. External battery testing should form part of a planned preventive UPS maintenance rule, while it can also be provided as a separate service.

Types of Battery Testing

Impedance Testing	Electro- chemical Testing	Load Bank Testing(Discharge Testing)	Partial Discharge Testing
• Applies AC Current to each battery through probes • Shares an indication of battery life	• It uses probes to measure voltage frequency and signals • It measures sulphation and electrolyte dry-out	• It evaluates which cell is charged and indicates those reaching end of service life • Batteries are treated externally	• Batteries are discharged upto 80% of the capacity • Battreies are reloaded within 8 hours

UPS Battery Monitoring

Dedicated battery monitoring systems also measure UPS battery performance. It is directed monitoring systems incorporate the parameters drawn by the globally recognized IEEE 1491 standard, including:

- String and cell float voltage
- String and cell charge and discharge voltage
- AC ripple voltage
- AC ripple current
- String charge current
- String discharge current
- Ambient and cell temperature
- Cell internal resistance

2.7.2 Replacing UPS Batteries to Maintain Uninterrupted Network Operations

Uninterrupted Power Supply (UPS) systems are critical in broadband and network installations because they provide backup power during outages, protect against voltage fluctuations, and ensure continuous operation of network devices such as routers, switches, servers, and PoE devices. Proper maintenance, including timely battery replacement, is essential for reliable network performance.

1. Importance of UPS Battery Replacement

- **Ensures Network Continuity**: Prevents downtime during power failures or fluctuations.
- **Protects Equipment**: Reduces risk of data loss, device damage, or network disruption.
- **Maintains PoE Functionality**: UPS supports powered devices during outages, ensuring continued operation.
- **Extends UPS Lifespan**: Timely battery replacement avoids overloading the UPS system.

2. Signs That UPS Batteries Need Replacement

- **Reduced Backup Time**: Network devices run for a shorter duration than expected during a power outage.
- **Frequent Alarms or Warnings**: UPS displays battery fault or low capacity alerts.
- **Physical Damage or Leakage**: Swelling, corrosion, or electrolyte leakage from batteries.
- **Age of Batteries**: Most sealed lead-acid UPS batteries last 3–5 years; check manufacturer recommendations.
- **Inconsistent Voltage Output**: Fluctuating or unstable voltage delivery during power cuts.

3. Safety Precautions Before Replacing UPS Batteries

- **Power Down Non-Critical Loads:** Ensure that devices not critical to operation are safely shut down.
- **Wear Personal Protective Equipment (PPE):** Insulated gloves, eye protection, and protective clothing when handling batteries.
- **Work in a Ventilated Area:** Prevent inhalation of gases released by lead-acid batteries.
- **Avoid Short Circuits:** Do not place metal tools across battery terminals.
- **Follow Manufacturer Guidelines:** Check the UPS manual for battery replacement instructions and specifications.

4. Steps to Replace UPS Batteries

Step 1 – Isolate the UPS

- Switch off the UPS and disconnect it from the main power supply.
- Disconnect all connected network devices if required, or ensure they are on alternate backup.

Step 2 – Access the Battery Compartment

- Open the UPS battery compartment following manufacturer instructions.
- Note the battery arrangement (series or parallel) for correct replacement.

Step 3 – Remove the Old Batteries

- Carefully disconnect battery terminals, starting with the negative terminal to prevent short circuits.
- Remove each battery and inspect for corrosion or leakage.

Step 4 – Install New Batteries

- Place new batteries in the compartment in the correct orientation.
- Connect terminals securely: first positive, then negative.
- Ensure proper alignment and tight connections to avoid loose contacts.

Step 5 – Check and Test

- Close the compartment and reconnect the UPS to the main power supply.
- Turn on the UPS and perform a battery self-test if available.
- Monitor the backup time and voltage output to confirm correct operation.

Notes

UNIT 2.8: Installation and repair of UPS

Unit Objectives

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

1. Show how to install and route power supply through UPS, ensuring equipment is protected against power fluctuations.
2. Explain the risks and consequences of not following structured wiring guidelines, safety procedures, and PoE power limits.

2.8.1 UPS Installation

Pre-Installation checks

1. Selecting the Right Company:

An intensive effort needs to be made to identify and select the resource which can assist in the decision-making process. A resource is critical as it also includes the installation of a specialized system.

2. Selecting the UPS:

To decide on the kind of UPS required, one needs to check on the following things-

- The amount of load UPS will protect
- Kind of equipment UPS will protect like, servers, medical equipment, etc.
- Tolerance level of downtime
- Stability of UPS in the long run
- Cost-effectiveness

3. Location to install

Along with UPS, batteries must also be safely lodged, thus floor must support the load. Space evaluation needs to be considered keeping in mind any possible future expansion. The environment of the location must be sufficiently air-conditioned and protected from extreme dust and dampness. On solid floors, a cable trench or UPS plinth will be compulsory to permit power cabling and termination under the UPS and battery.

Installation Procedure

1. Install the battery breaker kit in the bottom of the empty classic battery cabinet
2. Remove gland plates for signal and power cables
3. Drill and reinstall gland plates
4. Remove the eight screws holding the battery breaker plate
5. Remove the battery breakerplate
6. Connect the signal cables by installing the sensor to check the temperature
7. Align sensor cables through the top or bottom of the cabinet to UPS dry contact terminal
8. Align signal cables through the top or bottom of the cabinet to the battery beaker

9. After removing the cover, connect signal cables
10. Place the beaker cover on battery beaker
11. Connect power cables from the UPS by connecting PE and DC cables from UPS

Pic credit: https://www.productinfo.schneider-electric.com)

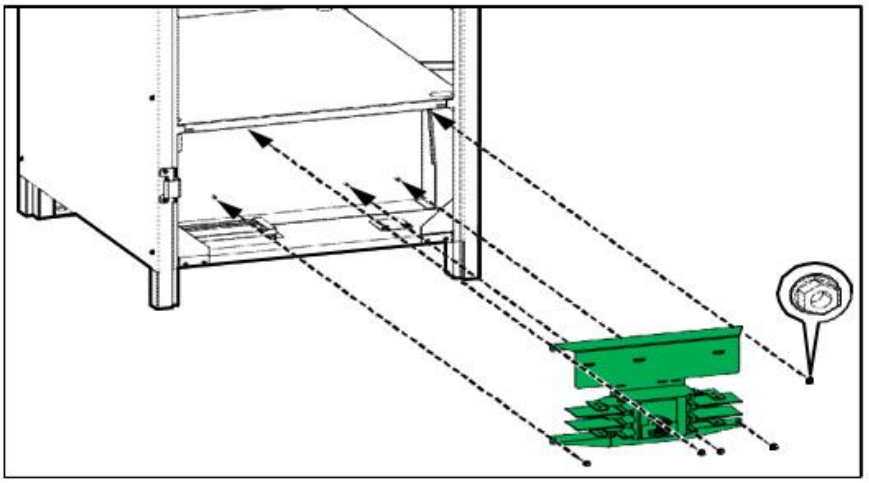


Fig 2.8.1: Front view of Empty battery cabinet

Procedure of installing and connecting the batteries

- Place the batteries on the shelves and connect the batteries
- Connect the battery cables (Batt+, N, Batt-) in the empty classic battery cabinet to the battery breaker
- Fix the protection cover over the terminals on the right side of the battery breaker
- Make a note of the battery configuration on the label

2.8.2 Checks in Defective UPS

Here are common problems which a UPS normally faces along with the process to fix the problems –

UPS is not working properly

- Check whether UPS batteries are charged to the proper level so that they can operate. Always refer UPS documentation for precise information
- Inspect the UPS power switch is in the "On" position. To comprehend on the location of the switch, check the UPS documentation
- Examine UPS software is the updated / latest version
- Ascertain the power cord is the correct type and study the country in which the server is located. Always refer UPS reference guide
- Inspect whether the line cord is connected
- Make sure circuit breakers are in the "On" position, if required, replace the fuse
- In case the sleep mode of UPS has started, disable it which turns off the configuration mode on the front panel
- Battery change needs to be done if damage was caused by excessive heat

Low battery warning is getting displayed

- Immediately plug the UPS into an AC grounded outlet for a minimum of 24 hours to charge the batteries, and then perform testing. If required, replace the batteries
- Confirm that alarm is set correctly by altering the amount of time given earlier to a low battery warning

Notes

UNIT 2.9: Basic Load Calculation

Unit Objectives

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

1. Demonstrate how to calculate equipment power load and compare it with UPS capacity to prevent overloading and ensure efficient power backup.

2.9.1 Basic Load Calculations

The list of appliances consumption is as follows:

HIGH CONSUMPTION APPLIANCES					
Iron	1000 Watts	100W Light Bulb	100 Watts	Security Cameras	60 Watts
Electric Kettke	2000 Watts	60W Light Bulb	60 Watts	Alarm System	50 Watts
Hairdryer	1500 - 2000 Watts	Cell Phone Charger	10 Watts	PABX	150 Watts
Home Airconditioner	1500 - 2500 Watts	Alarm System	20 Watts	Point of Sale	220 Watts
Swimming pool pump	1500 Watts	Gate Motor	500 Watts	Photo Copier	250 Watts
Power Drill	600 - 1200 Watts	DVD Player	30 Watts	Fax Machine	120 Watts
Toaster	800 Watts	Fish Tank	700 Watts	Hi-Fi System	200-500 Watts
Microwave Oven	600 - 1200 Watts	Personal Compter	300 Watts	Playstation	200 Watts
Stove	1550 - 3000 Watts	Ink Jet Printer	100 Watts	Electric Fence	20- 500 Watts
Tuble Dryer	2500 Watts	Electric Fence	200 Watts	Electric Blanket	50-100 Watts
Clothes Iron	1000 Watts	DVD Player	30 Watts	Water Feature	50 Watts
Vacuum Cleaner	200 - 1200 Watts	Laptop Computer	150 Watts	Slow Cooker	200 Watts
Washing Machine	500 - 1500 Watts	ADSL Model	20 Watts	Fridge/Freezer	500 Watts
Laser Printer	700 Watts	LCD TV	200 - 400 Watts	Ceiling Fan	70 Watts
Hot Plate	1200 Watts	DSTV	20 Watts	Garage Door	600 Watts
Geyser	2500 Watts	Plasma TV	200 - 400 Watts	X-Box	100 Watts
Coffee Maker	800 Watts				
TRY AVOID USAGE DURING LOAD SHEDDING					

Table. 2.9.1: Listing appliances consumptions

Sizing a UPS/Inverter Solution is a mathematical formula for multiplying CURRENT measured in amps and POWER in volts to get the LOAD rating in Volts-Amps (VA). Another method for load detection is by locating the Watts rating. The following four simple steps to get the load is:

Step 1: Start by listing and placing all the equipment that are protected by inverter or a UPS in one column. For example, computers, alarm, TV, DSTV, lights and fridge.

Step 2: Put the volts and amps of each of these items in column 'b'. This information will be available on nameplates of each item. For example, 120V x 2.0A is written on the plate.

Step 3: Calculate the product of the volts and the amps of each equipment and note the total in a column labelled as "VA". If the rating of the equipment is given in watts, convert the rating to VA by multiplying the figure by 1.43 and note it into your VA column.

Step 4: Add an additional 25% to the total VA load to adapt any future growth. This also helps to avoid any potential overloading of the Inverter/UPS.

Battery Run Example 1:

Inverter/UPS Rating: 1500VA

No. of Batteries: 2

Battery Rating: 12V

Battery Rating: 17Ah

UPS/Inverter Backup me (in Hr. s) = (No. of DC batteries x voltage rating of battery x Ah rating of battery) / VA of Inverter/UPS installed

Answer Equals:

(2 x 12 x 17) / 1500

408 / 1500

0,272 hours or +-15 minute

Example 2:

Computer requires: 2 Amps (current) Mains

Voltage: 230VAC (AC voltage)

Power: 0.6 (typical for computer equipment)

2A x 230V = 460W / 0.6 PF = 766 VA

An 800VA will work fine but keeping future requirements in mind it is advised to 20-25% capacity on top. In given example a 1000VA UPS (1KVA) will be optimum. In case of more than one system or equipment, add all the Amps together and do the calculation as shown.

Fig 2.9.1: Examples

Notes

UNIT 2.10: UPS and Battery Compatibility

Unit Objectives

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

1. Demonstrate how to calculate equipment power load and compare it with UPS capacity to prevent overloading and ensure efficient power backup. (Included here to ensure compatibility discussions along with load calculation, without repeating content).

2.10.1 UPS and Battery Compatibility

Selecting the optimum size of UPS along with the right kind of batteries is the most important aspect. Batteries come in different sizes and costs. They exhibit a variety of specifications and come with different warranty periods and life expectancies. Choose theone that best suits your needs.

The installation also depends on a number of factors, including:

- Maximum possible load
- Maximum expected load Power
- Redundancy level required
- Time used for switching to battery backup
- Time autonomy

The following types of batteries are generally selected for use with a UPS:

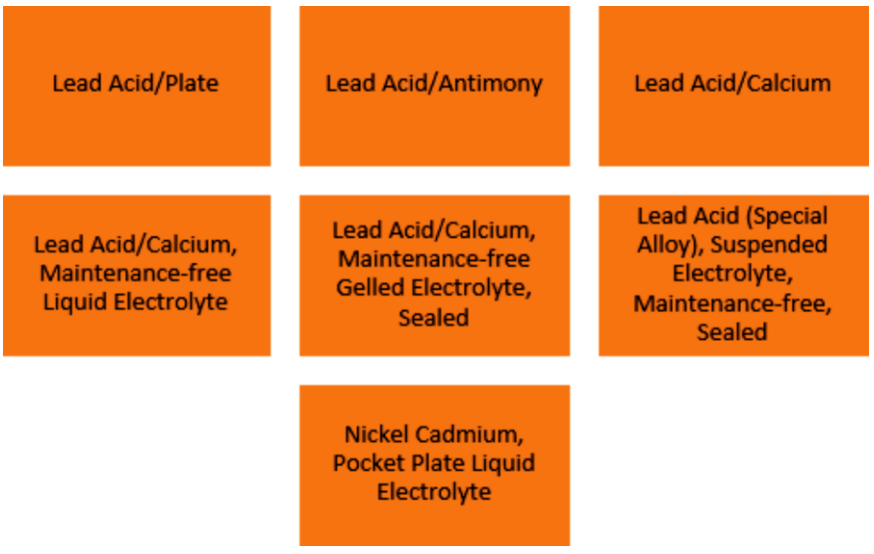


Fig. 2.10.1: Batteries, used for UPS

While choosing the most expedient battery one must consider parameters operations, maintenance and cost.

2.10.2 Battery Sizing

The calculations done in this module are by assuming the standard room temperature, 77°F (25°C). Calculations should be altered in case of variations in room temperatures.

Any UPS or battery supplier can be helpful in the following three types of calculations:

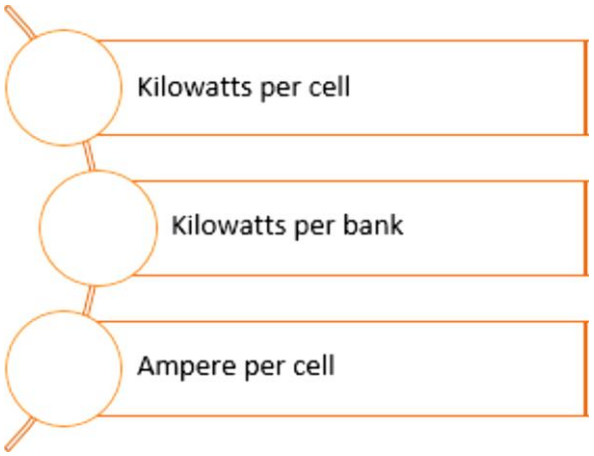


Fig. 2.10.2: Types of calculation for batteries

In general information given for lead acid batteries, designed for short discharge times,

typically, 5 -120 minutes, is in the form of kilowatts per cell. Thus, it is significant to calculate the total kilowatts, required for operating a particular UPS.

Notes

UNIT 2.11: Record Keeping and Documentation

Unit Objectives

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

1. Explain the importance of documentation and record-keeping for network infrastructure and PoE installations.
2. Describe best practices for customer communication, including explaining installation details and resolving customer queries.
3. Explain payment processing procedures and how to handle customer transactions professionally.
4. Describe proper waste disposal methods to ensure environmental safety and compliance with regulations.
5. Explain the importance of obtaining customer sign-off and how to verify customer satisfaction.
6. Demonstrate how to record installation details, including cable routes, device configurations, and test results.
7. Show how to update network plans to reflect any modifications, PoE device placements, and system changes.
8. Demonstrate how to complete installation documents, ensuring all required details are accurately filled in.
9. Show how to communicate with customers regarding installation completion, equipment usage, and troubleshooting guidelines.
10. Demonstrate how to process payments and issue receipts according to company policies.
11. Show how to obtain customer feedback and sign-off, ensuring their concerns and queries are addressed.

2.11.1 Importance of Documentation and Record-Keeping

Documentation and Record-keeping Guarantee Accountability and Coordination.

Why it is important to document and maintain proper records?

- Continuity of Care. While giving best possible service to the customer, following -up is considered to be a major aspect, and records in this step help by providing previous history of the case and brief overview. Records become essential in cases that involve different steps of service to resolve an intricate problem. Updated and factually correct records come in handy in times when the manager or person in charge is not available. To ensure coordinated service between the client and service provider, maintaining and updating the records and documents in timely manner will be prove to be fruitful.
- Accountability. The service provider should be able to produce the requested record or relevant information to the client as and when necessary.
- Service Improvement. It has been observed that employees of a company that stores its data in systematic manner are more in formative and updated than the one which does not focus on these crucial features. Having a substantial set of data helps the analytical team storead, plan and in corporate new policies, to further improve customer experience.

We all should follow proper record-keeping templates as per the organization's standard and fill it carefully.

Here is Sample Repair/Replacement form for your Understanding:

Company / Address of Beam Reseller **CONTACT DETAILS**

Company Name:		Contact Name:
Address:		Position:
		Telephone:
City / State:		Fax:
Postcode:	Country:	Email:

Company / Address of End User (Installation) **CONTACT DETAILS (if available)**

Company / Name:		Contact Name:
Address:		Position:
		Telephone:
City / State:		Fax:
Postcode:	Country:	Email:

Return Address of Repaired / Replaced Product

☐ Same as *"Company / Address of Beam Reseller" above*

☐ Same as *"Company / Address of End User (Installation)" above*

OR:

Company / Name:		Contact Name:
Address:		Position:
		Telephone:
City / State:		Fax:
Postcode:	Country:	Email:

Returned for Repair (Out of Warranty)*: ☐ PO#_____

**Note: Repair work can only be performed when Beam receives a Purchase Order # from your company.*

Fig 2.11.1: Sample of a repair/replacement form

2.11.2 Installation Report

Why Reporting is Important?

After the installation of software, it is very important to report to your supervisor so that he can understand: What was the local need?

- How was it determined?
- Who was the customer?
- What was your role?
- How was the action taken for repair?
- Do you have any customer quotes?
- Was the process followed by you was right?

With Reporting

- He can check your accountability
- He can monitor your progress in handling the customer
- He can evaluate your performance in handling the customer
- He can suggest improvements, if any?
- Installation report should be filled as per the following format

Every company has their own format of reporting and a technician should fill it accordingly. For your information a general template is as follows:

Broadband Installation Report	
Customer Name:	**Customer Phone:**
Customer Address:	
Contact name:	**Contact Position:**
Customer P.O. No.:	**Invoice Number:**
Product No:	**Product Description:**
COMPLAINT INFORMATION	
Installation Date:	**Installation done by:**
Installation Details	
Installation check list: o Modem o Router o Switch o Connector o Cable	

Fig 2.11.2: Sample of a reporting form

2.11.3 Feedback Form

Take feedback from the customer. Here is the template for customer satisfaction level to the product Installation:

	Very Satisfied	Satisfied	Unsatisfied	Very Unsatisfied	Not sure
Quality of services provided					
Professionalism and courtesy of the technician					
Timeliness of services provided					
Awareness of this service					

Fig 2.11.3: Sample of a feedback form

Test Your Reporting Skill

Broker name/Logo	Customer Complaint Report

However, in case the complaint is not get resolved within two working days, the technician should immediately report the same to his reporting manager.

Customer name:		Name of the member or technician working on the complaint			
Account No:		Name of the broker (which may remain same as above)			
Reason for Complaint:					
Details of complaint: **Source of complaint (phone/email/letter/in person, etc.):** **Actions already taken to resolve the complaint:** • One can record details here (although, optional) if the complaint is resolved on the next business day. Fill the 'Complaints resolved by the end of the business day' log and update the same on customer's file. • Once the issue gets resolved, pass the sheet containing the steps taken to resolve a particular issue along with the supporting documents to your manager.					
Signature of Staff:		Date:		Print Name:	
Complaints/ Compliance Manager Signature:		Date:		Print Name:	
Complaints Manager/Compliance Use Only Actions taken/Final Outcome: (please give a summary of actions/correspondence)					
Signature				Date	

Fig 2.11.4: Sample of a complaint form

Along with this report provide all supporting documents to the complaint manager.

2.11.4 Best Practices for Customer Communication During Broadband Installation

Effective communication with customers plays a vital role in ensuring satisfaction, trust, and smooth broadband installation. Technicians and service providers must not only perform the technical tasks but also explain the process, address concerns, and build confidence in the service provided. Below is a structured, textbook-style explanation of best practices for customer communication.

1. Importance of Customer Communication

- Builds Trust and Confidence: Clear communication helps customers feel informed and secure.
- Reduces Misunderstandings: Explaining procedures in simple terms prevents confusion or unrealistic expectations.
- Improves Service Satisfaction: Addressing queries promptly and patiently strengthens customer relationships.
- Supports Troubleshooting: Educated customers can assist in monitoring performance and reporting issues early.
- Enhances Brand Reputation: Positive interactions lead to referrals and repeat business.

2. Best Practices for Explaining Installation Details

a. Use Simple and Clear Language

- Avoid technical jargon unless the customer is familiar with it.
- Explain the purpose of each component in a relatable way.

Example: Instead of saying, "We are installing a Cat6 cable for gigabit transmission," say, "We are using a high-speed cable that ensures faster internet for streaming and video calls."

b. Provide Step-by-Step Information

- Explain what will be done before, during, and after the installation.
- Share expected timelines and safety precautions.

Example: "We will first check the connection point, then run the cable along the wall safely, and finally configure the router. The entire process will take around two hours."

c. Manage Expectations

- Inform customers about possible delays or disruptions.
- Clarify maintenance schedules or required restarts.

Example: "Once the installation is complete, you may need to restart your devices to apply the new settings."

d. Demonstrate Proper Use

- Show how to operate devices such as routers or network switches.
- Guide customers on how to check signal strength or reboot the system.

3. Best Practices for Resolving Customer Queries

a. Listen Actively

- Allow customers to fully explain their issues without interruption.
- Confirm understanding by repeating or summarizing their concerns.

b. Empathize with Customer Concerns

- Acknowledge any frustration or inconvenience.
- Reassure them that the issue will be addressed.

Example: "I understand that the slow internet is affecting your work, and I'm here to resolve this as quickly as possible."

c. Provide Accurate and Honest Information

- Avoid guessing or providing incomplete answers.
- If unsure, inform the customer that you will verify and follow up.

d. Offer Practical Solutions

- Present troubleshooting steps the customer can perform.
- Provide guidance for self-monitoring, such as checking cable connections or router lights.

e. Follow Up

- After resolving an issue, check back to ensure the problem is fully resolved.
- Offer contact details or helpline numbers for future support.

4. Additional Communication Tips

a. Maintain Professionalism

- Be punctual, respectful, and polite throughout the interaction.
- Dress appropriately and carry identification to build trust.

b. Be Patient

- Some customers may need extra time to understand procedures.
- Repeat explanations or demonstrations as necessary without appearing rushed.

c. Document Customer Requests

- Keep a record of queries and solutions for consistency in future interactions.

d. Use Visual Aids When Possible

- Diagrams, charts, or demonstration videos can help explain complex setups.

5. Communication Do's and Don'ts

Do's	Don'ts
Speak clearly and calmly	Use technical jargon unnecessarily
Listen actively	Interrupt or dismiss concerns
Offer reassurance	Promise unrealistic outcomes
Provide step-by-step guidance	Rush through the process
Follow up after resolution	Ignore recurring issues

2.11.5 Payment Processing Procedures and Handling Customer Transactions Professionally

Efficient and professional payment handling is a crucial part of broadband services. It ensures that customers feel secure, informed, and valued while completing their transactions. Clear procedures also help in minimizing disputes, ensuring transparency, and maintaining accurate financial records.

1. Importance of Proper Payment Handling

- Builds Customer Trust: Transparent and secure payment processes foster confidence in the service provider.
- Ensures Accuracy: Correctly processing payments prevents billing errors and disputes.
- Maintains Compliance: Following standard procedures ensures adherence to financial regulations and tax laws.
- Enhances Customer Satisfaction: Smooth transactions reflect professionalism and enhance the overall service experience.

2. Payment Processing Procedures

Step 1 – Confirm Billing Details

- Verify the customer's plan, package, and payment amount before initiating the transaction.
- Provide a written estimate or invoice showing all charges, taxes, and discounts.

Example: "Your monthly broadband plan is ₹1,200 plus taxes. Here's the detailed invoice."

Step 2 – Explain Payment Methods

Offer customers multiple options and explain how each method works:

1. **Cash Payment**
   - Provide a receipt immediately after receiving cash.
   - Count the cash in front of the customer to ensure accuracy.
2. **Digital Payment (UPI, Wallets, Net Banking)**
   - Guide customers through the transaction process.
   - Confirm the successful transfer before ending the session.
3. **Credit/Debit Cards**
   - Use secure card readers or point-of-sale (POS) machines.
   - Ensure the customer enters the PIN privately.
4. **Auto-Debit or Subscription Plans**
   - Help customers set up recurring payments.
   - Explain the schedule, cancellation policies, and notifications.

Step 3 – Process the Payment

- Initiate the transaction using the correct amount and customer details.
- Double-check before confirming the payment.
- Avoid rushing or making assumptions without customer approval.

Step 4 – Provide Documentation

- Always issue a receipt, invoice, or acknowledgment slip.
- Include transaction ID, payment method, date, and customer contact details.

Step 5 – Record and Report

- Update the billing system or ledger to reflect the payment.
- Report any failed transactions promptly and assist in troubleshooting.

2.11.6 Proper Waste Disposal Methods to Ensure Environmental Safety and Compliance with Regulations

Broadband installation and maintenance activities often generate waste materials such as cable cuttings, packaging, damaged components, and hazardous substances like batteries or solvents. Proper waste disposal is necessary to protect the environment, ensure workplace safety, and comply with local, national, and industry-specific regulations.

1. Types of Waste in Broadband Installations

- Non-hazardous waste: Cable scraps, packaging, cardboard boxes, plastic wraps.
- Hazardous waste: Used batteries (UPS or PoE devices), electronic components, soldering residues, chemicals.
- E-waste: Damaged routers, switches, connectors, and obsolete devices.

2. Best Practices for Waste Disposal

1. **Segregate Waste at Source**
   - Separate recyclable items from non-recyclables and hazardous waste.
   - Use clearly labeled containers for plastic, metal, paper, and electronic waste.
2. **Use Authorized Disposal Facilities**
   - Work with certified recycling centers or hazardous waste handlers.
   - Follow guidelines provided by local environmental protection agencies.
3. **Dispose of Hazardous Materials Safely**
   - Store used batteries and electronic waste in sealed containers.
   - Ensure proper transportation to disposal facilities without mixing with general waste.
4. **Minimize Waste Generation**
   - Cut cables only as required and reuse unused sections where possible.
   - Encourage manufacturers to supply biodegradable or recyclable packaging.
5. **Document Waste Disposal**
   - Maintain records of waste types, quantities, and disposal methods.
   - Ensure audits and inspections are passed by authorities.
6. **Regulatory Compliance**
   - Follow standards such as the Environment Protection Act, E-Waste Management Rules, or other local guidelines.
   - Ensure proper disposal of batteries, circuit boards, and other electronic waste to avoid environmental contamination.

2.11.7 Importance of Obtaining Customer Sign-Off and Verifying Satisfaction

Customer sign-off is a formal confirmation that the installation has been completed as agreed, and that the customer is satisfied with the work. It is essential for service accountability, dispute resolution, and legal protection.

1. Why Customer Sign-Off Matters

- Confirms Acceptance: Ensures that the customer agrees the work is completed properly.
- Prevents Future Disputes: Provides written evidence of services rendered.
- Builds Trust: Demonstrates transparency and professionalism.
- Enables Billing and Closure: Authorizes final invoicing or subscription activation.
- Improves Service Quality: Provides feedback on customer satisfaction for future improvements.

2. How to Verify Customer Satisfaction

- Explain Completed Work: Walk the customer through the installation process, devices installed, and tested parameters.
- Demonstrate Functionality: Show active connections, tested signal strength, and backup power (if applicable).
- Ask for Feedback: Encourage customers to express any concerns or requests for adjustments.
- Obtain Written or Digital Approval: Provide a sign-off form or electronic acknowledgment for the customer to confirm completion.
- Record Any Follow-Up Requirements: Note additional requests, pending tasks, or warranty coverage.

2.11.8 Record Installation Details

Accurate record keeping is critical for troubleshooting, audits, warranty claims, and future maintenance. It also ensures consistency across different sites and technicians.

1. What Information to Record

1. Cable Routes

- Entry and exit points, lengths, types (Cat6, fiber, etc.).
- Conduits used and separation from electrical lines.
- Obstacles or bends encountered during routing.

2. Device Configurations

- Router or switch model numbers and serial numbers.
- IP addresses, login credentials (if authorized), and network settings.
- Power supply details (UPS, PoE voltage).

3. Test Results

- Continuity checks and wire mapping results.
- Signal strength measurements and acceptable ranges.
- Attenuation, packet loss, or latency metrics.
- Backup power test durations.

4. Site Details

- Date and time of installation.
- Technician's name and contact details.
- Customer's name, address, and contact information.

2. Tools for Recording Information

- Installation Checklist Templates: Predefined forms to ensure no step is missed.
- Mobile Apps or Digital Forms: For real-time data entry, photo uploads, and signatures.
- Maps or Diagrams: To visually mark cable paths, device locations, and service points.
- Spreadsheets or Asset Management Software: For tracking installations, warranty periods, and service history.

3. Best Practices in Documentation

- Be Thorough but Clear: Avoid cluttered notes; organize information in sections for easy reference.
- Include Photos or Diagrams: Visual records help in troubleshooting and future installations.
- Verify Entries Before Submission: Double-check that lengths, settings, and customer details are correct.
- Secure Sensitive Data: Protect customer credentials and payment details according to privacy policies.
- Maintain Backup Copies: Store records in both physical and digital formats for reliability.

Exercise

Short Answer Questions:

1. Explain why it is important to keep cable lengths within permissible limits for both signal continuity and PoE power delivery.
2. Describe how you would conduct a site survey at a customer's premises before installing PoE-supported devices.
3. What are the key differences between UTP and STP cables, and where would you use each?
4. Explain the process for safely handling and using diagnostic tools like PoE testers during installation.
5. Why is proper documentation and record-keeping critical in structured cabling and PoE installations?

Multiple Choice Questions (MCQs):

1. Which connector is commonly used for Ethernet cables such as CAT5e, CAT6, and CAT6A?
   a) SC
   b) RJ-45
   c) LC
   d) BNC
2. What is the purpose of using UPS systems in network installations?
   a) Increase internet speed
   b) Provide uninterrupted power supply during outages
   c) Improve signal strength
   d) Prevent cable theft
3. Which cable type is best suited for environments with high electromagnetic interference?
   a) UTP
   b) Coaxial
   c) STP
   d) Twisted Pair
4. A PoE-enabled device is not receiving power. What should be checked first?
   a) The color of the cable
   b) The power load capacity of the UPS
   c) The correct termination and continuity of the cable
   d) The length of the fiber optic cable
5. Why is crimping essential when terminating cables?
   a) To increase data transfer speed
   b) To ensure proper electrical contact and stable connection
   c) To reduce the size of the cable
   d) To change the type of cable from UTP to STP

Fill in the Blanks:

1. The maximum length for Ethernet cables like CAT5e or CAT6 is _____ meters to maintain performance and power delivery.
2. The device that supplies power over the network cable is called a _____ injector or switch.
3. A common tool used to test continuity and signal strength in cables is a _____ tester.
4. The wiring standard that helps organize cabling from the Point of Presence (PoP) to customer premises is called _____ cabling.
5. Proper routing and clipping of cables within customer premises should follow _____ guidelines to avoid interference and ensure safety.

Notes

3. Configuring Equipment and Establishing Wireless Network Connectivity

Telecom Sector Skill Council

TEL/N0112

Key Learning Outcomes

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

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

UNIT 3.1: Network Topologies

Unit Objectives

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

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

3.1.1 App-Based and Automated Training Platforms

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

Network geometry is defined in following two ways:

1. Physical topology

2. Logical (or signal) topology

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

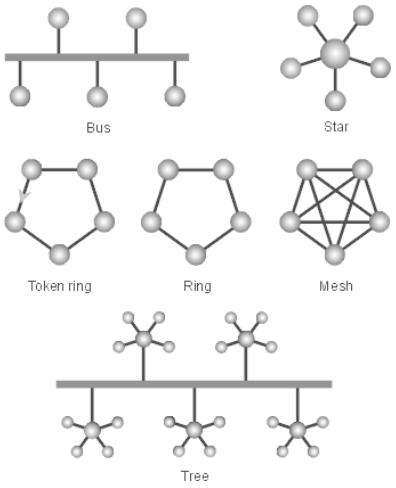


Fig 3.1.1 Types of topologies

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

3.1.2 Broadband Network Element

Network Gateway

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

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

IP address

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

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

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

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

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

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

Subnet Mask

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

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

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

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

Ethernet Address

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

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

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

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

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

MAC Address

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

NIC converts date into electrical signals.

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

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

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

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

Example are as follows:

Dell: 00-14-22

Nortel: 00-04-DCO

Cisco: 00-40-96

Belkin: 00-30-BD

Larger manufacturers may have more than one set of OUIs.

Networks and MAC addresses

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

Wireless Routers and MAC Filtering

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

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

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

a. Wired CPE Configuration

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

VLAN (Virtual Local Area Network):

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

NAT (Network Address Translation):

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

QoS (Quality of Service):

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

b. Wireless CPE Configuration

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

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

a. VPN (Virtual Private Network)

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

Benefits:

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

b. Internet Lease Line (ILL)

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

Benefits:

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

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

a. IPv6 Addressing

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

bits to 128 bits.

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

b. Subnetting

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

c. NAT in IPv6

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

d. Impact of QoS

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

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

Connectivity Options

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

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

Powerline Communication: Uses electrical wiring for network connectivity.

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

Advanced Wi-Fi Security Settings

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

3.1.7 Integrating Smart Home Systems with Broadband Networks

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

Integration Steps

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

3.1.8 Cybersecurity Fundamentals for Broadband Networks

a. Securing Home Networks

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

b. Firewall Configurations

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

c. Threat Mitigation Strategies

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

3.1.9 Escalation Matrix for Troubleshooting Major Network Failures and Handling Emergencies

Escalation Process

1. First Level – Technician Response

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

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

Emergency Handling

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

Notes

Scan the QR Code to watch the related videos

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

Network Topology

UNIT 3.2: Establishing Connectivity

Unit Objectives

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

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

3.2.1 Basic Commands

IPCONFIG Command ipconfig

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

Fig 3.2.1 Ipconfig Command

ipconfig /all

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

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

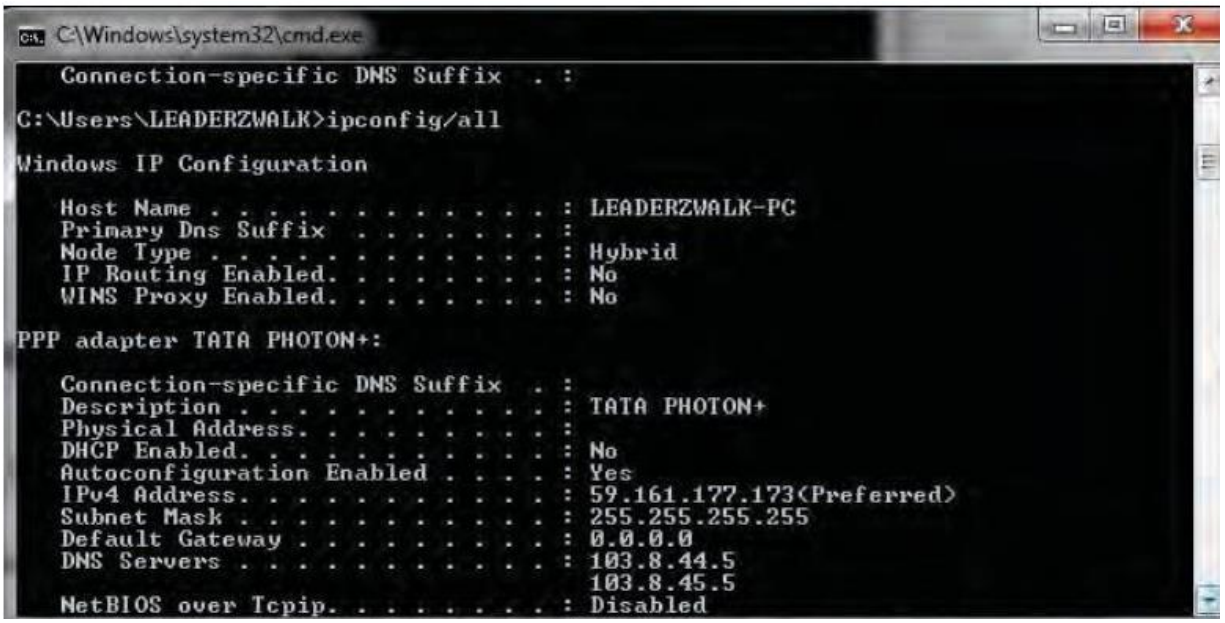


Fig 3.2.2 Finding IP address of gateway through ipconfig command

3.2.2 PING Command List

Ping

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

PING Command

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

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

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

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

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

Ping Command Switches

The switches may be used together.

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

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

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

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

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

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

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

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

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

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

Notes

UNIT 3.3: Connectivity of CPE and End User Devices

Unit Objectives

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

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

3.3.1 Broadband Connectivity

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

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

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

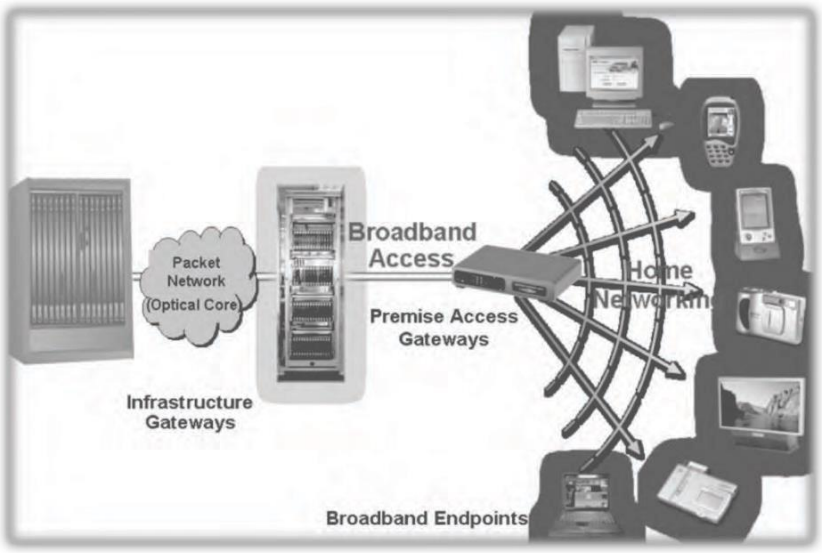


Fig 3.3.1: Broadband Connectivity

3.3.2 Connectivity

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

Fig 3.3.2: Steps for Internet browsing

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

3.3.3 Configurating TCP/ IP for Windows 11

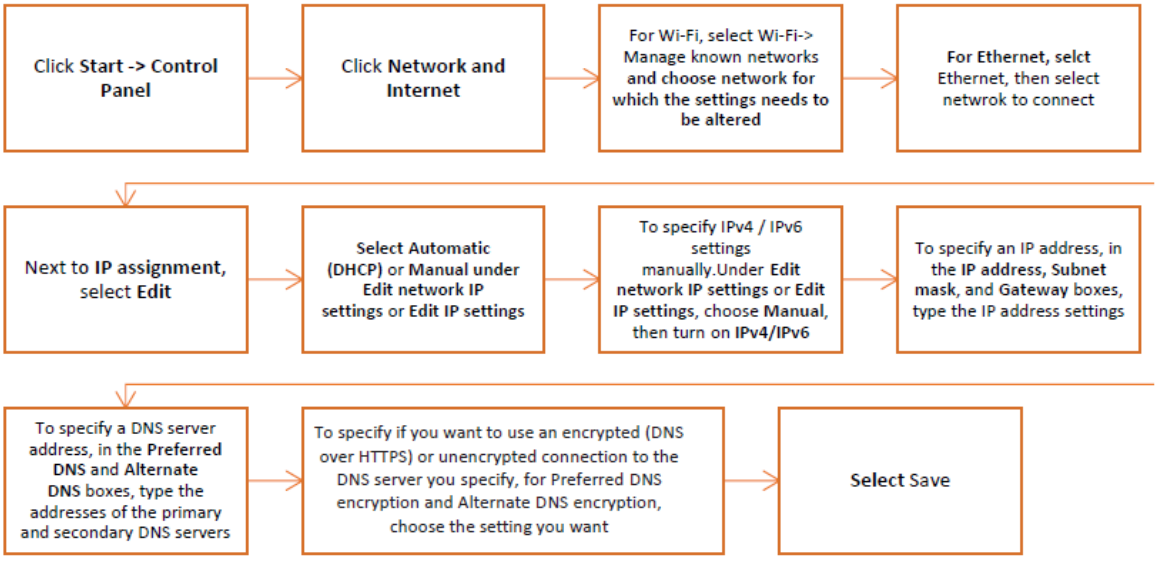


Fig 3.3.3 Steps to configure TCP/IP

3.3.4 Connecting Customer Devices to the CPE and Establishing Connectivity

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

1. Connecting a Laptop/PC to the CPE

A. Wired Connection (Using Ethernet Cable)

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

B. Wireless Connection (Wi-Fi)

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

2. Connecting a Smart/IP TV to the CPE

A. Wired Connection

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

B. Wireless Connection

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

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

A. Wireless Connection

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

B. Wired Connection (For Devices That Support Ethernet)

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

C. Security Considerations

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

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

A. Wired

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

B. Wireless

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

5. Verifying Network Connectivity

After connecting any device:

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

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

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

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

1. Understanding Customer Requirements

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

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

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

Setting Up a VPN

A. Hardware/Software Requirements

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

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

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

2. Enable VPN Service

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

3. Configure Tunnel Parameters

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

4. Define Local and Remote Subnets

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

5. Set Routing Rules

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

6. Test the VPN Tunnel

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

C. Setting Up Remote Access VPN

1. Enable VPN Server Functionality

- Allow users to connect individually.

2. Create User Accounts

- Assign usernames, passwords, and access permissions.

3. Configure Firewall Rules

- Permit VPN traffic through secure ports.

4. Distribute VPN Client Software

- Provide configuration files and instructions.

5. Test User Access

- Validate connection from external devices.

Setting Up an Internet Lease Line (ILL)

A. Requirements

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

B. Steps to Configure ILL

1. Connect the Physical Line

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

2. Enter ISP Credentials

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

3. Set Routing Preferences

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

4. Enable Monitoring Tools

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

5. Perform Speed and Stability Tests

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

6. Document Configuration

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

4. Security Measures During Setup

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

5. Testing and Customer Verification

A. Verify End-to-End Connectivity

- Perform tests from local and remote devices.

b. Check Performance Metrics

- Ensure bandwidth, latency, and jitter meet expectations.

c. Walk Customers Through Access

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

d. Provide Documentation

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

e. Obtain Customer Sign-Off

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

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

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

1. Importance of Integration

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

2. Pre-Integration Requirements

Before beginning the integration process, ensure the following:

A. Stable Broadband Connection

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

2. Compatible Devices

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

3. User Accounts

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

4. Updated Firmware

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

3. Integration with Amazon Alexa

Steps

1. Connect the Smart Device to Broadband

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

2. Open the Alexa App

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

3. Add Device

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

4. Enable Skills

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

5. Test Voice Commands

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

4. Integration with Google Home

Steps

1. Ensure Device Connectivity

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

2. Open Google Home App

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

3. Set Up Device

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

4. Configure Rooms and Routines

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

5. Test Functionality

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

5. Integration with Apple HomeKit

Steps:

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

6. Network Configuration Tips for Smart Home Integration

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

7. Security Best Practices

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

8. Testing and Verification

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

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

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

1. Importance of Verifying Cables and Connectors

Prevents service interruptions caused by loose or damaged cables.

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

2. Visual Inspection of Cables and Connectors

Steps

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

3. Using Tools to Verify Functionality

A. LAN Tester / Cable Tester

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

B. PoE Tester (for Power over Ethernet)

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

C. Multimeter (for Advanced Testing)

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

4. Functional Testing After Plugging In

A. Ethernet / Wired Connections

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

B. Power Connections

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

C. Fiber Connections

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

5. Troubleshooting Common Issues

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

6. Safety Precautions During Verification

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

7. Documenting Results

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

Notes

UNIT 3.4: Configuration Testing

Unit Objectives

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

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

3.4.1 Verifying IP address in Windows 11 for Wi-Fi

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

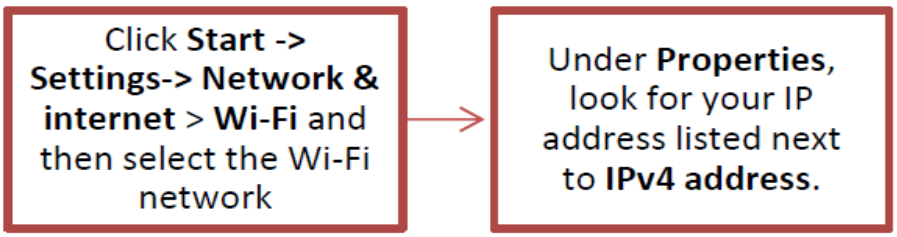
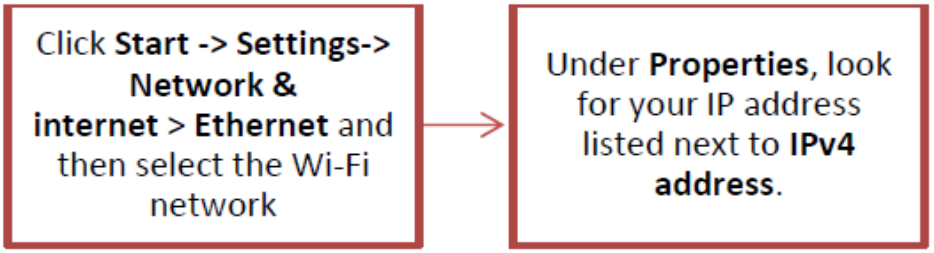


Fig 3.4.1: Steps to test TCP/IP configuration Windows 11

3.4.2 Verifying IP address in Windows 11 for Ethernet

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



3.4.3 Ping the Service Provider Gateway and Analyze Response Time

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

1. Purpose of Ping Test

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

2. Steps to Perform a Ping Test

Step 1: Identify the Service Provider Gateway

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

Step 2: Open the Command Interface

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

Step 3: Execute Ping Command

- Type:
- ping <gateway_IP>

Example:

ping 100.72.1.1

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

3. Analyzing the Ping Results

A standard ping result displays:

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

Key Metrics

1. **Bytes –** Size of the packet sent.
2. **Time (ms) –** Response time / latency between device and gateway.
    - <20 ms = Excellent (local network working fine).
    - 20–100 ms = Acceptable (normal ISP latency).
    - 100 ms = Potential congestion or line issue.
3. **TTL (Time To Live) –** Number of hops allowed; helps confirm routing.

Packet Statistics

After the test ends, results show:

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

4. Troubleshooting Based on Ping Results

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

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

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

1. Purpose of Pinging the CPE

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

.

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

Step 1: Identify the CPE's IP Address

1. Windows:

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

2. macOS/Linux:

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

3. Smartphones/Tablets:

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

Step 2: Run the Ping Command

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

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

Step 3: Observe and Analyze the Response

Example output:

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

Key Metrics

Time (ms):

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

Packet Loss:

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

Jitter:

If response times vary widely, connection instability is present.

3. Optimizing Network Settings for Stability

A. Adjust Router Placement

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

B. Check Wireless Channel

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

C. Secure Network Access

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

D. Update Firmware

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

E. Limit Background Applications

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

F. Enable QoS (Quality of Service)

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

G. Configure IP Settings

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

4. Advanced Diagnostics

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

5. Troubleshooting Based on Ping Results

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

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

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

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

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

1. Analyzing Latency (Response Time)

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

Typical Causes of High Latency

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

Interpreting Latency Values

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

How to Use Latency Results

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

2. Analyzing Throughput (Speed Test Results)

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

Factors Affecting Throughput

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

Interpreting Throughput Results

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

Using Throughput Results

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

3. Analyzing Packet Loss

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

Causes of Packet Loss

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

Interpreting Packet Loss Results

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

3.4.6 Quality of Service (QoS) Settings

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

1. When to Use QoS

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

2. Pre-Configuration Requirements

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

3. Step-by-Step Guide to Enable QoS

Step 1 – Log into the Router/CPE

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

Step 3 – Enable QoS

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

Step 4 – Choose a QoS Type

Common options include:

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

Step 5 – Define Rules

Example:

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

For device-based rules:

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

Step 6 – Save and Apply

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

Step 7 – Test QoS Functionality

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

Notes

UNIT 3.5: Comprehension and Interpretation of Technical Data

Unit Objectives

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

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

3.5.1 Interpretation of Technical Data

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

1. Why Monitoring Network Activity and Updating Firmware is Important

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

2. Guiding Customers to Monitor Network Activity

Step 1 – Access the Router's Dashboard

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

Step 2 – Show the Network Status Page

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

Step 3 – Analyze Bandwidth Usage

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

Step 4 – Enable Alerts or Logging (Optional)

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

3. Guiding Customers to Update Firmware

Step 1 – Check for Firmware Updates

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

Step 2 – Backup Settings (Optional but Recommended)

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

Step 3 – Perform the Firmware Update

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

Step 4 – Verify the Update

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

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

4. Key Objectives When Briefing Customers

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

5. Basic Troubleshooting Steps to Share with Customers

Step 1 – Check Physical Connections

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

Step 2 – Restart the Router/Modem

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

Step 3 – Check Device Connections

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

Step 4 – Run Speed and Connectivity Tests

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

Notes

Scan the QR Code to watch the related videos

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

Interpreting Technical Data

UNIT 3.6: Executing Speed Test and Analyze

Unit Objectives

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

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

3.6.1 Speed Test Measures

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

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

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

Certain terminologies

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

How to run a speed test

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

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

Interpret the Results

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

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

Troubleshoot a faulty speed test

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

3.6.2 Communication with Client

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

Troubleshoot a faulty speed test:

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

Exercise

Short Answer Questions:

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

Multiple-Choice Questions (MCQs):

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

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

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

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

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

Fill in the Blanks :

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

Notes

Scan the QR Code to watch the related videos

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

How to perform speed test

4. Troubleshoot and Rectify Faults

Telecom Sector Skill Council

Key Learning Outcomes

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

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

UNIT 4.1: Escalation Matrix

Unit Objectives

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

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

4.1.1 Escalation Matrix

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

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

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

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

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

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

To view the escalations list, go to Navigation:

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

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

4.1.2 Escalation Matrix Format

Let us take the sample escalation matrix format to understand it

Problem Escalation Matrix

How to Use This Form

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

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

Fig 4.1.1: Sample of an escalation matrix form

Notes

Scan the QR Code to watch the related videos

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

What Is An Escalation Matrix?

UNIT 4.2: Problem Solving

Unit Objectives

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

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

4.2.1 Reporting the Problem

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

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

Report the Problem

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

When the problem is reported

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

4.1.2 Solving the Problem

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

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

4.2.3 Following up after the Problem

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

Use the Information to Decide

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

Making Repairs

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

4.2.4 Checklist

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

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

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

Notes

UNIT 4.3: Identifying and Repairing Faulty Cables and Connectors

Unit Objectives

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

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

4.3.1 Identify Faulty Cables/Connectors

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

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

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

1. Loose cable connections at Switches and Outlets

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

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

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

2. Wire Connections Made with Electrical Tape

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

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

3. Two or More Wires Under One Screw Terminal

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

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

4. Loose Connections on Circuit Breaker Terminals

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

5. Faulty Neutral Wire Connections at Circuit Breaker Panels

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

4.3.2 Cable Testing Using OTDR / Signal Level Meters OTDR

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

Testing a Fiber Optic Cable

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

Equipment required to execute this test

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

Test Procedure

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

Signal Level Meters

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

It also ensures that signal levels are delivered as required.

Types of Signal Level Meters

Commonly, Signal Level Meters are categorized in three groups:

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

Guidelines to use a sound level meter:

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

4.3.3 Connecting a Cable to an RJ-45 Connector

Following tools are used to build cables with RJ45 connectors.

Tools

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

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

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

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

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

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

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

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

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

The following figure shows installing cable in an RJ45 connector:

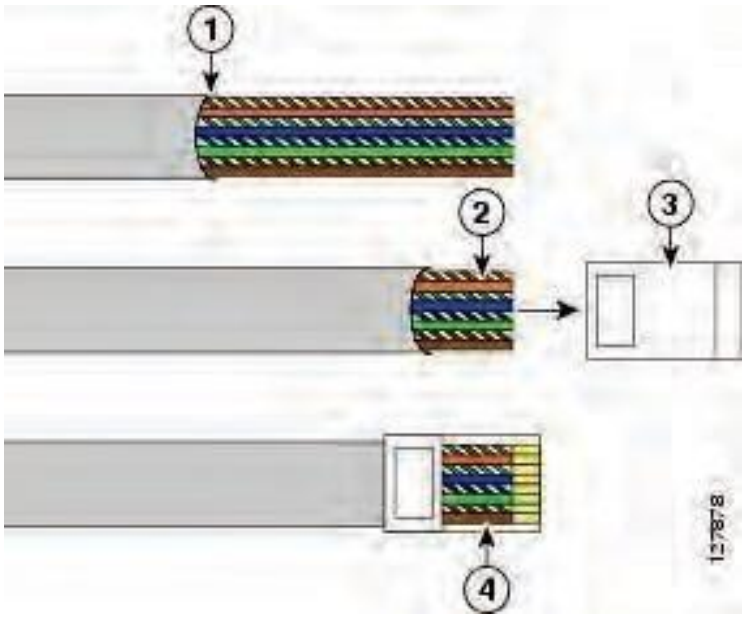


Fig 4.3.5: Illustration of installing a cable in RJ45 connector

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

4.3.3 Replace Faulty Connectors and Damaged Cables

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

Tools and Materials Required

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

Safety Precautions

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

Identifying Faulty Cables and Connectors

A. Visual Inspection

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

B. Testing

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

Step-by-Step Procedure for Replacing Connectors

Step 1 – Prepare the Cable

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

Step 2 – Insert Wires into Connector

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

Step 3 – Crimp the Connector

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

Step 4 – Test the New Connector

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

Step-by-Step Procedure for Replacing Damaged Cables

Step 1 – Disconnect the Cable

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

Step 2 – Measure and Cut a Replacement Cable

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

Step 3 – Terminate Both Ends

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

Step 4 – Reconnect and Test

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

Notes

Scan the QR Code to watch the related videos

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

Explaining Optical Time Domain Reflectometry (OTDR) Testing Method

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

Unit Objectives

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

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

4.4.1 Need of EMI & EMC

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

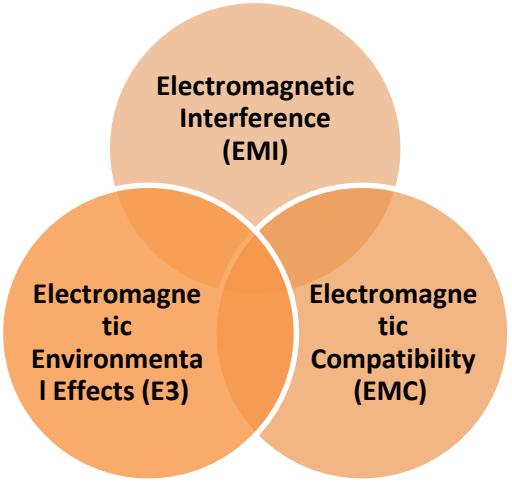


Fig. 4.4.1: Elements in electronic products and system integration

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

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

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

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

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

4.4.2 Electromagnetic Interference (EMI)

Electromagnetic Interference (EMI)

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

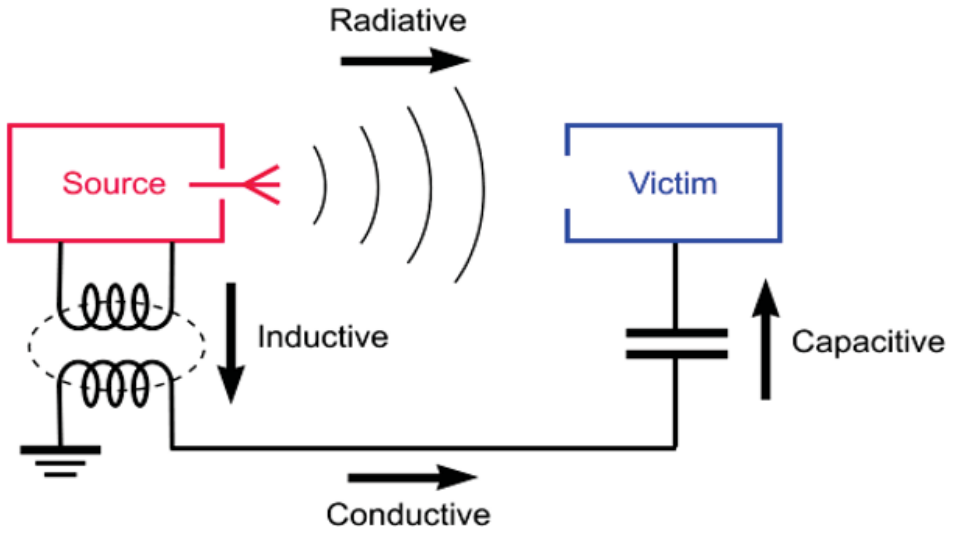


Fig 4.4.2: Electromagnetic interference

4.4.3 Electromagnetic Compatibility (EMC)

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

Notes

Scan the QR Code to watch the related videos

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

EMI - Electromagnetic Interference and EMC - Electromagnetic Compatibility Explained

UNIT 4.5: Crimping and Soldering

Unit Objectives

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

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

4.5.1 Crimping vs. Soldering

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

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

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

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

4.5.2 Soldering

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

Advantages for connectorization by solder method are as follows:

Preferred

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

Fig 4.5.1: Soldering

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

Preferred

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

Fig 4.5.2: Joint after soldering

For non-optimum technique soldering is tolerant.

Disadvantages of solder method:

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

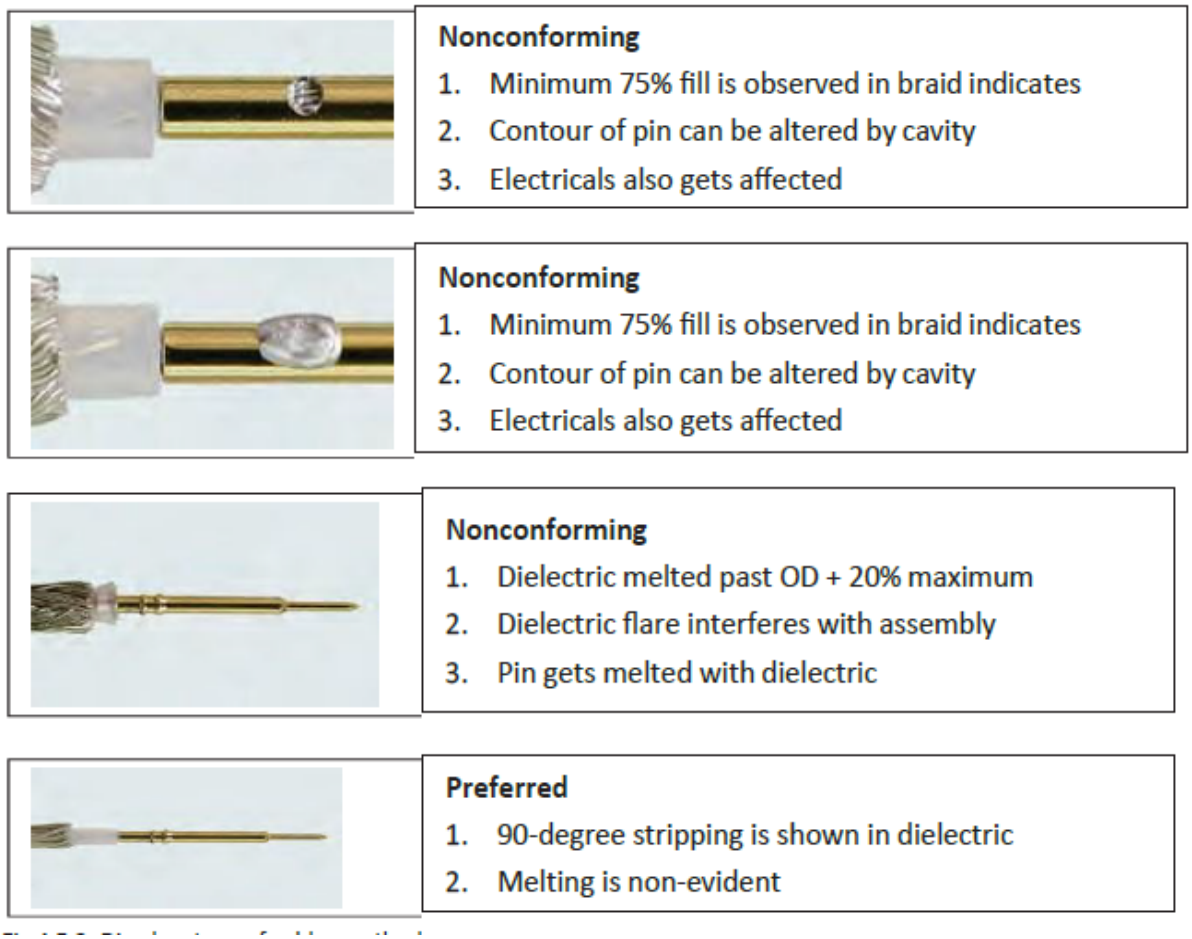


Fig 4.5.3: Disadvantage of solder methods

4.5.3 Crimping

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

Following reasons explain why crimp method is popular:

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

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

Preferred

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

Fig 4.5.4: Crimping

Disadvantages of the crimp method are:

Nonconforming

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

Nonconforming

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

Fig 4.5.5: Crimping disadvantages

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

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

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

Fig 4.5.6: Visualization of flagging and dog ears

Ferrule Cross Section

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

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

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

Fig 4.5.7: Bell mouth crimper

Notes

UNIT 4.6: Troubleshooting of Cable and Connector

Unit Objectives

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

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

4.6.1 Problems during First Startup

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

Table 4.6.1: Table showing problem during the first startup

4.6.2 Problems in Router

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

Table 4.6.2: Problems faced in router

Notes

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

Unit Objectives

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

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

4.7.1 Diagnosing the Cable Modem

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

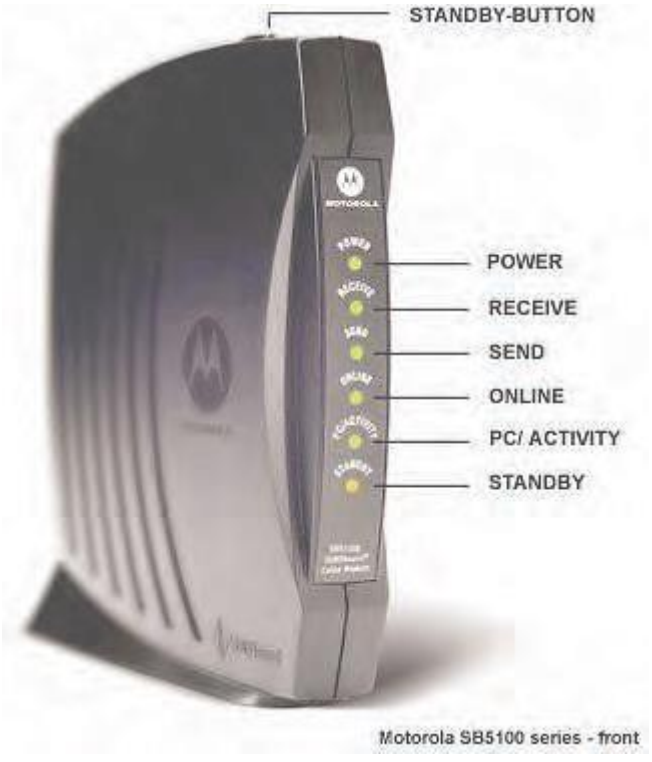


Fig 4.7.1: Front Panel

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

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

Table 4.7.1: Status light information the table below

Back/Rear Panel

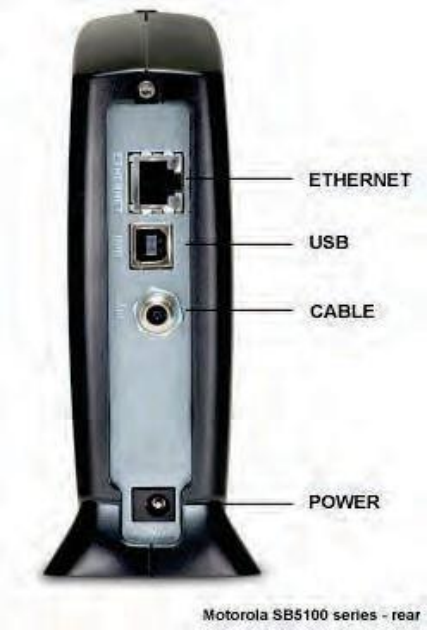


Fig 4.7.2: Rear Panel

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

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

Table 4.7.2: Ports at the back of the panel

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

4.7.2 Troubleshoot a Cable Broadband Connection

Power Cycle Equipment

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

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

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

Network Status

Unplanned network outages can interrupt the cable broadband service.

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

4.7.3 Troubleshooting using the Cable Modem Indicators

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

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

Table 4.7.3: Indicators on a cable modem

Notes

Scan the QR Code to watch the related videos

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

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

UNIT 4.8: Troubleshooting of Configuration and Connectivity CPE faults

Unit Objectives

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

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

4.8.1 Troubleshoot "No Data Transfer"

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

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

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

Table 4.8.1: Troubleshooting steps

Notes

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

Unit Objectives

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

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

4.9.1 Common Causes of Broken Internet Connection

1. Slow Connection

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

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

2. No Connection at all

Connection is lost due to:

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

3. Service Fluctuations

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

4. Equipment Failure

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

5. Operator Error

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

4.9.2 Diagnosing Internet Connection

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

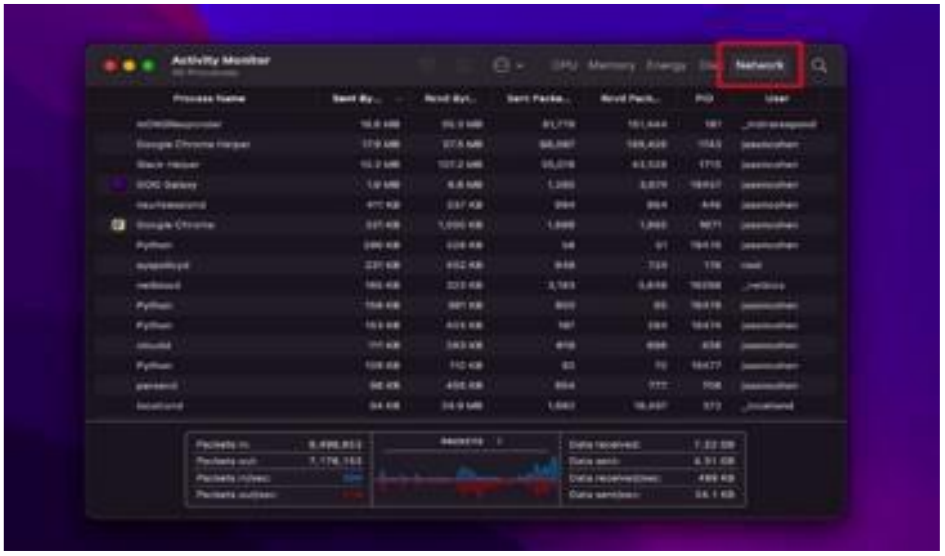


Fig. 4.9.2: Network screen
Pic credit : https://www.pcmag.com/

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

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

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

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

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

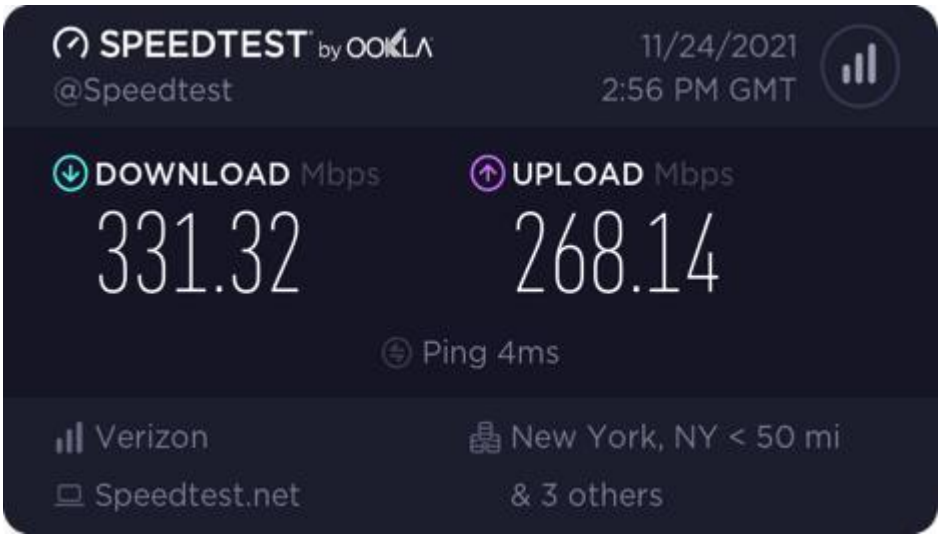


Fig.4.9.2: Speed Test screen

Exercise

Short Answer Questions:

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

Multiple-Choice Questions (MCQs):

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

Fill in the Blanks :

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

Notes

5. Follow Sustainable Practices in Telecom Infrastructure Installation

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

TEL/N9105

Key Learning Outcomes

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

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

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

Unit Objectives

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

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

5.1.1 Environmental Sustainability in Telecom Industry

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

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

Environmental Sustainability in the Telecom Industry

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

- **Energy consumption** — Telecom towers, data centers, and network operations consume large amounts of electricity, often generated from fossil fuels.
- **Material usage** — Manufacturing network equipment requires metals, plastics, and rare earth elements.
- **E-waste generation** — Obsolete telecom devices, batteries, and cables contribute to growing electronic waste streams.
- **Site construction impacts** — Building telecom towers, laying cables, and installing antennas can disturb local ecosystems.

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

Uses and Importance in the Telecom Industry

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

5.1.2 Environmental Laws and Regulations in Telecommunications

1. National Environmental Regulations

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

- **The Environment (Protection) Act, 1986:** This umbrella legislation empowers the government to set and enforce environmental quality standards, including emissions from telecom site generators and noise levels from cooling equipment.
- **The E-Waste (Management) Rules, 2022:** These rules impose **Extended Producer Responsibility (EPR)** on manufacturers, importers, and bulk consumers of electrical and electronic equipment, including telecom operators. Companies must collect and channel e-waste to authorized recyclers, meet annual collection targets, and maintain detailed records of disposal.
- **Hazardous and Other Wastes (Management and Transboundary Movement) Rules, 2016:** These rules classify hazardous substances, such as lead-acid batteries, PCB boards, and certain solvents, and mandate their safe handling, storage, and disposal.
- **The Energy Conservation Act, 2001**: This legislation encourages telecom operators to adopt energy-efficient practices, such as the use of high-efficiency power systems, renewable energy integration, and load optimization.
- **The Plastic Waste Management Rules, 2022**: These rules regulate the use of plastic in telecom equipment packaging, promoting recyclable and biodegradable alternatives.

2. International Standards and Agreements

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

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

5.1.3 E-Waste in the Telecom Industry

Understanding E-Waste

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

Fig. 5.1.1 E-Waste in Telecommunication Industry

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

Classification of E-Waste

Telecom e-waste is typically categorized into:

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

5.1.4 E-Waste Management Process in the Telecom Industry

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

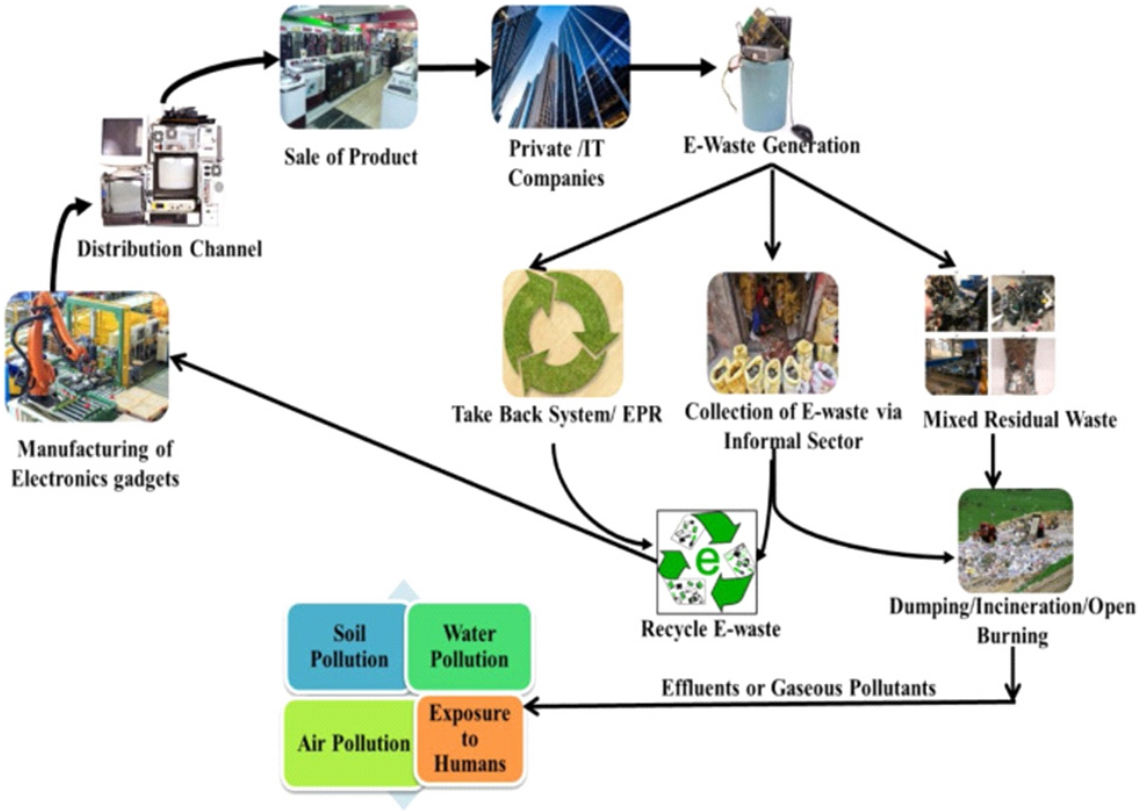


Fig. 5.1.2 E-waste Management

1. Identification and Segregation

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

Key Activities in Identification:

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

Segregation Process:

Once identified, materials are segregated into three main categories:

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

Best Practices:

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

Example:

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

2. Handling and Storage

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

Handling Guidelines:

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

Storage Practices:

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

Environmental Protection Measures:

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

3. Authorized Disposal and Recycling

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

Procedure for Authorized Disposal:

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

Refurbishment Programs:

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

Compliance and Reporting:

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

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

5.1.5 Occupational Safety in Environmental Practices for Telecom E-Waste Management

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

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

1. Risk Categories in Telecom E-Waste Handling

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

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

2. Personal Protective Equipment (PPE) for Telecom E-Waste Operations

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

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

3. Training Requirements

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

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

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

4. Emergency Procedures

Spills and Leaks:

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

Electrical Accidents:

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

Battery Fires:

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

5. Compliance and Monitoring

Telecom companies should:

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

5.1.6 Energy Optimization in Telecom Operations

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

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

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

a. Energy-Efficient Infrastructure

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

1. Advanced BTS (Base Transceiver Station) Design

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

2. Passive Cooling and Thermal Management

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

3. Efficient Lighting Systems

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

b. Renewable Energy Integration

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

1. Hybrid Solar-Diesel Systems

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

2. Wind Power Solutions

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

3. Energy Storage Advancements

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

4. Green Power Purchase Agreements (PPA)

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

5.1.7 Reducing the Carbon Footprint in Telecom

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

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

1. Network Function Virtualization (NFV)

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

Benefits in Carbon Reduction:

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

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

2. Equipment Rack Consolidation

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

Environmental Benefits:

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

Implementation Methods:

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

3. Green Fleet Initiatives for Maintenance Teams

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

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

Strategies:

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

4. Sustainable Logistics Partnerships

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

Examples:

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

5. Complementary Carbon Reduction Measures

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

5.1.8 Documentation and Compliance Tracking in Telecom Environmental Management

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

a. Purpose of Documentation in Telecom Environmental Practices

1. Regulatory Compliance:

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

2. Environmental Performance Monitoring:

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

3. Risk Management:

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

b. Types of Environmental Documentation in Telecom Operations

1. **Waste Disposal Registers**
    - **Contents:**
        - Type of waste (e.g., lead-acid battery, printed circuit board, copper cable).
        - Quantity (in kg or units).
        - E-waste classification code.
        - Date of disposal.
        - Name and license number of the authorized recycler.
        - Final waste destination (recycling, incineration, landfill).
    - **Format:**
        - Often digital, integrated into Enterprise Resource Planning (ERP) or Environmental Management Information Systems (EMIS).
2. **Waste Transfer Manifests**
    - Legal documents tracking the movement of hazardous or non-hazardous waste from telecom sites to processing facilities.
    - Includes chain-of-custody signatures at each transfer stage.
3. **Energy Consumption Logs**
    - Monitors site-level electricity usage, diesel generator runtime, and renewable energy contribution.
    - Data collected via IoT-based smart meters and Network Operations Center (NOC) dashboards.
4. **Sustainability Performance Reports**
    - Quarterly or annual reports consolidating environmental KPIs:
        - Energy savings (kWh/year).
        - CO_2 emissions avoided (tons/year).
        - EPR compliance percentage.
    - Often aligned with Global Reporting Initiative (GRI) standards.
5. **Audit Records**
    - Findings from internal and external sustainability audits.
    - Action plans for corrective measures.

c. Sustainability Audits in Telecom

Frequency:

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

Audit Scope:

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

Audit Tools & Methods:

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

d. Role of Technology in Compliance Tracking

Modern telecom operators increasingly rely on automated compliance systems:

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

e. Benefits of Robust Documentation Practices

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

Summary

- Environmental Sustainability in Telecom Industry
- Environmental Laws and Regulations in Telecommunications
- E-Waste in the Telecom Industry
- E-Waste Management 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

Exercise

A. Multiple Choice Question:

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

B. Descriptive Questions:

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

Notes

6. Employability Skills (30 Hours)

Telecom Sector Skill Council

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

DGT/VSQ/N0101

7. Annexure

Annexure I - QR Codes –Video Links

Annexure - I

QR Codes –Video Links

Chapter No.	Unit Name	Topic	Page No.	URL Links	QR code (s)
Chapter 2: Lay Cable/System Wiring and Install Equipment at Customer Premises	Unit 2.3- Customer Premise Equipment	Difference between hub, router, and switch	66	https://www.youtube.com/watch?v=1z0ULvg_pW8&ab_channel=PowerCertAnimatedVideos	
		How to install a router		https://youtu.be/dm4d2LZC2dk	
	Unit 2.6 - Checking of Voltage, Current and Earthing	Use of Multimeter and revise electricity basics	87	https://www.youtube.com/watch?v=r_migcta_Is	
Chapter 3: Configuring Equipment and Establishing Wireless Network Connectivity	Unit 3.1 - Network Topologies	Network Topology	126	https://www.youtube.com/watch?v=uSKdjjw5zow	
	Unit 3.5 - Comprehension and Interpretation of Technical Data	Interpreting Technical Data	157	https://www.youtube.com/watch?v=Hm6Urf8ng3M	
	Unit 3.6 - Executing Speed Test and Analyze	How to perform speed test	162	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?	179	https://www.youtube.com/watch?v=opB5oOvB3cI	

Chapter No.	Unit Name	Topic	Page No.	URL Links	QR code (s)
Chapter 4: Troubleshoot and Rectify Faults	Unit 4.3 - Identifying and Repairing Faulty Cables and Connectors	Explaining Optical Time Domain Reflectometry (OTDR) Testing Method	179	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	182	https://www.youtube.com/watch?v=I88Qzdahn_o	
	Unit 4.7 - Troubleshooting of CPE (Modem, Router, Switch)	Modem, Router, Switch, Hub and Access Point: What's the Difference?	195	https://www.youtube.com/watch?v=39zXmf61McI	

NCVET
कौशल गुणवत्ता प्रगति

Skill India
कौशल भारत-कुशल भारत

सत्यमेव जयते
GOVERNMENT OF INDIA
MINISTRY OF SKILL DEVELOPMENT
& ENTREPRENEURSHIP

N·S·D·C
RE IMAGINE FUTURE

Telecom Sector Skill Council

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